StopPhish Conference 2026: как Москва стала эпицентром борьбы с социальной инженерией

8 октября в Москве прошла StopPhish Conference 2026 — одно из самых ожидаемых событий года в сфере информационной безопасности. В центре повестки оказалась не «железо-программная» защита, а человек: организаторы последовательно доказывали, что именно человеческий фактор сегодня — и главная уязвимость, и главный рубеж обороны. Девиз конференции — «Человек — главная уязвимость или мощнейший патч?» — стал лейтмотивом всех дискуссий и задал тон напряжённым, но продуктивным дебатам между «защитниками» и «атакующими».

Конференция развернулась в Palmira Art Hotel — площадке, удачно сочетающей деловой формат и комфортную среду для нетворкинга. По данным организаторов, в мероприятии приняли участие более 250 специалистов из крупнейших российских компаний, включая представителей банков, телекома, промышленности и госсектора. Среди гостей были CISO, фрод-аналитики, специалисты по программам повышения осведомлённости (awareness), участники red/blue-команд, а также представители вендоров, интеграторов и профильных ведомств.

Высокий интерес к событию объясняется тем, что фишинг и социальная инженерия остаются одними из самых распространённых векторов атак: по статистике, значительная доля инцидентов начинается с письма, звонка или сообщения, где главную роль играет не уязвимость кода, а уязвимость восприятия.

Программа была разделена на два параллельных трека, чтобы дать участникам максимально практичные и разносторонние инструменты.

Awareness-трек был ориентирован на тех, кто выстраивает защиту изнутри. В фокусе оказались:

Психология манипуляции. Эксперты разбирали, как злоумышленники эксплуатируют базовые когнитивные искажения, заставляя даже опытных специалистов отключать критическое мышление.

Атаки на топ-менеджмент и VIP-персон. Отдельная секция была посвящена «целевому» фишингу: как готовят письма для руководителей, какие приёмы делают их неотличимыми от легитимных запросов и как выстроить дополнительный контур защиты для ключевых сотрудников.

Метрики и ROI. Важная часть трека касалась измерения эффективности программ обучения: как считать не количество пройденных курсов, а снижение числа успешных атак, как связать инвестиции в awareness с реальным снижением рисков и как обосновать бюджет перед руководством.

Культура безопасности. Обсуждались способы сделать безопасность частью повседневных рабочих привычек, а не отдельным «обязательным мероприятием».

Attack-трек давал взгляд с противоположной стороны баррикад и был особенно востребован у red-team специалистов и аналитиков угроз. Здесь говорили о:

Автоматизации разведки и OSINT. Как злоумышленники собирают данные о компании и сотрудниках, как используют открытые источники для подготовки точечных атак и какие контрмеры помогают усложнить эту работу.

Социотехническом профайлинге. Разбор методов, с помощью которых атакующие составляют психологический портрет жертвы, чтобы подобрать наиболее убедительную легенду.

ИИ и масштабировании угроз. Отдельный блок был посвящён тому, как искусственный интеллект меняет ландшафт атак: от генерации правдоподобных писем и голосовых дипфейков до автоматизации сбора данных и персонализации фишинговых кампаний.

Физическом доступе и «полевых» техниках. Эксперты делились примерами, когда проникновение в офис или доступ к инфраструктуре начинался не с цифрового взлома, а с грамотной социальной инженерии на месте.

Особенностью конференции стали не только доклады, но и практические форматы. В демо-зоне партнёры представили свои решения, и участники могли не просто послушать о продукте, а вживую посмотреть на его работу, задать вопросы инженерам и сравнить разные подходы. Это помогало уйти с мероприятия не только с идеями, но и с конкретными критериями для выбора инструментов.

StopPhish Conference 2026 закрепила за собой статус главной в России площадки, где публично разбирают реальные сценарии манипуляций, ошибки компаний и психологические механики атак. Участники получили не только теоретическую картину угроз, но и набор практических инструментов: от метрик для обоснования бюджета до тактик, которые можно внедрить уже на следующий день.

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