ПРОМЫШЛЕННОСТЬ — НОВАЯ МИШЕНЬ ДЛЯ КИБЕРПРЕСТУПНИКОВ

ПРОМЫШЛЕННЫЙ СЕКТОР СТАЛ ОСНОВНОЙ ЦЕЛЬЮ ДЛЯ КИБЕРПРЕСТУПНИКОВ, НА НЕГО ПРИШЛОСЬ 17% ВСЕХ УСПЕШНЫХ АТАК НА ОРГАНИЗАЦИИ, СВИДЕТЕЛЬСТВУЮТ ДАННЫЕ POSITIVE TECHNOLOGIES. ЭТОТ ПОКАЗАТЕЛЬ ВЫРОС НА 6 П. П. ПО СРАВНЕНИЮ С УРОВНЯМИ 2023 ГОДА И ПЕРВОЙ ПОЛОВИНЫ 2024-ГО. НА ВТОРОМ МЕСТЕ РАСПОЛОЖИЛСЯ ГОССЕКТОР (11%), СЛЕДОМ ИДУТ IT-КОМПАНИИ (9%) И ТЕЛЕКОММУНИКАЦИОННЫЙ СЕКТОР (7%). ЭКСПЕРТЫ РАССКАЗАЛИ О ПРИЧИНАХ И РИСКАХ И О ТОМ, НА ЧТО СЛЕДУЕТ ОБРАТИТЬ ВНИМАНИЕ БИЗНЕСУ. АЛЛА МИХЕЕНКО

Повышенное внимание злоумышленников к промышленности эксперты объясняют комплексом причин. «Промышленные предприятия стали главной мишенью из-за стратегической ценности их данных и производственных процессов, высокой цены простоя, а также значительной уязвимости инфраструктуры в связи с внедрением промышленного интернета вещей»,— отмечает Марина Холод, ведущий научный сотрудник Лаборатории искусственного интеллекта, нейротехнологий и бизнес-аналитики РЭУ им. Плеханова.

Ключевые риски связаны с возможными операционными последствиями. «Самый тяжелый риск связан с остановкой технологических процессов и нарушением цепочек поставок. В промышленности мы сразу имеем дело с физическими последствиями: сбоями в логистике или влиянием на качество продукции»,— указывает Сергей Крюков, генеральный директор exploitDog («НИР Груп»). Особую озабоченность, по его словам, вызывает ситуация в СЗФО, где добавляется фактор территориальной концентрации ключевых производств.

Эту точку зрения разделяет Николай Калуцкий, ведущий инженер-программист НОЦ ФНС России и МГТУ им. Баумана: «В первую очередь учитываем геополитический фактор, что представляет собой не цель выкупа, а нарушение технологической цепочки. Это несет за собой как коммерческий, так и иные виды ущерба».

Для Северо-Запада проблема киберугроз приобретает особую актуальность в силу специфики региона. «Северо-Запад — это энергетика, портовая логистика, металлургия и нефтехимия. Один инцидент в инфраструктуре, например, порта Усть-Луга, может привести к эффекту домино. Поэтому для предприятий СЗФО критично строить резервные контуры и налаживать обмен данными между IT- и OT-командами»,— считает Максим Власюк, директор по работе с промышленным сектором группы Arenadata.

При этом уязвимость промышленности носит системный характер. «Смещение фокуса киберпреступников в сторону промышленности объясняется высокой стоимостью простоя. Активное внедрение технологий „Индустрии 4.0“ расширяет „поверхность атаки“, а защита зачастую не успевает за темпами цифровизации»,— пояснил директор департамента расследований T.Hunter Игорь Бедеров.



FREEPIK

СМЕЩЕНИЕ ФОКУСА КИБЕРПРЕСТУПНИКОВ В СТОРОНУ ПРОМЫШЛЕННОСТИ ОБЪЯСНЯЕТСЯ ВЫСОКОЙ СТОИМОСТЬЮ ПРОСТОЯ ПРЕДПРИЯТИЙ

Наиболее уязвимы, по мнению экспертов, предприятия с непрерывным циклом, высокой ценой простоя, потенциалом серьезных физических последствий и ценной интеллектуальной собственностью: в энергетике, на транспорте, в нефтегазовой и оборонной промышленности.

ЧТО АТАКУЮТ Вариативность киберугроз растет. Ключевыми остаются программы-вымогатели, которые, по данным Positive Technologies, применялись в 49% атак на промышленные организации за полугодие 2025 года. Как пояснила госпожа Холод, успешная атака может полностью остановить производство. Также растет количество атак через цепочку поставок — через менее защищенных партнеров и поставщиков, что создает волновой эффект. На долю продвинутых угроз, связанных с кибершпионажем, приходится 19% атак, при этом свою роль играют и инсайдерские угрозы.

По словам господина Власюка, участились атаки на операционные технологические (OT) системы, управляющие физическими процессами. Данные Kaspersky ICS-CERT показывают, что во втором квартале 2025 года вредоносные объекты обнаруживались на каждом пятом компьютере в технологической сети.

Как отмечает CEO Concretto Ольга Болина, наиболее привлекательны для преступников объекты инфраструктуры с концентрацией стратегически важных данных, например, в оборонной промышленности или энергетике. При этом человеческий фактор и простые ошибки сотрудников остаются одними из главных рисков.

Руководитель проектов «Интеллектуальной аналитики» Тимофей Воронин перечисляет необходимые базовые меры защиты: регулярную смену сложных паролей, внедрение почтовых фильтров и использование дополнительных средств защиты.

Профессор Университета ИТМО Илья Лившиц обращает внимание на уязвимость физической инфраструктуры, включая центры обработки данных и системы электроснабжения. «Современные промышленные предприятия больше всего переживают за доступность — закрывают сети, внедряют безопасные каналы: VPN, шифрование и пр. Но линии связи уязвимы физически, те же центры обработки данных (ЦОД) могут быть недостаточно защищены. Если у компании или предприятия денег достаточно, они строят свои ЦОДы, а если нет, увы, приходится подключаться к внешним. Тот же „Яндекс“ „лег“ в этом году в Твери, в результате чего многие промышленные предприятия оказались отрезаны от своих данных»,— говорит эксперт. По его словам, для эффективной защиты необходимо внедрять полный замкнутый цикл обеспечения информационной безопасности в соответствии с международными стандартами.

ЗАТРАТЫ НА КИБЕРБЕЗОПАСНОСТЬ Финансирование защиты промышленных активов требует стратегического подхода. Как отмечает Татьяна Белоусова, директор направления ИБ ГК «УльтимаТек», специфика отрасли заключается в рисках физических разрушений, экологического ущерба и даже гибели людей при нарушении технологических процессов, что может привести к ущербу в сотни миллионов рублей.

Марина Холод акцентирует, что затраты на кибербезопасность следует рассматривать не как статью расходов, а как стратегические инвестиции в непрерывность бизнеса. По ее оценке, для малых и средних промышленных предприятий адекватные затраты составят более 15% IT-бюджета, для крупных — свыше 30%.

Сергей Крюков приводит более конкретные ориентиры: согласно международным и отечественным стандартам, на кибербезопасность рекомендуется выделять от 5 до 10% EBITDA компании. Доля бюджета ИБ в структуре IT-расходов обычно составляет от 10 до 20%, при этом для промышленного сектора чаще всего речь идет о примерно 10% бюджета.

ПРОГНОЗЫ НА 2026 ГОД Эксперты ожидают значительного усложнения киберугроз в 2026 году. Господин Бедеров прогнозирует увеличение общего количества успешных кибератак на 30–35%. Возрастет число целевых атак на объекты КИИ и ОПК, а также на системы промышленной автоматизации и IoT-устройства. Продолжится консолидация хактивистов в финансово мотивированные группировки.

Алексей Карпунин, партнер 5D Consulting, подтверждает тревожный тренд: количество атак и сбоев будет расти по мере цифровизации. Он подчеркивает необходимость рассматривать безопасность как часть корпоративной культуры, а не как отдельную функцию. ■

ТЕНДЕНЦИИ

7 → Госпожа Носаль приводит целый ряд рисков, связанных с применением искусственного интеллекта в сфере энергетики. На первом месте — проблемы кибербезопасности, так как интеграция ИИ и IoT увеличивает уязвимость энергетических систем к кибератакам. Поэтому компании должны усиливать меры кибербезопасности и разрабатывать системы защиты данных.

«Также сбор больших объемов данных может нарушать конфиденциальность как личных, так и коммерческих сведений. Это особенно актуально для защиты данных о потреблении энергии, которые могут раскрывать информацию о привычках потребителей или деловой активности компаний. Энергетическим компаниям необходимо строго соблюдать стандарты защиты данных для предотвращения утечек и манипуляций»,— отмечает эксперт.

Кроме этого, чрезмерная зависимость от ИИ повышает риски при сбоях систем, что может привести к остановке работы важных объектов инфраструктуры. Важно сохранять возможность ручного контроля и разрабатывать планы на случай сбоев. Также автоматизация процессов с помощью ИИ может привести к потере рабочих мест в ряде сфер, таких как обслуживание сетей и клиентские службы, но создает новые рабочие места в области кибербезопасности и анализа данных. Инвестиции в переобучение сотрудников помогут минимизировать этот риск.

Наконец, использование ИИ всегда связано с высокими начальными затратами. «Внедрение ИИ-систем требует значительных инвестиций, что может стать барьером для малых и средних компаний. Стратегическое планирование и государственная поддержка помогут смягчить этот риск»,— заключает госпожа Носаль.

По словам господина Фролагина, в целом для минимизации рисков необходимы комплексный подход к кибербезопасности, защита каналов передачи и хранения данных, постепенное внедрение ИИ, начиная с некритичных процессов, апробация технологий, сотрудничество энергокомпаний с разработчиками для создания отраслевых ИИ-решений, разработка нормативной базы и стандартов для применения ИИ в энергетике. Также важным является и последовательное обучение персонала отрасли цифровым компетенциям и работе с ИИ.

В целом эксперты уверены, что ИИ трансформирует топливно-энергетический сектор, предлагая значительные преимущества в эффективности и безопасности. Однако его внедрение требует тщательного подхода к управлению данными, безопасности и непрерывному обучению. Это, по словам экспертов, позволит максимально использовать потенциал ИИ и снизить возможные риски, обеспечивая устойчивое развитие энергетической отрасли в будущем. ■

Тематическое приложение к газете «Коммерсантъ» (онлайн-выпуск Санкт-Петербург, Guide «Цифровая экономика»)

Роман Уманский — генеральный директор АО «Коммерсантъ»
Михаил Лукин — главный редактор
Анатолий Гусев — автор дизайн-макета
Андрей Ершов — главный редактор СПб страниц
Александр Коряков — бильд-редактор
Алла Михеенко — выпускающий редактор
Марина Шевченко — корректор
Василиса Сатирская — верстка
Мария Кузнецова — отдел спецпроектов
Марина Победенная — рекламная служба

Адрес редакции и издателя: 123112, г. Москва, Пресненская наб, д.10 этаж 35. Тел. (495) 797-6970. Адрес редакции в Санкт-Петербурге: 191024, Харьковская ул., д. 8А, лит А. Тел. (812) 324-6949

Учредитель: АО «Коммерсантъ». Тематическое приложение к газете «Коммерсантъ», зарегистрировано Роскомнадзором, регистрационный номер и дата принятия решения о регистрации ПИ №ФС77-76923 от 11.10.2019 года

В печатном виде номер не выходит. Распространяется бесплатно. 16+

Фото на обложке: AI / pixabay