IT Security Day 2026: Москва станет площадкой для обсуждения новой парадигмы кибербезопасности

6 октября 2026 года в Москве состоится конференция IT Security Day 2026, организованная TAdviser. В центре внимания экспертов — стратегический переход от фрагментированной защиты к управляемой киберустойчивости. Это не просто смена терминологии, а фундаментальное переосмысление подхода к информационной безопасности: от точечного закрытия уязвимостей — к выстраиванию устойчивой, прогнозируемой и измеримой системы защиты, способной выдерживать комплексные кибератаки и минимизировать последствия инцидентов.

Современные цифровые инфраструктуры становятся всё более распределёнными: компании активно используют гибридные и мультиоблачные среды, удалённую работу, микросервисные архитектуры и сторонние API. При этом ландшафт киберугроз стремительно эволюционирует — злоумышленники всё чаще применяют инструменты на базе генеративного ИИ, автоматизируют атаки и используют сложные многоэтапные сценарии. В таких условиях традиционные «островки» защиты (отдельные антивирусы, фаерволы, DLP-системы) уже не справляются: они не дают полной картины, создают слепые зоны и замедляют реагирование.

Именно поэтому фокус смещается на управляемую киберустойчивость — способность организации не только предотвращать инциденты, но и быстро восстанавливаться после них, сохраняя непрерывность бизнес-процессов. На конференции разберут, как перевести эту концепцию из теории в практику: какие процессы, метрики и технологии для этого нужны, как обосновать инвестиции в безопасность перед топ-менеджментом и как измерить реальный эффект от внедрённых мер.

Одна из ключевых линий программы — интеграция важнейших компонентов ИБ-экосистемы:

NGFW (Next-Generation Firewall) — межсетевые экраны нового поколения, которые обеспечивают не только фильтрацию трафика, но и глубокую инспекцию приложений, контроль пользователей и защиту от современных угроз.

SIEM (Security Information and Event Management) — системы, собирающие и анализирующие события безопасности из разных источников, чтобы выявлять аномалии и коррелировать инциденты.

SOC (Security Operations Center) — центры мониторинга и реагирования, где специалисты в реальном времени отслеживают угрозы и координируют действия по их устранению.

EDR/XDR (Endpoint Detection and Response / Extended Detection and Response) — решения для обнаружения и реагирования на угрозы на конечных точках и в расширенном контексте всей инфраструктуры.

На конференции участники обсудят, как объединить эти технологии в единую систему: как настроить обмен данными между SIEM и SOC, как интегрировать NGFW в общую картину угроз, как использовать EDR/XDR для

автоматического расследования и сдерживания атак. Особое внимание уделят практическим кейсам: как избежать «информационного шума» при большом объёме событий, как автоматизировать рутинные операции и как выстроить процессы так, чтобы команда SOC могла фокусироваться на самых критичных инцидентах.

Помимо интеграции технологий, в повестке — широкий спектр актуальных тем:

Ландшафт угроз-2026: какие атаки стали массовыми, какие уязвимости эксплуатируются чаще всего и как меняется тактика злоумышленников.

Zero Trust: как внедрять принцип «никому не доверяй» в реальных условиях, с учётом существующих инфраструктур и бизнес-требований.

ИИ в защите и для атак: как использовать генеративные модели и автоматизацию для усиления безопасности, не создавая новых рисков.

Регуляторные изменения: новые требования к защите персональных данных, КИИ и других критически важных объектов, а также как адаптировать под них ИБ-стратегию.

Метрики и ROI: как измерять эффективность ИБ, какие KPI действительно важны для бизнеса и как обосновывать бюджет на безопасность с помощью данных.

Безопасность гибридных и облачных сред: как защищать распределённые инфраструктуры, удалённых сотрудников и филиалы, а также противостоять внутренним угрозам.

Конференция ориентирована на руководителей и специалистов, отвечающих за информационную безопасность и устойчивость ИТ-инфраструктуры: CISO, ИТ-директоров, архитекторов безопасности, руководителей SOC, аналитиков и инженеров ИБ. Это площадка для диалога между заказчиками, вендорами и интеграторами: здесь можно не только услышать экспертные мнения, но и обменяться опытом, разобрать реальные кейсы и подобрать решения под задачи своей организации.

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

Балицкий П.С.,
кандидат военных наук, доцент,
доцент кафедры «Безопасность жизнедеятельности»
Финансового университета при Правительстве РФ