rus.vessel_it_infrastructure

Alexandr Kirilov (https://github.com/alexandrkirilov)

IT инфраструктура на судне.

Для понимания принципов по которым нужно проектировать (моделировать) IT инфраструктуру судна, нужно все устройства представить как источники информации которые используются в тех или иных процессах информационного обмена на судне, которые в свою очередь обеспечивают жизнедеятельность на судне, например:

- Морской радар - источник информации о местоположении физических объектов поверхность которых способна отражать радиоволны определенной частоты, используется в процессах судовождения и навигации и оказывает на них влияние
- AIS (Automatic identification system) - источник информации о судах находящихся в радиусе действия самой системы, предоставляется другими судами, используется в процессах судовождения и навигации и оказывает на них влияние
- датчик уровня топлива - источник информации о количестве топлива в том или ином баке, используется в процессах использования и обслуживания судовых механизмов, оказывает влияние на процессы судовождения
- датчик уровня жидкости в балластном танке - источник информации о количестве воды в балластном танке, используется в процессах использования и обслуживания судовых механизмов, оказывает влияние на процессы судовождения
- датчик температуры двигателя - источник информации о …
- и т.д.

Точно так же как устройства, весь экипаж воспринимается как источник и потребитель информации и точно так же участвует в моделировании информационных процессов на основании которых строится IT инфраструктура.

В статье "Информационная безопасность на судне" описано как восприятие всего на судне как источников или потребителей информации, сильно упрощает процесс анализа возможных проблем связанных с информационной безопасностью, особенно для устройств которые используют устаревшие технологии коммуникации.

Теперь о процессах в которых используются эти источники информации. Все процессы на основании которых строиться IT инфраструктура судна может быть разделена на несколько групп:

- процессы обеспечения навигации и судовождения
- процессы связанные с грузом и обеспечением физической целостности и сохранности, в случае с пассажирами обеспечение физической безопасности их самих и личных вещей

- процессы обеспечения использования, контроля и поддержания технического состояния судна
- процессы мониторинга физической безопасности судна
- процессы связанные с коммуникацией и документооборотом между судном и береговыми службами
- процессы связанные с коммуникацией и документооборотом между судном и судовладельцем и (или) грузоотправителем
- процессы связанные с коммуникацией членов экипажа между собой и родственниками на берегу (крайне важный пункт при проектировании информационной безопасности на судне, по причине ОЧЕНЬ БОЛЬШИХ СЛОЖНОСТЕЙ И РИСКОВ связанных с контролем происходящего внутри этих процессов)

При большом объеме информации в каком-то из этих процессов может понадобиться дробление на подпроцессы. В пределах каждого судна или компании судовладельца, эти группы могут быть организованны с отличиями от представленных в этой статье.

Проектирование IT инфраструктуры происходит на основе построения информационной модели судна путем анализа всех данных поступающих из всех источников для всех потребителей информации в пределах всех процессов на судне. Собираться и анализируется то какие форматы данных используются, то какой объем информации используется при передачи, то на сколько доверительные источники информации и может ли эта информация быть фальсифицирована и т.д. - и на основании этой модели происходит подбор технических средств для компании в целом и для судна в частности.

По отдельности, каждая из этих групп процессов с точки зрения IT инфраструктуры проработана и оснащена очень хорошо, особенно всего, что касается электронной картографии и на современных судах мониторинг механизмов и устройств. Существуют системы для постоянного Internet соединения. Существуют системы расчета остойчивости судна. Очень много различных других систем по отдельности. Но существует 2 ОГРОМНЫХ ПРОБЛЕМЫ на данный момент:

- во время постановки задач для разработки существующих систем судно воспринималось как судно в море, и никто не думал о том что компьютер или какое-то устройство на судне могут быть взломаны (как его взломать? - судно же в море, а технологии ушли вперед).
- во время проектирования судовых коммуникаций никто не думал про судно как источник информации в целом, все системы проектировались разрозненно с огромным количеством стандартов, форматов и протоколов (пожарная сигнализация одно, радары - второе, датчики на дверях - третье и т.д., что так-же

вызывает огромные проблемы в обслуживании).

Самое интересное, что в данной ситуации на берегу существуют все решения для этих проблем, и причем не такие дорогие в разработке как может показаться с начала. По факту очень много наработок в той или иной сфере, их нужно просто адаптировать к использованию на судах в море.

Существует огромное количество средств организации и защиты локальных сетей в офисах: VPN, Firewall, WAN/NAT, IPsec и т.д. Но никто почему-то это не использует эти решения на судах (за некоторым исключением для пассажирских судов). Кто мешает представить, что судно - это удаленный офис или склад и организовать судовую сеть по тем же принципам используя тоже ПО что и в офисе??? - Никто, но почему-то это не делается.

Существует понятие IoT (Интернет Вещей) - по сути все судно это один небольшой LNoT (Local Network of Things), своего рода локальная сеть вещей, где вместо чайников и пылесосов - датчики и средства навигации. Никто не мешает начать воспринимать судно с точки зрения информации как LNoT и начать использовать стандарты и архитектурные решения из IoT. Нужно создать некий стандарт протокола информационного обмена для судов.

Никто не говорит о том чтобы слепо копировать, все должно быть протестировано неоднократно и в различных условиях. Из опыта работы большинство проблем будет связано не с ПО, а с физическими свойствами материалов из которых устройства на которых это ПО установлено созданы: качество проводов, качество металла на креплениях, вибростойкость пластика и т.д.

Для решения описанных проблем нужно:

- начинать как минимум экспериментировать с построением защищенных судовых сетей которые будут учитывать использование оборудования потенциально небезопасного или технологически устаревшего но обязательного к использованию по требованиям морского законодательства
- начинать разрабатывать некое подобие стандарта информационного внутрисудового и судно-берег информационного обмена (с введением беспилотного судовождение будет огромное количество проблем связанных с мониторингом и обслуживанием судна "на ходу", для примера простая замена воды в балластных танках по экологическим требованиям, как вы собираетесь сделать это не имя возможности удаленно оперировать устройствами судна)
- начинать разрабатывать программную платформу которая будет включать в себя стандарты и протоколы обмена и воспринимать судно как источник информации

предоставляя производителям судового оборудования единый интерфейс обмена данными (своего рода FreeBSD for Mariners или MarinerBSD, причины по которым за основу взята FreeBSD описаны в статьях "Почему FreeBSD?" и в статье "Информационная безопасность на судне")

- на основе платформы и протоколов создать технический регламент для устройств используемых на судах для того чтобы добиться уровня Plug&Play (как на компьютерах) для судовых устройств участвующих в информационных процессах с нужным уровнем безопасности (это позволит сильно сократить стоимость обслуживания и обеспечит нужный уровень безопасности)