Обзор киберинцидентов в сфере энергетики, транспорта и управления производством за 2022 год

Оглавление

Аннотация

В 2020-2021 годах на риски кибербезопасности АСУ ТП и IIoT повлияла пандемия COVID-19 ввиду резкого перехода на дистанционной режим работы и внедрения средств для дистанционного контроля и управления промышленными сетями. Мир не успел восстановиться после пандемии, когда в 2022 году на ситуацию повлияли новые геополитические потрясения.

С февраля 2022 года и началом СВО, большинство кибератак в СМИ приняли выраженный политический оттенок, регулярно стал употребляться термин «кибервойна», заговорили о спонсируемых государствами хакерских группировках.

За год мы стали свидетелями кибератак на объекты критической информационной инфраструктуры, затронувших различные отрасли.

Инциденты информационной безопасности вели не только к прямому финансовому ущербу вследствие простоя производства, но и имели долгосрочные последствия в виде упущенной выгоды и дополнительных затрат на восстановление, ущерба репутации.

В данном обзоре **приведено порядка 35 крупных киберинцидентов за 2022 год** из сфер энергетики, производства и транспорта, затронувших информационные системы, сети и системы управления предприятиями и организациями сфер жизнеобеспечения, включая атаки, касающиеся вопросов национальной безопасности.

Несколько фактов

94% производственных компаний столкнулись с инцидентами кибербезопасности в 2022 году, при этом **менее трети из них внедрили на своих объектах системы безопасности IIoT и OT**, согласно отчету поставщика решений по кибербезопасности Barracuda и исследовательской организации Vanson Bourne «The state of the industrial security in 2022». При это 89% опрошенных признали, что обеспокоены влиянием геополитической ситуации на ландшафт угроз.

Программы-вымогатели сохранили свое лидерство и остались главной угрозой для систем контроля производства — **70% атак было совершено с помощью программ-вымогателей**, заявили в компании Dragos, занимающейся вопросами кибербезопасности АСУ ТП.

Исследователи из Check Point Research (CPR) сообщили, что за 2022 год **объем кибератак вырос на 38%**. В среднем на одну организацию приходится 1168 атак в неделю. По прогнозам специалистов, в 2023 году активность хакеров увеличится из-за доступности технологий искусственного интеллекта.

Киберинциденты

Киберинциденты в сфере производства

В январе 2022 из-за кибератаки были отключены по всему миру ИТ-системы **производителя бумаги и упаковки CPH Group** (Перлен, Швейцария). Производство бумаги и упаковки на площадках в Перлене и Мюльхайме было остановлено.

В феврале 2022 **крупнейший автопроизводитель в мире**, компания **Toyota Motor**, была вынуждена остановить производство на всех 14 площадках на территории Японии. Кибератаке подверглись системы поставщика автомобильного гиганта — **Kojima Industries**, который не смог отгружать электронные компоненты и пластиковые детали для производства автомобилей. Простой на производстве длился 24 часа и ударил по выпуску 13 000 автомобилей.

Одновременно вирусом-вымогателем был атакован другой гигант автомобильной индустрии (в том числе поставщик для Toyota) **шинный завод Bridgestone.** В качестве предосторожности от дальнейшего распространения атаки шинные заводы в Северной и Центральной Америке были остановлены, а рабочие отправлены домой. Производство удалось возобновить только через неделю.

В марте 2022 году подтвердил кибератаку **колбасный завод «Тавр» (Россия)**, входящий в ООО «Группа Агроком». Посредством установки вредоносного ПО были атакованы рабочие станции, серверы и информационные системы предприятия, что

временно парализовало его работу. По сообщению представителя компании, атака нанесла большой экономический ущерб.

В том же месяце кибератаке с помощью вируса-шифровальщика подверглись **несколько производственных предприятий, входящих в агрохолдинг «Мираторг» (Россия).** В результате пострадавшие предприятия не могли оформлять производственные и транспортные документы в течение нескольких суток.

В мае 2022, в разгар посевного сезона, атакой программы-вымогателя были нарушены производственные и бизнес-операции **производителя сельскохозяйственного оборудования AGCO (США).** Атака затронула несколько производственных площадок, например, во французском Бове была остановлена линия сборки, а работники отправлены домой. Также были остановлены продажи тракторов в критический месяц для сельскохозяйственной отрасли.

В июне в США было атаковано дочернее подразделение японского **производителя шлангов для автомобильной промышленности** (используются в гидравлических и пневматических системах) — **Nichirin-Flex USA**. Как сообщили в головном офисе в Японии, атака вынудила отключить компьютеризированный контроль производства, и американское подразделение перешло на ручной контроль и отгрузку продукции.

В июне 2022 в Иране из-за кибератаки был остановлен **один из крупнейших сталелитейных заводов Ирана Khuzestan Steel Industries**. По сообщению иранских СМИ, атака не удалась, но на производственных площадках пришлось остановить производство во избежание повреждения производственных линий и воздействия на цепочки поставок. Одновременно пострадали еще два завода сталелитейной промышленности Ирана: Mobarakeh Steel Company (MSC) и Hormozgan Steel Company (HOSCO).

В августе 2022 атакой с помощью вируса-вымогателя была нарушена деятельность мирового лидера в области **производства медицинских изделий Medi.** Атака была совершена на ИТ-системы производителя, но в результате инцидента ИБ было остановлено производство, нарушены операции доставки и логистики, а работников попросили не выходить на работу.

В сентябре от хакерской атаки пострадал **производитель шоколада Läderach (Швейцария)**. Представители компании не уточнили детали нападения, но от атаки пострадали производственные, логистические и административные процессы, которые приостановили деятельность компании.

В октябре кибератаке подвергся **крупнейший производитель меди в Европе, компания Aurubis (Германия).** Хакеры атаковали ИТ-системы компании, что повлияло и на производственные процессы. Производственные площадки продолжили работу, часть операций пришлось проводить в ограниченном режиме: прием и отгрузка

продукции совершались вручную, также инцидент ИБ ограничил бизнес-операции производителя.

В конце октября жертвой хакерской группировки (предположительно, Lockbit 3.0) стал **французский производитель упаковки Cartonnerie Gondardennes.** В результате кибератаки пострадали серверы управления гофроагрегатами, вследствие чего многие участки завода работали вхолостую или были полностью парализованы. Простой производства длился около недели.

В ноябре компьютерная атака нанесла огромный ущерб **производителю аэрокосмического литья EMA (Италия),** включая полную остановку производства. EMA является поставщиком высокотехнологичных компонентов для реактивных двигателей гражданской и военной авиации, а ее клиентами являются гиганты Boeing и Airbus. Помимо остановки производственных площадок, из строя были выведены все ИТ-системы компании, а на восстановление серверов, оборудования и программного обеспечения ушло несколько дней. С 21 по 25 ноября на работу не вышло почти 1000 человек.

В декабре мишенью для кибератак снова стала сталелитейная промышленность — был атакован **гигант промышленного машиностроения ThyssenKrupp (Германия)**. Помимо сталелитейного производства, в группу компании входит военное кораблестроение. Службе ИТ-безопасности удалось обнаружить инцидент на ранней стадии, и злоумышленники не успели нанести серьезный ущерб компании, но кибератака повлияла на отдел материалов и затронула корпоративные процессы.

В конце года произошел крупный инцидент ИБ с **корпорацией по производству меди Copper Mountain Mining Corporation (Канада).** ИТ-системы на руднике и корпоративные сети в офисе были атакованы с помощью программы-вымогателя. Компания изолировала операции и перешла на ручные процессы, а в работа завода была остановлена. Производство удалось возобновить только в начале января 2023 года. Во время простоя компания отправляла медный концентрат из запасов рудника в порт Ванкувера.

Киберинциденты в топливо-энергетическом комплексе

В январе 2022 года сразу **два предприятия топливно-энергетического комплекса Германии** стали жертвами кибератаки: **Oiltanking GmbH Group** и **Mabanaft Group,** которые занимаются хранением и поставкой нефти и нефтепродуктов (для таких компаний, как Shell). Oiltanking подтвердила, что терминалы работали с ограниченной пропускной способностью, а Mabanaft объявила форс-мажор для большей части своей деятельности по поставкам в Германии. Кибератака повлияла и на клиентов компаний, например, Shell столкнулась со сбоями в работе, и ей пришлось перенаправлять заказы.

Немецкий **гигант по обслуживанию ветряных турбин Deutsche Windtechnik** (обеспечивает работу более 8000 ветряных турбин в Европе, США и Тайване) подвергся целевой кибератаке в апреле 2022, из-за чего компании на 2 суток пришлось отключить системы для удаленного мониторинга ветряных турбин.

В конце сентября 2022 был атакован объект КИИ и **крупнейший поставщик электроэнергии Ганы — ECG (Electricity Company of Ghana).** Из-за хакеров часть систем компании была отключена, и в результате на 5 дней жители Ганы остались без электроэнергии. Инцидент ИБ потенциально затронул национальную безопасность Ганы.

Киберинциденты в сфере транспорта и логистики

В январе 2022 была атакована с помощью программы-вымогателя швейцарская **компания по предоставлению авиационных услуг Swissport** (выполняет работы по загрузке и разгрузке, заправке топливом и другие). Из-за возникших проблем было задержано 22 рейса в аэропорте Цюриха.

Инцидент информационной безопасности в апреле привел к отменам и длительным задержкам ряда рейсов канадской **авиакомпании Sunwing Airlines.** В результате инцидента множество пассажиров не смогли вылететь или вернуться в страну, застряв в аэропортах Центральной Америки.

Кибератаке также с помощью программы-вымогателя в мае подверглись системы **авиакомпании SpiceJet (Индия)**. Атака повлияла на выполнение рейсов, из-за чего рейсы были задержаны на 6–8 часов, а пассажиры оказались заперты в терминалах различных аэропортов.

В марте 2022 кибератакам подверглись **системы управления железными дорогами в Польше и Чехии**. В нескольких пунктах управления произошли компьютерные сбои, что привело к отмене поездов или задержке более, чем на два часа.

Жертвами хакеров в 2022 году неоднократно становились порты и терминалы.

В феврале подверглись атаке **нефтяные терминалы компаний SEA-Invest** из Бельгии и **Evos** из Нидерландов, что привело к хаосу в портах Европы. Киберинцидентом были нарушены операции разгрузки нефтепродуктов в 17 терминалах в Антверпене, Гамбурге, Амстердаме, Генте и Тернезене: нефтяные танкеры пришлось перенаправить в другие терминалы регионов. В течение нескольких суток терминалы продолжали работать с ограниченной пропускной способностью.

Тогда же, в феврале 2022, кибератаке подвергся **терминал порта Джавахарлала Неру (Индия),** который считается основным портом для обработки контейнерных грузов, через него проходит половина объема контейнерных грузов страны. Предположительно, атака была совершена с помощью вируса-вымогателя и затронула критически важные системы управления портом, в результате порт прекратил принимать суда и перенаправлял их в ближайшие работающие терминалы.

Кибератака на системы Национального института надзора за лекарственными препаратами и продуктами питания **INVIMA (Колумбия)** привела к отключению цифровой платформы, с помощью которой оформлялись операции по импорту товаров. В течение двух недель все операции выполнялись вручную. Все это привело к простою тысяч контейнеров в терминалах портов и аэропортов, в свою очередь, каждый день простоя привел к экономическим потерям и к росту цен на продукты.

Киберинциденты, связанные с конфликтами между государствами

В марте 2022 кибератаке подверглась **сеть космических спутников Viasat**, обслуживающих Европу и Украину. В результате атаке возникли помехи в обслуживании десятка тысяч точек спутникового интернета, а спустя две недели некоторые точки так и не восстановили свою работу. Высшее командование Франции назвало ущерб от кибератаки «непоправимым».

В июне 2022 в Израиле была **взломана система оповещения о ракетном нападении**. Ложные сирены были активированы в Иерусалиме и Эйлате и звучали в течение часа. Эксперты кибербезопасности высказали предположение, что кибератака могла быть произведена Ираном.

Прошедший 2022 год запомнился множеством сообщений о кибератаках, которые связывают с СВО. Часто о кибератаках сообщали сами хакерские группировки, хотя информация о них впоследствии оставалась неподтвержденной. Большое количество инцидентов являлись атаками типа «отказ в обслуживании» (DDoS) и ограничивались сайтами предприятий или государственных структур.

Например, еще в январе 2022 компьютерной атаке, названной худшей за последние 4 года, подверглись и были выведены из строя сайты **70 государственных учреждений Украины.**

В марте из-за выведенных из строя маршрутизаторов приостановил работу **провайдер телекоммуникационных услуг Triolan**. Тогда же были атакованы и системы **оператора связи Укртелеком**, оказывающего услуги военным формированиям.

В мае 2022 в России компьютерная атака на **ЕГАИС** вызвала масштабные сбои, вызвавшие нарушение поставок алкогольной продукции: заводы не могли отгружать цистерны со спиртом, а магазины не могли получить готовую продукцию.

В июле 2022 кибератаке подверглась **энергетическая компания ДТЭК** (Украина). По заявлению представителей компании, атака была направлена на нарушение технологических процессов генерирующих и распределительных компаний.

В России в сентябре масштабной кибератаке подверглись **системы электронного документооборота**, были атакованы **серверы правительства Москвы**. Вследствие кибератак в обоих случаях была нарушена работа с системами. Также сообщалось об атаке на **национальную платежную систему «Мир».**

Заключение

По мере развития технологий (в том числе и в кибербезопасности), совершенствуются и методы злоумышленников, которыми они могут совершать разрушительные атаки. Соответственно, в будущем кибератаки будут носить более сложный характер. В прошедшем году кибератаки приобрели политическую направленность, и в 2023 году следует ожидать сохранение данного тренда, в том числе усиление попыток нанести физический ущерб объектам КИИ.

По мере изменения ландшафта угроз организациям требуются актуальные и продвинутые решения для обеспечения защиты от широкого диапазона кибератак, а специалистам по кибербезопасности необходима гибкость для адаптации к новым типам угроз.

В текущей обстановке, когда кибератака может парализовать производство, организациям необходимо уделить особое внимание безопасности IIoT и OT, чтобы обеспечить защиту своих активов и избежать разрушительного ущерба не только в локальных, но и национальных масштабах.

Мониторинг утечек на сайте InfoWatch

На сайте Экспертно-аналитического центра InfoWatch регулярно публикуются отчеты по утечкам информации и самые громкие инциденты с комментариями экспертов InfoWatch.

Следите за новостями утечек, новыми отчетами, аналитическими и популярными статьями на наших каналах:

- Рассылка InfoWatch
- ВКонтакте
- Telegram
