Аналитика кибератак на военные корабли

Случаи необъяснимых инцидентов с судами ВМС в спорных водах

21.08.2017	• Столкновение американского ракетного эсминца USS John S. McCain с танкером Alnic MC в восточном Малаккском проливе
17.06.2017	• Столкновение американского ракетного эсминца USS Fitzgerald недалеко от побережья Японии с контейнерным судном ACX Crystal, следующим под флагом Филиппин
9.05.2017	• Ракетный крейсер ВМС США «Лэйк Чемплейн» столкнулся с небольшим рыболовецким судном рядом с Корейским полуостровом

Важные факты об инцидентах

- Все три судна принадлежат исключительно 7-му флоту США, который отвечает за работу в районе спорных островов в Желтом море – территории, на которую активно и агрессивно претендует Китай
- В отставку отправлен командующий 7 флотом ВМС США адмирал Джозеф Окойн и командующий Тихоокеанским флотом США адмирал Скотт Свифт
- Официальные отчеты о столкновениях явно неполные, согласно экспертом в морской навигации. Пояснения ВМС США давать отказывается
- Молчаливая реакция Китайских властей при явной поддержке инцидентов в национальной прессе и социальных сетях

Важные факты об инцидентах

Адмирал William Moran
Vice Chief of Naval Operations

Адмирал William Moran (Vice Chief of Naval Operations) в официальном интервью признал, что к расследованию причин столкновения были привлечены специалисты Киберкомандования на море, а также специалисты по активным воздействиям на информационные системы.

Отчеты специалистов в заключительном отчете о расследовании не представлены.

Столкновение американского ракетного эсминца USS Fitzgerald

Эсминец США "USS Fitzgerald" столкнулся с контейнеровозом "ACX Crystal» у берегов Японии, в 01:30 ночи

Столкновение пробило корпус эсминца ниже ватерлинии и затопило жилые помещения, где находилось 35 человек.

Семерым членам экипажа "USS Fitzgerald" не удалось спастись.

USS Fitzgerald

USS Fitzgerald

Водоизмещение: 8775 тонн
Длина: 153,92 м.
Ширина: 20, 1 м.
Осадка: 9,3 м
Двигатели: 4 газотурбинные установки
Мощность: 108000 л. с.
Скорость хода: 32 узла (максимальная)
Экипаж: 337 человек

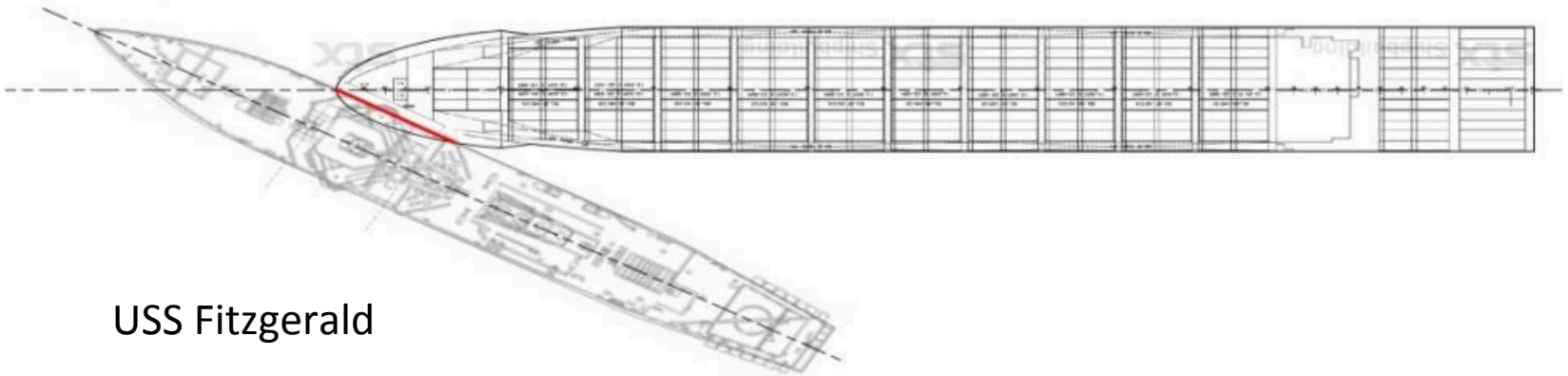
Контейнеровоз ACX Crystal

Контейнеровоз ACX Crystal

Водоизмещение: 39,565 тонн
Длина: 222.6 м.
Ширина: 30.1 м.
Осадка: 12 м
Двигатели: MAN-B&W
Мощность: 38,730 л. с.
Скорость хода: 25 узла (максимальная)
Экипаж: 20 человек

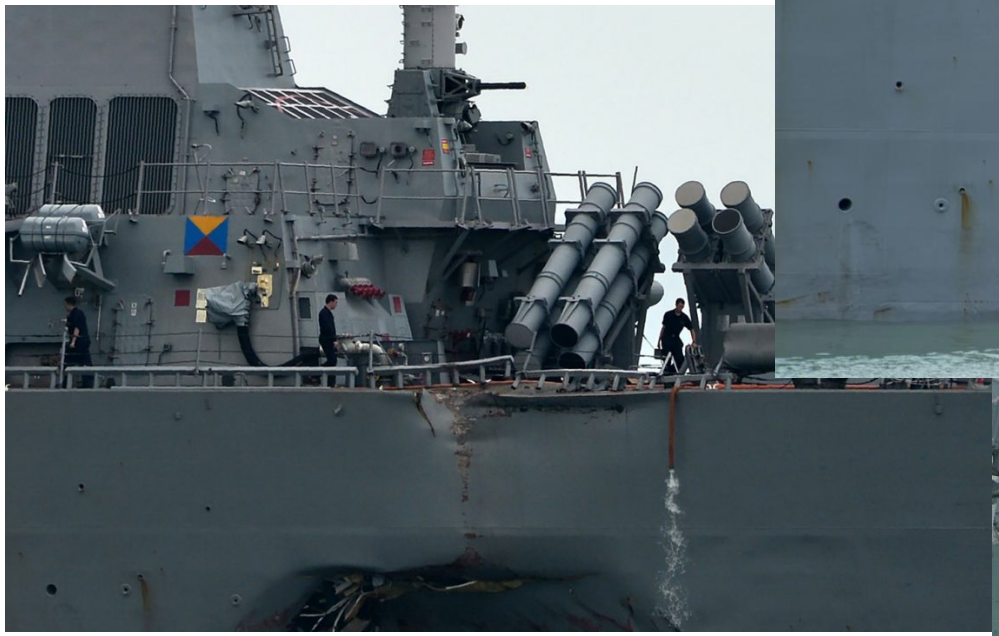
Схема столкновения

Контейнеровоз ACX Crystal



USS Fitzgerald

ПОСЛЕДСТВИЯ СТОЛКНОВЕНИЯ



КЛЮЧЕВЫЕ ФАКТЫ НАВИГАЦИИ

Международные правила предупреждения столкновений судов (COLREGS-72)

Когда два судна с механическими двигателями идут пересекающимися курсами так, что возникает опасность столкновения, то судно, которое имеет другое на своей правой стороне, должно уступить дорогу другому судну и при этом оно должно, если позволяют обстоятельства, избегать пересечения курса другого судна у него по носу.

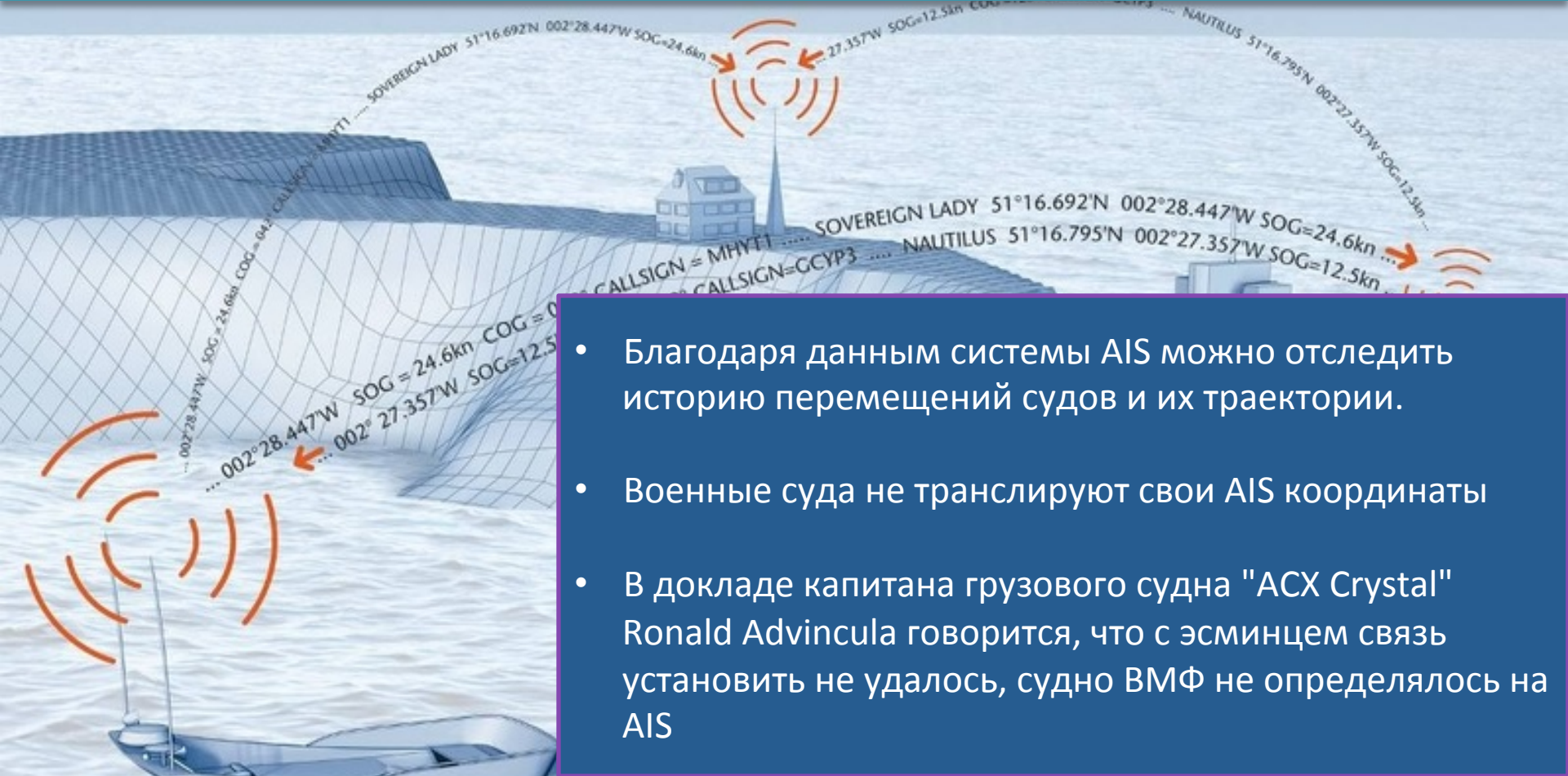
КЛЮЧЕВЫЕ ФАКТЫ НАВИГАЦИИ

AIS (Automatic Identification System) — автоматическая идентификационная система. Служит для передачи идентификационных данных судна (в том числе о его грузе), информации о его состоянии, текущем местоположении и курсе. Также используется для предупреждения столкновений судов, мониторинга их состояния.

AIS работает посредством передачи сигналов в УКВ-диапазоне между судами, плавающими ретрансляторами и береговыми AIS-шлюзами, которые подключены к интернету.

Все суда, совершающие международные рейсы, суда вместимостью более 500 регистровых тонн, а также все пассажирские суда должны быть оснащены AIS.

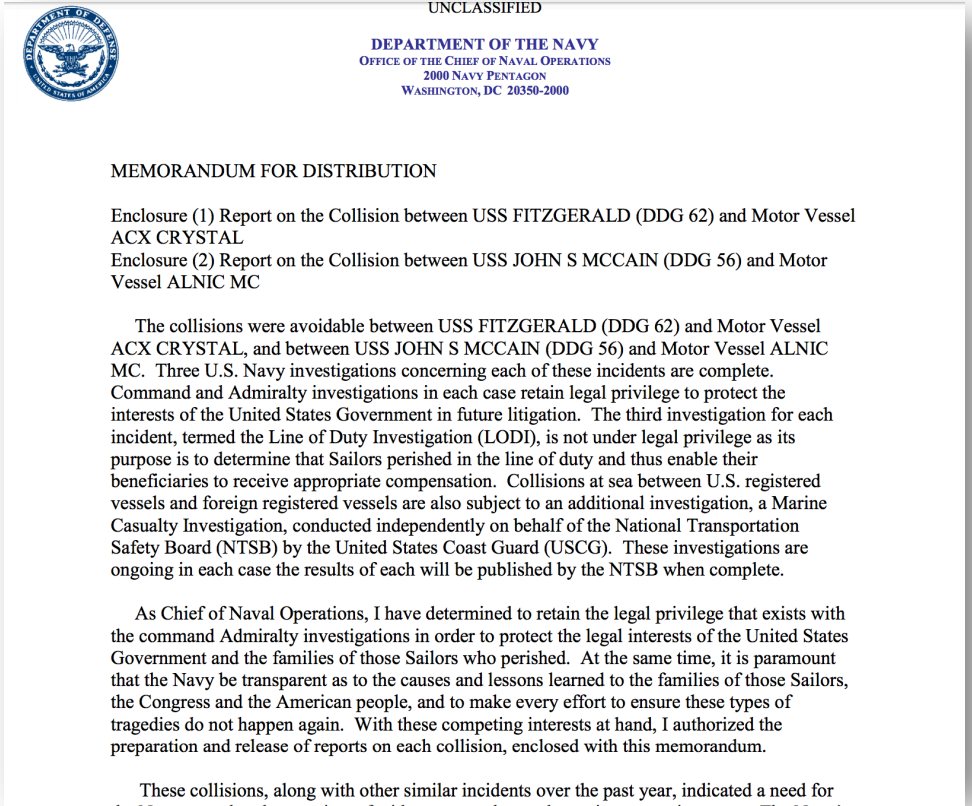
КЛЮЧЕВЫЕ ФАКТЫ НАВИГАЦИИ



- Благодаря данным системы AIS можно отследить историю перемещений судов и их траектории.
- Военные суда не транслируют свои AIS координаты
- В докладе капитана грузового судна "ACX Crystal" Ronald Advincula говорится, что с эсминцем связь установить не удалось, судно ВМФ не определялось на AIS

ПУБЛИЧНАЯ ЧАТСЬ ОТЧЕТА ВМС США

Согласно результатам расследования виновными в происшествии были признаны находившиеся на вахте моряки эсминца, которые в нарушение Международных правил предупреждения столкновений судов (COLREGS-72) не предоставили преимущества двигавшемуся справа торговому судну.



UNCLASSIFIED

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, DC 20350-2000

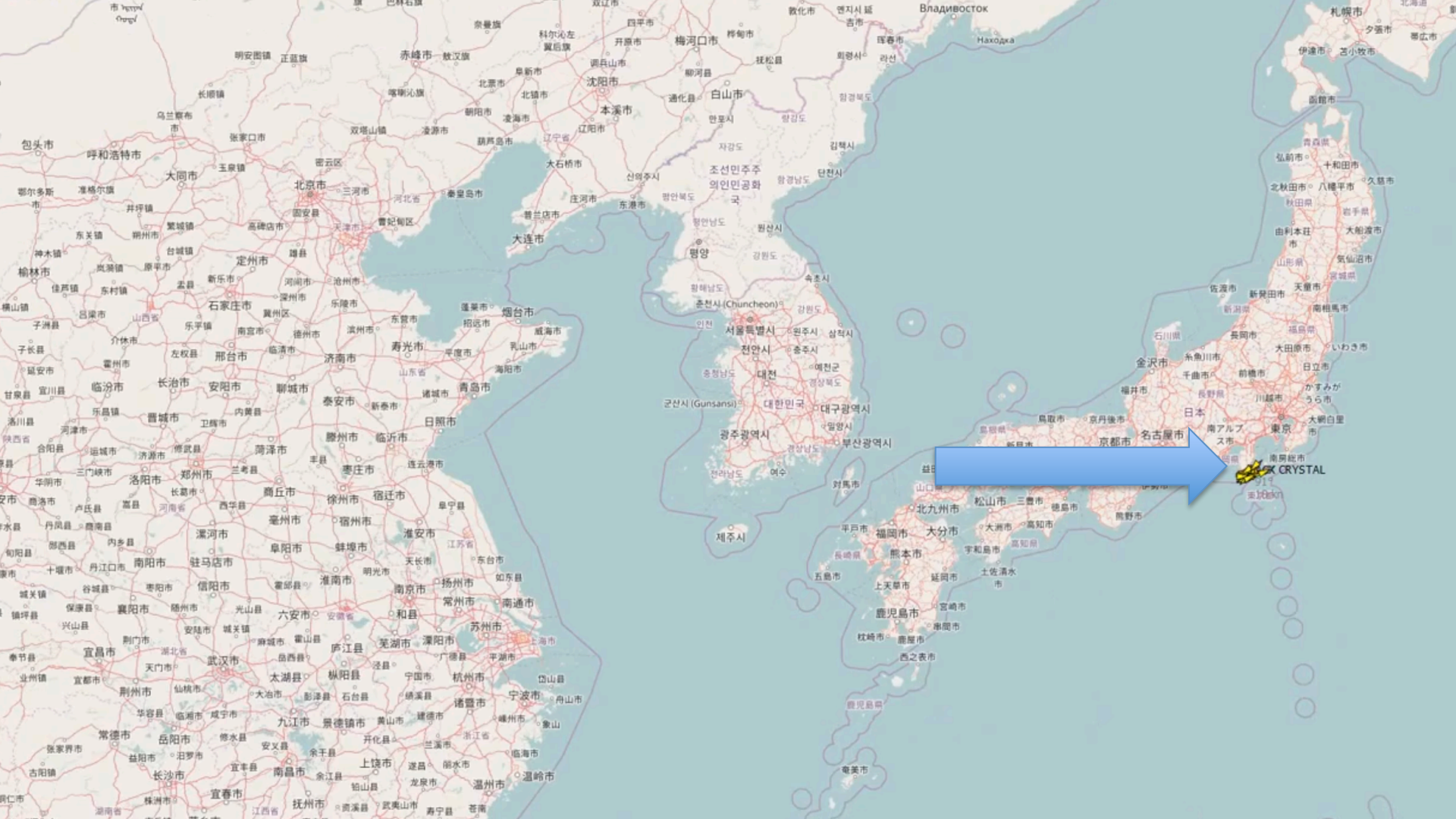
MEMORANDUM FOR DISTRIBUTION

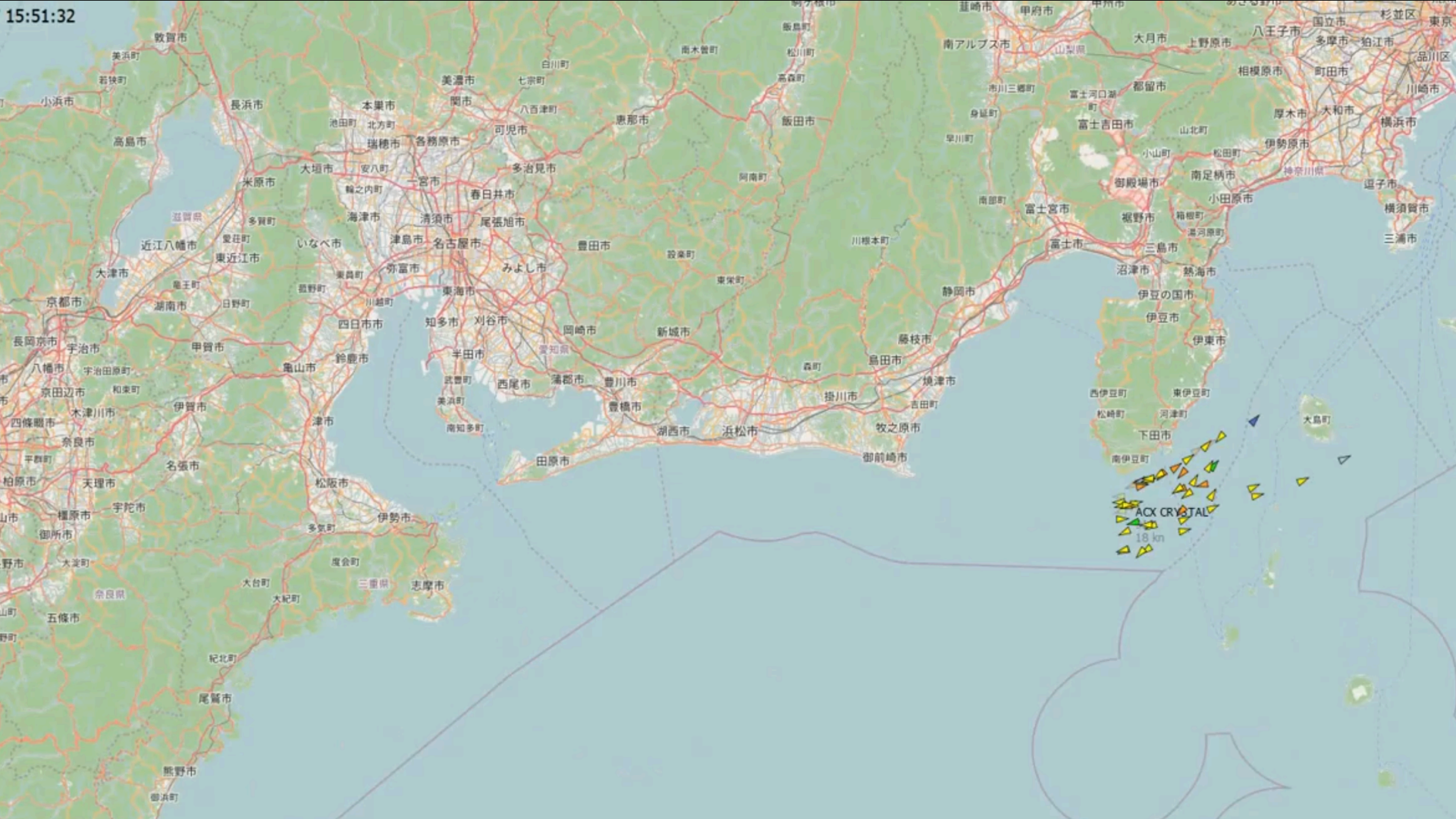
Enclosure (1) Report on the Collision between USS FITZGERALD (DDG 62) and Motor Vessel ACX CRYSTAL
Enclosure (2) Report on the Collision between USS JOHN S MCCAIN (DDG 56) and Motor Vessel ALNIC MC

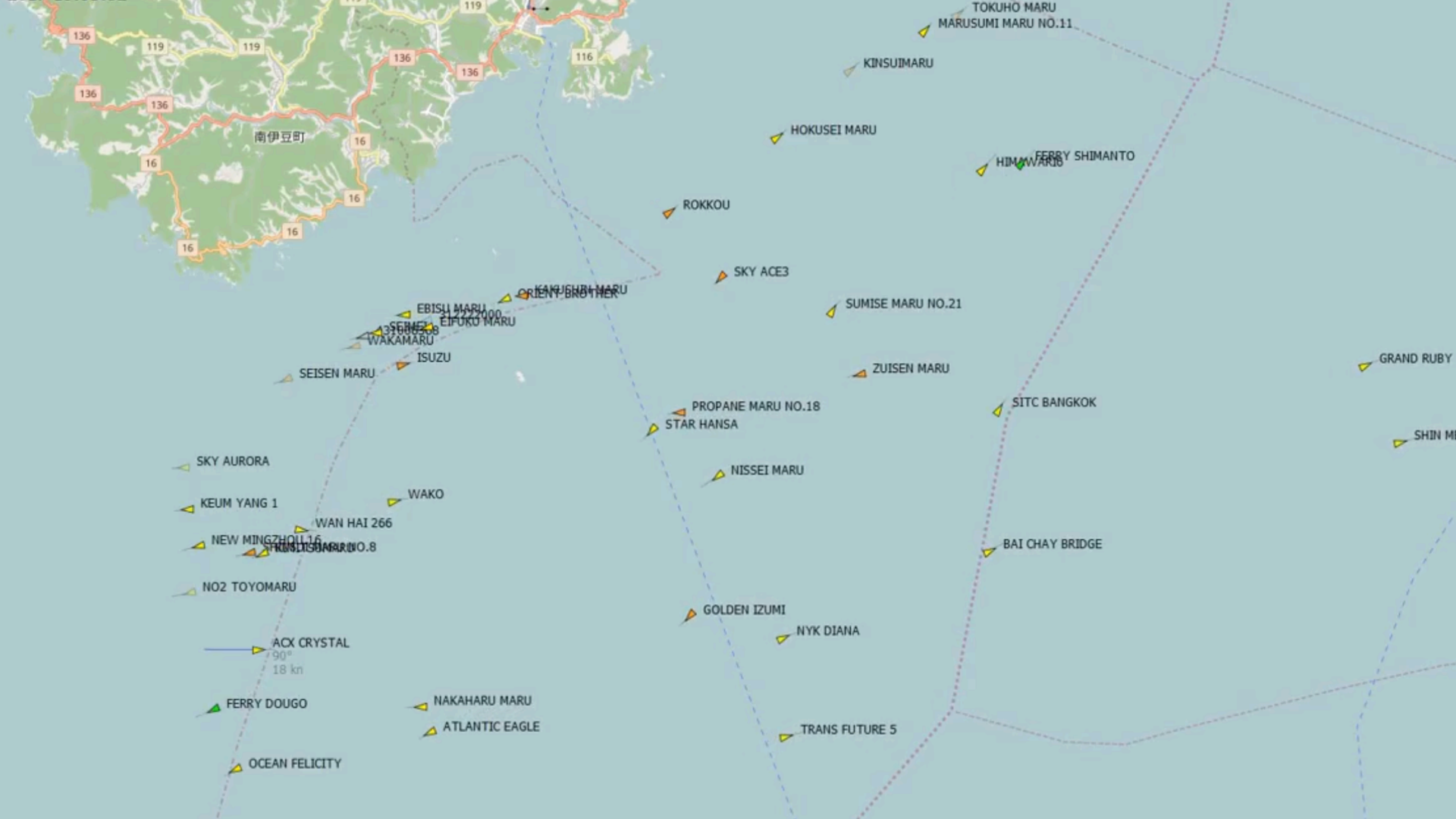
The collisions were avoidable between USS FITZGERALD (DDG 62) and Motor Vessel ACX CRYSTAL, and between USS JOHN S MCCAIN (DDG 56) and Motor Vessel ALNIC MC. Three U.S. Navy investigations concerning each of these incidents are complete. Command and Admiralty investigations in each case retain legal privilege to protect the interests of the United States Government in future litigation. The third investigation for each incident, termed the Line of Duty Investigation (LODI), is not under legal privilege as its purpose is to determine that Sailors perished in the line of duty and thus enable their beneficiaries to receive appropriate compensation. Collisions at sea between U.S. registered vessels and foreign registered vessels are also subject to an additional investigation, a Marine Casualty Investigation, conducted independently on behalf of the National Transportation Safety Board (NTSB) by the United States Coast Guard (USCG). These investigations are ongoing in each case the results of each will be published by the NTSB when complete.

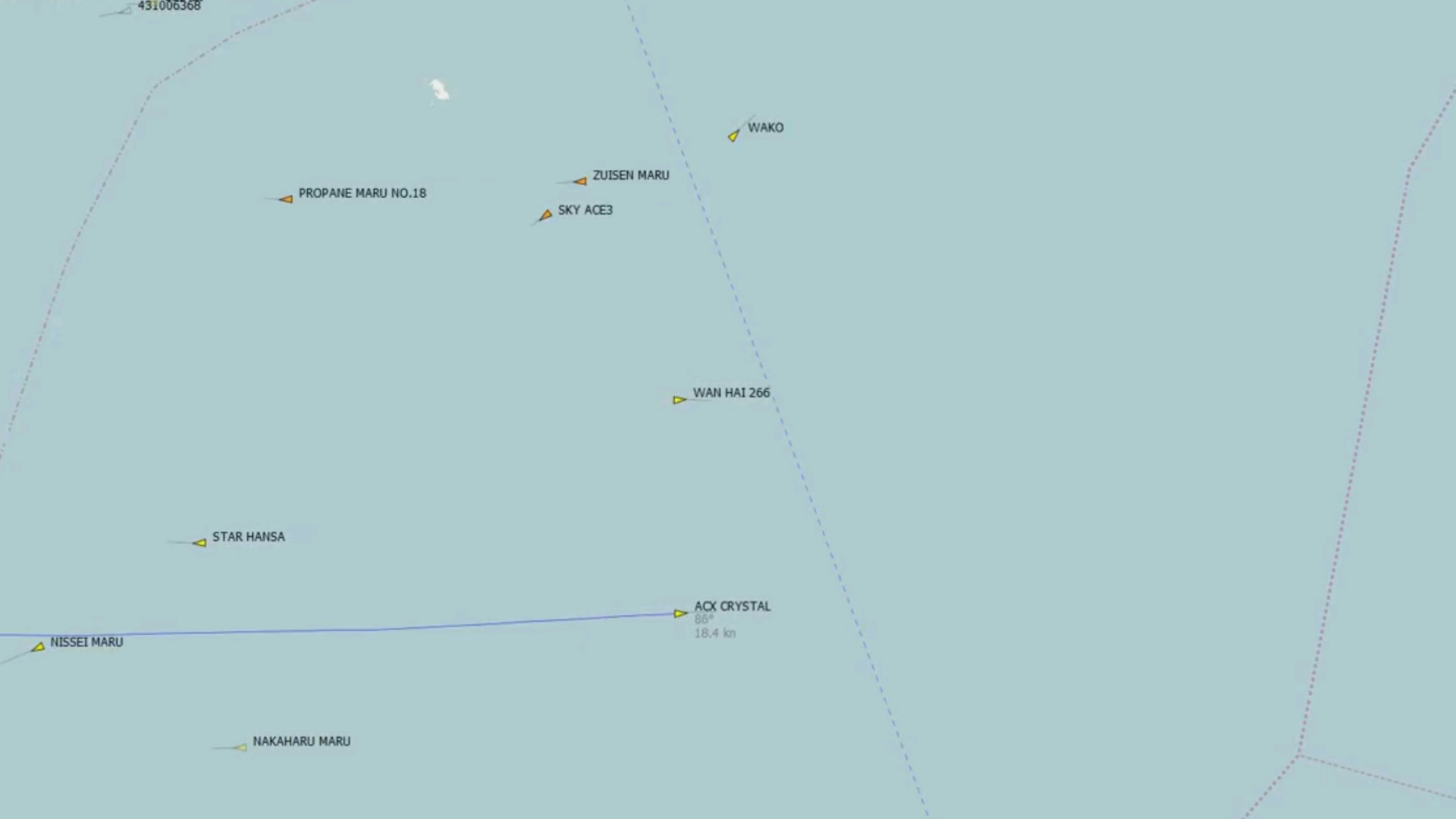
As Chief of Naval Operations, I have determined to retain the legal privilege that exists with the command Admiralty investigations in order to protect the legal interests of the United States Government and the families of those Sailors who perished. At the same time, it is paramount that the Navy be transparent as to the causes and lessons learned to the families of those Sailors, the Congress and the American people, and to make every effort to ensure these types of tragedies do not happen again. With these competing interests at hand, I authorized the preparation and release of reports on each collision, enclosed with this memorandum.

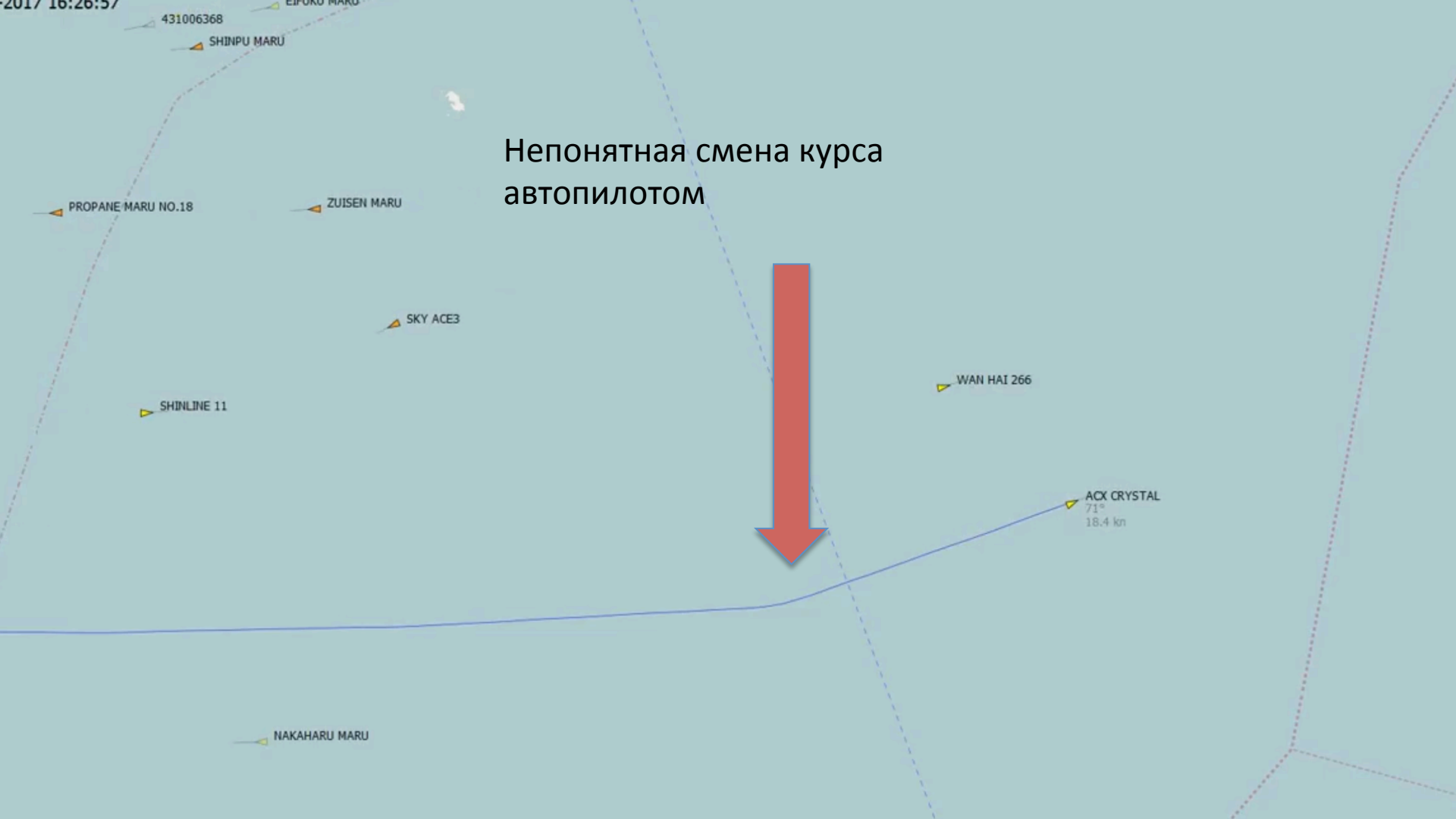
These collisions, along with other similar incidents over the past year, indicated a need for


CRYSTAL


15:51:32
ACX CRYSTAL
18 kn


TOKUHO MARU
MARUSUMI MARU NO.11
KINSUIMARU
HOKUSEI MARU
FERRY SHIMANTO
ROKKOU
SKY ACE3
SUMISE MARU NO.21
ZUISEN MARU
GRAND RUBY
PROPANE MARU NO.18
STAR HANSA
SITC BANGKOK
NISSEI MARU
BAI CHAY BRIDGE
GOLDEN IZUMI
NYK DIANA
TRANS FUTURE 5
EBISU MARU
EIFUKU MARU
WAKAMARU
ISUZU
SEISEN MARU
SKY AURORA
KEUM YANG 1
WAKO
WAN HAI 266
NEW MINGZHOU 16
NO2 TOYOMARU
ACX CRYSTAL
90°
18 kn
FERRY DOUGO
NAKAHARU MARU
ATLANTIC EAGLE
OCEAN FELICITY
南伊豆町

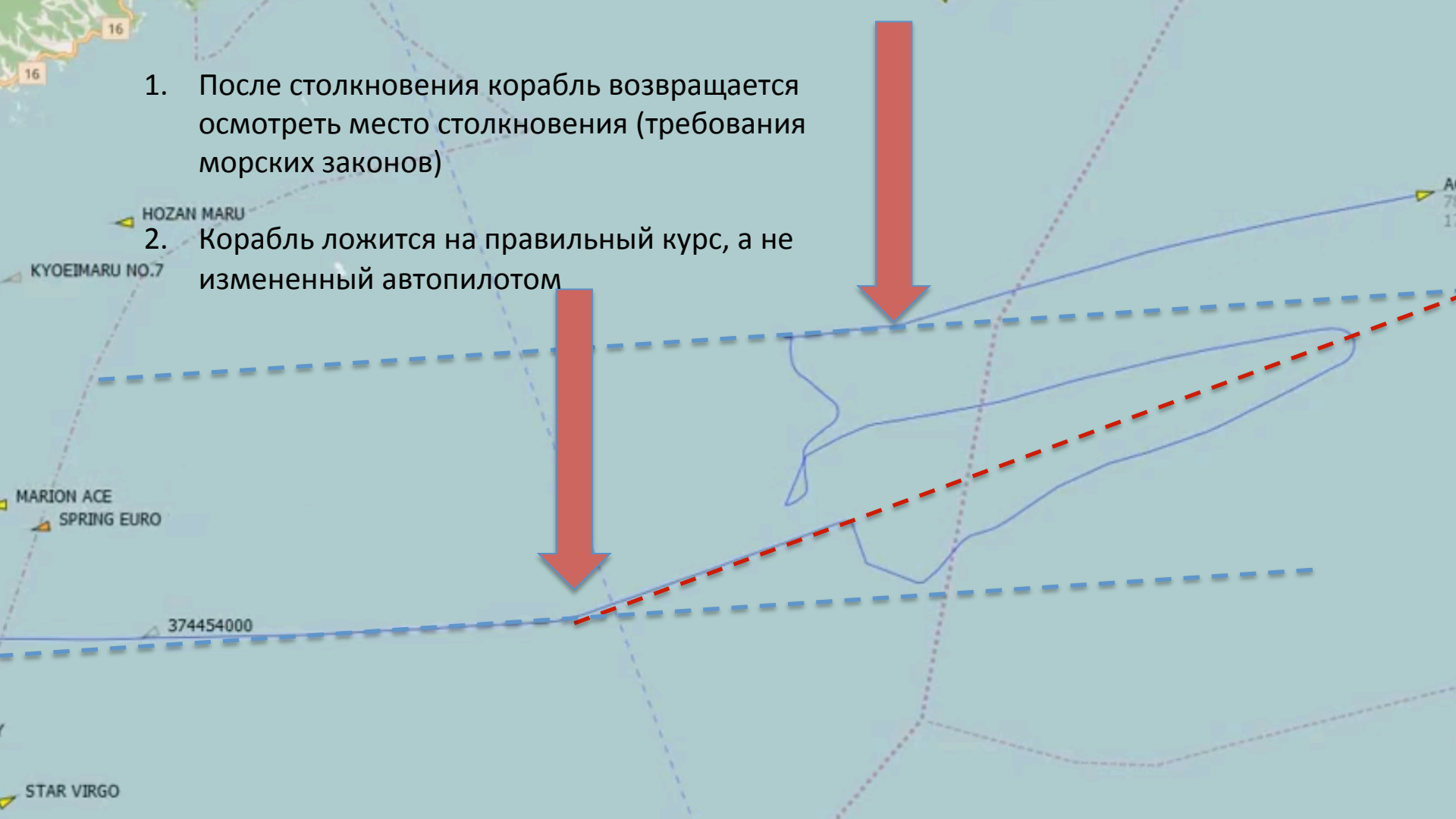

431006368
WAKO
ZUISEN MARU
PROPANE MARU NO.18
SKY ACE3
WAN HAI 266
STAR HANSA
ACX CRYSTAL
86°
18.4 kn
NISSEI MARU
NAKAHARU MARU


-2017 16:26:57
431006368
SHINPU MARU
Непонятная смена курса автопилотом
PROPANE MARU NO.18
ZUISEN MARU
SKY ACE3
WAN HAI 266
SHINLINE 11
ACX CRYSTAL
71°
18.4 kn
NAKAHARU MARU

Столкновение через 10 минут после необоснованной смены курса


Возращение на курс
автопилотом
BAI CHAY BRIDGE
ACX CRYSTAL
70°
12.9 kn
MAERSK EVORA

В течение 20 минут капитан не мог дойти до управления кораблем, курс выправлял автопилот


1. После столкновения корабль возвращается осмотреть место столкновения (требования морских законов)
2. Корабль ложится на правильный курс, а не измененный автопилотом
HOZAN MARU
KYOEIMARU NO.7
MARION ACE
SPRING EURO
374454000
STAR VIRGO

СИСТЕМА УПРАВЛЕНИЯ ACX Crystal

IBS (Integrated Bridge System) - Интегрированная Мостиковая Система - это сопряженные в единый комплекс системы судовождения и управления судном с целью повышения эффективности обработки информации и управления судном, обеспечивающий повышение навигационной безопасности плавания.

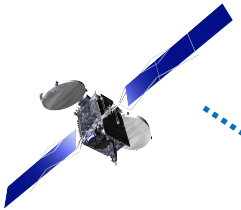
IBS система на судне является главным объектов атаки

СИСТЕМА УПРАВЛЕНИЯ ACX Crystal

AIS (Automatic Identification System) — система для передачи идентификационных данных судна

Vsat — Спутниковый канал

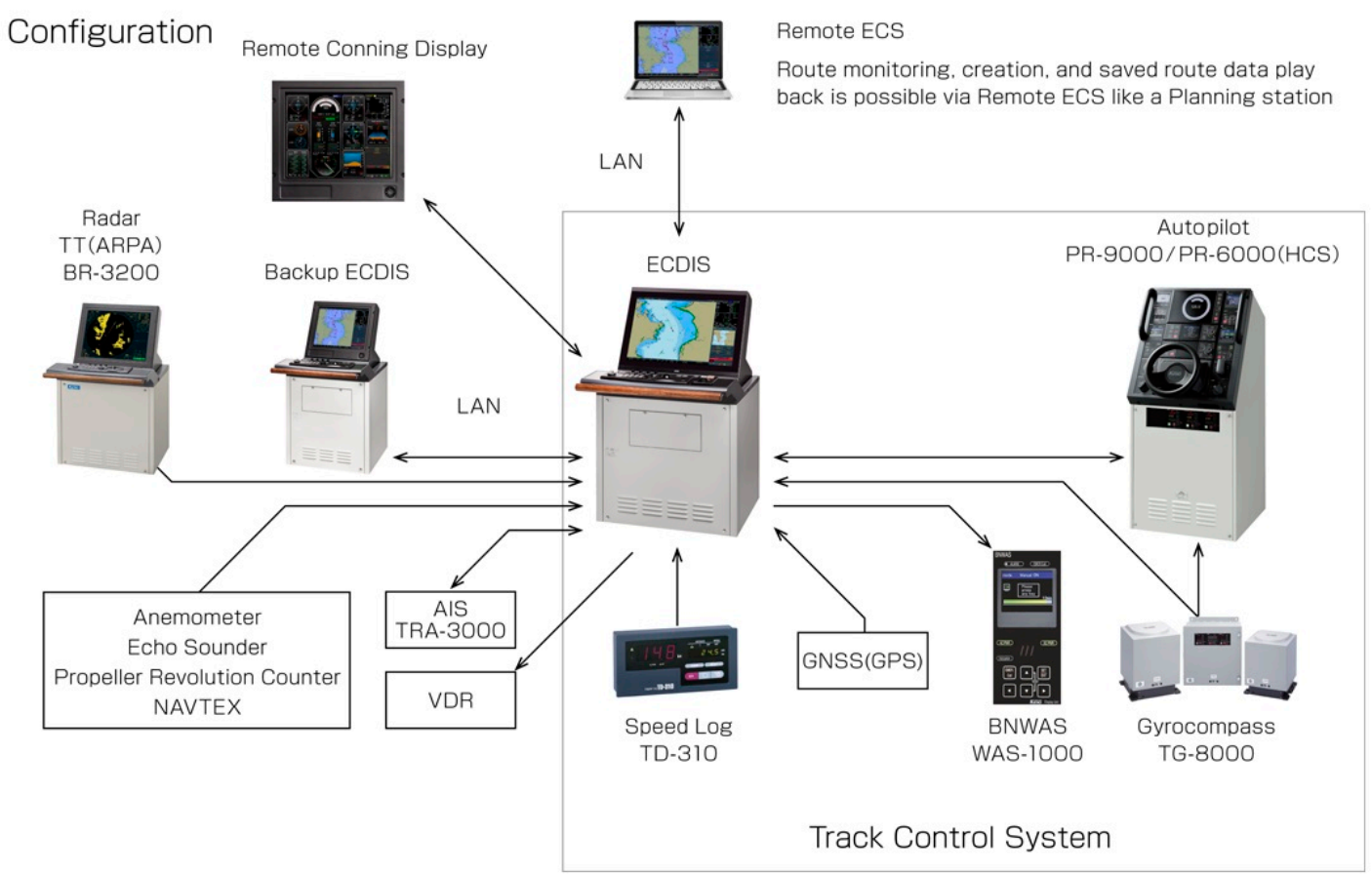
GPS Системы глобального позиционирования



VDR (Voyage Data Recorder) — регистратор данных рейса, бортовой самописец

ECDIS (Electronic Chart Display and Information System) — электронно-картографическая навигационно-информационная система судна

СИСТЕМА УПРАВЛЕНИЯ ACX Crystal



СИСТЕМА УПРАВЛЕНИЯ ACX Crystal

СИСТЕМА УПРАВЛЕНИЯ ACX Crystal

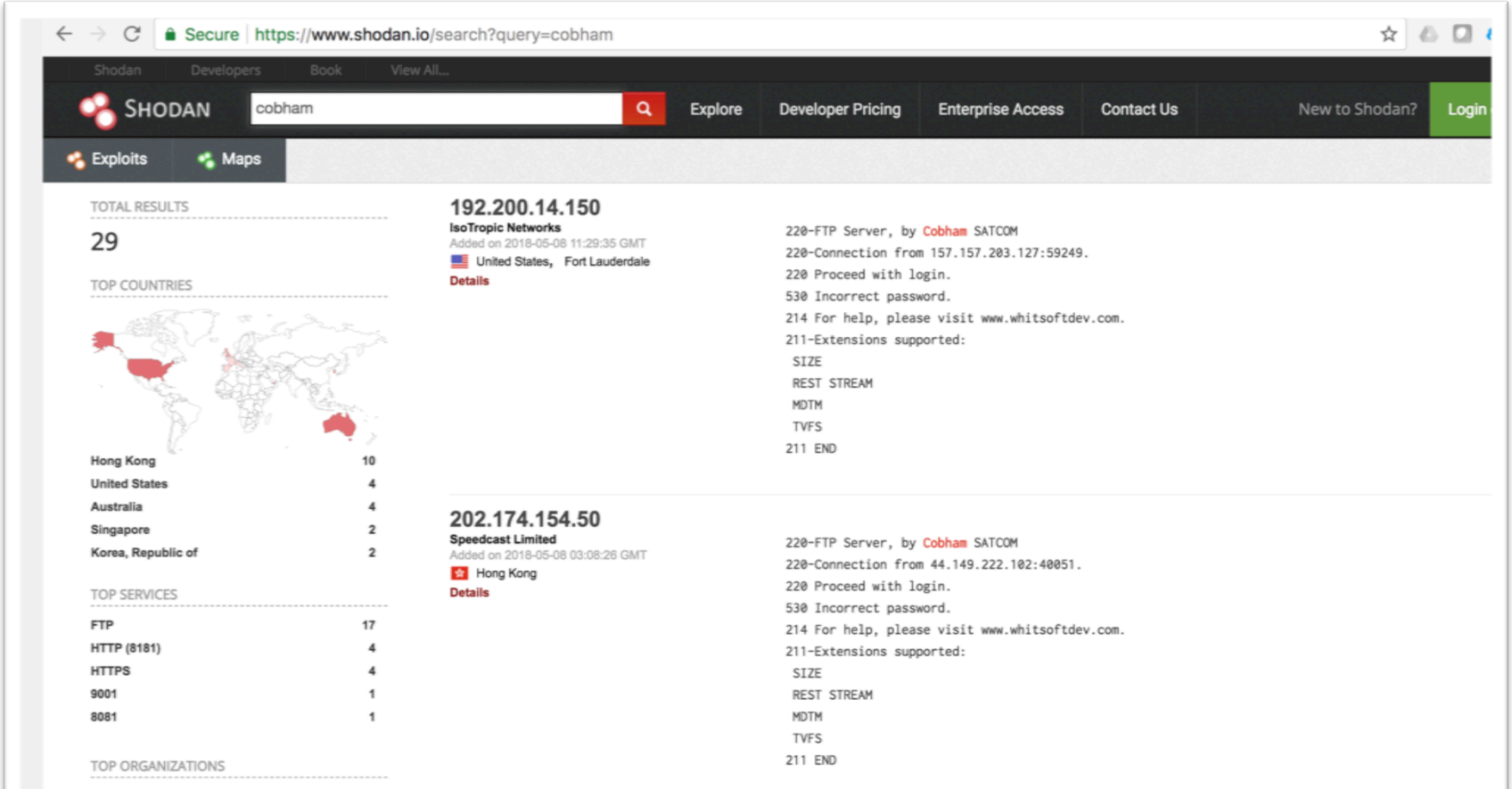
СИСТЕМА УПРАВЛЕНИЯ ACX Crystal

COBHAM

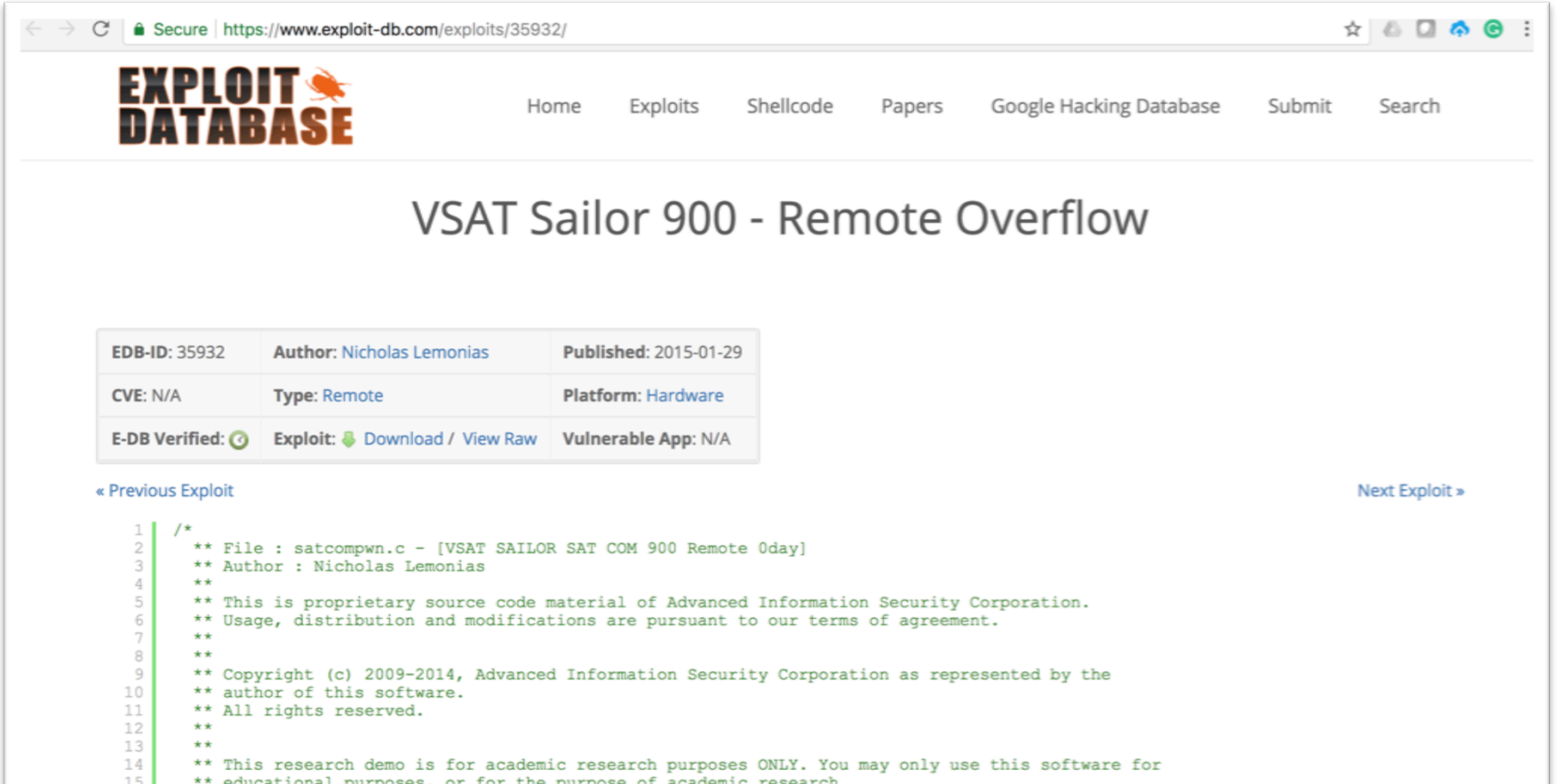
SAILOR 900 VSAT

Technical manual

SATCOM на SHODAN



SATCOM на SHODAN



Secure | https://www.exploit-db.com/exploits/35932/

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

VSAT Sailor 900 - Remote Overflow

EDB-ID: 35932	**Author**: Nicholas Lemonias	**Published**: 2015-01-29
CVE: N/A	**Type**: Remote	**Platform**: Hardware
E-DB Verified:	**Exploit**: Download / View Raw	**Vulnerable App**: N/A

« Previous Exploit Next Exploit »

```
/*
  ** File : satcompwn.c - [VSAT SAILOR SAT COM 900 Remote 0day]
  ** Author : Nicholas Lemonias
  **
  ** This is proprietary source code material of Advanced Information Security Corporation.
  ** Usage, distribution and modifications are pursuant to our terms of agreement.
  **
  **
  ** Copyright (c) 2009-2014, Advanced Information Security Corporation as represented by the
  ** author of this software.
  ** All rights reserved.
  **
  **
  ** This research demo is for academic research purposes ONLY. You may only use this software for
```

СИСТЕМА УПРАВЛЕНИЯ ACX Crystal

4.1.6 NMEA 0183 connector (RS-422)

Connect the ship's gyro to this connector.

Outline (on the ACU)	Pin number	Pin function	Wire color
	1	Not connected	—
	2	NET-H (NMEA 2000)	White
	3	NET-L (NMEA 2000)	Blue
	4	NET-S (NMEA 2000)	Red
	5	NET-C (NMEA 2000)	Black
	6	Not connected	—
	7	Not connected	—
	8	Shields. Ship ground. Connect only at one end.	
	9	Line B (+) NMEA 0183	
	10	Line A (-) NMEA 0183	
	11	Not connected	—

Table 4-4: NMEA 0183/2000 connector, outline and pin assignment

СИСТЕМА УПРАВЛЕНИЯ ACX Crystal

NMEA 0183 (от «*National Marine Electronics Association*») — стандарт определяющий текстовый протокол связи морского (как правило, навигационного) оборудования (или оборудования, используемого в поездах) между собой.

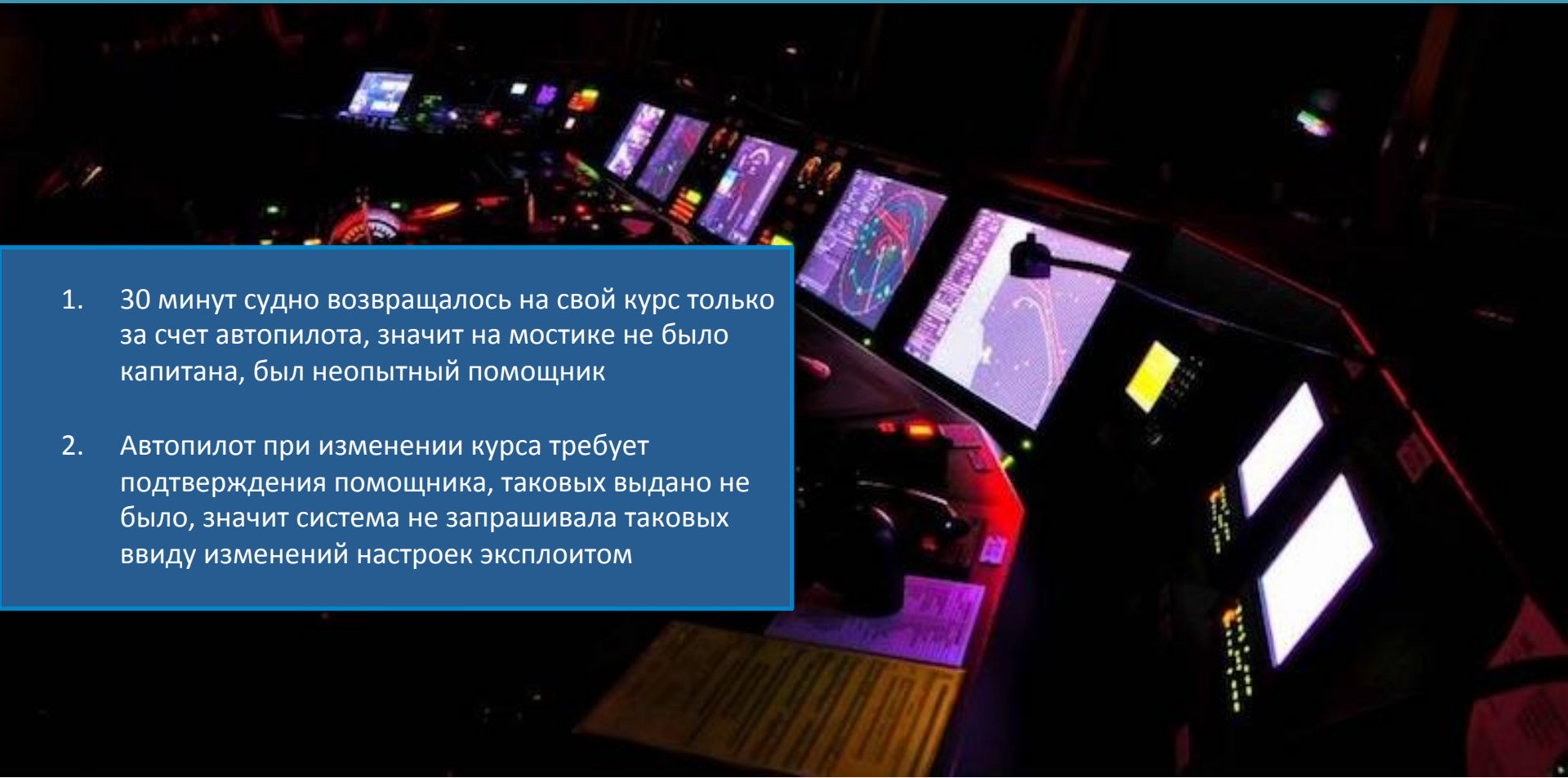
ПРИМЕР NMEA

$GPAPA,A,A,0.10,R,N,V,V,011,M,DEST,011,M*82

GPAPA – обращение к автопилоту

‘011,M’ – новая точка поворота для автопилота

Вид навигационного оборудования в час столкновения на Crystal



1. 30 минут судно возвращалось на свой курс только за счет автопилота, значит на мостике не было капитана, был неопытный помощник

2. Автопилот при изменении курса требует подтверждения помощника, таковых выдано не было, значит система не запрашивала таковых ввиду изменений настроек эксплоитом

СИСТЕМА VDR

VDR (Voyage Data Recorder) — регистратор данных рейса, бортовой самописец, аналог «черного ящика», используемого в авиации. Основные задачи — запись важной рейсовой информации судна, включая как технические и курсовые данные, так и голосовые записи с капитанского мостика, и ее сохранение в случае чрезвычайной ситуации

СИСТЕМА VDR

VDR состоит из двух модулей: DCU (Data Collection Unit) и DRU (Data Recording Unit).

- DCU – Linux - машина с набором интерфейсов (USB, IEEE1394 и LAN) для подключения к судовым сенсорам, датчикам и другим системам, а также оснащенную HDD с частичной копией данных второго модуля.
- DRU - стек из флеш-дисков, рассчитанных на запись данных за 12-часовой период, DRU модуль находится внутри защищенного от агрессивных внешних воздействий модуля

VDR для эксплоита:

- изменение и удаление данных как с диска DCU, так и с DRU с помощью NMEA команд

СИСТЕМА VDR

В отчете США не упоминается информация с VDR (обязательно при расследовании) и не упоминается информация о том, было ли информирование автопилотом об изменении курса сразу перед столкновением, то есть такая информация либо не записывалась на VDR, либо VDR был стерт

UNCLASSIFIED

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, DC 20350-2000

MEMORANDUM FOR DISTRIBUTION

Enclosure (1) Report on the Collision between USS FITZGERALD (DDG 6
ACX CRYSTAL
Enclosure (2) Report on the Collision between USS JOHN S MCCAIN (DD
Vessel ALNIC MC

The collisions were avoidable between USS FITZGERALD (DDG 62) a
ACX CRYSTAL, and between USS JOHN S MCCAIN (DDG 56) and Mot
MC. Three U.S. Navy investigations concerning each of these incidents are
Command and Admiralty investigations in each case retain legal privilege to
interests of the United States Government in future litigation. The third inve
incident, termed the Line of Duty Investigation (LODI), is not under legal pr
purpose is to determine that Sailors perished in the line of duty and thus enal
beneficiaries to receive appropriate compensation. Collisions at sea betwee
vessels and foreign registered vessels are also subject to an additional invest

Интеллектуальный комплекс защиты и обучения морской кибер безопасности навигационных, инженерных и связных систем судов и объектов морской инфраструктуры на базе программно-аппаратных средств

ВВЕДЕНИЕ

НА СЕГОДНЯШНИЙ ДЕНЬ СУЩЕСТВУЮТ РАЗЛИЧНЫЕ ВИДЫ УГРОЗ И УЯЗВИМОСТЕЙ В ОБЛАСТИ КИБЕР БЕЗОПАСНОСТИ В СУДОВОЙ И ПОРТОВОЙ ИНФРАСТРУКТУРАХ:

Наличие возможности перехвата данных внутри сетевой инфраструктуры портов;

Возможность перехвата и подмены данных каналов связи судно-порт;

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 морской локации;

Возможность сделать существующее судно «невидимым»;

Фальсификация сигналов EPIRB, активирующих тревогу на находящихся поблизости судах;

Отправка ложной погодной информации конкретным судам, чтобы заставить их изменить курс для обхода несуществующего шторма;

Активация ложных предупреждений о столкновении, что может стать причиной автоматической корректировки курса судна;

Возможность проведения DoS-атаки на всю систему путем инициирования увеличения частоты передачи AIS-сообщений.

ЗАКОНОДАТЕЛЬНАЯ БАЗА

Ведущими участниками морской отрасли, в том числе и государственными, ввиду высокой активности хакерских атак и растущего количества угроз были выпущены ряд законодательных, резолюционных и рекомендательных требований для обеспечения защиты морской инфраструктуры от кибер угроз:

- «Рекомендации по управлению киберрисками в морской отрасли» Приложение № 1 отчета о работе Комитета по упрощению формальностей (ФАЛ) на 41-й сессии – документ ФАЛ 41/17)
- «Управление киберрисками в системах управления безопасности морской отрасли» Резолюция (КБМ) MSC.428(98)
- «Рекомендации по управлению киберрисками в морской отрасли» Циркуляр КБМ-ФАЛ (MSC-FAL./Circ.3)
- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

СОСТАВ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА КИБЕР ЗАЩИТЫ СИСТЕМ СУДОВ И ОБЪЕКТОВ МОРСКОЙ ИНФРАСТРУКТУРЫ

Специализированный программно-аппаратный комплекс защиты осуществляет мониторинг каналов передачи данных на предмет запрещенных, нелегитимных пакетов. Построен с использованием специализированного алгоритма обнаружения угроз типичных для объектов морской инфраструктуры и состоит из следующих ключевых модулей:

Ядро безопасности

система контроля состояния локально вычислительной сети, контроль пакетного обмена данными и трафика. Мониторинг каналов передачи данных на предмет запрещенных, нелегитимных пакетов.

Модуль контроля и мониторинга

при возникновении угрозы данная система блокирует опасные команды. Комплекс уведомляет оператора о попытке несанкционированного воздействия. Модуль сочетает новейшие технологии защиты систем управления, включая сигнатурный анализ, проактивный, поведенческий подход и эвристические методы контроля безопасности.

Модуль оценки угроз

интерактивный перечень узлов системы, составленный на основе алгоритма мониторинга, прогнозирования сценариев атак и возможных угроз. Дает детальную информацию о степени защищенности и уязвимости узлов системы объекта.

Модуль интерактивной карты безопасности ЛВС

наглядное схематичное представление для оператора текущей системы объекта с указанием активных систем защиты узлов, данных о конфигурации устройств. Информирование и сигнализирование в интерактивном режиме о текущем состоянии системы в целом и обнаруженных уязвимостях, атаках, проникновениях.

ФУНКЦИИ ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА КИБЕР ЗАЩИТЫ СИСТЕМ СУДОВ И ОБЪЕКТОВ МОРСКОЙ ИНФРАСТРУКТУРЫ

Программно-аппаратный комплекс предусматривает различные схемы включения в систему судна или объекте для обеспечения гибкости вариантов обеспечения защиты в зависимости от поставленных задач.

Таким образом, программно-аппаратный комплекс «Центр мониторинга безопасности» осуществляет следующие функции:

Защита всех уровней системы от несанкционированного удаленного доступа с управляющих компьютеров, промежуточных узлов между управляющими компьютерами и оборудованием или с устройств нарушителя, подключаемых к промежуточным узлам и напрямую к линиям передачи данных

Защита от последствий подключения к линиям передачи данных (находящихся, в том числе на неконтролируемых территориях)

Защита от недокументированных возможностей иностранного оборудования, установленного на всех уровнях системы судна или объекта

Защита от вредоносного программного обеспечения на уровне управления и сбора данных (диспетчерские, операторские пульты)

Контроль исполнения политик безопасности и правил управления

Уведомление о факте несанкционированного прямого физического воздействия

СОСТАВ ИНТЕЛЛЕКТУАЛЬНОГО ТРЕНАЖЕРНОГО КОМПЛЕКСА

<u>Тренажерный комплекс обучения морской кибер безопасности судовых систем</u> включает в себя следующие модули:

VDR (Регистратор данных рейса)

EPIRB (Аварийный радиобуй)

AIS (Автоматизированная идентификационная система)

АРМ Центра мониторинга информационной безопасности судна

Система навигации (GPS/GLONASS)

АРМ Моделирования сценариев

СОСТАВ ИНТЕЛЛЕКТУАЛЬНОГО ТРЕНАЖЕРНОГО КОМПЛЕКСА

Функциональные возможности тренажерного комплекса включают в себя моделирование следующих векторов атак:

01 атаки на систему AIS (перехват и искажение)

02 атаки на спутниковые каналы (перехват трафика, подмена трафика, блокирование передачи данных, специфичные уязвимости Immarsat и других спутниковых систем)

03 атаки на систему VDR (удаление и искажение данных)

04 атаки внесения ложных сигналов на основе EPIRB

05 атаки на программное обеспечение IBS (троянские программы, социальная инженерия, взлом бортовой операционной систем)

06 атаки на системы автоматизации бортовых систем кораблей

07 эксплуатация уязвимостей контроллеров и систем автоматизации морских судов

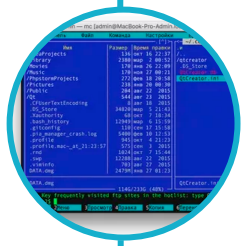
СОСТАВ ИНТЕЛЛЕКТУАЛЬНОГО ТРЕНАЖЕРНОГО КОМПЛЕКСА

Тренажерный комплекс обучения кибер безопасности объектов морской инфраструктуры включает в себя следующие модули:

Системы обработки и управления грузов

Система контроля доступа, Системы обслуживания и управления пассажирами

АРМ Центра мониторинга информационной безопасности судна



TOS (Терминальная Операционная Система), CTS (Система Отслеживания Контейнеров)

Административные системы и системы социального обеспечения экипажа

АРМ Моделирования сценариев

СОСТАВ ИНТЕЛЛЕКТУАЛЬНОГО ТРЕНАЖЕРНОГО КОМПЛЕКСА

Функциональные возможности тренажерного комплекса включают в себя моделирование следующих векторов атак:

01 специализированные вирусы для эксплуатации уязвимостей TOS/CTS систем,

02 эксплоиты информационных систем портов (TOS/CTS),

03 искажение данных информационных систем/внесение ложных данных,

04 сценарии атак на информационные системы портов с использованием социальной инженерии,

05 программные и аппаратные закладки для информационных систем портов (TOS/CTS),

06 специализированные вирусы для эксплуатации промышленных морских систем,

07 эксплоиты промышленных морских систем,

08 искажение данных промышленных морских систем

СОСТАВ ИНТЕЛЛЕКТУАЛЬНОГО ТРЕНАЖЕРНОГО КОМПЛЕКСА

АРМ

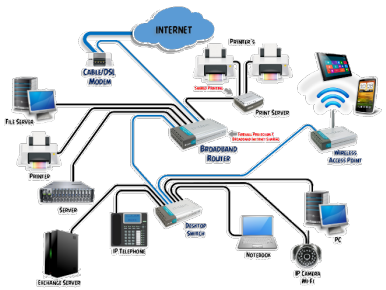
Центра мониторинга безопасности

АРМ

Моделирования сценариев

Схема блокировок работы инженерных систем

Оценка Угроз



Интерактивная карта безопасности ЛВС