УДК 004.056
EDN XKLFUC

Б. С. РИВКИН

КИБЕРБЕЗОПАСНОСТЬ НА МОРЕ. НАВИГАЦИОННЫЙ АСПЕКТ

Статья представляет собой обзор публикаций, посвященных вопросам кибербезопасности на море, связанным с навигационным обеспечением мореплавания. Обсуждаются киберугрозы в отношении ЭКНИС, автоматической идентификационной системы, регистратора данных рейса и интегрированной навигационной системы в целом. Отмечаются специфика кибербезопасности беспилотных судов, влияние на кибербезопасность человеческого фактора, анализируется нормативная база по борьбе с киберугрозами.

Ключевые слова: кибербезопасность, ЭКНИС, АИС, регистратор данных рейса, интегрированная навигационная система, беспилотное судно, человеческий фактор, Международная морская организация.

Введение

Значение морской транспортной системы для мировой экономики невозможно переоценить. Ежегодно во всем мире примерно 94 000 судов со стоимостью активов почти 1,5 триллиона долларов США перевозят грузы на общую сумму более 19 триллионов долларов США с ежегодным увеличением этой цифры примерно на 3% [1]. Современное судно представляет собой сложный киберфизический объект, управляемый с мостика, оснащенного на судах дедвейтом свыше 300 тонн интегрированной навигационной системой (ИНС, INS*), в состав которой в том числе входят следующие средства:

- электронная картографическая навигационная информационная система (ЭКНИС, ECDIS);
- приемник сигналов глобальных навигационных спутниковых систем (ГНСС, GNSS);
- автоматическая идентификационная система (АИС, AIS);
- электромагнитный или доплеровский лаг;
- магнитный и гироскопический компас;
- регистратор данных рейса (РДР, VDR);
- эхолот;
- система радаров.

Существенно, что ИНС, большая часть аппаратуры которой размещается в составе интегрированной мостиковой системы (ИМС, IBS), является одной из важнейших киберсистем корабельного базирования, основанной на информационно-коммуникационных технологиях (ИКТ, ICT) и обрабатывающей критически важную для безопасности судна информацию.

Ривкин Борис Самуилович. Кандидат технических наук, начальник Центра компетенций в области навигации АО «Концерн «ЦНИИ «Электроприбор» (С.-Петербург). Действительный член международной общественной организации «Академия навигации и управления движением»

*Здесь и далее вместе с русскими приводятся и соответствующие широко употребляемые английские аббревиатуры, традиционно не расшифровываемые в англоязычной литературе.

Последние несколько лет внедрение ИКТ на борту судов растет впечатляющими темпами. Сегодняшние ведущие производители судов применяют инновации, выходящие за рамки традиционного проектирования судов; такие суда именуются «кораблями с поддержкой киберпространства» (Cyber-Enabled Ships – C-ES)» [2]. В первую очередь к ним относятся суда, которые могут управляться удаленными береговыми службами в любое время и практически из любой точки, а также полностью автономные, которые далее будут называться беспилотными судами (БПС, MASS).

Одновременно ИНС как никакие другие информационные системы подвержены угрозе кибератак, под которыми понимаются модификация, отключение или уничтожение систем, кража или несанкционированное использование данных и др. [3]. Они могут быть направлены на системы как информационных технологий (ИТ, IT), обеспечивающих обработку данных, так и операционных (ОТ, OT), которые с помощью аппаратных средств и программного обеспечения (ПО) непосредственно управляют физическими устройствами и процессами [4]. Для повышения производительности ИТ- и ОТ-процедуры на борту судов интегрированы посредством локального сетевого подключения и Интернета, что сделало их более уязвимыми для кибератак. Злоумышленники могут взломать киберсистемы через слабозащищенные сетевые соединения и обойти межсетевые экраны, чтобы нарушить работу служб и украсть данные для продажи или потребовать выкуп, облегчить незаконное перемещение грузов, собрать разведданные и знания о критически важных системах/инфраструктуре, получить политические выгоды и многое другое, включая даже использование судна в качестве оружия для нападения на другие потенциальные цели.

Несмотря на обширные исследования и усилия во всем мире, число внешних воздействий на системы с интеллектуальной поддержкой растет с завидным постоянством. В этом отношении морской сектор, который еще недавно считался безопасным из-за отсутствия непосредственного подключения к Интернету и изолированного положения судов в море, демонстрирует 900-процентное увеличение нарушений кибербезопасности применительно к ОТ [5]. Если верить Лондонскому Ллойду, ущерб от кибератак в морской отрасли оценивается в 200 млрд долларов в год. В последнее время злоумышленники не ограничиваются кражей данных ИТ-систем, а стремятся взять под контроль командные и контрольные системы судна [6].

За примерами далеко ходить не надо. В феврале 2017 года судно водоизмещением 220000 тонн было полностью взломано на пути с Кипра в Джибути [7]. В течение 10 часов злоумышленник владел его навигационной системой, и капитан был бессилен что-либо сделать, чтобы вернуть корабль на маршрут. В том же году спуфинг-атака на корабль ВМС США, подменившая данные о его местоположении и параметрах движения, привела к его столкновению с южнокорейским рыболовным судном [8]. В ходе другого киберинцидента недавно построенный сухогруз был задержан на несколько дней в порту захода, поскольку его ЭКНИС была заражена неизвестным вирусом [9]. Затраты на ремонт, а главное, потери из-за задержки плавания составили несколько сотен тысяч долларов США. Наконец, в работе [10] приводятся многочисленные примеры столкновений кораблей и иных морских происшествий, вызванных неисправностями навигационных систем, порожденных кибератаками.

Рост автоматизации и попыток использования искусственного интеллекта при растущей цифровизации сектора морских услуг открывают, увы, все новые возможности для кибератак на судовые системы, и прежде всего на ИНС. Еще острее стоит эта

проблема в отношении БПС в варианте их применения в автономном режиме, когда отсутствие экипажа резко усугубляет трудности борьбы с внешними воздействиями. Все сказанное ранее, широко обсуждающееся в зарубежных изданиях, слабо освещается в отечественной технической литературе, что и послужило побудительным мотивом для написания данной статьи.

Дальнейшая ее структура такова. Прежде всего обсуждается киберустойчивость навигационных систем, более всего подверженных эффективным кибератакам, и ее специфика применительно к БПС. Затем анализируется влияние человеческого фактора при борьбе с киберугрозами и нормативная база кибербезопасности. Завершают статью сведения о кибербезопасности в России и заключение.

Киберустойчивость навигационных систем

Прежде чем переходить к изложению материала, обозначенного в заголовке, приведем перечень основных типов кибератак, характерных для навигационных приложений [11, 12]. К ним относятся:

- атака с помощью вредоносного ПО (malware) – направлена на повреждение компьютера; содержит трояны, вирусы и черви;
- атака с помощью программы-вымогателя (ransomware) – шифрует файлы на отдельных рабочих станциях, доступ к которым возможен только после выплаты выкупа;
- социальная инженерия (social engineering) – нетехнический подход к кибератакам, используемый (обычно посредством взаимодействия через социальные сети) для принуждения персонала к нарушению требований безопасности;
- атака типа «грубая сила» (brute force) – многократные попытки расшифровать пароль сети или сетевого устройства;
- атака типа «отказ в обслуживании» (denial of service – DoS) – блокировка доступа к информации авторизованных пользователей, как правило, путем переполнения трафика обращений к компьютерам или серверам;
- атака на цепочку поставок (supply chain) – злоумышленник на каком-то из этапов поставки внедряет уязвимость в аппаратное или программное обеспечение судна, чтобы впоследствии манипулировать ими;
- спуфинг – атака путем трансляции ложного сигнала, чтобы ввести в заблуждение получателя, например приемник сигналов ГНСС;
- «человек посередине» (man in the middle) – активная атака, когда злоумышленник перехватывает информацию, чтобы удалить или изменить данные;
- «человек на стороне» (man on the side) – атака, при которой злоумышленник может перехватывать сообщения, пересылаемые между участниками сетевой коммуникации, и отправлять в ответ на них пакеты со своими данными, но не имеет возможности модифицировать или удалить данные сети.

Многочисленные исследования киберустойчивости судовых навигационных систем (см., например, [13]) фиксируют тот факт, что более всего подвержена внешним вмешательствам аппаратура ЭКНИС, АИС, ГНСС, РДР и ИНС в целом. Учитывая, что проблемам помехоустойчивости приемников сигналов ГНСС, будь то интеллектуальный спуфинг или вульгарное глушение, посвящены уже тысячи статей, сосредоточимся на описании проблем, возникающих при кибератаках на остальную аппаратуру из приведенного списка.

ЭКНИС

ЭКНИС, являющаяся чрезвычайно важным информационным ресурсом для судоводителя, обычно входит в состав ИМС и представляет собой рабочую станцию, по большей части функционирующую под управлением Windows XP [14]. К ней, как правило, подключаются приемник ГНСС, АИС, курсоуказатели, лаг, эхолот, радар и навигационный телекс (NAVTEX). На современных судах данные от этих изделий транслируются через судовую локальную сеть, которая, в свою очередь, имеет шлюз в Интернет (сама ЭКНИС может подключаться к локальной сети ходового мостика). Для нормального функционирования ЭКНИС в нее должны быть загружены электронные навигационные карты (ЭНК, ENC), которые используются для отображения текущего места судна, прокладки курса, навигации и мониторинга хода рейса, а также фиксации целого ряда навигационных данных. ЭНК загружаются в ЭКНИС непосредственно через Интернет либо вручную с CD/DVD или USB-накопителя.

Очевидно, что простейшей угрозой для ЭКНИС является внедрение вируса через USB-накопитель или через Интернет. Как только это произойдет, можно будет:

- подменять выходные параметры упомянутых датчиков, влияя на процесс принятия решений вахтенным штурманом, что в принципе грозит столкновением или посадкой судна на мель;
- скомпрометировать локальную сеть и получить доступ к размещенным в ней данным.

Вместе с тем ЭКНИС, по сути дела, не что иное как программный пакет, установленный на персональном компьютере с предустановленной операционной системой (ОС). Исходя именно из такого представления, в работе [15] оценивается кибербезопасность ЭКНИС путем сканирования ее уязвимостей с использованием специального ПО. Исследования проводились применительно к ЭКНИС Navi-Sailor 4000, разработанной тогда еще российской компанией «Транзас», с помощью сканера Nessus Professional.

Всего было обнаружено 60 уязвимостей, что удивительно много для системы, занимающей значительную долю рынка ЭКНИС и позиционирующей себя как изделие «номер один» в своем классе [74]. Из них наиболее значимы те, которые относятся к ОС Navi-Sailor 4000, при этом к критическим была отнесена уязвимость сетевого протокола Server Message Block (SMB) версии 1. Уязвимость протокола SMB примечательна для морской отрасли из-за одного из наиболее известных инцидентов в сфере морской кибербезопасности – атаки программы-вымогателя NotPetya на контейнерную судоходную компанию Maersk, стоившей ей 300 млн долларов США [16]. Программа NotPetya также использовала уязвимость в SMB.

Решением обсуждаемой проблемы, в дополнение к обновлению ОС и разработке ПО для защиты от вредоносных программ, является отключение или блокировка сервиса SMB v 1, что может привести к затруднению удаленного доступа к общим ресурсам ЭКНИС. В условиях эксплуатации ЭКНИС на судне это приемлемо, так как она может и должна работать в автономной конфигурации.

Среди уязвимостей ОС имелись 5 средней критичности и по одной высокой и низкой [15]. Обнаруженные уязвимости высокой и средней критичности связаны с нарушениями в работе сервисов, обслуживающих ЭКНИС, что делает возможным несанкционированное удаленное выполнение кода и несанкционированное получение удаленного доступа. Возможные решения – обновление ОС и адекватная на-

стройка ее путем отключения или блокировки уязвимых сервисов. Обнаруженная уязвимость низкой критичности связана с работой терминала, что указывает на низкий уровень шифрования, поэтому следует предпринять рекомендуемые действия по соответствующей настройке ОС.

Одновременно на основе проведенного сканирования были качественно проанализированы киберугрозы для выявления и оценки уровня их риска для ЭКНИС. Воздействие угроз было определено как величина ущерба, причиненного реализацией уязвимости в процессе эксплуатации изделия. Наибольший риск, как оказалось, связан с резервированием ЭКНИС (в последнее время на судах из соображений надежности зачастую устанавливаются две идентичные ЭКНИС, которые оказываются идеальной средой для распространения вредоносных программ), подключением к Интернету, а также обновлением и настройкой ОС. Наконец в статье [15] было показано, что основные киберугрозы ЭКНИС фактически возникают из-за недостатков, связанных с ОС.

Скрупулезному исследованию кибербезопасности резервированной структуры ЭКНИС посвящена работа [17], где рассматриваются рабочие станции одного производителя и модели ECDIS JAN 9201 Japan Radio Company, объединенные в локальную сеть вместе с коммутатором для сбора информации с датчиков. В то время как данные ГНСС, АИС и радаров поступают на вход ЭКНИС напрямую через последовательные интерфейсы, посредством коммутатора локальной сети датчиков осуществляется сбор данных от гирокомпаса, лага, NAVTEX и эхолота. В качестве инструмента тестирования использовался все тот же сканер Nessus Professional.

Всего были обнаружены четыре уязвимости, из которых две отнесены к критической степени опасности и две – к средней. Количество и серьезность обнаруженных дефектов оказались одинаковы для обеих рабочих станций ЭКНИС, что свидетельствует об одинаковом уровне кибербезопасности для каждой из них. К обнаруженным уязвимостям относятся:

- опять же некорректная работа сервиса SMB v 1 (критическая), которая может позволить удаленному злоумышленнику выполнить код без авторизации;
- разрешение системой доменных имен (DNS) ОС Windows удаленному злоумышленнику выполнить произвольный код (критическая);
- подверженность атакам типа «человек посередине» (средняя);
- нарушение работы менеджера учетных записей безопасности (Security Accounts Manager – SAM) Windows, в котором хранятся пароли пользователей, что позволяет злоумышленнику выдать себя за аутентифицированного пользователя и получить доступ к базе данных SAM (средняя).

Борьба с этими уязвимости аналогична мероприятиям, изложенным ранее, – отключение SMB v 1 и доработка ОС.

Выше мы говорили об уязвимости резервированной структуры. При определении же киберрисков необходимо учитывать вероятность реализации той или иной уязвимости в процессе эксплуатации ЭКНИС. В этом случае, как показано в статье, прежде всего следует:

- уделять особое внимание корректности объединения ЭКНИС в сеть и обслуживанию ОС;
- регулярно тестировать на кибербезопасность судовые навигационные системы, подключенные к ЭНИС, особенно при использовании сетевых устройств.

АИС

АИС является еще одной системой, предназначенной для интеллектуализации морских перевозок [18]. В соответствии с правилом V/19.2.4 Международной конвенции по охране человеческой жизни на море (СОЛАС, SOLAS) АИС подлежит установке на все суда валовой вместимостью 300 тонн и более, совершающие международные рейсы, грузовые суда валовой вместимостью 500 тонн и выше, не участвующие в международных рейсах, и пассажирские суда независимо от их размера. В результате в настоящее время АИС установлена более чем на 300 000 судов по всему миру.

В качестве идентификационной системы АИС предназначается для повышения уровня безопасности мореплавания и эффективности судовождения и выполняет следующие функции:

- способствует решению задач предупреждения столкновений;
- обеспечивает береговые системы управления движением судов (СУДС) необходимыми для этого данными;
- снабжает компетентные береговые службы информацией о судне и грузе;
- осуществляет слежение за движением судов и принимает участие в операциях по поиску и спасению (Search and Rescue – SAR).

В процессе функционирования АИС, сопряженная с приемником ГНСС и навигационными датчиками судна, вырабатывает и транслирует окружающим судам и СУДС следующую информацию [19]:

- динамическую (в том числе координаты, время, курс и скорость судна, углы качки);
- рейсовую (пункт назначения, время прибытия, осадка судна, данные о грузе, количество людей на борту, сообщения для обеспечения безопасности грузоперевозок);
- статическую – номер MMSI, номер IMO, название судна, тип и габариты (MMSI – идентификатор морской мобильной службы, выданный государством флага судна, а IMO – Международная морская организация).

В последнее время многие веб-сайты собирают информацию от АИС и создают базы данных, чтобы любой мог найти данные о любом судне, оснащенном АИС, в режиме, близком к реальному времени [20]. Однако это ничто по сравнению с сайтами-агрегаторами, транслирующими в мировую паутину местоположение тысяч судов по всему миру, такими как FindShip, MarineTraffic, VesselFinder, Vesseltracker и другие. Комитет по безопасности на море IMO предупреждал об опасности утечки этой информации еще в 2004 году, отмечая, что «публикация данных АИС, передаваемых судами, может нанести ущерб безопасности судов и портовых средств и подрывает усилия IMO и ее государств-членов по повышению безопасности судоходства» [21].

Переходя к анализу киберустойчивости аппаратуры АИС, перечислим типовые угрозы ее нормальному функционированию, отмеченные в работе [20]:

1) подслушивание – простая пассивная атака, которая может быть легко осуществлена, так как АИС по определению является широковещательной радиосистемой, сообщения которой обычно передаются в незашифрованном виде;
2) глушение – может происходить на уровне как наземной станции, так и судна, и содержать атаку типа «отказ в обслуживании», делающую слоты передачи АИС недоступными;
3) внедрение сообщений – вставка ложных сообщений в транслируемые АИС данные. Это возможно из-за того, что последние не шифруются, а их источник не проходит проверку подлинности;

4) удаление сообщения – осуществляется путем создания в нем значительного количества битовых ошибок, в результате чего принимающая сторона отбрасывает его из-за повреждения данных;
5) модификация сообщения – инициируется путем изменения битового потока (как правило, путем переворота битов – изменения 0 на 1 или 1 на 0 или затенения, т.е. использования более мощного источника передачи данных для перезаписи части или всего целевого сообщения).

Наиболее опасными атаками на АИС являются те, где данные могут быть интегрированы в передаваемую АИС информацию; многие из них могут быть реализованы в программно-генерируемых передачах, а не путем атаки на сами радиочастоты. Примечательно, что наиболее существенные уязвимости в АИС связаны с отдельными сообщениями, а не с самой системой. Наконец, осуществимость атаки трудно поддается количественной оценке, потому что ее реализуемость часто зависит от противника. В любом случае любой из выявленных уязвимостей АИС злоумышленники могут легко воспользоваться.

Если ранее рассматривались типовые виды атак на АИС, то в работе [22] анализируются конкретные процедуры вмешательства в ее функционирование. Первая из них – создание несуществующего судна путем подмены транслируемых АИС данных с присвоением вымышленному судну статической информации, такой как название судна, MMSI, тип судна, тип груза, габариты, а также динамической: статуса судна (например, на ходу или на якоре), координат, скорости, курса и пункта назначения. При этом можно «создать» судно, находящееся под юрисдикцией враждебной страны или имеющее груз с ядерным оружием, плавающее в водах безъядерной страны.

Следующий вид атаки – подмена навигационной информации в данных АИС, чтобы побудить целевое судно совершить ошибку при маневрировании, прежде всего при решении задачи расхождения судов с использованием понятия «точка ближайшего сближения» (Closest Point of Approach – CPA). Она определяется путем вычисления минимального расстояния между двумя судами, когда хотя бы одно из них находится в движении. С помощью этого понятия можно настроить аппаратуру судна на выдачу оповещения о приближении к CPA как визуально на консоли капитана, так и акустически посредством сирены, и на изменение курса, чтобы избежать столкновения. Угроза состоит в возможности имитировать судно, как бы идущее по курсу столкновения с целевым судном, что провоцирует выработку предупреждения о столкновении и в результате связанного с этим маневра может привести к его столкновению со скалой или посадке на мель.

Важно отметить, что на сегодня нет официально признанных способов борьбы с приведенными выше угрозами. Одно из предложений состоит в том, чтобы ввести криптографическую систему с открытым ключом, который передается по незащищенному каналу и используется для проверки электронной подписи и для шифрования сообщения [22]. Другой обсуждаемый вариант – внедрение различных методов машинного обучения для распознавания аномалий в данных АИС.

РДР

РДР является морским эквивалентом «черного ящика», используемого в авиации, и устанавливается на борту всех коммерческих судов валовой вместимостью от 3000 тонн (и любых пассажирских валовой вместимостью более 150 тонн) для сбора

целого ряда данных с судовых систем. Записывая их в защитную капсулу с акустическим маяком, РДР выполняет функции автоматизированного судового журнала и является одной из наиболее важных систем на борту судна, обеспечивая расследование причины судовых аварий.

В аппаратуре РДР, как правило, содержится следующая навигационная информация:

- координаты, дата и время по данным ГНСС;
- данные о скорости и курсе;
- данные с радара или АИС, если для видеозаписи с радара недоступен конвертер;
- снимки экрана ЭКНИС каждые 15 секунд и список используемых навигационных карт каждые 10 минут или при смене карты;
- глубина под килем.

Вместе с тем РДР могут быть ненадежными свидетелями происходящего на судне [23]. Как отмечается в отчете, недавно опубликованном охранной фирмой IOActive, РДР могут быть взломаны, а их данные – похищены или уничтожены.

Так, исследователи IOActive проанализировали изделие фирмы Furuno марки VR-3000. Блок сбора данных (Data Collection Unit – DCU) VR-3000 по сути представляет собой персональный компьютер на базе Linux с несколькими интерфейсами связи, такими как USB, IEEE1394 и LAN, и с определенными мерами по обеспечению безопасности. При его изучении были выявлены следующие уязвимости:

- слабое шифрование файлов голосовых данных (записываются все разговоры, происходящие на мостике и его крыльях) с использованием общего пароля;
- программные сервисы позволяют удаленным злоумышленникам выполнять код на DCU, включая возможность удалять определенные разговоры, происходящие на мостике, и радиолокационные изображения, либо изменять данные о скорости или местоположении;
- возможность превратить РДР в удаленный «жучок», позволяющий шпионить за экипажем корабля, поскольку к нему напрямую подключены микрофоны, расположенные как минимум на мостике.

Для удаленной атаки злоумышленнику требовался только доступ к сети. Поскольку многие системы, подключенные к РДР, используют Интернет и находятся в той же сети, что и системы спутниковой связи (некоторые из них, как известно, уязвимы для атак), существует ряд потенциальных способов исказить данные РДР, не находясь на борту судна.

Более детально роль DCU, в состав которого входит резервный жесткий диск, частично копирующий хранящуюся в блоке записи данных (Data Registration Unit – DRU) информацию, исследуется в [24]. Это устройство хранит все необходимые навигационные данные и, кроме того, в течение 12 часов файлы с разговорами на мостике и радиолокационные изображения.

Наконец, с оценкой киберрисков применительно к РДР можно ознакомиться в работе [25]. Поскольку современные РДР могут быть подсоединены к Интернету для передачи данных, иметь сетевые подключения к критически важным системам судна (АИС, ЭКНИС и т.д.) и возможность записи потенциально конфиденциальной информации, соображения их кибербезопасности играют решающую роль. Исследование осуществлялось с использованием метода анализа видов и последствий отказа (Failure Modes & Effects Analysis – FMEA), который позволяет анализировать

компоненты, модули и подсистемы изделия, а также определять режимы, причины и последствия отказа системы.

Согласно результатам анализа, наиболее опасен ввод ложной информации в РДР, учитывая, что она может быть доставлена в каждую его часть и обычно имеет высокую вероятность реализации при низком уровне обнаруживаемости. По сути, это не прямая кибератака на РДР, а косвенная, нацеленная на другие бортовые системы, размещаемые в ИМС, которые обеспечивают РДР данными. Примерами этому являются несанкционированный удаленный доступ к ЭКНИС, подмена данных GPS или АИС. Эти атаки варьируются в зависимости от уязвимости технической инфраструктуры каждого судна и способны привести к выходу из строя каждого из устройств РДР, изменению содержащейся в нем информации или проникновению в другие части интегрированной системы. В частности, могут быть удалены или изменены карты и маршруты ЭКНИС, в силу чего РДР предоставит ложную информацию при расследовании причины судовых аварий.

В соответствии с параметром RPN (Risk Priority Number – количественная мера, используемая в FMEA для определения приоритетов и оценки относительного риска потенциальных видов отказов), второе место занимают атаки с внедрением в ПО произвольных команд. Они являются критическими для DCU, имеют риск среднего уровня для защитной капсулы, а также для панели управления РДР. Вирусы, которые отличаются относительно высокой величиной RPN, также считаются серьезными киберрисками. Шпионское ПО наиболее опасно для микрофона, размещенного на мостике. Способы предотвращения несанкционированного доступа, кражи и удаления данных РДР вредоносными программами заключаются в создании безопасных систем резервного копирования для хранения и более безопасных сетей для передачи данных.

Наиболее уязвимый компонент РДР – DCU со множеством протоколов обмена и стандартных интерфейсов для обмена данными, в результате чего у него больше уязвимых точек для проникновения злоумышленников. Более того, DCU – самое важное устройство для сбора данных, которые остаются в нем дольше всего. По этой причине, когда какая-либо из упомянутых атак затрагивает DCU, влияние ее чрезвычайно велико. Вторым рискованным компонентом РДР является аппаратура для подключения и организации удаленного доступа, обеспечивающая передачу данных РДР через спутник в соответствующий офис.

Наконец, третье место по рискам занимает панель управления РДР с интерфейсом для регулярного тестирования изделия, которая показывает любые системные ошибки с функциями оповещения, обладает кнопками для остановки или начала записи, интерфейсом для USB-накопителя и питается от DCU.

ИНС

Детальный обзор двадцати двух ИНС, позволяющий оценить реальную кибербезопасность систем этого класса в целом, представлен в [26]. Интересно отметить, что 15 из них были оснащены многофункциональные дисплеями, благодаря которым оператор может переключаться между ЭКНИС, радаром и коннинг-дисплеем. 11 из них в качестве ОС использовали Windows и лишь одна – Linux (в остальных системах ОС не была известна). В 18 случаях ИНС получают информацию от навигационных датчиков через последовательные интерфейсы (соответствующие стандарту

IEC 61162-1/NMEA 0183) и обеспечивают единый источник сенсорных данных для рабочих станций. Конфигурация ИНС варьируется, но в 19 из них сеть представляет собой своего рода Ethernet LAN на основе протокола IP.

Стандарты IMO требуют [27], чтобы в ИНС осуществлялся «мониторинг целостности» за счет сравнения данных, вырабатываемых резервированными источниками навигационной информации. И если для защиты от неисправностей этого обычно достаточно, то, увы, при кибератаках ситуация иная. Если ИНС подверглась атаке, нет никаких гарантий, что данными входящих в ее состав систем не манипулируют. Изучив архитектуру вышеупомянутых ИНС, авторы работы предложили следующий перечень контрмер для обеспечения нормального их функционирования:

1) разумно предположить, что фейковые данные распространяются с помощью многоадресной рассылки, следовательно, контрмеры должны это учитывать;
2) хотя в большинстве из 22 ИНС имеется подключение к Интернету, следует защищать ИНС и в том случае, когда входящие в ее состав системы работают в автономном режиме;
3) должны быть предусмотрены средства борьбы с атаками типа «человек посередине», опасными манипулированием и фабрикацией ложных навигационных данных;
4) специальные меры должны быть предусмотрены для защиты блока интеграции навигационных данных.

Авторы рассматриваемой работы предлагают и ряд мер для решения перечисленных проблем. Так, требования (1) и (3) предполагают решение с опорой на криптографию с открытым ключом, когда отправитель (в данном случае блок интеграции датчиков) криптографически подписывает сообщения закрытым ключом, в то время как несколько получателей (рабочих станций) проверяют подписи с помощью копии соответствующего открытого ключа. Требование (4) можно обеспечить внесением порядкового номера или отметки времени в подписанные сообщения. К сожалению, требование (2) исключает возможность использования инфраструктуры открытых ключей (Public Key Infrastructure), но в работе приводится решение, предполагающее задействование подписи на основе идентификации пользователя [28].

Если в предыдущем случае исследовались общие вопросы обеспечения кибербезопасности ИНС, то в статье [29] она изучалась применительно к конкретной системе NACOS MULTIPILOT Platinum 2017 производства Wärtsilä SAM Electronics GmbH. Экспертиза была основана на комбинированном подходе, сочетающем опрос судоводителей для выявления реализованных мер безопасности и тестирование ИНС на кибербезопасность с привлечением сканера уязвимостей Nessus Professional. В состав навигационного оборудования ИНС входит стандартный набор датчиков, обменивающихся информацией с обрабатывающим центром через высокоскоростную локальную сеть.

Результаты опроса судоводителей показали, что соответствующие процедуры, касающиеся системы управления кибербезопасностью, были тщательно доведены до сведения экипажа и регулярно пересматривались. Обучение судоводителей проводилось поставщиком ИНС, а осведомленность о кибербезопасности была на достаточно высоком уровне. Бортовые навигационные средства ИНС не были подключены к сети Интернет. Осуществлялась физическая защита от несанкционированного доступа персонала, а аппаратные интерфейсы ИНС хранились в запертом шкафу. Портативное за-

поминающее устройство для обновления ЭНК, предоставленное поставщиком ИНС, строго контролировалось. Кибергигиена вахтенных штурманов не имела нареканий.

Теперь о том, что выявил сканер. Критическая уязвимость – нештатная работа все того же сервиса SMB, которая отмечалась в разделе, посвященном ЭКНИС, с теми же рекомендациями по устранению дефекта. Высокая степень уязвимости была присвоена службе удаленного рабочего стола (Remote Desktop Services – функция сервера Microsoft Windows), допускающей дистанционное выполнение злоумышленником произвольного кода. Средней уязвимостью была охарактеризована работа службы протокола удаленного рабочего стола (Remote Desktop Protocol – протокол для удаленного подключения к компьютеру или серверу с ОС Windows), из-за низкого уровня шифрования грозящая возможностью атаки типа «человек посередине» с доступом к ИНС хакера. Последние две уязвимости устраняются путем обновления ОС, что должно выполняться уполномоченным персоналом поставщика ИНС.

Были оценены и киберугрозы. Наиболее опасными из них по воздействию были признаны (далее в скобках приведена вероятность их реализации):

1) эксплуатация ИНС с устаревшей ОС (0,4);
2) переустановка базовой ОС (0,4);
3) соединение ИНС с Интернетом (0,1);
4) несанкционированный доступ (0,1).

Одновременно было отмечено, что при подключении ИНС к сети Интернет уровень риска всех выявленных киберугроз повысится до критического уровня, требующего немедленных действий по защите.

В [30] представлены результаты эксперимента по оценке кибербезопасности ИНС путем создания атаки типа «человек посередине» с использованием технологии Cyber Kill Chain [31]. При этом планировалось вмешательство в работу ИНС в предположении, что одной из вероятных целей противника будет смещение координат, вырабатываемых GPS-приемником, на незначительную величину.

Использовавшееся в эксперименте судно было оснащено коммерческой ИНС с коммерческими же компьютерами, оснащенными ОС Windows 7. Навигационные датчики были связаны через интегратор. Навигационные данные поступали в ИНС через резервированную локальную сеть, которая обеспечивала все многофункциональные устройства необходимой информацией.

После того как атака была спланирована, соответствующий софт был загружен через USB-порт с помощью специального устройства. Вредоносная программа была размещена в ОС, после чего система была перезапущена, причем создавалось впечатление, что ЭКНИС не имеет сбоев и работает в штатном режиме. Более того, итоговое ПО было протестировано с использованием сайта VirusTotal (www.virustotal.com) на 60-ти наиболее распространенных антивирусных программах, доступных для покупки. Только две из них обнаружили в ПО какой-либо подозрительный код, в то время как остальные 58 классифицировали ПО как «чистое». Таким образом, можно сделать вывод, что установка антивирусной программы не даст достаточной защиты от подобной кибератаки.

В рассматриваемой ИНС связь с Интернетом отсутствовала, так что удаленное воздействие на ее функционирование было исключено. По этой причине вредоносное ПО было запрограммировано на срабатывание при пересечении судном предопределенной линии, после чего оно начинало вносить в показания GPS погрешности в выра-

ботке координат, соответствующие движению со скоростью 0,8 м/с в направлении на северо-восток, что в итоге приводило бы к «контролируемой» посадке на мель.

Этот эксперимент показал, что кибератаки на ИНС относительно легко реализуемы. Безопасность ИНС в значительной степени зависит от ее физической защиты, в то время как сама система оказывается незащищенной, после того как доступ к ней установлен. Фаза подготовки атаки (или «разведки», по определению Cyber Kill Chain) является наиболее ресурсозатратной для потенциального атакующего. Именно на этом этапе злоумышленник должен обладать знаниями о системе и процедурах, выполняемых экипажем, чтобы получить такую информацию, как, например, пароли для входа в систему на более высоких уровнях обслуживания.

VSAT

В последнее время суда все чаще оснащаются морским спутниковым связным терминалом с очень малой апертурой (Very Small Aperture Terminal – VSAT) [56]. VSAT обслуживает различные бортовые системы, такие как ЭКНИС, АИС, телефон и Интернет. Компания IOActive [57] протестировала несколько VSAT от разных производителей и пришла к выводу, что все они имеют уязвимости, поскольку используют передачу открытого текста без аутентификации, шифрования и проверки. В результате слабой защиты злоумышленники могут отправить на устройство ложные сигналы или вредоносный код, чтобы вывести его из строя или поставить под угрозу систему, лишая судно возможности безопасной навигации. Реальный риск заключается и в том, что сетевые интерфейсы VSAT можно найти в Интернете с помощью таких инструментов, как Shodan Ship Tracker. Это позволяет добыть ценные сведения, которые могут быть использованы в кибератаках. Стандартная информация обычно доступна на веб-сайтах поставщиков, и многие из них при проектировании терминалов продолжают использовать одни и те же заводские настройки, включая имя пользователя и пароль сервера. Злоумышленник может изменить координаты и настройки GPS, а также загрузить вредоносное ПО, если обнаружит открытый интерфейс VSAT, что позволит осуществить дальнейший взлом сети и получить доступ к критически важным устройствам ИНС.

Кибербезопасность БПС

Ранее уже отмечалось, что обеспечение кибербезопасности БПС, особенно четвертого типа по классификации IMO, когда экипаж на судне попросту отсутствует и не может вмешаться в происходящее на борту, является нетривиальной задачей. И хотя самим технологиям ИНС для БПС не более 20-25 лет, литература по их кибербезопасности достаточно обширна.

Начнем с анализа киберугроз судам этого типа, чему посвящена работа [32], где с этой целью широко используется метод STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege – спуфинг, фальсификация, непризнание, раскрытие информации, отказ в обслуживании, повышение привилегий) [33]. Здесь фальсификация – это изменение данных или нарушение работы диска, сети или памяти системы. Непризнание – отрицание факта получения или отправления сообщения. Раскрытие информации – передача конфиденциальной информации пользователям, которым она не должна быть доступна. Отказ в обслуживании – нарушение доступности системы, реализация которого состоит в невоз-

можности загрузить ресурсы, необходимые системе для правильной работы. Повышение привилегий – нарушение правил доступа, в результате чего злоумышленник получает возможность выполнять несанкционированные действия. С использованием STRIDE было установлено, что наиболее уязвимыми в БПС являются АИС, ЭКНИС и ИНС в целом, а также аппаратура, обеспечивающая человеко-машинный интерфейс при наличии на борту экипажа.

С точки зрения вероятности осуществления атак наиболее критичными оказались отказ в обслуживании и спуфинг. Фальсификация и повышение привилегий были признаны угрозами среднего уровня, поскольку они относятся к более сложным в исполнении атакам, и, чтобы воспользоваться этими уязвимостями, злоумышленник должен быть высоко мотивирован. Наконец, непризнание и раскрытие информации являются угрозами низкой критичности для систем БПС.

В силу специфики эксплуатации БПС важную роль в решении задачи навигационной безопасности плавания, мониторинга и отслеживания важнейших операций судна, а также защиты от нападений террористов и пиратов играют системы видеонаблюдения [58]. Однако недавно они были признаны уязвимыми для нескольких типов кибератак, и возник ряд проблем с их кибербезопасностью [59]. Например, исследователи из Bitdefender обнаружили, что две модели камер видеонаблюдения, применяемые на современных судах, подвержены ошибкам переполнения буфера. Воспользовавшись этим, исследователи смогли отследить деятельность взломанной камеры и перезаписать пароли доступа [60]. Эта уязвимость может привести к сбою видеосистемы или, что еще хуже, создать точку входа для других кибератак.

Более детальный анализ киберугроз и методов защиты от их воздействия для БПС приведен в [34], где выделен ряд атак, делящихся на две категории, в которых злоумышленники:

- предпочитают вмешиваться в работу судовой аппаратуры посредством физического доступа или на близком расстоянии;
- используют дефекты работы аппаратуры удаленно.

Одной из наиболее распространенных уязвимостей, обнаруженных на морских судах и в ОС, является относительная легкость, с которой вредоносный код, например программы-вымогатели, шпионское ПО и вирусы, могут быть внедрены в критически важные системы. Это происходит чаще всего с помощью зараженных съемных носителей, а также через вредоносные обновления прошивки. Атака с внедрением вредоносного ПО может быть предпринята либо умышленно, либо непреднамеренно персоналом, имеющим надлежащие учетные данные для доступа к системе судна. Кроме того, выяснилось, что некоторые РДР подвержены переполнению буфера, а также некорректной работе механизма обновления прошивки [35].

В последнее время в судовых вычислительных сетях БПС все чаще используется шина CAN (Controller Area Network), позволяющая подключенным узлам транслировать друг другу данные. Не секрет, что протокол обмена CAN уязвим [36]. Вредоносный узел, подключенный к шине CAN, может не только выполнять захват транслируемого пакета, но и внедрять модифицированный вредоносный трафик или отправлять недействительные данные (фальсификация и превышение привилегий по STRIDE). Такие атаки могут раскрывать конфиденциальные данные, вызывать сбои, обрабатывать ошибки и перезапускать систему, а также перегружать бортовые датчики с ограниченными вычислительными возможностями.

Следующий тип атаки – спуфинг сигнала ГНСС, который нацелен на то, чтобы убедить бортовую систему позиционирования БПС в корректности транслируемого поддельного сигнала, что неминуемо приводит к выходу судна на ложный маршрут. Для этого, как правило, необходимо разместить соответствующий излучатель в достаточной близости от БПС (например, на параллельно идущем морском носителе). Не менее опасно для БПС и глушение сигнала ГНСС, приводящее к потере прецизионного знания своего местоположения.

При этом спуфинг АИС, осуществляющей передачу данных с помощью УКВ-связи, не требует физического присутствия рядом с БПС. Поскольку в АИС почти не существует шифрования, аутентификации или проверки полученных данных, авторы [22, 37] сообщили о многочисленных ее уязвимостях. Наиболее показательно то, что Бальдуцци (Balduzzi) и др. [22] удалось с помощью простого скрипта на языке программирования Python организовать удаленную атаку спуфинга АИС, которая произвольно изменяла информацию о судне (например, его принадлежность и местоположение).

Какие меры общего характера должны прежде всего применяться для охраны ИНС БПС от кибератак? Естественно использование традиционных компьютерных и сетевых средств защиты. Так, методы разделения сети помогают свести к минимуму широковещательный трафик, а сами сети должны иметь современную защиту конечных точек для обнаружения вирусов и вредоносных программ. Чтобы свести к минимуму влияние глушения сигнала, может быть установлено избыточное оборудование. Только доверенному персоналу должно быть разрешено вносить изменения в аппаратуру ИНС.

Эффективным средством борьбы с киберугрозами является и интегрирование информации, циркулирующей в ИНС. Например, совместная обработка данных о местоположении судна, вырабатываемых инерциальной навигационной системой, которая является непременной составной частью ИНС БПС, и фиксируемых приемником ГНСС, при создании соответствующего эффективного алгоритма может решить проблему спуфинга ГНСС. Процедуры загрузки данных должны быть организованы таким образом, чтобы обеспечить своевременное отслеживание, выявление и устранение текущих уязвимостей и угроз для систем ИНС. Кроме того, должна оперативно осуществляться безопасная загрузка новых версий встроенного ПО.

Если ранее в этом разделе речь шла о судах-автоматах, то в работе [38] рассматривается специфика создания ИНС для судна, управляемого дистанционно. В этом случае, естественно, существенной проблемой становится ситуационная осведомленность (СО) о происходящем на борту БПС, и прежде всего о состоянии навигационной аппаратуры. Проводимые в последнее время исследования дистанционно управляемой навигации судов показывают, что на берегу нет отчетливого представления о происходящем на борту, и сосредоточены прежде всего на качественном анализе получаемой информации, в связи с чем трудно представить все возможные сценарии, которые могут возникнуть на практике [39].

Очевидно, что для обеспечения приемлемого уровня безопасности БПС, повышения качества обслуживания системы дистанционного управления и обучения операторов берегового базирования необходимо количественно оценить СО. На март 2019 г. уже существовал ряд методов, позволяющих решить эту проблему, среди которых на практике применялись методика глобальной оценки СО (Situation Awareness Global Assessment Technique – SAGAT) [40] и методика оценки СО (Situation Awareness Rating Technique – SART) [41]. Однако с их помощью нельзя

было оценить СО решения хотя бы одной задачи одновременно для ряда БПС, что требовалось на практике, и обеспечить работу в реальном времени.

Этих недостатков лишен метод, предложенный в [38] для разработанной Вробелем (Wrobel) структуры безопасности [42] и основанный на байесовском подходе. Он предполагает обработку данных как от датчиков, входящих в состав ИНС, так и от датчиков, характеризующих внешнюю по отношению к БПС обстановку, и исходит из того, что при отсутствии киберопасности оператор в центре управления судами может контролировать перемещение нескольких БПС, к тому же находящихся в разных морях.

Предложенная в работе модель количественной оценки СО способствует повышению эффективности оценки риска столкновения БПС с окружающими объектами [43] и качества самой СО, что помогает лучше оценить текущую ситуацию на борту управляемого БПС. Проведенное в работе моделирование подтверждает очевидный факт – даже при наличии адекватной величины СО вероятность отказа ИНС управляемого БПС выше, чем у обычного судна.

Неудивительно, что в общем случае при проектировании ИНС для БПС рекомендуется принимать специальные меры безопасности и защиты, чтобы повысить устойчивость к внешним и внутренним угрозам [44]. Прежде всего необходимо создать систему непрерывного мониторинга, которая сможет в режиме реального времени обеспечивать осведомленность о безопасности судна [45]. В этом контексте в ряде исследований для повышения безопасности управления автономными судами было предложено использовать технологию блокчейна. Согласно [46], она будет играть важную роль в идентификации и сертификации, обеспечении целостности данных и информационной безопасности ИНС автономных судов. Присущие блокчейну отслеживаемость, прозрачность и возможность проверки обеспечат безопасность связи и хранения данных, которыми обмениваются суда и береговой центр управления.

В соответствии с [47], одним из механизмов, который может повысить безопасность навигации, является система аутентификации навигационных сообщений (Navigation Message Authentication – NMA), которая предназначена для предотвращения их подделки. Схема NMA допускает включение данные аутентификации в поток навигационных сообщений, что позволяет установить подлинность источника, а также защитить криптографическую целостность навигационных данных [48]. Благодаря этому удается обнаружить злоумышленников, пытающихся сгенерировать или изменить навигационные данные и не имеющих возможности имитировать сообщение аутентификации, не зная соответствующего ключа.

Наконец высказываются идеи о том, что для функционирования электронной системы доверия судоходному сообществу следует внедрить инфраструктуру открытых ключей (Public Key Infrastructure-PKI) [49]. Это позволит пользователям и системам проверять легитимность объектов, владеющих сертификатами, а также безопасно обмениваться информацией между ними. Последнее чрезвычайно важно именно для БПС. Может быть настроена и транспортная PKI с IMO в качестве высшего доверенного лица, выступающего в роли «корневого центра сертификации» (Root Certificate Authority), с наличием отделений в государствах флага [50]. Государства флага будут иметь право выдавать новые ключи властям прибрежных государств, судам, плавающим под их флагом, признанным организациям, портам и другим лицам, которым требуется сертификат открытого ключа, доступный на международном уровне.

И последнее, но, тем не менее, важное. Вторая конференция по морской кибербезопасности, состоявшаяся в октябре 2022 г. под эгидой Европейского агентства морской безопасности (European Maritime Safety Agency) и организованная Агентством Европейского союза по кибербезопасности (European Union Agency for Cybersecurity), была призвана изучить динамику киберугроз и проблемы, с которыми сталкивается морской сектор [52]. Выяснилось, что сами типы атак меняются по мере перехода от традиционных кораблей к БПС, в результате чего фокус борьбы с киберугрозами смещается с бортовых политик безопасности, таких как управление паролями и социальная инженерия, на сетевые аспекты.

Человеческий фактор

Технологической основой для обеспечения безопасного обмена информацией в ИНС является ряд процедур, с которыми имеют дело пользователи различного оборудования и ПО. К ним, например, относятся:

- поддержка корректной конфигурации ПО и сети;
- мониторинг ИТ-сети изделия;
- использование антивирусной защиты и межсетевого экрана;
- модернизация системы и своевременное обновление вирусной базы данных;
- обновление криптографических протоколов;
- создание резервных копий информации (данных);
- мониторинг мошеннического поведения и управление политикой доступа к ресурсам (контроль паролей и удаленного доступа, управление учетными записями пользователей);
- удаленное управление ПО пользователя (удаление или блокировка ненужных программных функций и плагинов).

Как следствие, рекомендуется ввести регулярное обучение судоводителей кибербезопасности и безопасной эксплуатации технических систем. Экипаж судна должен понимать потенциальные уязвимости в компьютерных системах и знать о соответствующих технических и процедурных мерах защиты. Успешное предотвращение, обнаружение и борьба с кибератаками требует навыков по обеспечению кибербезопасности и умения оценивать потенциальные риски.

Авторы работы [51] в 2019 г. провели анализ случайно выбранных десяти программ бакалавриата по навигации в десяти европейских морских университетах. Ни одна из них не включала специальные курсы по морской кибербезопасности, и лишь в две входили основы информатики с некоторыми элементами кибербезопасности.

Чтобы выяснить ситуацию более подробно, ими был подготовлен вопросник по проблеме кибербезопасности на 37 позиций, разосланный 110 адресатам, связанным с судоходством. Цель исследования – выяснить уровень знаний в области кибербезопасности и оценить влияние человеческого фактора. Опрос выявил трудности в понимании корреспондентами основных понятий кибербезопасности (таких как доступность и целостность) и в знании основных систем безопасности судна. Это подтвердило гипотезу о том, что морская кибербезопасность находится на низком уровне.

Что касается вклада человеческого фактора в морскую кибербезопасность, то для изучения этого вопроса были проведены тесты с использованием критерия $\chi 2$. Содержание полученных ответов практически не зависело от социального положения

и возраста опрашиваемых. Выяснилось значительное влияние человеческого фактора, причем как положительное, так и отрицательное. Так (положительный пример), большинство участников опроса знало, что обновление ЭКНИС может быть выполнено либо через USB-накопитель, либо через Интернет. С другой стороны, 9 из 10 не смогли ответить на вопрос: что происходит с кибербезопасностью, когда АИС выходит из строя? Следовательно, в этой ситуации они не будут способны предпринять адекватные меры при атаке на ИНС. По мнению авторов работы [51], если исходить из того, что почти 80% морских аварий вызваны человеческой ошибкой, то это также относится и к морской кибербезопасности.

С учетом роли человеческого фактора, в 2013 г. в США по рекомендации Альянса оборонной промышленности Юго-Восточной Новой Англии (Southeastern New England Defense Industry Alliance) был создан Морской центр кибербезопасности в качестве специального ресурса, ориентированного на поддержку потребностей в рабочей силе по борьбе с кибератаками [52]. Задачами центра являются:

- повышение осведомленности населения, предприятий, отраслей и образовательных учреждений о проблеме кибербезопасности;
- создание сообществ практиков для углубления понимания и распространения информации среди этих коллективов и связанных с ними специалистов;
- подготовка квалифицированных специалистов, которые могут выявлять и решать проблемы кибербезопасности;
- предоставление платформы для непрерывного обучения и защиты в области кибербезопасности.

Если раньше речь шла о принципиальных проблемах борьбы с кибератаками, то в работе [53] оцениваются конкретные результаты их воздействия. С этой целью на базе Таллиннского технического университета (Tallinn University of Technology) были проведены учения по кибербезопасности, все участники которых были магистрантами или аспирантами. Учения проходили с использованием интегрированного навигационного тренажера, состоящего из:

- 4 мостиковых тренажеров Navi-Trainer Professional Simulator NTPRO 5000 фирмы «Транзас»;
- 8 ноутбуков с ПО Windows 10 и программным обеспечением картплоттера Sea Clear II на базе ПК;
- беспроводной сети без доступа к Интернету.

Программа учений предполагала проверку безопасности морских навигационных систем, сбор разведывательных данных с реальных кораблей, находившихся в море во время учений, и выявление возможных кибератак. В процессе учений были взломаны размещавшиеся на кораблях ЭКНИС с захватом управления курсом корабля и манипуляциями картографическими данными, осуществлено вмешательство в работу АИС и глобальной морской системы связи при бедствии. Одновременно во время учений удалось:

- завладеть 7536 именами пользователей и паролями, используемыми сотрудниками и экипажами военных кораблей НАТО;
- убедиться, что корабли НАТО можно отслеживать с помощью SNAPMAP (map.snapchat.com), Twitter, Facebook и других социальных сетей;
- установить, что в Twitter имеется большое количество конфиденциальных данных членов экипажей.

О влиянии человеческого фактора свидетельствуют и выводы работы [55], где отмечается наличие небезопасных практик, таких как использование личных устройств на судовых системах, обращение к подозрительным веб-сайтам и обмен между судоводителями конфиденциальной информацией через социальные сети. Съемные носители сторонних производителей также применяются без предварительного их сканирования, что подвергает риску судовые системы.

Нормативная база обеспечения кибербезопасности

Судя по публикациям, борьба с киберугрозами развернулась в начале третьего тысячелетия, и первые 10-15 лет разработчики соответствующей аппаратуры, оставаясь наедине со своими проблемами, всякий раз принимали решения, эффективность которых можно было оценить лишь путем анализа практики их применения. Об унификации подходов к обеспечению кибербезопасности речь даже не шла.

Первыми, кто рискнул навести хоть какой-то порядок в решении обсуждаемой проблемы, оказались, как ни странно, представители не структур IMO, а эксплуатирующего суда сообщества во главе с Балтийским и Международным морским советом (Baltic and International Maritime Council – BIMCO), который в сотрудничестве с Международной ассоциацией круизных линий (Cruise Lines International Association), Международной палатой судоходства (International Chamber of Shipping), а также ассоциациями Intercargo и Intertanko выпустил в 2016 г. отраслевое «Руководство по кибербезопасности на борту судов» (The Guidelines on Cyber Security onboard Ships) [61]. Версия 2 этого документа увидела свет в июле 2017 г., версия 3 – в декабре 2018 г., а версия 4 – в декабре 2020 г.

Документ этот [62] направлен на повышение уровня охраны и безопасности моряков, окружающей среды, грузов и судов. Цель его – оказание помощи в разработке надлежащей стратегии управления киберрисками в соответствии с передовой практикой действий на борту судна и акцентом на рабочие процессы, оборудование, обучение, реагирование на инциденты и контроль за восстановлением отказов. Объясняется, почему и как следует действовать при наличии киберугроз в контексте судоходства. Приводится список сопроводительной документации, необходимой для проведения оценки рисков, и описывается сам этот процесс с объяснением роли, которую играет каждый компонент киберриска. Подчеркивается важность при проведении анализа киберрисков оценки как их вероятности, так и самой угрозы, а также возможного воздействия и соответствующих уязвимостей. Содержатся советы о том, как реагировать на киберинциденты и восстанавливаться после них.

В июне 2017 г. IMO публикует резолюцию MSC.428(98) «Управление морскими киберрисками в системах управления кибербезопасностью» (Maritime Cyber Risk Management in Safety Management Systems), базирующуюся на документе MSC-FAL.1/Circ.3 «Руководство по управлению рисками в киберпространстве на море» (Guidelines on Maritime Cyber Risk Management), который утвержден Комитетом по безопасности на море (Maritime Safety Committee) и Комитетом по упрощению формальностей (Facilitation Committee), и учитывающую требования Международного кодекса по управлению безопасностью (International Safety Management Code) [63, 54].

Согласно резолюции, киберриски должны надлежащим образом учитываться в системах управления безопасностью судоходных компаний, и контроль за ними на

борту судов является обязательным с 1 января 2021 г. [64]. Резолюция подтверждает, что существующая практика управления рисками должна использоваться для устранения операционных угроз, возникающих в результате возросшей зависимости от различных операций, основанных на цифровой обработке данных, а также использования в судовом пространстве ИТ и ОТ.

Одновременно IMO объявило, что:

1) с 1 января 2021 г. требования к кибербезопасности будут внесены в главу IX Международной конвенции по охране человеческой жизни на море (International Convention for the Safety of Life at Sea), правила 1–6 «Управление безопасной эксплуатацией судов» [65];
2) Международная электротехническая комиссия (International Electrotechnical Commission) в сотрудничестве с ИМО готовит новый морской стандарт для морского навигационного оборудования и систем радиосвязи IEC 63154 «Кибербезопасность – общие требования, методы тестирования и требуемые результаты испытаний» (Cybersecurity – General Requirements, Methods of Testing and Required Test Results) [17], что и было реализовано в 2021 г.

Важную роль в организации борьбы с киберугрозами сыграли выпущенные в 2020 г. Международной ассоциацией классификационных обществ (International Association of Classification Societies) «Рекомендации по обеспечению киберустойчивости» (Recommendation on Cyber Resilience), известные как рекомендации №166 [66]. Цель этого документа состоит в том, чтобы сообщить заинтересованным сторонам технические требования, позволяющие проектировать и поставлять суда, чья киберустойчивость может поддерживаться на протяжении всего срока их службы.

Киберустойчивость в документе понимается как характеристика, которая предоставляет экипажу и судну в целом возможность эффективно справляться с киберинцидентами, происходящими в компьютерных системах на борту. Наиболее эффективным методом борьбы с инцидентом является предотвращение его возникновения, поэтому в данном контексте оно даже важнее, чем «лечение». Сами рекомендации направлены на обеспечение того, чтобы проектирование, интеграция и/или обслуживание компьютерных систем поддерживали безопасную эксплуатацию и гарантировали защиту от несанкционированного доступа, неправомерного применения, изменения, уничтожения или ненадлежащего раскрытия информации, генерируемой, архивируемой или задействованной в бортовых компьютерных системах или передаваемой в сетях, соединяющих такие системы.

Ряд документов, определяющих требования к разработке процедур для борьбы с киберугрозами, выпущен в США. И первым был «Циркуляр по навигации и инспекции судов» (Navigation and Vessel Inspection Circular) 2020 г. с подзаголовком: «Руководство по устранению киберрисков на объектах, регулируемых Законом о безопасности морского транспорта» (Guidelines for Addressing Cyber Risks at Maritime Eransportation Security Act (MTSA) Regulated Facilities) [67]. Примечательно, что, согласно циркуляру, если управление киберрисками после 1 января 2021 г. не было включено в систему контроля за безопасностью судна, то оно может быть задержано в порту с требованием проведения в течение 3 месяцев внешнего аудита.

В январе 2021 г. США опубликовали «Национальный план морской кибербезопасности» (National Maritime Cybersecurity Plan to the National Strategy for Maritime Security) [68]. Он содержит три основных раздела:

1) «Риски и стандарты»;
2) «Обмен информацией и разведданными» с заинтересованными неправительственными организациями;
3) «Создание рабочей силы в области кибербезопасности на море».

В нем подробно описаны первоочередные действия, которые необходимо предпринять для развития каждого компонента. При этом было заявлено, что план знаменует наличие пробелов в обеспечении морской безопасности США и одной из первых задач будет создание стандартов кибербезопасности морской транспортной системы.

Самым значимым документом последних лет, выпущенных под эгидой IMO, является версия 2022 г. «Руководства по управлению рисками в киберпространстве на море» [70].

Под управлением киберрисками здесь понимается процесс выявления, анализа, оценки и информирования об угрозе, связанной с киберпространством, а также предотвращения или смягчения ее до приемлемого уровня с учетом затрат и выгод от действий, предпринимаемых заинтересованными сторонами. Одним из общепринятых подходов к достижению вышеизложенного является всесторонняя оценка и сравнение текущих и желаемых позиций организации в области управления киберрисками.

Считается целесообразным включение в структуру управления рисками следующих процедур, выполняемых параллельно и непрерывно:

1) определение роли и обязанностей персонала по управлению киберрисками, а также выявление систем, активов, данных и возможностей, которые в случае сбоя создают угрозы для выполняемых на судне операций;
2) внедрение процессов и мер по контролю рисков, а также планирование действий для защиты от киберсобытий на случай непредвиденных обстоятельств;
3) разработка и осуществление мероприятий, необходимых для своевременного обнаружения киберсобытий;
4) подготовка и реализация мероприятий по обеспечению устойчивости и восстановлению систем, нарушенных в результате киберсобытия;
5) определение мер по резервному копированию и, в случае необходимости, восстановлению киберсистем, необходимых для выполнения операций, затронутых киберсобытием.

Существенно, что в п.2.2.3 руководства отмечается: приводимые в нем положения по управлению киберрисками носят рекомендательный характер. Это означает лишь одно – на настоящий момент структуры IMO не могут постулировать конкретные требования к системам управления киберрисками, задаваемые числом и мерой, и судоводитель, столкнувшийся с кибератакой, оказывается, по сути дела, один на один с выявленной проблемой.

Кибербезопасность в России

«В России морская информационная безопасность не является актуальной темой для отрасли. Русскоязычных публикаций на эту тему практически нет, осведомленность находится в среднем на рудиментарном уровне». Это цитата из статьи начальника ФБУ «Служба морской безопасности», опубликованной на сайте Российского совета по международным делам в сентябре 2020 г. [6]. По мнению автора, на тот момент в Российской Федерации не существовало специального нормативного пра-

вового регулирования информационной безопасности на море, этот вопрос не рассматривался и в доктринальных документах (например, в «Морской доктрине РФ»). Правительство Российской Федерации также не наделяло Росморречфлот полномочиями в области обеспечения информационной безопасности на море.

Однако было невозможно не откликнуться на упомянутую выше резолюцию IMO MSC.428(98), требующую наличия с 1 января 2021 г. хоть каких-нибудь подтверждений о существовании на борту судов внедренных процедур по борьбе с киберугрозами. В связи с этим в конце 2020 г. Российский морской регистр судоходства подготовил «Руководство по обеспечению кибербезопасности», ориентированное на реализацию положений резолюции [71]. Оно было призвано подсказать, как составить план обеспечения кибербезопасности судна, который описывает потенциальные уязвимости существующих систем, имеющиеся риски, оценки последствий и меры по их минимизации, включая подготовку персонала. Увы, этот документ, как и все прочие рассмотренные ранее, не регламентирует, какое именно оборудование или технические решения следует применять для борьбы с конкретными типами рисков.

В какой-то мере решению обсуждаемой проблемы способствует утверждение в июле 2021 г. «Стратегии национальной безопасности Российской Федерации», в которой четвертым по значимости стратегическим национальным приоритетом обозначена информационная безопасность [72]. Хотя информационной безопасности транспортной отрасли, и в том числе морской, стратегия отдельного внимания не уделяет, часть сформулированных в ней задач актуальна и для морского транспорта, включая развитие системы прогнозирования, выявления и предупреждения угроз, определения их источников и оперативной их ликвидации.

Тем не менее очевидно, что без выпуска специального документа, регламентирующего порядок и средства борьбы с киберугрозами именно на морском транспорте, решение означенной проблемы в РФ будет непростым.

Заключение

Подводя итоги, можно сделать следующие выводы.

1. Борьба с киберугрозами применительно к морской навигации находится на начальной стадии, что, впрочем, неудивительно, так как на законодательном уровне она была инициирована лишь в январе 2021 г.
2. Повышение уровня цифровизации процесса судовождения приводит к росту проблем, связанных с кибербезопасностью. Можно предположить, что при реализации «Стратегического плана внедрения е-Навигации» [73], основанного в том числе на тотальном применении Интернет-процедур и спутниковой связи, положение усугубится.
3. Аналогичная ситуация имеет место и по мере развития беспилотных судов до судов-автоматов, что сопровождается не только усложнением киберобстановки в связи с отсутствием на борту экипажа, имеющего возможность оперативно отвечать на кибератаки, но и изменением спектра киберугроз. Последнее потребует от разработчиков навигационной аппаратуры гибкого реагирования на изменяющиеся внешние воздействия.

ЛИТЕРАТУРА

1. **The Review of Maritime Transport** [Электронный ресурс]. URL: https://unctad.org/system/files/official-document/rmt2017_en.pdf (дата обращения: 16.01.2024).
2. **Cyber-enabled ships**, Lloyd's Register, 2016.
3. **Fosen, J.,** Cyber Security Awareness in the Maritime Industry, January 2019. [Электронный ресурс]. URL: https://www.gard.no/Content/25634225/Cyber%20Security_Presentation%20(ID%201418279).pdf (дата обращения: 15.01.2024).
4. **Cyber security threats in maritime industry**, DNV, 2019.
5. **Akpan, F., Bendiab, G., Shiaeles, S., et al**., Cybersecurity challenges in the maritime sector, Network, 2022, 2(1), pp. 123–138, doi:10.3390/network2010009.
6. **Семенов С.** Морская кибербезопасность – ситуация, проблемы и риски [Электронный ресурс] // Российский совет по международным делам» (НП РСМД). URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/morskaya-kiberbezopasnost-situatsiya-problemy-i-riski/ (дата обращения: 16.01.2024).
7. **Roberts, F.S., Egan, D., Nelson, C., and Whytlaw, R.,** Combined cyber and physical attacks on the maritime transportation system, *NMIOTC Marit. Interdiction Oper. J.*, 2019, 18, 22.
8. **Cohen, Z.** US Navy ship collides with South Korean fishing boat [Электронный ресурс], *CNN*, 2024. URL: https://edition.cnn.com/2017/05/09/politics/fishing-vessel-hits-us-navy-ship-south-korea/index.html (дата обращения: 18.01.2024).
9. **The Guidelines on Cyber Security Onboard Ships**. Version 3 [Электронный ресурс]. URL: https://safety4sea.com/wp-content/uploads/2018/12/BIMCO-Guidelines-on-cyber-security-onboard-ships-2018_12.pdf (дата обращения: 19.01.2024)
10. **Al-Mhiqani, M.N., Ahmad, R., Yassin, W., Hassan, A., Abidin, Z.Z., Ali, N.S., and Abdul-kareem, K.H.,** Cyber-security incidents: A review cases in cyber-physical systems, *Int. J. Adv. Comput. Sci. Appl*., 2018, 1, 499–508.
11. **Andersen, I.,** The 10 Most Common Types of Cyber Security Attacks Today 3 [Электронный ресурс]. May 15, 2018. URL: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/ (дата обращения: 16.01.2024).
12. **The Guidelines on Cyber Security Onboard Ships.** Version 4 [Электронный ресурс]. URL: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships (дата обращения: 13.01.2024).
13. **Mednikarov, B., Tsonev Y., and Lazarov, A.,** Analysis of cybersecurity issues in the maritime industry, *Information & Security*, 2020, vol. 47, no. 1, pp. 27–43, doi: 10.11610/isij.4702.
14. **Yevgen Dyryavyy**, Preparing for Cyber Battleships – Electronic Chart Display and Information System Security [Электронный ресурс], 2014. URL: https://research.nccgroup.com/wp-content/uploads/2020/07/2014-03-03_-_ncc_group_-_whitepaper_-_cyber_battle_ship_v1-0.pdf (дата обращения: 13.01.2024).
15. **Svilicic, B., Brčić, D., Žuškin, S., and Brčić, D.,** Raising awareness on cyber security of ECDIS, TransNav the Int., *J. on Marine Navigation and Safety of Sea Transportation*, 2019, 13(1), pp. 231–236, doi:10.12716/1001.13.01.24
16. **'Petya' ransomware attack:** what is it and how can it be stopped? [Электронный ресурс], *The Guardian*, 2017. URL: https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how (дата обращения: 17.01.2024).
17. **Svilicic, B., Kristić, M., Žuškin, S., and Brčić, D.** Paperless ship navigation: Cyber security weaknesses, Journal of Transportation Security, 2020, 13, pp. 203–214. https://doi.org/10.1007/s12198-020-00222-2.
18. **Revised guidelines** for onboard operational use of AIS (safety4sea.com) [Электронный ресурс]. URL: https://safety4sea.com/revised-guidelines-for-the-onboard-operational-use-of-shipboard-ais/ (дата обращения: 16.01.2024).
19. **Botunac Ive,** Analysis of software threats to the automatic identification system, *Brodogradnja*, 2017, 68(1), pp. 97–105, doi:10.21278/brod68106.
20. **Kessler, G., Craiger, P., and Haass, J.,** A taxonomy framework for maritime cybersecurity: a demonstration using the automatic identification system, *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 2018, 12(3), pp. 429–437, doi:10.12716/1001.12.03.01.
21. **Strohmeier, M., Lenders, V., & Martinovic, I.,** On the Security of the Automatic Dependent Surveillance // Broadcast Protocol, IEEE Communications Surveys & Tutorials, 2015, 17(2), pp. 1066–1087.
22. **Balduzzi, M., Pasta, A. and Wilhoit, K.,** A security evaluation of AIS automated identification system, *Proc. 30th Annual Computer Security Applications Conference*, New Orleans, 2014, pp. 436–445.

23. **Gallagher, S.,** Hacked at sea: Researchers find ships' data recorders vulnerable to attack [Электронный ресурс]. URL: https://arstechnica.com/information-technology/2015/12/hacked-at-sea-researchers-find-ships-data-recorders-vulnerable-to-attack/ (дата обращения: 16.01.2024).
24. **Anand, N.,** Voyage Data Recorder of Prabhu Daya may have been tampered with [Электронный ресурс]. URL: http://www.thehindu.com/news/national/tamil-nadu/voyage-data-recorder-of-prabhu-daya-may-have-been-tampered-with/article2982183.ece (дата обращения: 16.01.2024).
25. **Soner, O., Kayişoğlu, G., Bolat, P.Y., and Tam, K.,** Cybersecurity risk assessment of VDR, *Journal of Navigation*, 2023, 1–18. https://doi.org/10.1017/S0373463322000595.
26. **Lund, M.S., Gulland, J.E., Hareide, O.S., Jøsok, Ø., and Weum, K.O.C.,** Integrity of Integrated Navigation Systems, *IEEE Conference on Communications and Network Security (CNS)*, 2018, doi:10.1109/CNS.2018.8433151.
27. **Resolution MSC.252(83):** Adoption of the Revised Performance Standard for Integrated Navigation Systems (INS), International Maritime Organization (IMO), 2007.
28. **Shim, K.-A.,** A survey of public-key cryptographic primitives in wireless sensor networks, *IEEE Commun. Surveys Tuts.*, 2016, vol. 18, no. 1, pp. 577–601.
29. **Svilicic, B., Rudan, I., Jugović, A., and Zec, D.,** Security threats in a shipboard integrated navigational system, *Journal of Marine Science and Engineering*, 2019, 7(10):364, doi:10.3390/jmse7100364.
30. **Hareide, O.S., Jøsok, Ø., Lund, M.S., Ostnes, R., and Helkala, K.M.,** Enhancing navigator competence by demonstrating maritime cyber security, *Journal of Navigation,* 2018, 71 (5), pp. 1025–1039, doi: 10.1017/S0373463318000164.
31. **Hutchins, E.M., Cloppert, M.J., & Amin, R.M.,** Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, *Leading Issues in Information Warfare & Security Research*, 2011, 1, 80.
32. **Kavallieratos, G., Katsikas, S., and Gkioulos, V.**, Cyber-attacks against the autonomous ship, *in Katsikas, S., et al., Computer Security. SECPRE CyberICPS 2018, Lecture Notes in Computer Science*, 2019, vol. 11387, Springer, Cham, https://doi.org/10.1007/978-3-030-12786-2_2.
33. **Shostack, A.,** *Threat Modeling: Designing for Security*, 1st edn, Wiley, Hoboken, 2014.
34. **Silverajan, B., Ocak, M., and Nagel, B.,** Cybersecurity attacks and defences for unmanned smart ships, I*EEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, doi:10.1109/cybermatics_2018.2018.00037
35. **Santamarta, R.,** Maritime Security: Hacking into Voyage [Электронный ресурс]. URL: https://blog.ioactive.com/2015/12/maritime-security-hacking-into-voyage.html (дата обращения: 19.01.2024).
36. **Hammerschmidt, Ch.,** CAN FD vulnerability threatens vehicle security [Электронный ресурс]. URL: https://www.eenewseurope.com/en/can-fd-vulnerability-threatens-vehicle-security/ (дата обращения: 19.01.2024).
37. **Bosnjak, R., Simunovic, L., and Kavran, Z.,** Automatic Identification System in Maritime Traffic and Error Analysis, *Transactions on Maritime Science*, 2012, 1(02), pp. 77–84.
38. **Zhou, X., Liu, Z., Wu, Z., and Wang, F.,** Quantitative processing of situation awareness for autonomous ships navigation, *TransNav Int J Mar Navig Saf Sea Transport*, 2019, 13 (1), pp. 25–31. doi:10.12716/1001.13.01.01.
39. **Wróbel, K., Montewka, J., and Kujala, P.,** Towards the development of a system-theoretic model for safety assessment of autonomous merchant vessels, *Reliability Engineering & System Safety*, 2018, vol. 178, pp. 209–224, doi:10.1016/j.ress.2018.05.019.
40. **Endsley, M.R**., Toward a theory of situation awareness in dynamic systems, *Human factors*, 1995, vol. 37, pp. 32–64, doi: 10.1518/001872095779049543.
41. **Taylor, R.M.,** Situational awareness rating technique (SART): The development of a tool for aircrew systems design, *Situational Awareness, Routledge*, 2017, pp.111–128, doi:10.4324/9781315087924-8.
42. **Wróbel, K., Montewka, J., and Kujala, P.,** System-theoretic approach to safety of remotely-controlled merchant vessel, *Ocean Engineering*, 2018, vol. 152, pp. 334–345, doi: 10.1016/j.oceaneng.2018.01.020.
43. **Zhou, X., Liu, Z., Wang, F., and Ni, S.,** Collision risk identification of autonomous ships based on the synergy ship domain, *Chinese Control and Decision Conference (CCDC)*, 2018, pp. 6746–6752, doi:10.1109/CCDC.2018.8408320.
44. **Silverajan, B., Ocak, M., and Nagel, B.,** Cybersecurity attacks and defences for unmanned smart ships, Proc. I*EEE Int. Conf. on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Compu-ting (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada, 30 July–3 August 2018, pp. 15–20.
45. **Zhou, X., Liu, Z., Wu, Z., and Wang, F.,** Quantitative processing of situation awareness for autonomous ships navigation, *Int. J. Mar. Navig. Saf. Sea Transp.*, 2019, 13, 25–31.

46. **Bechtsis, D., Tsolakis, N., Bizakis, A., and Vlachos, D.,** A blockchain framework for contain-erized food supply chains, *Computer Aided Chemical Engineering*, Elsevier: Amsterdam, The Netherlands, 2019, vol. 46, pp. 1369–1374, doi:10.1016/B978-0-12-818634-3.50229-0.
47. **Wullems, C., Pozzobon, O., and Kubik, K.,** Signal authentication and integrity schemes for next generation global navigation satellite systems, *European Navigation Conference (ENC-GNSS)*, 2005, 2005-07-19–2005-07-22.
48. **Caparra, G., Sturaro, S., Laurenti, N., Wullems, C., and Ioannides, R.T.,** A novel navigation message authentication scheme for GNSS open service, P*roc. 29th Int. Tech. Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, Portland, OR, USA, 12–16 September 2016, pp. 2938–2947, doi:10.33012/2016.14692.
49. **Reddy, G.N. and Reddy, G.,** A study of cybersecurity challenges and its emerging trends on latest technologies, *arXiv*, 2014, 1402.1842.
50. **Bour, G., Bernsmed, K., Borgaonkar, R., and Meland, P.H.**, On the Certificate Revocation Problem in the Maritime Sector, i*n Asplund, M., Nadjm-Tehrani, S. (eds) Secure IT Sys-tems. NordSec 2020. Lecture Notes in Computer Science*, 2021, vol. 12556, Springer, Cham., https://doi.org/10.1007/978-3-030-70852-8_9.
51. **Pseftelis, T. and Chondrokoukis, G.,** A Study about the role of the human factor in maritime cybersecurity, *SPOUDAI Journal of Economics and Business*, 2021, vol. 71, no. 1–2, pp. 55–72.
52. **Exercise Neptune:** Maritime Cybersecurity training using the Navigational Simulators [Электронный ресурс]. URL: https://www.researchgate.net/publication/338753306_Exercise_Neptune_Maritime_Cybersecurity_training_using_the_Navigational_Simulators (дата обращения: 17.01.2024).
53. **Heering, D. and Lovell, K.N.,** Exercise Neptune: Maritime cybersecurity training using the navigational simulators, *5th Interdisciplinary Cyber Research Conference*, Tallinn, Estonia, 2019 [Электронный ресурс]. URL: https://www.researchgate.net/publication/338753306_Exercise_Neptune_Maritime_Cybersecurity_training_using_the_Navigational_Simulators.
54. **Caprolu, M., DiPietro, R., Raponi, S., Sciancalepore, S., and Tedeschi, P.,** Vessels Cyber-security: Issues, Challenges, and the Road Ahead, *IEEE Communications Magazine*, 2020, 58 (6): 90–96.
55. **Kamlesh Kanwal, Wenming Shi, Christos Kontovas, Zaili Yang, & Chia-Hsun Chang**, Maritime cybersecurity: are onboard systems ready? [Электронный ресурс], *Maritime Policy & Management*, 16 Sep 2022, doi: 10.1080/03088839.2022.2124464. URL: https://www.tandfonline.com/doi/full/10.1080/03088839.2022.2124464 (дата обращения: 17.01.2024).
56. **Wu, Z., Pan, Q., Yue, M., Ma, S.,** An Approach of Security Protection for VSAT Network, *17th IEEE International Conference On Trust, Security and Privacy in Computing and Communications, 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*, New York, NY, USA, 1–3 August 2018, pp. 1511–1516.
57. **Maritime Security:** Hacking into a Voyage Data Recorder (VDR) [Электронный ресурс]. URL: https://ioactive.com/maritime-security-hacking-into-a-voyage-data-recorder-vdr/ (дата доступа 16.01.2024).
58. **Heffner, C.,** Exploiting network surveillance cameras like a Hollywood hacker [Электронный ресурс]. URL: https://privacy-pc.com/articles/exploiting-network-surveillance-cameras-like-a-hollywood-hacker.html (дата доступа 16.01.2024).
59. **Ben Farah, M.A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., Bellekens, X.,** Cybersecurity in the maritime industry: A systematic survey of recent advances and future trends, *Information*, 2022, 13, 22, Article 22, https://doi.org/103390/info13010022.
60. **Bugeja, J., Jönsson, D., Jacobsson, A.,** An investigation of vulnerabilities in smart connected cameras, *Proceedings of the 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Athens, Greece, 19–23 March 2018, pp. 537–542, doi:10.1109/PERCOMW.2018.8480184.
61. **The Guidelines on Cyber Security onboard Ships** (05 October 2023). [Электронный ресурс]. URL: https://www.intercargo.org/guidelines-cyber-security-onboard-ships/ (дата обращения: 18.01.2024).
62. **The Guidelines on Cyber Security onboard Ships**, Version 4, December 2020 [Электронный ресурс]. URL: https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf (дата обращения: 17.01.2024).
63. **Maritime cyber risk management in safety management systems** (RESOLUTION MSC.428(98), 16 June 2017) [Электронный ресурс]. URL: https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428(98).pdf (дата обращения: 17.01.2024).
64. **Ahvenjärvi, S., Czarnowski, I., Kåla, J., Kyster, A., Meyer, I., Mogensen, J., Szyman, P.,** Safe information exchange on board of the ship, *TransNav: International Journal on Marine Naviga-tion and Safety of Sea Transportation*, 2019, vol. 13, no. 1, doi: 10.12716/1001.13.01.17 [Электронный ресурс]. URL: https://paperity.org/p/275182587/safe-information-exchange-on-board-of-the-ship (дата обращения: 17.01.2024).

65. **Dean, M.,** New ECDIS Cyber Security Regulations & Requirements [Электронный ресурс], Feb 08, 2020. URL: https://www.amnautical.com/es/blogs/news/keep-ecdis-secure-with-software-updates (дата обращения: 19.01.2024).
66. **NaviSailot 4000** ECDIS Overview Brochure [Электронный ресурс]. URL: https://static.mackaycomm.com/wp-con-tent/uploads/2021/08/Transas_ECDIS_NaviSailor_4000_Summary_Dec11_Mackay_v01HR.pdf.
67. **Recommendation on Cyber Resilience No. 166** (Apr 2020) [Электронный ресурс]. URL: https://www.steamshipmutual.com/sites/default/files/downloads/articles/2020/IACS-Recommendation-on-Cyber-resilience-No-166-2020_04.pdf (дата обращения: 18.01.2024).
68. **Cybersecurity for the maritime industry** [Электронный ресурс]. URL: https://www.maritime-cybersecurity.com/ (дата обращения: 18.01.2024).
69. **National Maritime Cybersecurity Plan Released** [Электронный ресурс]. Vincent Milano, Jan 12, 2021. URL: https://www.hsdl.org/c/national-maritime-cybersecurity-plan-released/ (дата обращения: 17.01.2024).
70. **Guidelines on maritime cyber risk management MSC-FAL.1/Circ.3/Rev.**1 [Электронный ресурс]. 14 June 2021. URL: https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf (дата обращения: 19.01.2024).
71. **Афонин А.** Кибербезопасность в судоходстве. Актуальные вызовы. [Электронный ресурс]. 2021. URL: https://www.korabel.ru/news/comments/kiberbezopasnost_v_sudohodstve_aktualnye_vyzovy.html (дата обращения: 19.01.2024).
72. **Семенов С.** Морские вести России [Электронный ресурс] // Морская кибербезопасность. Новое в 2021 году. URL: https://morvesti.ru/analitika/1692/92320/ (дата обращения: 19.01.2024).
73. **Ривкин Б.С.** е-Навигации – десять лет // Гироскопия и навигация. 2015. №4. С. 173–191. 10.17285/0869-7035.2015.23.4.173-191.

Rivkin, B.S. (Concern CSRI Elektropribor, JSC, St. Petersburg, Russia)
Maritime Cybersecurity. Navigational Aspect, *Giroskopiya i Navigatsiya*, 2023, vol. 31, no. 4 (123), pp. 167–191.

Abstract. This article is a review of publications on maritime cybersecurity with the focus made on navigation support. Cyber threats to ECDIS, automatic identification system (AIS), voyage data recorder, and integrated navigation system as a whole are considered. The specific features of cybersecurity of maritime autonomous surface ships (MASS) as well as the impact of the human factor on cybersecurity are discussed, and the regulatory framework for preventing cyber threats is analyzed.

Key words: cybersecurity, ECDIS, AIS, voyage data recorder, integrated navigation system, MASS, human factor, International Maritime Organization.

Материал поступил 10.10.2023