Актуальные киберугрозы для российских промышленных предприятий

На протяжении последних нескольких лет **промышленность** является **одной из самых атакуемых отраслей как в мире, так и в России**. С 2024 года интенсивность атак на российский промышленный сегмент значительно возросла по сравнению с другими секторами: прирост доли атак в 2024 году составил 5 п. п., в 2025 году — 8 п. п.

16% успешных атак в России в 2024

19% успешных атак в России в 2025

Сектор характеризуется уникальным сочетанием социально-экономических и технологических факторов, формирующих благоприятную среду для осуществления кибератак. Помимо этого, в России интерес злоумышленников к промышленности обусловлен некоторыми специфичными причинами:

- **Геополитическая напряженность.** Обострение международных отношений вызывает волну атак.
- **Статус России как ведущей энергетической державы.** Сектор интересует разные группы злоумышленников: от тех, кто ищет финансовую выгоду, до организованных и геополитически мотивированных субъектов, стремящихся воздействовать на экономическую стабильность через вмешательство в критически важные процессы.

22% всех атак на российскую промышленность в 2024-2025 направлены на **энергетику и ТЭК**

- **Уход из страны в 2022 году западных вендоров ИТ-решений**, из-за чего импортозамещение происходило в сжатые сроки без полноценного тестирования и оценки рисков, что повысило вероятность ошибок и повлияло на возникновение уязвимостей. Но не все перешли на отечественные продукты – известные уязвимости могут не устраняться и эксплуатироваться киберпреступниками.
- **Дефицит специалистов по информационной безопасности,** который отмечается экспертами[1].

[1] По данным hh.ru за период с января по август 2025 года

Количество кибератак на промышленные организации в России в ближайшие годы **не снизится**. Важная задача для промышленных организаций: построение надежной системы защиты, невозможное без знаний о тенденциях в сфере ИБ.

- Основными методами кибератак на отечественные промышленные предприятия в 2024–2025 годы оставались использование вредоносного программного обеспечения (ВПО) и применение социальной инженерии. Одна из причин продолжающегося роста использования ВПО в атаках — активное развитие теневого рынка.

Главным каналом социальной инженерии в успешных атаках на российские промышленные организации была электронная почта. Наиболее часто злоумышленники маскировали фишинговые приманки под вложения, связанные с рабочей деятельностью. Другой популярной тематикой фишинга были сообщения, отправленные якобы от государственных органов.

В каждой восьмой кибератаке киберпреступники прибегали к использованию легитимного ПО, в частности, инструментам для удаленного мониторинга и управления (RMM). Подобные классы решений обычно не воспринимаются антивирусными средствами защиты как вредоносные, а злоумышленники могут использовать их в качестве альтернативы RAT-троянам.

x2 доля инцидентов, связанных **с компрометацией цепочки поставок и доверенных каналов связи, в России превышает общемировую величину**

Хотя этот показатель остается сравнительно небольшим (4%), ситуация сигнализирует: отечественные промышленные компании особо уязвимы в областях, где есть взаимодействие с партнерами. Одна компания нередко имеет прямой доступ к инфраструктуре и внутренней информации десятков клиентов. Дополнительно, доступ через партнера выглядит легитимным, что создает условия для длительного скрытого присутствия злоумышленника в инфраструктуре жертвы.

- Распределение типов ВПО, используемого в атаках на промышленность в России за последние два года, существенно отличалось от общемирового. Для страны характерна высокая доля применений ВПО для удаленного управления и шпионского ПО, в то время как в мире главной киберугрозой для промышленных организаций в мире остаются шифровальщики. Это может указывать: **приоритет для злоумышленников – долгосрочное пребывание в инфраструктуре и сбор данных, а не немедленное вымогательство**.

В атаках на Россию также используются шифровальщики, но как минимум половина случаев их применений имеют хактивистскую направленность. Высокую долю хактивистов в регионе отражает и доля использований ПО, удаляющего данные – оно использовалось в 11% атак с применением ВПО.

За 2024-2025 российскую промышленность атаковало **55 группировок**. **Кибершпионские структуры** - самая активная категория злоумышленников в промышленном секторе России: они совершили **47% атак** на отрасль. Основные мотивы группировок: стратегическая ценность промышленных объектов и информации, которая с ними связана, изучение инфраструктуры и потенциальных точек воздействия, широкие связи с другими отраслями.

Более четверти успешных атак на российские промышленные компании были совершены **хактивистами**. Их главной задачей становилось полное разрушение скомпрометированной инфраструктуры.

25% инцидентов осуществлялось **финансово мотивированными преступниками**. Целью групп становилось получение выкупа и кража конфиденциальной информации для ее последующей монетизации.

В полной версии исследования мы подробно рассматриваем ключевые методы и инструменты, используемые каждой группой преступников.

Наиболее опасной частью атаки на промышленное предприятие являются **действия злоумышленников в технологическом сегменте**, но их описание редко становится публичным в силу репутационных рисков и секретности сведений о конфигурации производственных систем. Дополнительный риск — ограниченный выбор инструментов для защиты: требуются специализированные решения, совместимые с промышленным оборудованием и учитывающие особенности производственных процессов.

Тем не менее для построения эффективной стратегии защиты необходимо понимать, как действуют атакующие. Мы рассмотрели наиболее распространенные угрозы на примере отчетов с нескольких кибербитв Standoff, а также подготовили с командой PT ISIM рекомендации по обнаружению описываемых атак и реагированию на них.

75% атак на технологический сегмент начинается с нарушений в ИТ-инфраструктуре[2]

[2] По данным Zero Networks

Получив первоначальный доступ к технологическому сегменту злоумышленники переходят к разведке на уровне сети, затем — к повышению привилегий и обходу авторизации. Следующие шаги — подготовка инструментов и непосредственное воздействие на технологический процесс.

- Чаще всего атаки на российскую промышленность приводили **к утечкам конфиденциальной информации** (61%) и **нарушениям основной деятельности** (33%). Преимущественно из организаций похищалась **коммерческая тайна** (29%), доля ее краж существенно превышала общероссийский показатель по всем отраслям – злоумышленников больше интересует техническая документация, сведения о разработках и ноу-хау.

Похищенные сведения не всегда остаются исключительно в руках злоумышленников.

52% объявлений об утечках из российских промышленных организаций связаны с **бесплатной раздачей** украденных данных

14% объявлений об утечках из российских промышленных организаций связаны с **продажей** украденных данных

300 тыс. $ стоимость самой дорогой утечки, продаваемой в даркнете

- По мере цифровизации предприятий и роста связности между ИТ- и ОТ-сегментами требования к безопасности смещаются от защиты отдельных систем к обеспечению киберустойчивости производственной среды в целом. Промышленным компаниям необходимы не только базовые меры ИБ, но и специализированные решения.

Актуальные киберугрозы
для российских
промышленных предприятий

Узнать больше об исследованиях
Positive Technologies