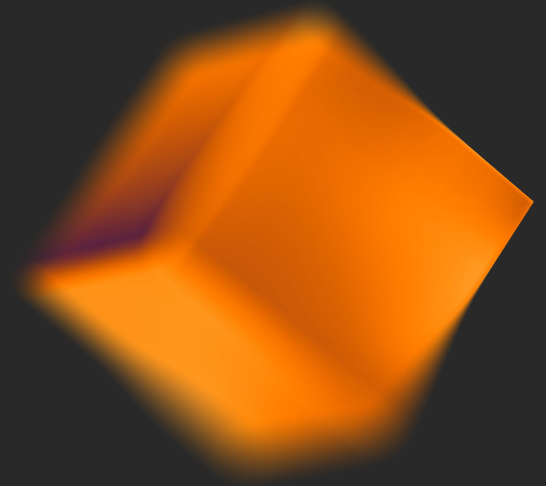
Открываем горизонты цифрового будущего

Особенности защиты информации в АСУ ТП на металлургическом производстве. Практический опыт: основные векторы кибератак на субъекты КИИ в 2024 году

(ТБ-ФОРУМ)



Подготовил: Севостьянов Александр Владимирович

Директор ДЭБ АО «ДИАЙПИ» – Советник Службы экономической безопасности ПАО «ТМК»

07 марта 2025 г

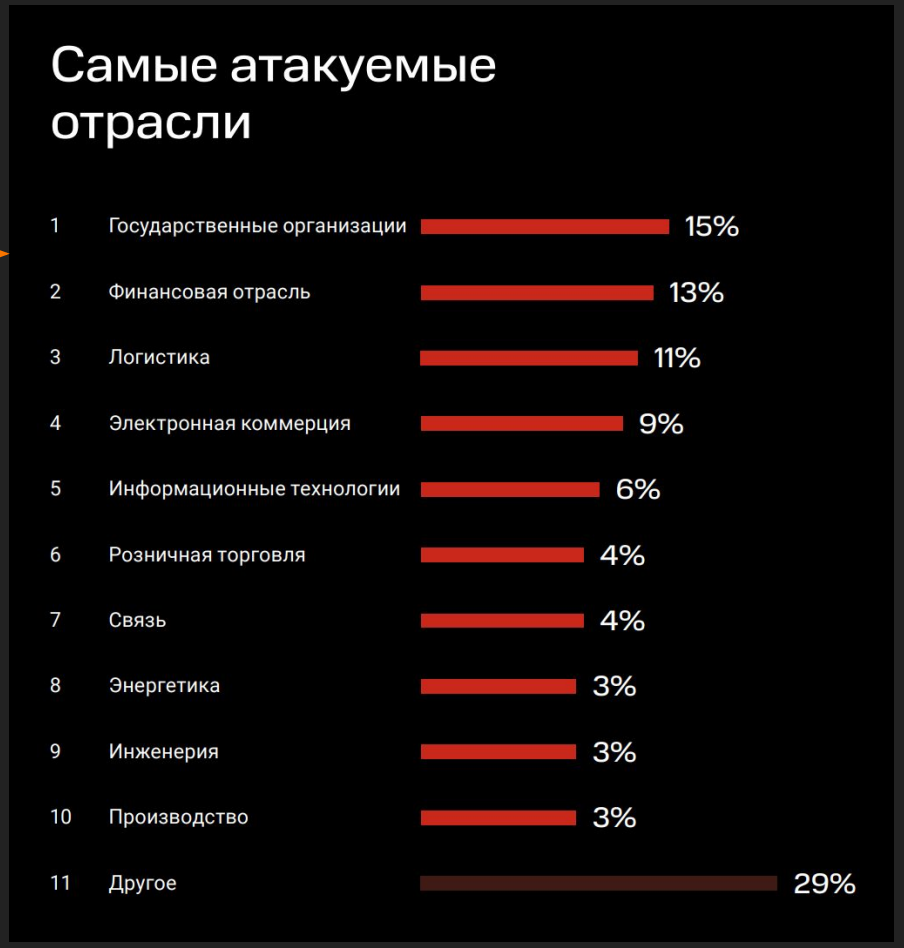
2024 год. Итоги

Атака на отраслевого «якорного партнёра» - угроза Субъекту! (актуально 2024 - 2025)

МОСКВА, 16 янв - РИА Новости. Роскомнадзор за 2024 год зафиксировал **135** случаев утечек баз данных, в которых содержалось более **710** миллионов записей о россиянах

(Пдн. в ряде атак на Субъекта являются отправной точкой для реализации преступных намерений!)

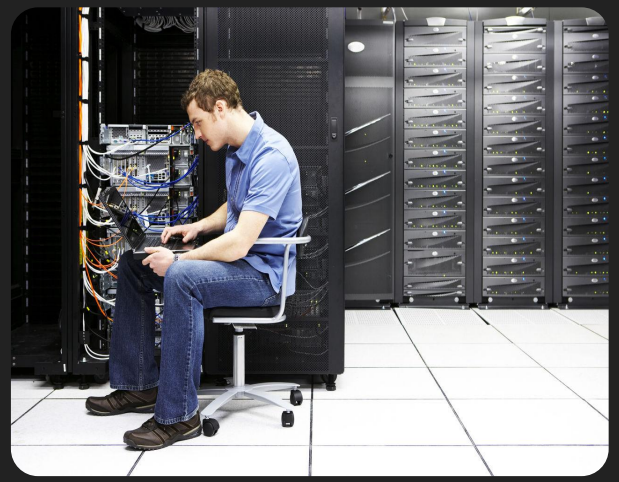
Самые атакуемые отрасли



«THREAT ZONE»/BI.ZONE Исследование российского ландшафта киберугроз 2025

Особенности металлургического предприятия

- Почти все предприятия промышленности – субъекты КИИ и операторы персональных данных (187-ФЗ, Указ Президента №250, 152-ФЗ, 149-ФЗ
- Значительная доля промышленного программного обеспечения и компьютерного оборудования – иностранного производства
- Необходимость перехода на СЗИ и ОС отечественного производства, пока уступающих иностранным аналогам по ряду классов средств защиты (NGFW и т.д.)
- Острая нехватка квалифицированного персонала в области ИБ и КИБ
- Риски параллельного импорта (экономические, информационные и правовые)
- Нахождение в состоянии «постоянно под атакой» (особенно в компаниях подсанкционных списков)



Основные вектора атак 2024

Подрядчики услуг
ИТ/сервисы
(шифрование инфраструктуры)

Персонал
(фишинг)

Web
(ddos)

Основной вектор кибер-атак сместился с Субъекта (стало сложно) на его партнёров, подрядчиков и персонал (потому что их проще)!

Как защищаемся и что делать

Угроза	От чего защищаемся	Что делать?
Несанкционированный доступ к ИТ-инфраструктуре	• Риски нанесения ущерба в следствии компьютерных атак через подрядчика (включая остановку производственной деятельности)	• услуги под контролем через сочетание двух систем в реальном времени: PAM + SIEM (SOC) • подписание NDA • качественная проверка юр.лица на благонадежность; • проверка модели исполнения работ (удаленка; офис; локация) • выдача служебной техники исполнителям • сегментация сети • разделение КСПД от ПСПД • установление уровня зрелости ИБ/ИТ подрядчика (идём на прямой диалог)
Нарушение конфиденциальности информации ограниченного доступа	• Риски нанесения ущерба субъекту Пдн. • Риски нанесения ущерба от утраты секретов производства вследствие промышленного шпионажа	Локализация критических информационных систем внутри ИТ-периметра Предприятий (ИСПДн., СУБД с НИР/НИОКР; разработка; ДБО; АСУТП), т.е. уходим из «облаков» + DCAP
Компрометация персонала через фишинг	• Риски нанесения ущерба работнику • Риски нанесения ущерба Предприятию вследствие НСД к данным работника (атака через персонал)	Оптимизация привилегированных пользователей; регулярное информирование персонала после каждого случая атаки; исключение из корп. коммуникаций иностранных мессенджеров

Спасибо за внимание!