

Эволюция мотивации кибератак на промышленные объекты

Доцент кафедры «Безопасность жизнедеятельности» Финансового университета при Правительстве Российской Федерации, к.э.н., доцент Данилина М.В. отмечает, что буквально несколько лет назад кибератаки на промышленные объекты воспринимались преимущественно как инструмент государственного противостояния. Основными мотивами назывались промышленный шпионаж и кибервойна. Ситуация начала меняться после 2010 года, когда червь Stuxnet, классифицированный как первое кибероружие, продемонстрировал, что цифровая атака способна физически разрушить промышленное оборудование. Этот инцидент обозначил переход от простого сбора информации к целенаправленному воздействию на технологические процессы.

Доцент кафедры «Безопасность жизнедеятельности» Финансового университета при Правительстве Российской Федерации, к.э.н., доцент Рожков Р.С., говорит о том, что если ранее почти половина атак (47%) была связана со шпионажем, то теперь такая же доля инцидентов мотивирована получением прямой финансовой выгоды. Эта тенденция подтверждается данными о росте атак на промышленный комплекс: в первом полугодии 2026 года их доля увеличилась вдвое, достигнув 11%. Киберпреступники осознали, что остановка производства – это мощный рычаг давления, поскольку промышленные предприятия зависят от непрерывности операций, а любой простой ведёт к огромным финансовым потерям.

На смену классическому шпионажу пришли вымогательство и продажа инструментов для взлома. Финансово мотивированные группировки, такие как Clubfoot Wolf, целенаправленно атакуют небольшие организации химической промышленности, делая ставку на массовость и слабую защиту инфраструктуры. Суммы выкупа варьируются от 15-30 млн рублей для компаний среднего размера до 100-200 млн рублей в отдельных случаях. Более того, на теневом рынке появились специализированные фреймворки для атак на промышленную инфраструктуру стоимостью от 500 долларов, что резко снижает порог входа для злоумышленников.

Эксперты отмечают, что параллельно с финансовой мотивацией усиливается и геополитическая составляющая. Хактивистские группы всё чаще рассматривают промышленные объекты как площадку для демонстрации силы. Геополитическая напряжённость в Восточной Европе и на Ближнем Востоке катализировала рост хактивистских коллективов,

действующих как государственные прокси или независимые идеологи. Показательным примером стал инцидент 2026 года, когда хакеры, связанные с Ираном, проникли в системы промышленного объекта в Великобритании и смогли остановить энергетическую установку. Это открыло новую страницу в противостоянии, где цифровая атака напрямую влияет на физические процессы.

Эксперт Данилина М.В. говорит о том, что дополнительный импульс эволюции мотивации придаёт искусственный интеллект. По данным «Лаборатории Касперского», 28% промышленных предприятий в мире в 2025 году сталкивались с атаками с применением ИИ, включая создание дипфейков и автоматизацию социальной инженерии. ИИ «снижает барьеры для входа» в киберпреступность, позволяя атакующим с самыми разными мотивами (от личной неприязни до политических убеждений) планировать и проводить операции. Это приводит к размыванию границ между государственными, криминальными и идеологическими мотивами: один и тот же инструмент может использоваться как для шпионажа, так и для вымогательства.

Таким образом, эволюция мотивации кибератак на промышленные объекты отражает более широкую трансформацию киберугроз: от узконаправленных операций государственных акторов к многополярной среде, где финансовые, политические и идеологические мотивы переплетаются. Для промышленных предприятий это означает необходимость пересмотра моделей безопасности с учётом того, что атака может преследовать не одну, а сразу несколько целей.

Рожков Р.С.,

кандидат экономических наук, доцент,
доцент кафедры «Безопасность жизнедеятельности»
Финансового университета при Правительстве РФ

Данилина М.В.,

кандидат экономических наук, доцент,
доцент кафедры «Безопасность жизнедеятельности»
Финансового университета при Правительстве РФ