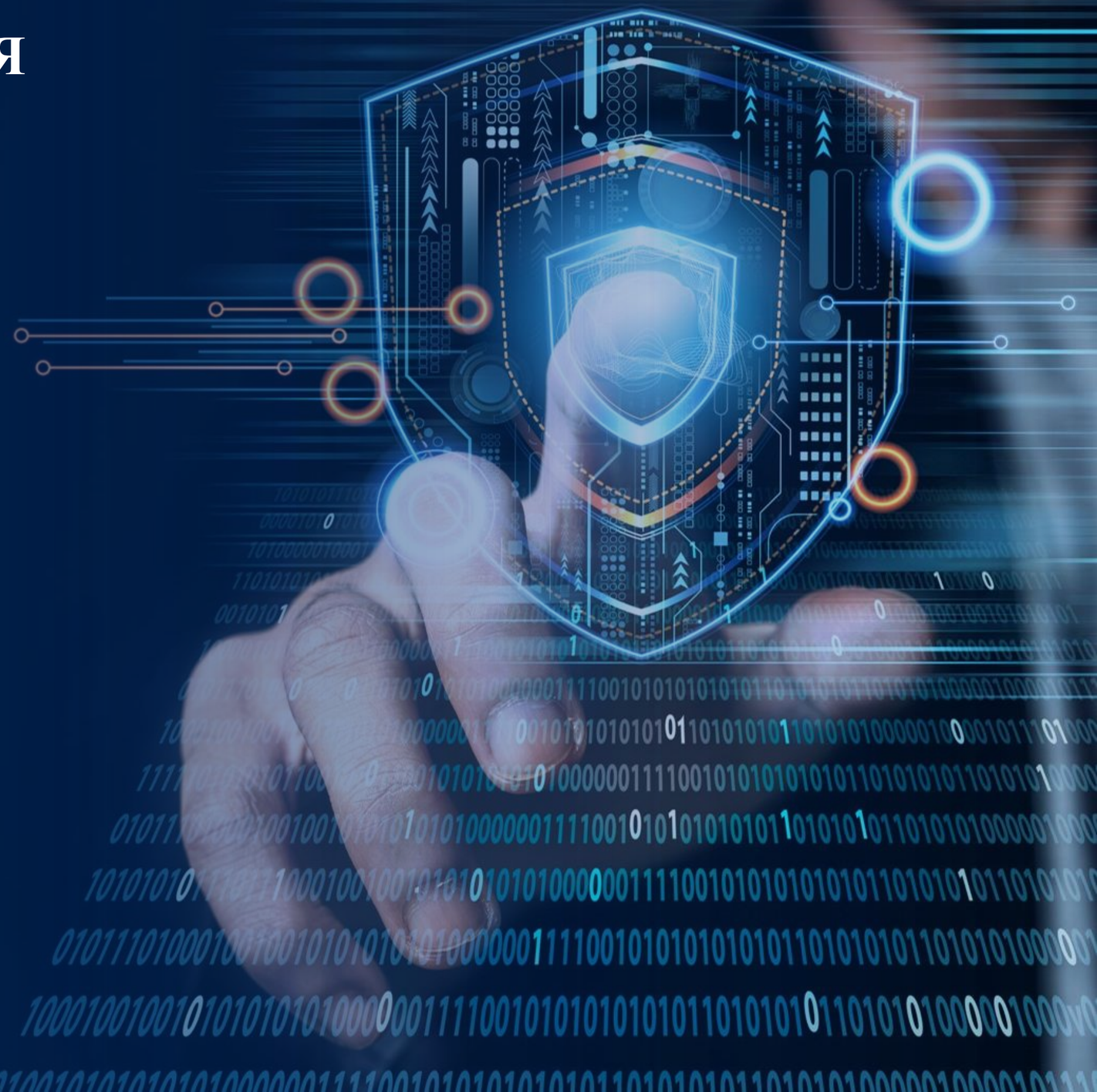
CNEWS: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ 2025

ТРЕНДЫ УГРОЗ КБ В 2025 ГОДУ



BELYAEV

Директор по КБ: Беляев Дмитрий Александрович

ОБО МНЕ

Беляев Дмитрий Александрович

•Более 10 лет в ИБ;

• Имею 3 образования;

•Имею более 130 сертификатов/дипломов и благодарностей по тематике ИБ;

•Победитель в рейтинге ТОП-100 Лидеров ИТ;

•В прошлом руководил 5-ю стартапами (в т.ч и по ИБ) и командой из более 100 человек;

• Имею за плечами более 70 выступлений на публику суммарной численностью >5000 человек (TADVISER, ТБ Форум, Территория Безопасности, CISO Форум, CNews, ITsec, Security Summit и т.д).

СТАВКИ ВЫСОКИ

- Лавина судов и потенциальных банкротств компаний, в связи с утечкой ПДн по оборотному штрафу;
- Всплеск атак с использованием программ-вымогателей;
- Мошенничество в играх выйдет на новый уровень;
- Внедрение ВПО в прошивку железа;
- Рост доступности инструментов искусственного интеллекта для вредоносных целей (Трамп отменил указ о мерах безопасности в области ИИ)*

* - https://rb.ru/news/trum-ai-biden/

ОБЛАКО ТРЕНДОВ КБ 2025

* - https://rb.ru/news/trum-ai-biden/

ЛУЧШЕ УЧИТЬСЯ НА ЧУЖИХ ОШИБКАХ

Как ушел на дно интернет бизнес и бухгалтерская компания

Кража ПДн привела Vastaamo к банкротству

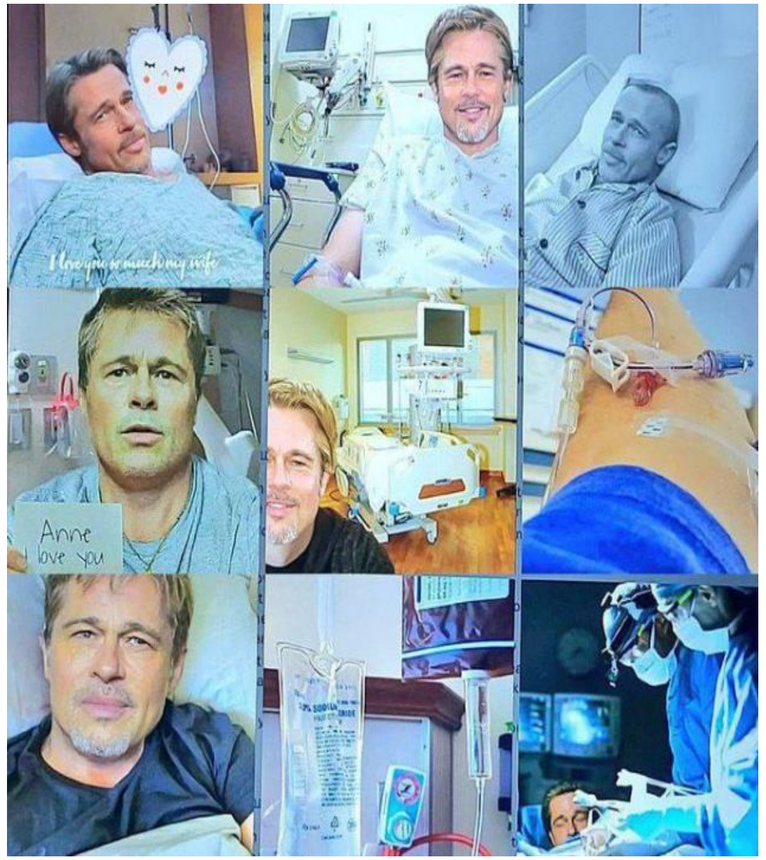
Атака вымогателей обанкротила фирму, занимающуюся полиграфией

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ПАЛКА О ДВУХ КОНЦАХ

- Вредоносное ПО на основе ИИ адаптируется в режиме реального времени, обходя стандартные антивирусные программы;
- Автономные боты выявляют и используют уязвимости;
- Контент, созданный искусственным интеллектом, используется для атак с применением социальной инженерии, чтобы обманывать сотрудников.

ВЗЛОМАННАЯ РЕАЛЬНОСТЬ

- Дипфейки могут имитировать реальных людей, поэтому их трудно обнаружить.
- Они используются в мошеннических схемах и кампаниях по дезинформации.
- Ожидается, что дипфейки будут распространяться, создавая серьёзную проблему для кибербезопасности.



СТАТИСТИКА

- Количество дипфейков увеличилось на 550% с 2019 по 2023 год*
- Количество программ-вымогателей выросло на 81% в годовом исчислении с 2023 по 2024 год*

* - https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

ЧЕЛОВЕЧЕСКИЙ ФАКТОР: АТАКИ ЧЕРЕЗ СОЦИАЛЬНУЮ ИНЖЕНЕРИЮ

- Социальная инженерия на основе ИИ использует сгенерированные ИИ голоса и видео.
- Киберпреступники используют местные языки и диалекты, чтобы повысить доверие.
- Дипфейки и контент, созданный искусственным интеллектом, используются для создания убедительных мошеннических схем.

КРИТИЧЕСКАЯ ИНФРАСТРУКТУРА НА ПРИЦЕЛЕ

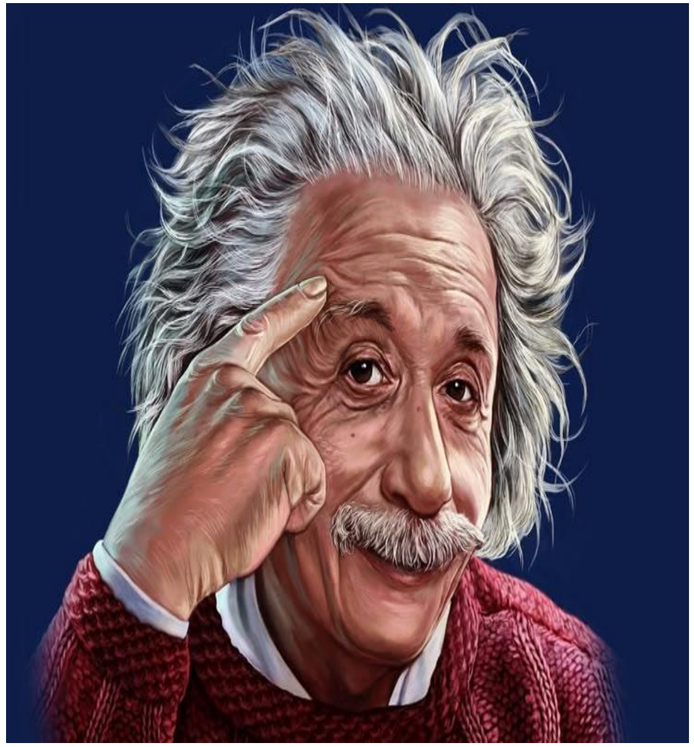
- Нефть/Газ;
- Электроэнергия;
- Транспортные сети;
- Запасы воды;
- ВПК.

ВНУТРЕННИЙ ВРАГ: БОРЬБА С ИНСАЙДЕРСКИМИ УГРОЗАМИ

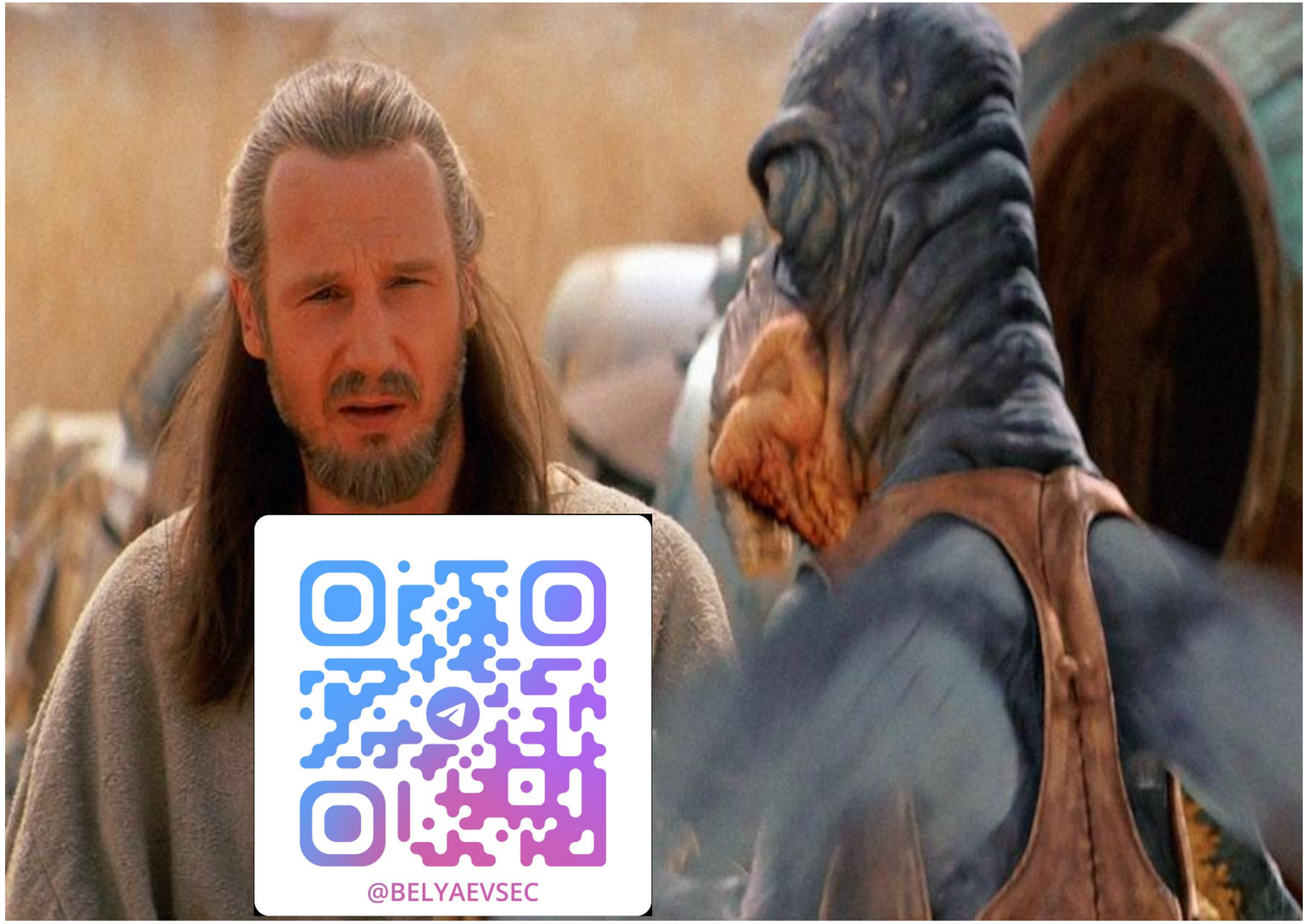
- Злоумышленники внедряют инсайдеров в качестве сотрудников или подрядчиков.
- Они компрометируют компании, участвующие в слияниях и поглощениях.
- Они используют легитимные учетные данные для нанесения ущерба.

ЧТО ДЕЛАТЬ?

- Разрабатывать решения для обеспечения безопасности на основе искусственного интеллекта;
- Обеспечить автоматизацию кибербезопасности;
- Обеспечить динамическое реагирование на инциденты;
- Строить архитектуру ИТ и КБ с нулевым доверием;
- Внедрять более сильные методы MFA;
- Проводить регулярные обновления программного обеспечения;
- Обеспечить проверку сотрудников с помощью полиграфа;
- Проводить регулярные обучения сотрудников.



Подпишитесь на канал



Спасибо за внимание!

Вопросы?