DOI 10.37882/2223–2966.2022.10–2.18

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ЗАЩИТЫ СИСТЕМЫ УПРАВЛЕНИЯ МОРСКИХ СУДОВ

INCREASING THE EFFICIENCY OF PROTECTION OF THE CONTROL SYSTEM OF SEA VESSELS

Z. Medzhidov

Summary. Rapid globalization has led to the emergence of the most advanced trading networks with large and fast ships, robotic ports and extensive computer databases to track shipments. Marine vessels are increasingly using systems that rely on digitization, integration and automation, which require on-board cyber risk management. The purpose of the study: to analyze the current state of the information security market in marine vessels, on the basis of which to determine the promising directions of their development. The results of the study include the fact that cyber standards and measures for managing cyber risks in various countries are systematized, violators of the information security of ships are identified.

Keywords: information security, information security, ships, cybersecurity.

Меджидов Заур Уруджалиевич
К.э.н
Дагестанский государственный университет народного хозяйства»
zaur-medzhidov@mail.ru

Аннотация. Стремительная глобализация привела к появлению самых передовых торговых сетей с большими и быстрыми судами, портами, управляемыми роботами, и обширными компьютерными базами данных, позволяющими отслеживать грузы. Морские суда все чаще используют системы, которые полагаются на оцифровку, интеграцию и автоматизацию, что требует управления киберрисками на борту. Цель исследования: проанализировать текущее состояние рынка защиты информации в морских судах на основе чего определить перспективные направления их развития. К результатам исследования следует отнести то, что систематизированы киберстандарты и меры по управлению киберрискамив различных странах, определены нарушители информационной безопасности морских судов.

Ключевые слова: информационная безопасность, защита информации, морские суда, кибербезопасность.

Введение

Сегодня около 80% международной торговли осуществляется морским транспортом [1]. По сути, морской транспорт является лидирующим перевозчиком на международных линиях.

В силу того, что информационные технологии на борту судов постоянно развиваются, объединяются в сеть и все чаще связаны с Интернетом, повышается риск несанкционированного доступа или вредоносных атак на системы и сети судов. Это становится новой проблемой для морских операций [2]. При чем, такие угрозы могут появиться и в кибернетических системах, доступных персоналу, находящемуся на тот момент на борту, например, путём внедрения вредоносного программного обеспечения на съёмных носителях. Последствия неготовности к таким киберинцидентам могут быть значительными, носить экологический и коммерческий смысл.

По данным портала «Морские вести России» «в период с сентября 2020 года по октябрь 2021 г. подверглись кибератакам итальянское классификационное общество RINA, французская контейнерная судоходная компания CMA CGM, британская паромная компания Red Funnel, норвежская круизная компания Hurtigruten, оператор паромной переправы Steamship Authority в Массачусетсе, флагманский контейнерный перевозчик Южной Кореи HMM и японская судоходная компания KawasakiKisenKaisha, известная как «K» Line, не названные иранский и индийский порты, а также речной порт Кенневик в штате Вашингтон, США» [3].

Кроме того, в последние годы от действий киберпреступников пострадали:

- 17 из 76 грузовых терминалов компании Maersk (Дания);
- порты Барселоны (Испания) и Сан-Диего (США);
- терминал Шахид Раджаи (Иран);
- логистическая группа компаний Toll Group (Австралия);
- крупнейшая судоходная контейнерная компания MediterraneanShipping (Италия-Швейцария);
- зашифрованы приблизительно 370 (20%) рабочих станций и 20 (10%) серверов компании Anglo-Eastern (Гонконг).

С целью выработки конкретных мер по управлению киберрисками, Международная морская организация

выпускает «Руководство по кибербезопасности на судах». В документе содержатся «практические рекомендации по проектированию, изготовлению, обслуживанию и проведению испытаний судовых компьютеризированных систем, а также рекомендации, применимые к системам управления безопасностью» [4].

Тем не менее, в процессе сегодняшней гонки за повышением технологичности морских грузоперевозок всё так же на низком уровне остаётся вопрос обеспечения информационной безопасности на морском транспорте. Поэтому степень важности темы не требует доказательства и обусловлена тем неопровержимым фактом, что сростом информатизации мореходства, как и любой отрасли, повышается и риск угроз подтверждения атакам, в частности кибератакам.

Вопросами изучения различных мер противодействия киберугрозам в морских судах посвящены труды ряда зарубежных ученых-практиков.

Группа ученых (K. Tam, K. Jones, M. Papadaki) занимаются исследованием возможные кибератак на морские системы для навигации, движения и функций, связанных с грузом. Авторы иллюстрируют потенциальную серьезность проблемы, предоставляя несколько сценариев, демонстрирующих возможные атаки после того, как судно было скомпрометировано, и их сопутствующие последствия [5].

Другие ученые (I. Ashraf, S. Hur, Y. Park, Sung Won Kim) проводят обзор киберугроз в морской отрасли с поддержкой Интернета вещей, современных систем безопасности для судов, а также датчиков и устройств, используемых на современных кораблях. Кроме того, обсуждаются методы оценки рисков для определения потенциальной угрозы и степень серьезности, а также схемы и механизмы снижения киберрисков [6].

Иные ученые (D. Heering, O. Maennel, A. Venables) рассматривают вопросы с повышением компетенций в области кибербезопасности морского персонала. По их мнению: «Моряки должны быть готовы справиться с растущим числом киберугроз на борту судов, при этом осведомленность о кибербезопасности играет важную роль в управлении чрезвычайными ситуациями и кризисами. К сожалению, текущие программы морского образования и обучения не предоставляют морякам достаточно информации о кибербезопасности, чтобы они могли выявлять и нивелировать ущерб от киберугроз» [7].

Рассматриваемая нами тема исследования также носит предметный характер и в работах отечественных ученых, экспертов.

Семёнов С.А. в своем исследовании проводит аудит нормативного правого регулирования морской кибербезопасности в РФ, рассматривает международные и российские источники права. «На основании анализа прогнозирует вероятность коллизий между различными нормативными правовыми актами в области морской кибербезопасности, акцентируется внимание необходимости их гармонизации» [8].

«Выявление киберрисков и угроз для различных секторов морской индустрии в условиях наступления четвёртой промышленной революции и развитию цифровых технологий приводит к радикальным переменам в мировом хозяйстве в целом и морской отрасли, в частности». К такому умозаключению пришла группа ученых Бабурина О.Н., Гуриева Л.К. В этой связи, Международная морская организация, учитывая актуальность проблемы, разработала и приняла ряд документов по обеспечению кибербезопасности морской транспортной системы.

Другие ученые занимаются изучением перспектив использования технологии blockchain в целях обеспечения информационной безопасности на морском транспорте. Подобная технология уже хорошо зарекомендовала себя как надёжное средство ведения учёта, хранения данных, обработки транзакций и могла бы быть применена в организации документооборота на морском транспорте [9].

Таким образом, указанная проблема носит весьма практический и научный характер. Вместе с тем отдельные вопросы повышения эффективности защиты системы управления морских судов требуют тщательного изучения, что и предопределило выбор темы исследования.

Киберстандарты и меры по управлению киберрисками

Сегодня киберстандарты и меры по управлению киберрисками разрабатываются во многих странах мира. Ниже представлены некоторые задачи, опубликованные в официальных документах, решение которых ставят перед собой правительства ряда стран (таблица 1).

В настоящее время не существует исключения киберпространства во взаимном покрытии P&I Club (Клуб взаимного страхования- особая форма организации морского страхования на взаимной основе между судовладельцами) и для традиционных P&I рисков. На практике это означает, что цифровой сбой или взлом, создающий P&I претензию, будет покрываться до тех пор, пока член организации благоразумно и старательно обеспечивает управление надлежащим обра-

Таблица 1. Киберстандарты, применяемые в различных странах

Страна	Название документа	Основные задачи
США	Национальный план морской кибербезопасности США	Разработать структуру рисков для систем портовых операционных технологий, с целью налаживания общего языка рисков между страховщиками, судовладельцами и грузоотправителями; Выявить пробелы в правовых полномочиях и эффективности «для устранения конфликтных ролей и ответственности за стандарты кибербезопасности морской транспортной системы»; Разработать «процедуры для выявления, приоритезации, смягчения и расследования рисков кибербезопасности в критических системах судов и портов»; Разработать стандарты обучения кибербезопасности в морском секторе, что обеспечит ликвидацию пробелов во всех компонентах морской транспортной системы.
Европейский союз	Руководство для европейских портовых операторов по управлению киберрисками в условиях цифровой трансформации и ужесточения регулирования	Систематически выявлять активы и услуги, связанные с киберпространством; Принять комплексный подход к выявлению и оценке киберрисков, который «включает индикаторы рисков и анализ влияния на бизнес, вовлекает все соответствующие заинтересованные стороны и интегрируется на организационном уровне»; Осуществить общеорганизационные программы повышения осведомленности и технической подготовки в области кибербезопасности; Разработать комплексную программу кибербезопасности, с учетом обязанностей высшего руководства.
Россия	Стратегия национальной безопасности Российской Федерации	«Развить системы прогнозирования, выявления и предупреждения угроз информационной безопасности страны, определения их источников, оперативной ликвидации последствий реализации таких угроз»; «Предотвратить деструктивные информационно-технические воздействия на российские информационные ресурсы, включая объекты критической информационной инфраструктуры»; «Создать условия для эффективного предупреждения, выявления и пресечения преступлений и иных правонарушений, совершаемых с использованием информационно-коммуникационных технологий».

зом киберрисками своих судов и их соответствие требованиям государства флага и класса.

Тем не менее, останется множество незащищенных рисков. Атака национального государства или террориста будет представлять собой военный риск и, следовательно, не покрывается типичной P&I политикой, и владельцам придется искать прикрытие у андеррайтеров военного риска, многие из которых могут иметь киберисключения в своей политике. Кроме того, владельцы и фрахтователи с фиксированной премией вместо взаимного страхования обычно обнаруживают, что их полисы теперь содержат исключения киберрисков.

Сегодня рынок киберстрахования морских рисков ограничен. Но в свете растущего числа кибератак и очень видимых последствий для некоторых из крупнейших судоходных компаний Astaara ожидает, что спрос на покрытие будет быстро расти, и вопрос только в том, есть ли у страхового рынка желание или способность реагировать.

По мнению Счетной палаты США, киберстраховщики и держатели полисов сталкиваются с проблемами на развивающемся рынке. По данным Счетной палаты США, доля клиентов, выбирающих киберстрахование, выросла с 26% в 2016 году до 47% в 2020 году.

Ключевыми тенденциями в киберстраховании являются снижение лимитов покрытия в секторах с высоким риском и рост премий.

Рост цен. Отраслевые источники сообщили, что рост цен совпал с повышением спроса и ростом расходов страховщиков от более частых и серьезных кибератак. В недавнем опросе страховых брокеров более половины опрошенных клиентов отметили, что в конце 2020 года цены вырастут на 10–30%.

Появление киберспецифической политики. Страховщики все чаще предлагают полисы, специфичные для кибериска, вместо того чтобы включать этот риск в пакеты с другим покрытием. Этот сдвиг отражает стремление

Таблица 2. Основные нарушители морской кибербезопасности

Субъекты кибератак	Мотивация	Цель
Активисты (включая недовольных сотрудников)	репутационный ущерб срыв операций	уничтожение данных публикация конфиденциальных данных внимание СМИ отказ в доступе к целевому сервису или системе
Преступники	финансовая выгода коммерческий шпионаж промышленный шпионаж	продажа украденных данных выкуп украденных данных работоспособность системы выкупа организация мошеннической перевозки груза сбор информации для большего изощренное преступление, точный груз местоположение, судоходство и планы обработки и т.д.
Оппортунисты	Соревнование	прохождение защиты от кибербезопасности финансовая выгода
Государства и спонсируемые государством организации Террористы	политическая выгода «шпионаж	получение знаний подрыв экономики и критической национальной инфраструктуры

к большей ясности в отношении того, что покрывается, и к более высоким пределам охвата киберспецифики.

Индустрия киберстрахования сталкивается с многочисленными проблемами. Заинтересованные стороны отрасли предложили Счетной палате США варианты решения этих проблем.

Серьезной проблемой для киберстрахования являются ограниченные исторические данные о потерях. Без всеобъемлющих, высококачественных данных о киберпотерях может быть трудно оценить потенциальные потери от кибератак и, соответственно, ценовую политику. Некоторые участники отрасли заявили, что федеральные правительства, правительства штатов и промышленность могут сотрудничать в сборе и обмене данными об инцидентах для оценки рисков и разработки продуктов киберстрахования.

Страховщики говорят о том, что киберполитика не имеет общей терминологии. Заинтересованные стороны отрасли отметили, что различные определения политических терминов, таких как «кибертерроризм», могут привести к отсутствию ясности в отношении того, что охватывается. Они предложили, чтобы федеральные правительства и правительства штатов, а также страховая отрасль могли совместно работать над разработкой общих определений.

Для российского законодательства об информационной безопасности также серьезной проблемой является отсутствие и единого понятийного аппарата. Как видим, отсутствие единого понятийного аппарата американскими страховщиками расценивается как серьезная проблема развития рынка киберстрахования.

В прошлом году, специализирующаяся в области морской кибербезопасности компания NavalDome (Израиль) провела серию успешных демонстрационных кибератак на морские суда. В результате атак «хакерами» были «изменены сведения о местоположении судна, введен в заблуждение дисплей РЛС, включалось и выключалось судовое оборудование, были взяты под контроль системы управления топливом, рулевое управление и балластная система» [10].

Нарушители информационной безопасности морских судов

В 2020 г. журнал «SafetyatSea» совместно с организацией BIMCO провели опрос на тему морской кибербезопасности. В результате около 64% опрошенных заявили, что их «компании имеют план обеспечения непрерывности деятельности в случае киберинцидента». Полученный в ходе опроса процент кажется существенным. Однако это доля только среди тех, кто согласился принять участие в опросе [11].

Вместе с тем, следует обратить внимание на то, что кибербезопасность не заканчивается на том, чтобы вписать несколько строк в существующую систему управления безопасностью судна. В частности, ре-

комендуемое Международная морская организация «Руководство по кибербезопасности на борту судов» определяет следующий круг субъектов кибератак:

- активисты (включая недовольных сотрудников);
- преступники;
- оппортунисты;
- государства;
- спонсируемые государством организации;
- террористы.

Если против первой категории система управления безопасностью еще как-то может помочь, то для защиты от всех остальных категорий она защитить не способна. Здесь необходима более серьезная система мер. Следующее примеры дают некоторое представление об угрозах и потенциальных последствиях для компаний и корабли, которыми они управляют (таблица 2).

В рамках настоящего исследования целесообразно также упомянуть о решении Cydome. Cydome Onboard Suite предоставляет собой многоуровневое решение для обеспечения кибербезопасности морских судов. Специально разработан для защиты морской отрасли от кибератак. Cydome предлагает инновационные и передовые методы и услуги безопасности, соответствующие конкретные проблемы на борту судов, основанные на многолетнем опыте как кибербезопасность и морская промышленность. Он защищает деловые и экипажные сети судна, обеспечивая надзор, безопасность оповещение об угрозах и контроль над всей ИТ-инфраструктуры судна

В рамках использования Cydome предлагаются следующие решения в различных направлениях [12]:

- Флот. Предоставляется полная карта активных пользователей, подключенных к корпоративной сети, в режиме реального времени. Нет больше слепых зон. Кроме того, проводятся автоматизированные встроенные проверки кибербезопасности, в соответствии с требованиями Международной морской организации;
- Яхты. Решение помогает как менеджерам / операторам яхт, так и экипажу на борту легко использовать и демонстрировать инспекторам соблюдение требований и лучше преодолевать морские «киберрегуляторные проливы»;
- Порты. Понимание киберуязвимости флота и объектов в море привело к разработке дополнительного решения для кибербезопасности, чтобы защитить порты от небезопасных заходящих судов. Охраны портов на уровне берега недостаточно, чтобы идентифицировать и блокировать входящие суда, подверженные киберугрозам.
- Иные морские объекты. Прочие морские объекты, должны справляться с такими же киберрисками, как и любое другое судно, и даже больше. Такие объекты должны обеспечивать свою устойчивость к кибербезопасности в качестве объекта в море, а также против судов, находящихся в опасности, приближающихся к объекту.

Заключение

Исходя из проведенного исследования можно выделить основные особенности морских судов и типы угроз, которым подвержено автономное судоходство.

Особенности обеспечения кибербезопасности современных морских судов:

- интегрированное управление основными системами;
- разнородные сегменты: управление движением, служебные, пассажирские и т.д.;
- спутниковые и радиоканалы дистанционного управления и мониторинга, обмена навигационной и идентификационной информацией, интернет;
- ограничения по габаритам и вычислительным мощностям устанавливаемых технических средств.

Основные типы угроз:

- вредоносное программное обеспечение (включая закладки), инфицирующее критически важные системы управления судном;
- программы-вымогатели (атакуют используемые кораблем системы и серверы непосредственно вовремя рейса);
- подмена или глушение приема (навигационной) информации;
- цепочки поставки оборудования и программного обеспечения (предустановленные аппаратные импланты и программные закладки, скрытая установка вредоносных программ при обслуживании).

В условиях встраиваемых корабельных систем вычислительные мощности оборудования ограничены.

Задача обнаружения инцидентов нарушения безопасности требует обработки, анализа и хранения информации по большому количеству инцидентов.

Предложенный принцип проектирования планируется использовать в качестве архитектурного решения для системы управления кибербезопасностью, предназначенной для применения в автономном морском судоходстве.

ЛИТЕРАТУРА

1. UNCTAD, Review of Maritime Transport. Available at: http://unctad.org/en/PublicationsLibrary/rmt2016en.pdf. (date of the application: 11.06.2022 г.)
2. Svilicic B., Kamahara J., Rooks M., Yano Y. Maritime Cyber Risk Management: An Experimental Ship Assessment // The Journal of Navigation. 2019. Vol. 72(5), pp.1–13.
3. Морская кибербезопасность. Новое в 2021 году. Электронный ресурс: http://www.morvesti.ru/analitika/1692/92320/. (дата обращения: 15.06.2022 г.)
4. Руководство по обеспечению кибербезопасности (четвертая версия, 2021 г.).Электронный ресурс: https://lk.rs-class.org/regbook/getDocument2?type=rules3&d=BD2581FF-C53E-49FB-B8F8–0021E7F08005&f=2–030101–040. (дата обращения: 18.06.2022 г.).
5. K. Tam, K. Jones, M. Papadaki. Threats and Impacts in Maritime Cyber Security // Engineering & Technology Reference. 2016. Vol. 5. pp. 1–13. DOI: 10.1049/etr.2015.0123
6. I. Ashraf, S. Hur, Y. Park, Sung Won Kim (ets.). A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry // IEEE Transactions on Intelligent Transportation Systems. 2022. pp. 1–14. DOI: 10.1109/TITS.2022.3164678
7. D. Heering, O. Maennel, A. Venables. Shortcomings in cybersecurity education for seafarers // in book: Developments in Maritime Technology and Engineering, 1st Edition. Publisher: CRCPress.pp.49–61. DOI:10.1201/9781003216582–6
8. Семёнов С.А. Морская кибербезопасность в России // Транспорт Российской Федерации. 2019. № 3 (82). С. 11–14.
9. Semyonov S.A. Morskaya kiberbezopasnost' v Rossii // Transport RossijskojFederacii. 2019. № 3 (82). pp. 11–14.
10. Каменная Е.В., Полещук Е.М., Путилова С.Е., Щербинина И.А. Перспективы использования технологии blockchain в целях обеспечения информационной безопасности на морском транспорте // Транспортное дело России. 2018. № 6. С. 194–197.
11. Морская кибербезопасность. Электронный ресурс: http://www.morvesti.ru/analitika/1692/86359/. (дата обращения: 06.06.2022 г.).
12. Safety at Sea and BIMCO cyber security white paper. Available at: https://cdn.ihsmarkit.com/www/pdf/1019/Safety-at-Sea-and-bimco-cyber-security-white-paper.pdf. (date of the application: 01.06.2022g.).

Журнал «Современная наука: актуальные проблемы теории и практики»