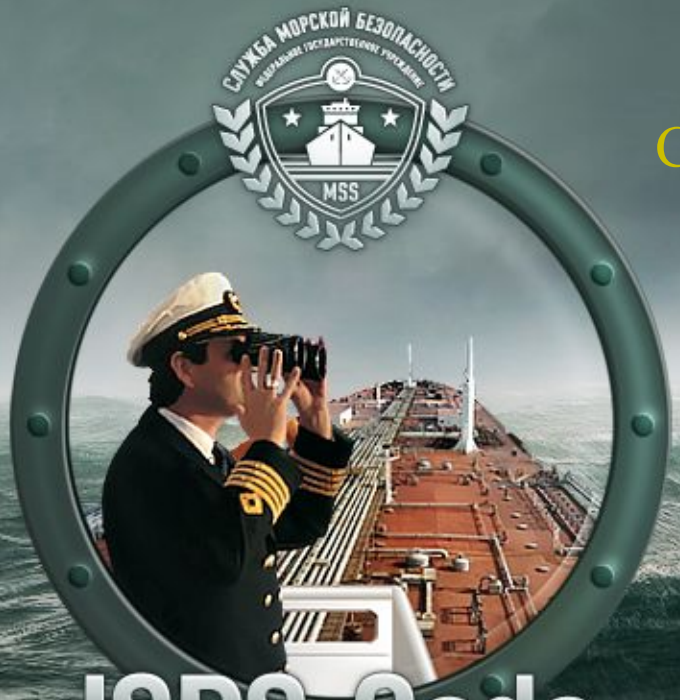


СЕМЕНОВ
Сергей Александрович

ФЕДЕРАЛЬНОЕ АГЕНТСТВО МОРСКОГО И РЕЧНОГО ТРАНСПОРТА

СЛУЖБА МОРСКОЙ БЕЗОПАСНОСТИ

Морская кибербезопасность в Российской Федерации: оценка состояния и возможные перспективы развития

Возможные сценарии кибератак на судовые системы:

- изменение данных о судне, включая его местоположение, курс, информацию о грузе, скорость и имя;
- создание «кораблей-призраков», опознаваемых другими судами как настоящее судно в любой локации мира;
- отправка ложной погодной информации конкретным судам, чтобы заставить их изменить курс для обхода несуществующего шторма;
- активация ложных предупреждений о столкновении, что также может стать причиной автоматической корректировки курса судна;
- возможность сделать существующее судно «невидимым»;
- создание несуществующих поисково-спасательных вертолетов;
- фальсификация сигналов аварийного радиобуя, активирующих тревогу на находящихся поблизости судах;
- возможность проведения DoS-атаки на всю систему путем инициирования увеличения частоты передачи сообщений автоматической идентификационной системы.

Международная морская организация (IMO)
к уязвимым судовым системам относит:

1. Системы ходового мостика;

2. Системы обработки и управления грузом;

3. Системы управления двигателями, машинами и энергопитанием;

4. Системы контроля доступа;

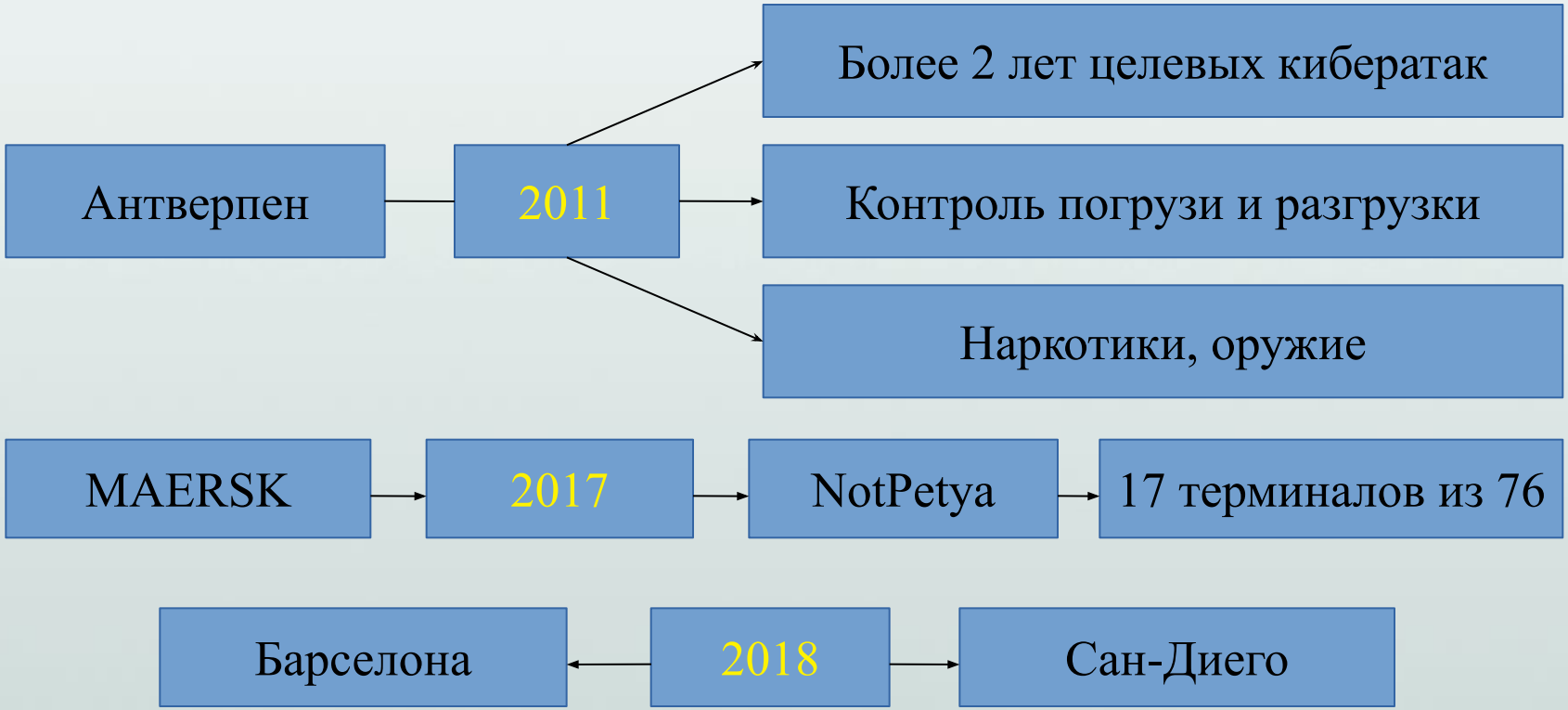
6. Системы обслуживания и управления пассажирами;

7. Публичные Интернет-сети судна, предназначенные для использования пассажирами;

8. Административные системы и сети;

9. Системы связи.

ПОРТОВАЯ КИБЕРБЕЗОПАСНОСТЬ



Международная морская организация (IMO):

Руководство по управлению морскими киберрисками (*Guidelines on maritime cyber risk management*)

IMO рекомендует:

- **Руководство по кибербезопасности на судах (*Guidelines on Cyber Security on board)* BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, OCIMF, IUMI и Всемирного совета судоходства**
- **Рамочная программа Национального института стандартов и технологий Соединенных Штатов Америки по совершенствованию критической инфраструктуры кибербезопасности (*the NIST Framework*).**
- **Стандарт ISO / IEC 27001**

Классификационные общества:

DNV GL**: Управление устойчивостью к кибербезопасности для судов и мобильных морских установок в эксплуатации *(Cyber security resilience management for ships and mobile offshore units in operation)***

ClassNK**: базовый подход к обеспечению бортовой кибербезопасности для судов.**

Федеральный закон от 26.07.2017 № 187-ФЗ
«О безопасности критической информационной инфраструктуры Российской Федерации»

Объекты критической информационной инфраструктуры:

- **информационные системы,**
- **информационно-телекоммуникационные сети,**
- **автоматизированные системы управления субъектов**

Проект резолюции XVIII Международной конференции «Терроризм и безопасность на транспорте» (пункт 16)

«федеральные органы исполнительной власти при рассмотрении угроз совершения актов незаконного вмешательства в деятельность объектов транспортной инфраструктуры при проведении оценки уязвимости и разработке планов обеспечения транспортной безопасности учитывать способы совершения актов незаконного вмешательства с использованием кибератак…, внести соответствующие изменения в описание угроз».

ПРОБЛЕМЫ:

- **в Российской Федерации отсутствует транспортный отраслевой центр компетенции по информационной безопасности.**
- **ФСТЭК не учитывает отраслевые особенности.**
- **разница между международным и российским подходами к кибербезопасности**
- **разница в понятийном аппарате**
- **российское законодательство различные аспекты безопасности регулирует разными, не взаимоувязанными нормативными правовыми актами**

СЛЕДСТВИЯ:

- **реализация единого и комплексного подхода к обеспечению безопасности судна практически невозможна.**
- **одновременное и параллельное исполнение международных норм и ФЗ-187**
- **информационная безопасность отдельно, а транспортная - отдельно**

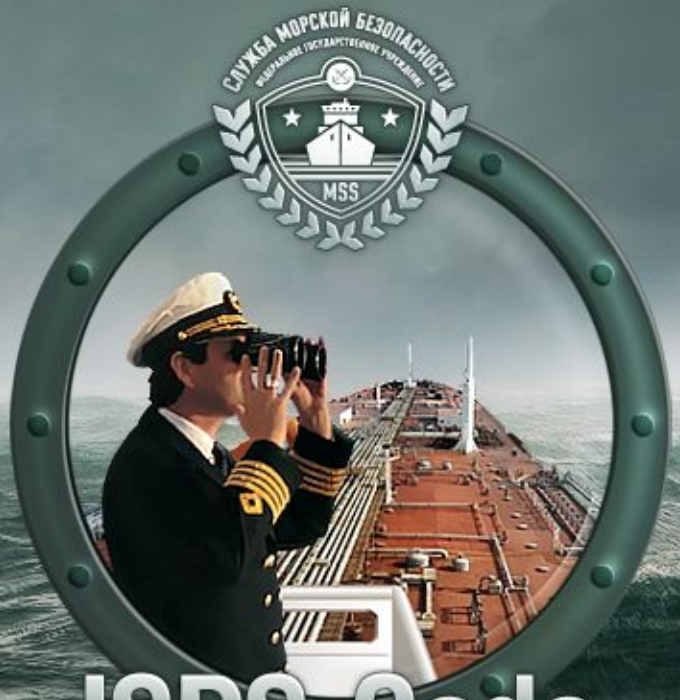
ТС ОТБ, как объект правового регулирования

- **подлежат обязательной сертификации (п. 8 ст.12.2 ФЗ-16)**
- **поднадзорны РМРС**
- **объект технического наблюдения РМРС**
- **должны иметь сертификат типового одобрения (СТО)**
- **установка в соответствии с согласованной в РМРС проектной документацией**
- **объект правового регулирования ФЗ-187**
- **объект правового регулирования «Руководства по управлению морскими киберрисками» ИМО**

ПРЕДЛОЖЕНИЯ:

- **гармонизации существующих правовых норм по морской кибербезопасности и упрощение формальностей**
- **организаторы - отраслевые профессиональные объединения**
- **привлечение Российского Морского Регистра Судоходства**
- **взаимодействие с ФСТЭК**

«Служба морской безопасности»
готова принять участие в работе



ФЕДЕРАЛЬНОЕ АГЕНТСТВО МОРСКОГО И РЕЧНОГО ТРАНСПОРТА

СЛУЖБА МОРСКОЙ БЕЗОПАСНОСТИ

Спасибо за внимание!

Доклады и презентации будут размещены на сайте http://www.msecurity.ru
в группах в Телеграмм https://t.me/transsecurity и в Вконтакте

trans.security