Обзор наиболее значимых киберинцидентов в сфере управления производством и услугами за 2021 год

По оценкам экспертов из области кибербезопасности, прогнозы о ландшафте угроз в мире на 2021 год оправдались уже по итогам его первого квартала. Действия хакерских группировок с помощью вирусов-вымогателей против АСУТП и IIoT, включая системы управления критически важными объектами, уже годом ранее набирали обороты, эта же тенденция стала ключевой и на протяжении всего 2021 года. Хакеры поняли, что предприятия не могут допустить остановку производства и, скорее всего, заплатят выкуп вымогателям. Их ожидания оправдались: лишь исходя из опубликованных случаев, в 2021 году сумма уплаченного выкупа за один инцидент достигала $11 миллионов, а экономические потери составляли одного предприятия — до $600 миллионов.

Согласно исследованию, проспонсированному компанией Dragos, занимающейся вопросами кибербезопасности АСУТП, **средняя стоимость одного инцидента с АСУТП обходится компании почти в $3 миллиона.** В эту сумму входят лишь расходы на устранение самого инцидента и не включают упущенную выгоду и штрафы [1].

Стоит также отметить, что в отличие от атак, которые затрагивают ИТ-сети, атаки на производственные системы (ОТ-сети) позволяют получить доступ к управлению технологическими процессами, и в лучшем случае это лишь приостановит производство, а в худшем — станет реальной угрозой для жизни человека.

В связи с продолжением пандемии COVID-19 одной из самых привлекательных целей для киберпреступников оставалось здравоохранение.

Ущерб вследствие таких атак неминуем, однако не всегда пострадавший оглашает размер своих потерь. В данном обзоре мы собрали, в том числе, те случаи, когда ущерб был оглашен спустя месяцы после совершения кибератак.

Далее приведены примеры самых значимых киберинцидентов за 2021 в сфере управления производством с точки зрения последствий и экономических потерь.

Одной из атак, с которой начался 2021 год, стала атака с помощью программы-вымогателя на австрийского производителя кранов-манипуляторов **Palfinger**. В результате серьезно пострадали ИТ-системы большинства филиалов по всему миру: с компанией было невозможно связаться по электронной почте, компания не могла получать и обрабатывать заказы и совершать отгрузки [2].

В тот же день была совершена атака и на крупного производителя упаковки **WestRock** Company (США), из-за чего был нарушен график поставок с некоторых его предприятий. Компания подтвердила, что инцидент с программой-вымогателем затронул «некоторые ее операционные и информационные системы», хотя и не опубликовал точных сведений о влиянии инцидента на ОТ- и ИТ-системы [3].

Тогда же, в январе, по сообщению ФБР из-за вируса-вымогателя **сельскохозяйственная ферма в США потеряла $9 миллионов**, поскольку атака парализовала ее работу. Доступ в сеть фермы был осуществлен с помощью скомпрометированной учетной записи администратора [4].

В США произошел **инцидент с системой управления водоснабжением**: 5 февраля в Олдсмаре (штат Флорида) хакер, воспользовавшись установленной программой удаленного доступа TeamViewer, получил доступ к системе очистки воды и попытался отравить целый город с населением 15 000 человек, повысив щелочность воды в 100 раз. Сотрудник компании вовремя заметил вторжение в систему и успел снизить уровень содержания гидроксида натрия [5].

В феврале был атакован французский производитель лодок **Bénéteau**, в результате чего нарушилась работа производственных площадок в Бордо и Вандее. Если в день атаки производство шло в обычном режиме, поскольку необходимые детали были уже привезены, но на следующий день заводы прекратили свою работу до устранения последствий атаки [6].

От вируса-вымогателя в марте 2021 в США пострадала пятая по величине пивоварня в мире**Molson Coors** (производит бренды Pilsner, Miller, Blue Moon, Grolsch, Foster's, Killian's и др.). Кибератака привела к значительным нарушениям бизнес-операций, включая производство и отгрузку продукции [7]. Несмотря на то, что компания приняла все возможные меры по ликвидации последствий инцидента, даже спустя месяц после атаки она все еще сталкивалась со сбоями в работе, включая функционирование систем пивоваренного завода. Потери продукции вследствие инцидента компания оценила на $140 миллионов [8].

В том же месяце был атакован и немецкий химический завод по производству краски **Remmers** в Лёнингене, из-за чего пришлось остановить большую часть производства. Компания воздержалась от предоставления дополнительной информации о кибератаке [9].

В апреле в итальянском Винченце из-за хакерской атаки приостановлено производство на заводе **фармацевтической компании Zambon**. Атаку быстро идентифицировали и изолировали, однако простой завода, на котором работает 217 человек, продлился 5 дней [10].

Примером громкой атаки с помощью программы-вымогателя на сектор здравоохранения стала некоммерческая организация **Scripps Health** (Сан-Диего, США), которая управляет пятью больницами и 19 амбулаторными учреждениями. Несмотря на то, что ИТ-системы продолжили работу в автономном режиме, из-за атаки стало невозможно оказывать услуги некоторым пациентам, а для экстренной помощи пострадавших пришлось перенаправлять в другие учреждения [11].

Спустя три месяца, квартальный отчет Scripps Health показал, что **убытки из-за кибератаки составили почти $107 млн.** Большую часть (около $92 млн) составила упущенная выгода за тот месяц, который потребовался для восстановления ИТ-систем после инцидента кибербезопасности [12].

В мае была совершена одна из крупнейших кибератак на системы управления критически важными объектами в США (объекты КИИ в терминологии РФ). Кибератака с помощью программы-вымогателя привела к остановке крупнейшего нефтепровода (протяженность — 8850 км) компании **Colonial Pipeline**, который ежедневно обеспечивал топливом все Восточное побережье США. Министерство транспорта США объявило чрезвычайное положение в нескольких штатах.

Чтобы сдержать атаку, компании пришлось отключить системы, управляющие нефтепроводом, вследствие чего были отключены четыре магистральные линии. Это привело к росту мировых цен на нефть на 1%, а цена на бензин в США поднялась более чем на 3%. Ответственность за кибератаку взяла на себя группировка DarkSide, которой **компания заплатила выкуп в размере $4,4 млн** за получение ключа-дешифратора [13].

В мае программой-вымогателем Conti была атакована и государственная система здравоохранения Ирландии — **Health Service Executive**. Организации пришлось отключить ИТ-системы, обслуживающие медицинские учреждения по всей

территории Ирландии, вынудив врачей вернуться к процессам с помощью ручки и бумаги [14]. По оценкам, стоимость восстановления составит $600 миллионов, из них $120 млн уже ушло на непосредственное восстановление систем [15].

Примерами похожих атак, но в меньших масштабах, случились в июне. Жертвами стали больница **Humber River** в Торонто [16] и **St. Joseph's/Candler** в Саванне (штат Джорджия, США) [17].

В конце мая от атаки в Люксембурге пострадал производитель упаковки **Ardagh.** В данном случае основной производственный процесс был продолжен, но многие операции пришлось проводить в ручном режиме [18].

Завершился май 2021 громкой кибератакой **на JBS — крупнейшего производителя мяса в мире**. Для сдерживания атаки компания предприняла меры и отключила свои ИТ-системы, в результате которых остановилось производство на ряде предприятий в Канаде, США и Австралии, что привело к нехватке мяса и росту оптовых цен на 25% [19]. Для разблокировки систем **компания заплатила выкуп в размере $11 миллионов** [20].

В июне 2021 года известный японский производитель фототехники **Fujifilm** отказался платить выкуп хакерам, а зашифрованные вирусом-вымогателем файлы пришлось восстанавливать из резервных копий. В результате атаки на некоторое время были нарушены поставки продукции [21].

С помощью программы-вымогателя был атакован **французский завод фасадных покрытий Produits de Revêtement du Bâtiment (PRB).** Из-за атаки была полностью остановлена деятельность завода, и 650 работникам пришлось отправиться домой [22].

В июне 2021 года из-за похожей атаки были нарушены поставки **Edward Don** (США) — одного из крупнейших дистрибьюторов оборудования и материалов для точек общественного питания. Из-за кибератаки пострадали бизнес-операции, в том числе были недоступны сеть и электронная почта, вследствие чего нарушился график поставок в больницы, отели, рестораны и бары [23].

Следом из-за кибератаки в штате Висконсин (США) были вынуждены закрыться на несколько дней **казино и отель Menominee Casino Resort** [24].

Печально известный вирус-вымогатель Ruyk, с помощью которого шифровали ИТ-системы целых городов, отличился и в 2021 году. В июне были атакованы

муниципальные ИТ-сети города Льеж (Бельгия), вследствие чего стали недоступны сервисы полиции и большинства услуг для населения — например, ЗАГС [25].

Буквально на следующий день масштабная кибератака парализовала штаб-квартиру и третий по величине **молочный завод Австрии** — **Salzburgmilch**. Из-за полного отказа ИТ-систем остановилось производство, а сотрудники были вынуждены отправиться домой, также пострадали логистика и корпоративные сети [26].

В июле 2021 произошла крупная атака на цепочку поставок через Kaseya VSA — программное обеспечение для удаленного управления и работы серверов в розничной торговле, которая затронула компании по всему миру. Одной из первых жертв кибератаки стала **сеть шведских супермаркетов Coop**. Из-за атаки перестали работать кассовые аппараты и компании пришлось закрыть около 500 супермаркетов [27].

Атаки на сектор здравоохранения продолжились и в июле. Один из примеров — **больница для животных** в Йорке (США). В результате атаки с помощью программы-вымогателя была стерта информация о болезнях животных за 4 года. По словам владельца больницы, восстановление после инцидента кибербезопасности займет не менее года [28].

В середине июля 2021 **Счетная палата Республики Молдовы** подверглась разрушительной кибератаке, в результате которой хакеры взломали веб-сайт палаты и уничтожили общедоступные базы данных. Ситуацию усугубило то, что кибератака была совершена в период отчетности и официального опубликования результатов аудиторских проверок [29].

В июле 2021 **железнодорожная служба Ирана** стала жертвой атаки хакеров. В результате взлома хакеры на табло вокзалов всей страны разместили фейковые сообщения об отмене или задержке рейсов. Стало недоступно также электронное отслеживание поездов на территории Ирана, перестали работать веб-сайты национальной железной дороги и Министерства транспорта [30].

В результате кибератаки пострадали ИТ-системы крупной **южноафриканской железнодорожной, портовой и трубопроводной компании Transnet.** Компания сразу среагировала и предприняла все шаги для обеспечения непрерывности

операций, однако пострадала система контейнерных терминалов NAVIS, вследствие чего был простой в отправке грузов [31].

Полицейская служба в Канаде стала жертвой атаки с помощью программы-вымогателя в августе 2021, вследствие которой стал недоступен номер экстренного вызова 911 [32].

В сентябре 2021 пострадала отрасль сельского хозяйства США: сразу два субъекта критической информационной инфраструктуры (КИИ) стали мишенью для хакеров. По сообщениям обеих компаний, атака на КИИ серьезно подорвала их деятельность, а дальнейший простой принесет последствия хуже, чем атака в мае не трубопровод Colonial Pipeline. Первым подвергся атаке **производитель кормов и зерна NEW Cooperative** (США, штат Айова), имеющий более 60 филиалов по всему штату. Около 40% производства зерна зависит от поврежденного программного обеспечения, также от поставок этой компании зависит график кормления 11 млн голов скота [33].

Второй инцидент кибербезопасности произошел спустя два дня. Мишенью стал также производитель зерна — **сельскохозяйственный кооператив Crystal Valley**, обслуживающий фермы в Миннесоте и северной Айове. Для сдерживания атаки Crystal Valley также пришлось отключить свои информационные и управляющие системы, что уже прервало работу компании, а также сделало недоступным платежи по кредитным картам [34].

Из-за кибератаки сотни книжных магазинов во Франции, Бельгии и Нидерландах были вынуждены вернуться к операциям с помощью ручки и бумаги. Целью кибератаки стала платформа для управления продажами и движением запасов компании **TiteLive** — французской ИТ-компании, ее продуктом Medialog пользуются порядка 1000 книжных магазинов во Франции, Бельгии и Нидерландах [35].

В октябре 2021 кибератака с помощью вируса-вымогателя нарушила работу крупнейшего банка Эквадора **Banco Pichincha.** Из-за атаки были отключены банкоматы, а также не работали приложение банка, электронная почта и самообслуживание. На время отключения ИТ-систем для получения услуг клиентам пришлось обращаться напрямую в кассы банка [36].

От программы-вымогателя пострадала и шотландская инжиниринговая компания **Weir**. Компания быстро среагировала на атаку, однако она все равно помешала

выполнению операций и в итоге вынудила отложить поставки на общую сумму 50 млн фунтов стерлингов. По оценкам, **данный инцидент будет стоить** для Weir до 5 млн фунтов стерлингов (**около $7 млн**) [37].

В США с помощью вируса-вымогателя были зашифрованы серверы и рабочие станции, в результате чего вышли из строя телеканалы **Sinclair Broadcast Group**. Из-за повреждения корпоративных ИТ-систем стала недоступна и почта, в связи с чем сотрудникам пришлось создать новые почтовые ящики Gmail для общения со зрителями. Для эфиров им также пришлось делать презентации в MS PowerPoint и вручную рисовать графики на досках [38].

В конце октября в немецком Нойнкирхене кибератака привела к остановке завода электронных систем для автомобильной промышленности **Eberspächer** [39].

В США, штате Висконсин, были остановлены заводы и распределительных центров крупного производителя молочной продукции штата **Schreiber Foods**. Из-за кибератаки производство и отгрузки смогли возобновить лишь через 5 дней [40].

Компьютерный сбой привел к закрытию множества **автозаправочных станций по всей территории Ирана.** Автомобилисты по всей стране остались в длинных очередях на станциях с выключенными насосами и закрытыми заправками [41].

К декабрю 2021 стало известно о крупном инциденте, произошедшем в феврале 2021 у французского дистрибьютора офисного оборудования **Manutan**, имеющего 25 филиалов по всей Европе. Вирус-вымогатель зашифровал 1200 серверов компании — две трети всех имеющихся серверов. Работа была полностью парализована на 10 дней и полностью не была возобновлена вплоть до мая. Кибератака привела к ремонту пострадавших ИТ-систем, который продлится до 18 месяцев. Величину потерь компания не огласила [42].

В мае 2021 была совершена кибератака с помощью вируса-вымогателя на Департамент здравоохранения округа Вайкато (Новая Зеландия). Из-за атаки была парализована работа одного из четырех **региональных онкологических центров страны**. Вследствие этого Агентство по борьбе с раком объявило чрезвычайное положение в Новой Зеландии, чтобы перевести пациентов с опасными для жизни онкологическими заболеваниями в другие больницы [43].

В конце декабря 2021 от кибератаки пострадал норвежский сельскохозяйственный кооператив **Nortura.** Для сдерживания атаки кооперативу пришлось отключить

свои ИТ-системы, вследствие чего была приостановлена работа нескольких перерабатывающих заводов, а также офисов [44].

Выводы

Обращаем внимание, что, в данном обзоре идет речь только о ряде опубликованных случаях, поскольку многие компании не публикуют информацию о произошедших инцидентах. Однако по вышеописанным инцидентам можно судить о масштабе последствий кибератак на системы управления производством и услугами.

Киберинциденты оказываются разрушительными не только с точки зрения финансовых потерь, ведь последующий за ними репутационный ущерб может оказаться для компании куда более разрушительным.

На текущий момент промышленные предприятия по-прежнему сосредотачиваются на обеспечении безопасности данных и корпоративных информационных систем, часто пытаясь применить аналогичные решения по защите информации и для производственных систем (OT-сетей: АСУТП, IIoT), которые в большинстве случаев малоэффективны из-за специфики, вследствие чего OT-сети зачастую остаются фактически незащищенными. В свою очередь, сами OT-сети состоят из устаревших систем, для которых отсутствуют современные системы обеспечения кибербезопасности.

Источники:

1. The 2021 State of Industrial Cybersecurity: https://www.dragos.com/resource/2021-state-of-industrial-cybersecurity-ponemon/
2. Global cyber-attack: https://www.palfinger.com/en-us/news/global-cyber-attack_n_832132
3. WestRock Provides Update on Ransomware Incident: https://ir.westrock.com/press-releases/press-release-details/2021/WestRock-Provides-Update-on-Ransomware-Incident-8dfde2fca/default.aspx
4. US farm loses $9 million in the aftermath of a ransomware attack: https://therecord.media/us-farm-loses-9-million-in-the-aftermath-of-a-ransomware-attack/?__cf_chl_jschl_tk__=pmd_BbjvHLE6a7_Naw9MtpPJjrMrMGliHMXvunIlupOJUo8-1631176620-0-gqNtZGzNAmWjcnBszQp9
5. Someone tried to poison a Florida city by hacking into the water treatment system, sheriff says: https://amp.cnn.com/cnn/2021/02/08/us/oldsmar-florida-hack-water-poison/index.html
6. Vendée: l'entreprise Bénéteau victime d'une cyberattaque: https://www.francebleu.fr/infos/economie-social/vendee-l-entreprise-beneteau-victime-d-une-cyberattaque-1613755995
7. Molson Coors brewing operations disrupted by cyberattack: https://www.bleepingcomputer.com/news/security/molson-coors-brewing-operations-disrupted-by-cyberattack/
8. Molson Coors reports substantial progress in restoring systems after cybersecurity incident: https://industrialcyber.co/threats-attacks/molson-coors-reports-substantial-progress-in-restoring-systems-after-cybersecurity-incident/
9. Polizei ermittelt nach Cyberattacke auf Lackhersteller: https://www.ndr.de/nachrichten/niedersachsen/oldenburg_ostfriesland/Polizei-ermittelt-nach-Cyberattacke-auf-Lackhersteller,aktuelloldenburg6886.html
10. Attacco hacker alla casa farmaceutica Zambon: https://sicurezza.net/cyber-security/attacco-hacker-casa-farmaceutica-zambon
11. Security Incident Leads Scripps Health to Postpone Care: https://www.healthcareinfosecurity.com/security-incident-leads-scripps-health-to-postpone-care-a-16514

12. Healthcare provider expected to lose $106.8 million following ransomware attack: https://therecord.media/healthcare-provider-expected-to-lose-106-8-million-following-ransomware-attack/
13. Colonial Pipeline Confirms Ransomware Causing Disruptions: https://www.bankinfosecurity.com/colonial-pipeline-cybersecurity-attack-causes-disruptions-a-16549
14. Ransomware Attack Leads to IT Shutdown for Irish Hospitals: https://www.govinfosecurity.com/ransomware-attack-leads-to-shutdown-for-irish-hospitals-a-16618
15. Irish Ransomware Attack Recovery Cost Estimate: $600 Million: https://www.databreachtoday.com/irish-ransomware-attack-recovery-cost-estimate-600-million-a-16931
16. Code Grey - Update: https://www.hrh.ca/2021/06/15/code-grey/
17. Savannah hospital system experiences outage after ransomware attack: https://www.wavy.com/news/national/savannah-hospital-system-experiences-outage-after-ransomware-attack/
18. Cyberattack hits packaging giant Ardagh: https://www.siliconrepublic.com/enterprise/ardagh-cyberattack
19. Media Statement: JBS USA Cybersecurity Attack: https://www.globenewswire.com/news-release/2021/05/31/2239049/0/en/Media-Statement-JBS-USA-Cybersecurity-Attack.html
20. Meat processor JBS paid $11 million in ransom to hackers: https://www.databreaches.net/meat-processor-jbs-paid-11-million-in-ransom-to-hackers/
21. Unauthorized access to Fujifilm servers: https://www.fujifilm.com/jp/en/news/hq/6642-2
22. Vendée : l'entreprise PRB touchée par une cyberattaque https://www.francebleu.fr/infos/faits-divers-justice/vendee-l-entreprise-prb-touchee-par-une-cyberattaque-1622814480
23. Foodservice supplier Edward Don hit by a ransomware attack: https://www.bleepingcomputer.com/news/security/foodservice-supplier-edward-don-hit-by-a-ransomware-attack/
24. Menominee Casino Resort temporarily closes after cyberattack: https://www.nbc26.com/news/local-news/menominee-casino-resort-temporarily-closes-after-cyberattack

25. City of Liege, Belgium hit by ransomware: https://www.databreaches.net/city-of-liege-belgium-hit-by-ransomware/
26. SalzburgMilch von Hackern lahmgelegt: https://bauernzeitung.at/salzburgmilch-von-hackern-lahmgelegt/
27. Coop supermarket closes 500 stores after Kaseya ransomware: attackhttps://www.bleepingcomputer.com/news/security/coop-supermarket-closes-500-stores-after-kaseya-ransomware-attack/
28. Ransomware attackers wanted $80,000 from York Animal Hospital. They won't pay. https://www.seacoastonline.com/story/news/crime/2021/07/12/york-animal-hospital-maine-ransomware-cyberattack-wipes-pet-medical-records-suspects-russia-bitcoin/7938174002/
29. Public databases of Moldova's Court of Accounts destroyed by cyber attack: https://www.moldpres.md/en/news/2021/07/15/21005099
30. Iran's Rail Service Hacked With Fake Delay Messages Urging Users To Call Khamenei: https://www.republicworld.com/world-news/middle-east/irans-rail-service-hacked-with-fake-delay-messages-urging-users-to-call-khamenei.html
31. Violence in SA | Transnet operations return to normal: https://www.enca.com/business/violence-sa-transnet-operations-return-normal
32. Sault Ste. Marie Police Service victim of ransomware attack: https://www.databreaches.net/sault-ste-marie-police-service-victim-of-ransomware-attack/
33. US farmer cooperative hit by $5.9M BlackMatter ransomware attack: https://www.bleepingcomputer.com/news/security/us-farmer-cooperative-hit-by-59m-blackmatter-ransomware-attack/
34. Second farming cooperative shut down by ransomware this week: https://www.bleepingcomputer.com/news/security/second-farming-cooperative-shut-down-by-ransomware-this-week/
35. Ransomware : un logiciel malveillant s'en prend aux librairies françaises et belges: https://actualitte.com/article/102604/technologie/ransomware-un-logiciel-malveillant-s-en-prend-aux-librairies-francaises-et-belges
36. Cyberattack shuts down Ecuador's largest bank, Banco Pichincha: https://www.bleepingcomputer.com/news/security/cyberattack-shuts-down-ecuadors-largest-bank-banco-pichincha/
37. Engineering firm Weir hit by major ransomware attack: https://www.bbc.com/news/uk-scotland-scotland-business-58801753

38. Sinclair Broadcast Group Provides Information On Cybersecurity Incident: https://www.sec.gov/Archives/edgar/data/0000912752/000119312521300540/d245680dex991.htm
39. Cyber-Angriff legt Eberspächer lahm: https://www.sr.de/sr/home/nachrichten/politik_wirtschaft/eberspaecher_neunkirchen_cyberangriff_100.html
40. Schreiber Foods hit with cyberattack; plants closed: https://www.wisfarmer.com/story/news/2021/10/26/schreiber-foods-hit-cyberattack-plants-closed/8558252002/
41. Cyber attack closes Iran's petrol stations: https://www.maitlandmercury.com.au/story/7485884/cyber-attack-closes-irans-petrol-stations/
42. Recovering from ransomware: One organisation's inside story: https://www.computerweekly.com/news/252510116/Recovering-from-ransomware-One-organisations-inside-story
43. Waikato DHB cyberattack: Cancer hub out of action in chaotic aftermath: https://www.nzherald.co.nz/nz/waikato-dhb-cyberattack-cancer-hub-out-of-action-in-chaotic-aftermath/TULGWXLIE3TI7NDDVPJOSAIX7E/
44. Nortura er utsatt for et dataangrep: https://www.nortura.no/nyheter/nortura-er-utsatt-for-et-dataangrep