CYBERSECURITY

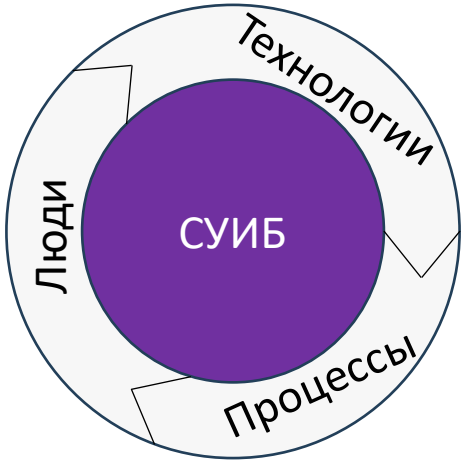
Построение СУИБ, SOC/ОЦИБ

Нехватка кадров на рынке

Поддержка ИТ и руководства

Обучение сотрудников ИБ

Инвестиции



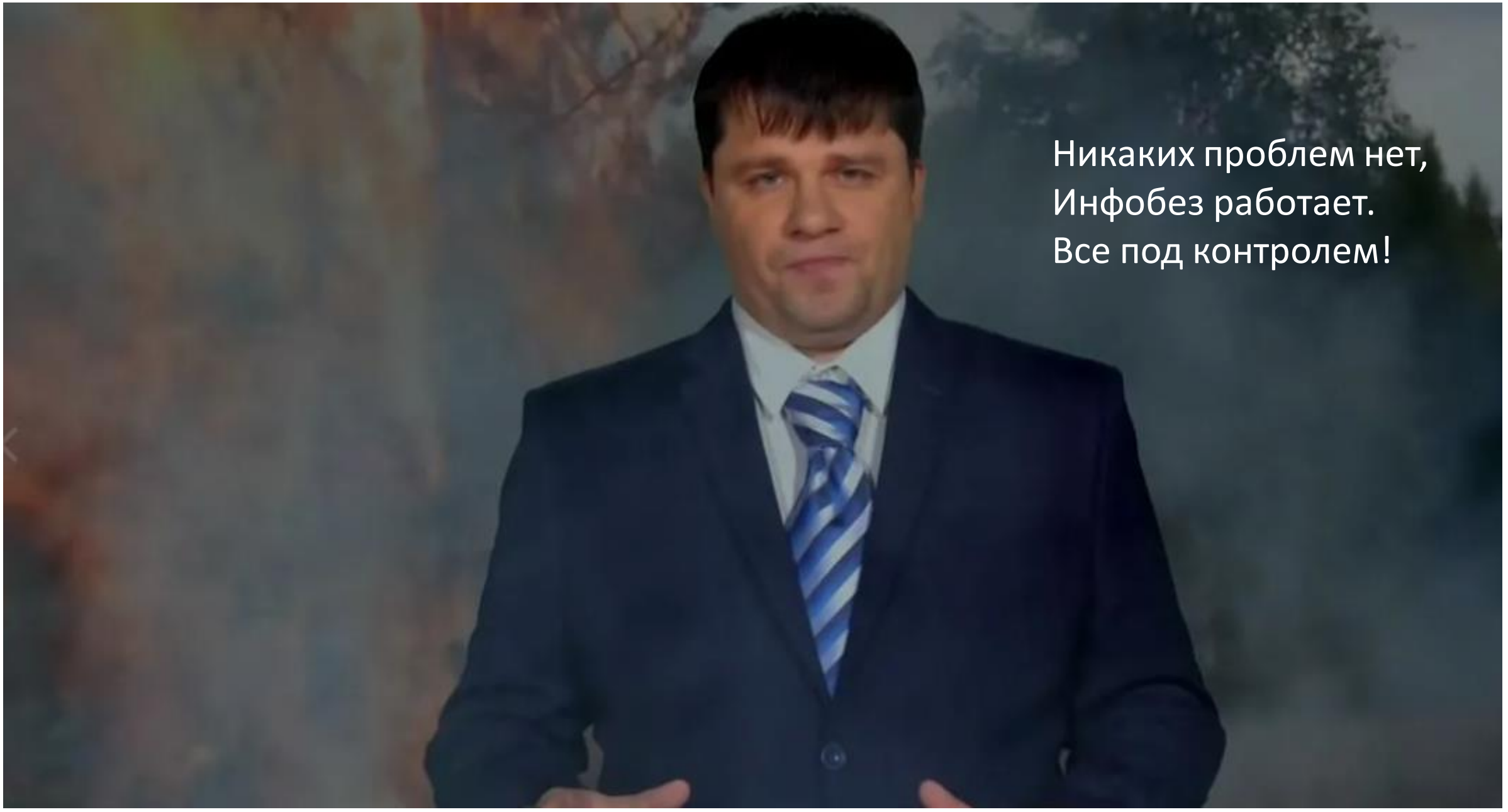
Что нужно, чтобы стать ОЦИБ?

Сертифицированные сотрудники
- Специалисты с дипломами по профилю ИБ (3 чел)
- Специалисты аудиторы по ISO 27001 (2 чел)
- Специалисты по направлению компьютерной криминалистики (1 чел)
- Специалисты по направлению Reverse Engineering (1 чел)
- Специалисты по направлению этичного хакинга (1 чел)
- Специалисты по направлению администрирования серверных ОС (2 чел)

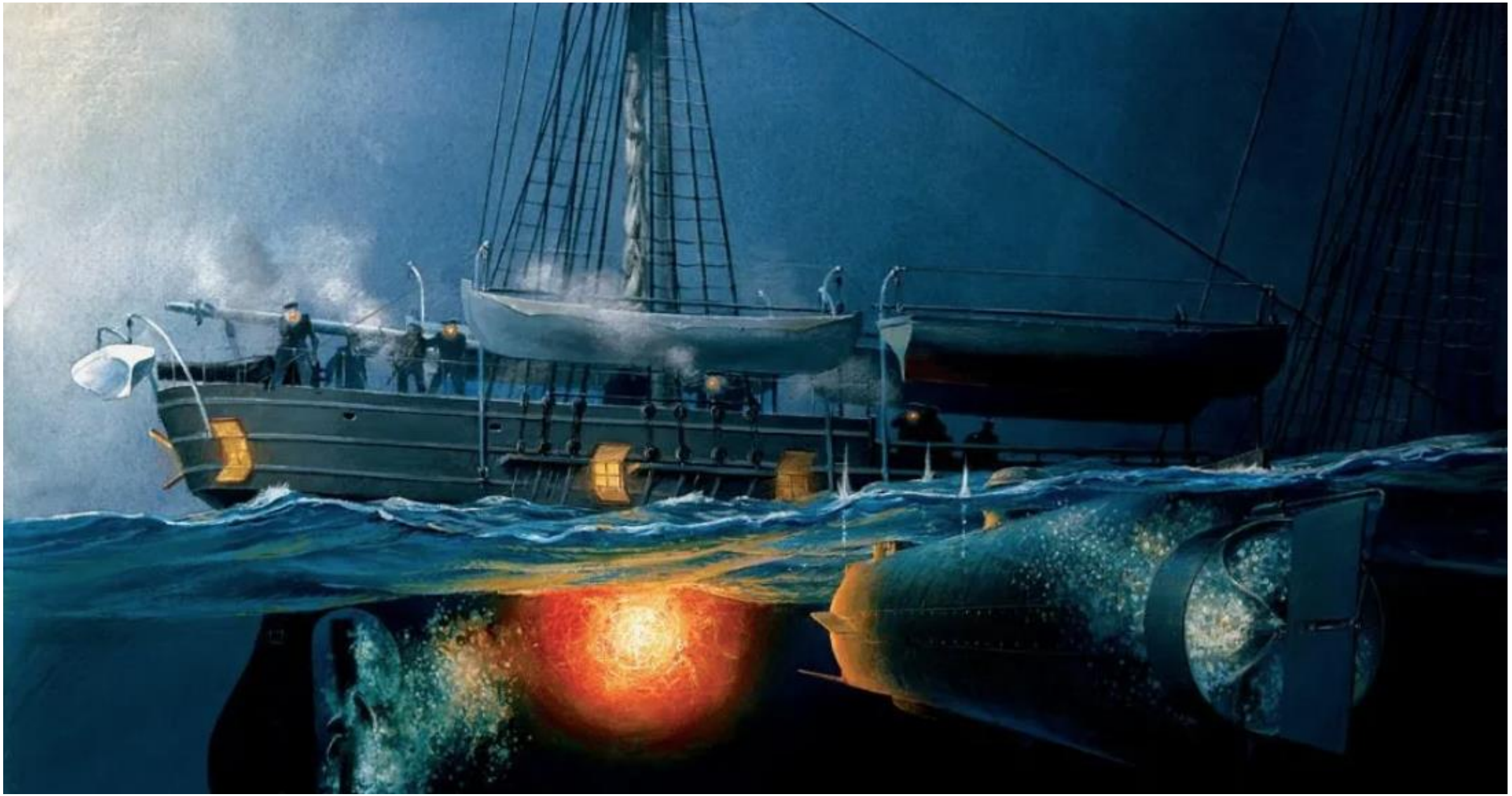
Технологии и системы
- Платформа реагирования на инциденты (IRP)
- Решения класса next-generation firewall или unified threat management
- Система защиты веб-приложений (WAF)
- Система защиты от DDoS атак
- Endpoint Threat Detection and Response
- Система управления событиями ИБ (SIEM)
- Система управления уязвимостями
- Средство динамического анализа вредоносных программ
- Средство предотвращения утечки информации (DLP)
- Средство проактивного поиска и обнаружения угроз (Threat hunting)

Документы и процедуры
- Методика оказания услуг
- Документы на офис (офис, физ охрана, пож. сиг.)
- Документы на ПО

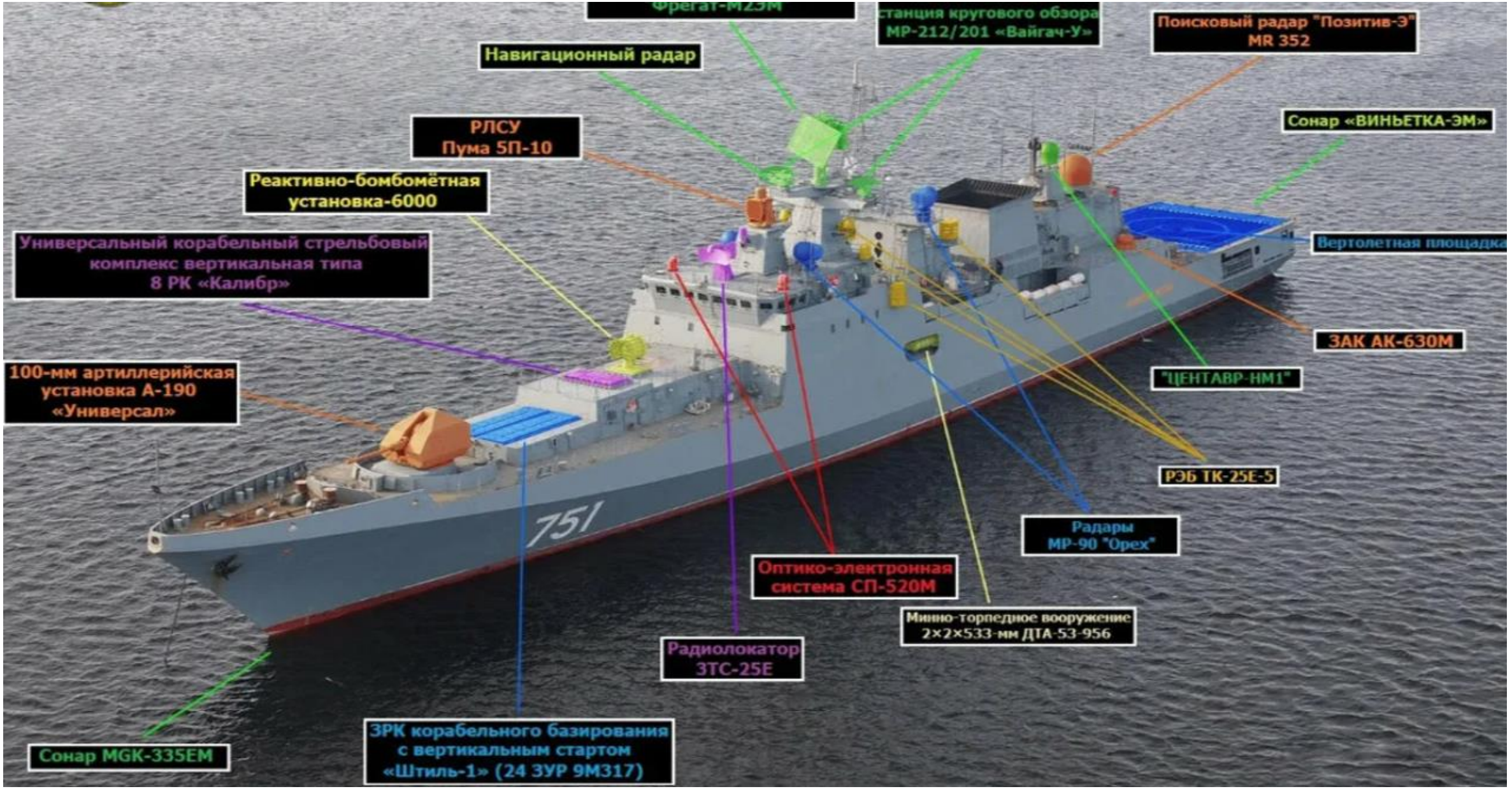
Если есть проблемы, нужно сообщить руководству



Посчитать, зафиксировать риски и предложить «таблетку»



Представить и утвердить план/стратегию



Главное не забыть о команде!

Нехватка кадров…

Blue Team

Red Team

Purple Team

CISO

Эксперты

Инженера

Студенты/практиканты

Зачем хакер или Red Team в отделе?

Команда Kcell, победители CyberKumbez KazHackStan 2023

- Развитие Application Security
- Наглядно показать, что может сделать атакующий
- Выстраивать защиту от кибератак
- Держать в тонусе команду Blue Team
- Улучшение процессов Blue Team
- Подготовка и запуск к Bug Bounty

Thank You!