Обзор

Статистика и тенденции киберинцидентов АСУ ТП за 2022 год

© Экспертно-аналитический центр InfoWatch. 2023 г.

Недавно экспертно-аналитический центр InfoWatch выпустил обзор самых крупных инцидентов с АСУ ТП и IIoT за прошедший год. В данном обзоре мы приводим общую статистику по инцидентам за 2022 год по зарубежным данным.

За 2022 год объем кибератак вырос на 38%, сообщили исследователи из **Check Point** прогнозам специалистов, в 2023 году активность хакеров увеличится из-за доступности технологий искусственного интеллекта.

Согласно отчету Всемирного экономического форума «Global Risks Perception Survey 2022-2023», в числе главных рисков на 2023 год, помимо кризиса энергоснабжения и инфляции, признаны **кибератаки на критическую инфраструктуру**:

Рисунок 1

Источник: World Economic Forum Global Risks Perception Survey 2022–2023

Опрос проводился в конце 2022 года среди 1200 представителей и экспертов из научных кругов, бизнеса, правительства.

В краткосрочной (на период до 2 лет) и в долгосрочной перспективе (до 10 лет) респонденты проранжировали риски следующим образом:

	Short term		Long term
1	Cost-of-living crisis	1	Failure to mitigate climate change
2	Natural disasters and extreme weather events	2	Failure of climate-change adaption
3	Geoeconomic confrontation	3	Natural disasters and extreme weather events
4	Failure to mitigate climate change	4	Biodiversity loss and ecosystem collapse
5	Erosion of social cohesion and societal polarization	5	Large-scale involuntary migration
6	Large-scale environmental damage incidents	6	Natural resource crises
7	Failure of climate-change adaption	7	Erosion of social cohesion and societal polarization
8	Widespread cybercrime and cyber insecurity	8	Widespread cybercrime and cyber insecurity
9	Natural resource crises	9	Geoeconomic confrontation
10	Large-scale involuntary migration	10	Large-scale environmental damage incidents
11	Debt crises	11	Misinformation and disinformation
12	Failure to stabilize price trajectories	12	Ineffectiveness of multilateral institutions and international cooperation
13	Prolonged economic downturn	13	Interstate conflict
14	Interstate conflict	14	Debt crises
15	Ineffectiveness of multilateral institutions and international cooperation	15	Cost-of-living crisis
16	Misinformation and disinformation	16	Breakdown of critical information infrastructure
17	Collapse of a systemically important industry or supply chain	17	Digital power concentration
18	Biodiversity loss and ecosystem collapse	18	Adverse outcomes of frontier technologies
19	Employment crises	19	Failure to stabilize price trajectories
20	Infectious diseases	20	Chronic diseases and health conditions
21	Use of weapons of mass destruction	21	Prolonged economic downturn
22	Asset bubble bursts	22	State collapse or severe instability
23	Severe mental health deterioration	23	Employment crises
24	Breakdown of critical information infrastructure	24	Collapse of a systemically important industry or supply chain
25	State collapse or severe instability	25	Severe mental health deterioration

Рисунок 2

Источник: World Economic Forum Global Risks Perception Survey 2022–2023

Как видно из рисунка выше, и в краткосрочной, и в долгосрочной перспективе киберпреступления входит в первую 10-ку. Риск нарушения работы критической информационной инфраструктуры в долгосрочной перспективе заняло 16 место, в краткосрочной — 24.

Согласно отчету поставщика решений по кибербезопасности **Barracuda** и исследовательской организации **Vanson Bourne «The state of the industrial security** сообщили, что сталкивались с инцидентами ИБ за последние 12 месяцев. По отраслям инциденты распределились следующим образом:

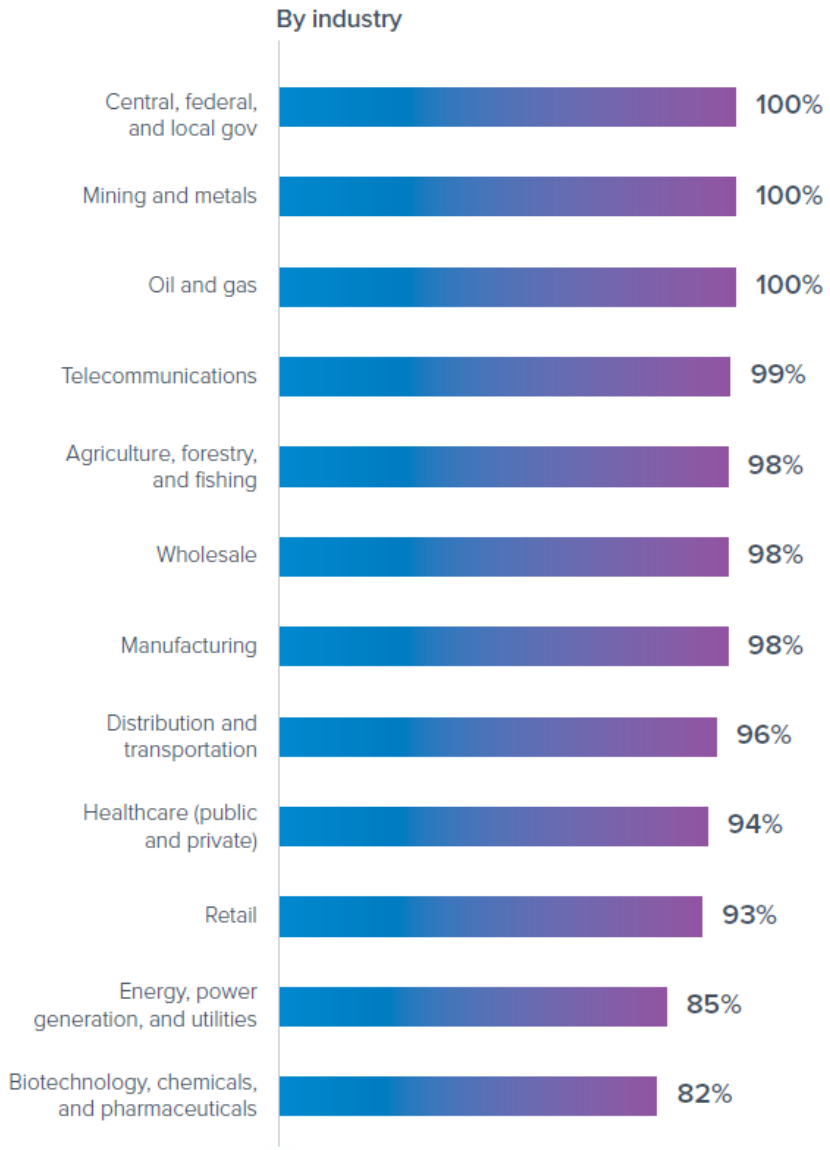

Рисунок 3

Источник: The state of the industrial security in 2022

То есть все специалисты из госсектора единогласно отметили, что сталкивались с инцидентами безопасности в 2022 году. Также отметили 100% опрошенных из отрасли металлургии и добывающей промышленности.

Представителей организаций также спросили, какое влияние на деятельность их организации оказал самый значительный инцидент безопасности, произошедший за последние 12 месяцев.

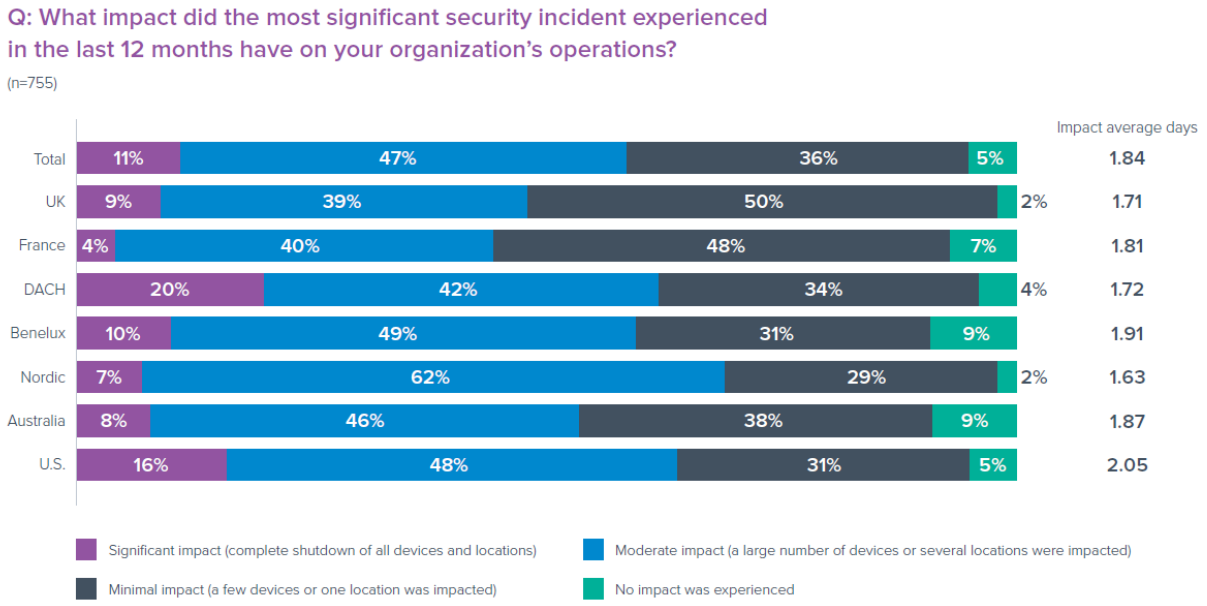

Рисунок 4

Источник: The state of the industrial security in 2022

Наиболее разрушительные для деятельности организаций инциденты ИБ (полная остановка производства) произошли в США и немецкоязычных странах (Германия, Австрия, Швейцария).

Как ответили представители различных отраслей:

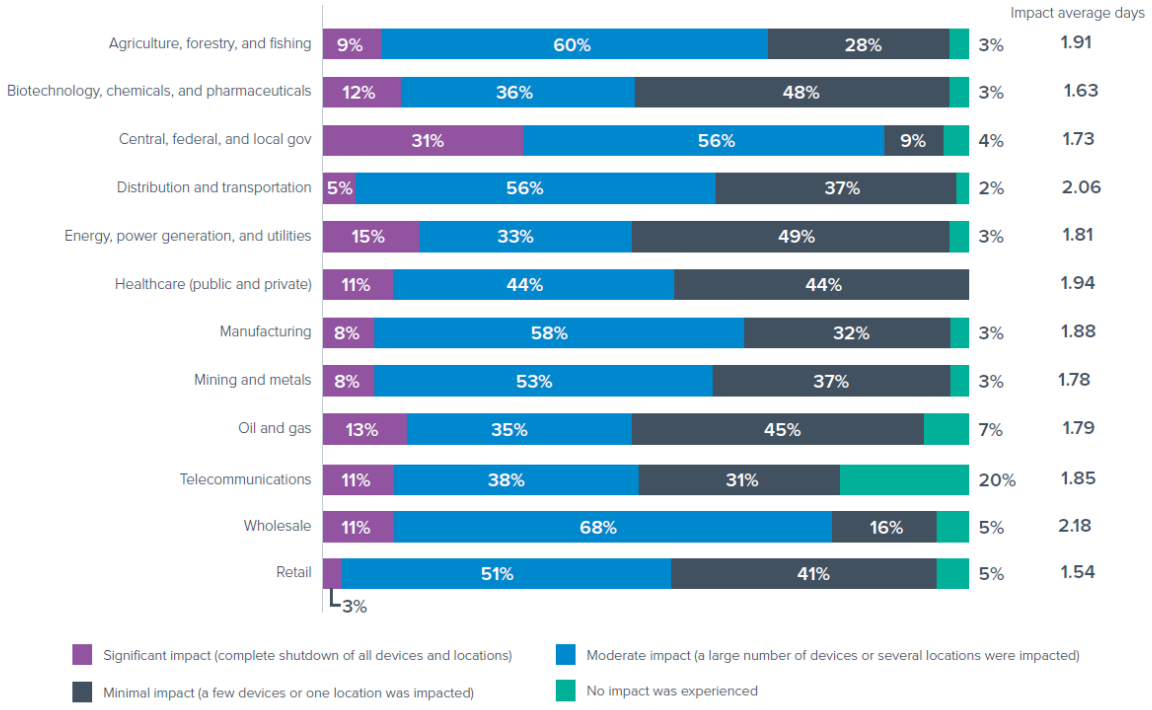

Рисунок 5

Источник: The state of the industrial security in 2022

Наибольшее влияние инцидентов информационной безопасности на деятельность организации отмечено в госсекторе, а также в топливно-энергетическом комплексе.

Самыми распространенными инцидентами были атаки на веб-приложения, вредоносное внешнее оборудование или съемные носители, DDoS-атаки и скомпрометированный удаленный доступ. Подробнее на рисунке:

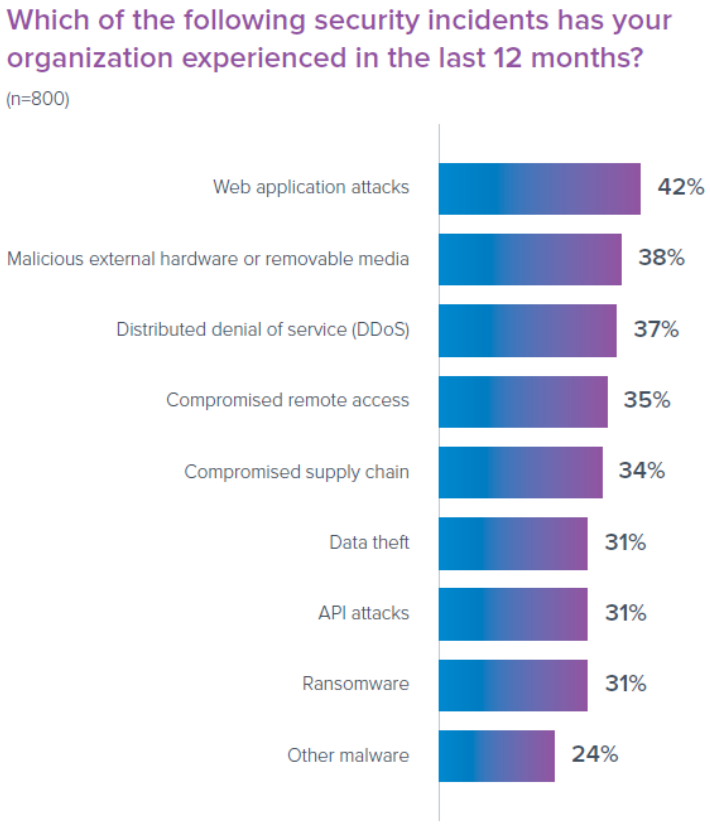

Рисунок 6

Источник: The state of the industrial security in 2022

Компания **Dragos** в ежегодном исследовании **«ICS/OT Cybersecurity. Year in review**

- Зафиксировано более 600 атак на промышленные организации, что на 87% больше, чем в 2022 году.
- Групп программ-вымогателей, нацеленных на ИТ и ОТ-среды промышленных предприятий, стало на 35% больше.
- 72% всех атак программ-вымогателей были нацелены на организации из сектора производства (437), далее самой привлекательно для злоумышленников отраслью стала пищевая промышленность, энергетика, фармацевтическая промышленность и нефтегазовая отрасль.

В отчете **«OT/IoT Security Report 2022»** (**Nozomi Networks**) были проанализированы все сообщения о раскрытых уязвимостях, опубликованные CISA за 2 полугодие 2022 года.

5 основных секторов, затронутых обнаруженными уязвимостями:

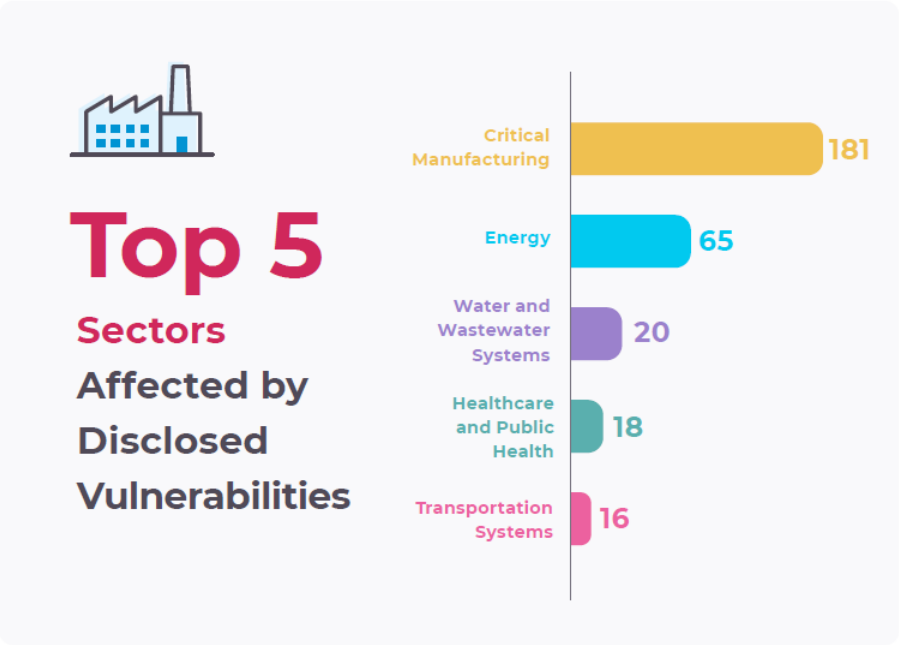

Рисунок 7

Источник: OT/IoT Security Report 2022, Nozomi Networks

Согласно анализу, отмечены две новые уязвимые отрасли:

- водоснабжение и водоотведение,
- транспортные системы.

По мнению представителей различных промышленных секторов, продеставленных в исследовании компании **SANS «The State of ICS/OT Cybersecurity in 2022 and** процессы, в сферах бизнес-услуг, здравоохранения и в том, числе, критически важные производственные процессы. Полный список представлен ниже:

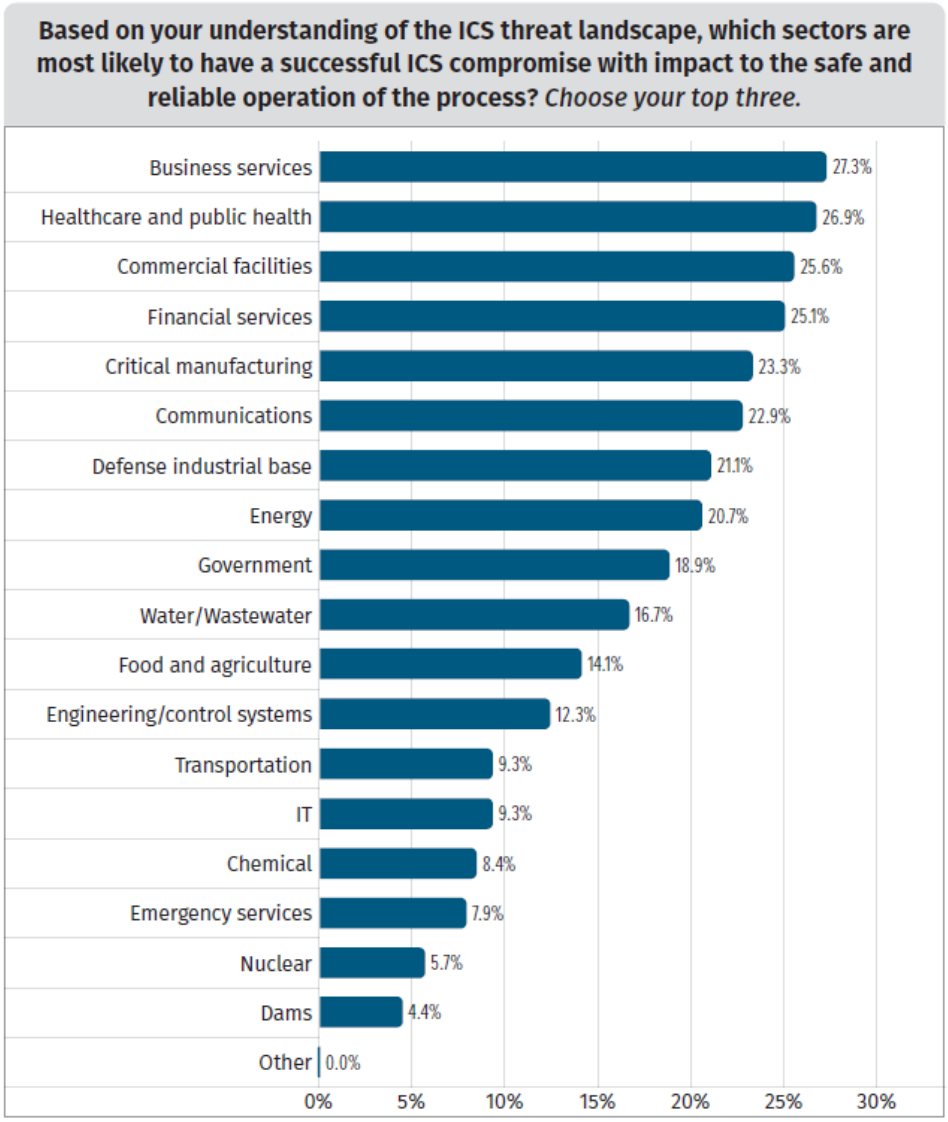

Рисунок 8

Источник: The State of ICS/OT Cybersecurity in 2022 and Beyond, SANS

За последние 12 месяцев 36,6% опрошенных сообщили, что их производственные организации подверглись менее 10 атакам. 24,4% респондентов ответили, что их организации подверглись 21 до 50 атак за последний год. Подробнее представлено на рисунке:

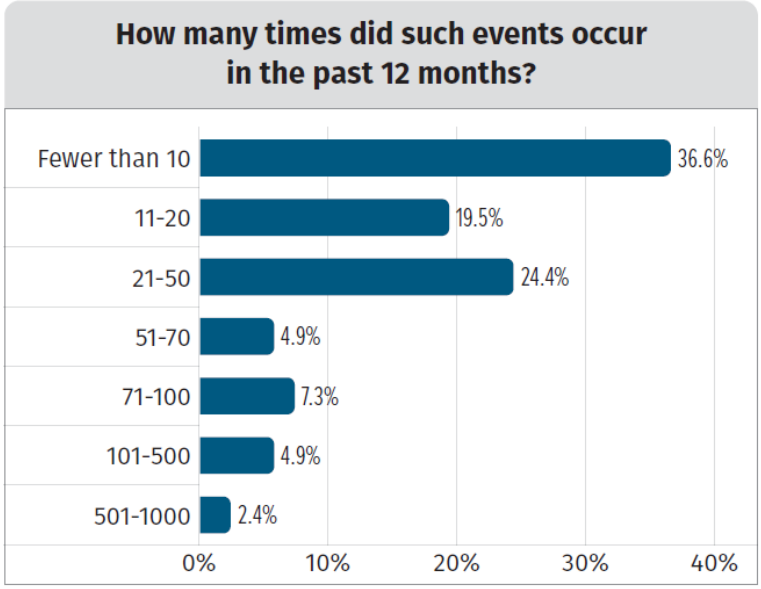

Рисунок 9

Источник: The State of ICS/OT Cybersecurity in 2022 and Beyond, SANS

Начальные вектора атак:

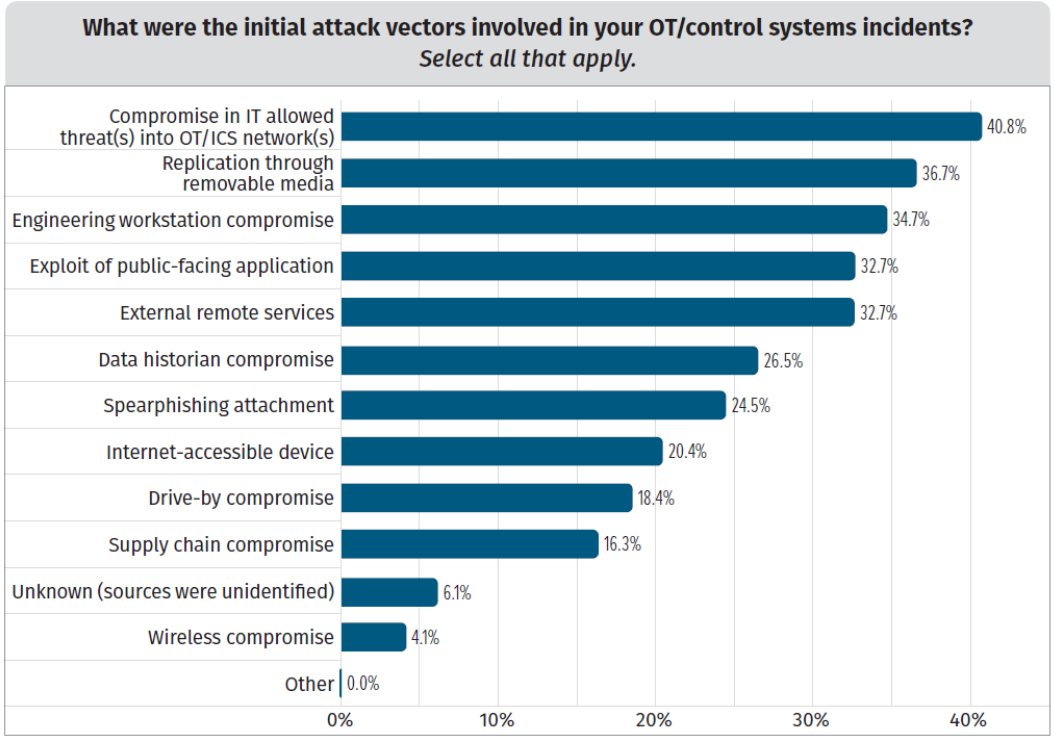

Рисунок 10

Источник: The State of ICS/OT Cybersecurity in 2022 and Beyond, SANS

Как видно из рисунка выше, более трети респондентов (40,8%) сообщили, что причинение вреда сети промышленной АСУ произошло через уязвимости IT-сети. На втором (36,7%) месте стала репликация через съемный носитель, и на третьем — компрометация инженерной рабочей станции.

Мониторинг утечек на сайте InfoWatch

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

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

- Рассылка InfoWatch
- ВКонтакте
- Telegram

InfoWatch

Полное воспроизведение, опубликование материалов запрещено.

Цитирование возможно только при указании ссылки на источник.