Кибербезопасность морского и речного транспорта

С. А. Семёнов,
начальник ФБУ «Служба морской безопасности»

Сегодня информационная безопасность водного транспорта характеризуется избыточным административно-правовым регулированием. Для решения проблемы необходима дальнейшая гармонизация международного и российского законодательства в этой сфере, а также положений, принятых в разных институтах российского права.

Транспортировка грузов морским транспортом составляют 90% объема международных перевозок **[1]**. В наши дни общемировой тенденцией стала прогрессирующая цифровизация экономики, что в полной мере касается морского и речного транспорта. Суда увеличиваются, а команды уменьшаются вследствие все большей автоматизации процессов. Некоторые бортовые системы получают обновления во время плавания, у команд есть выход в Интернет.

По мнению ряда специалистов, вопросам информационной безопасности объектов морской и речной транспортной инфраструктуры, морских и речных судов уделяется крайне мало внимания **[2]**. Это легко проверить на сайтах отечественных компаний, предоставляющих услуги и производящих продукты и решения для морского и речного транспорта. Как правило, в описании услуг, продуктов и решений вопросы информационной безопасности не затрагиваются. В лучшем случае упоминается возможность разграничения доступа с помощью паролей и логинов или использование сетевых экранов.

Ситуация в сфере кибербезопасности

Согласно отчету ENISA, озадаченность вопросами кибербезопасности в морском секторе находится на низком уровне либо вовсе не наблюдается **[3, 4]**. Недостаточную обеспокоенность вопросами, связанными с киберугрозами, отмечают и аналитики компании CyberKeel, специализирующейся на безопасности морской индустрии. Они отмечают, что многие из занятых в морской сфере привыкли быть частью «практически невидимой» отрасли, незаметной обывателю **[3]**.

В отчете Allianz о безопасности судоходства за 2015 г. **[4]** говорится, что подверженность кибератакам (помимо утраты данных) растет. Отмечен ряд серьезных киберинцидентов, и развитие технологий, включая Интернет и электронную навигацию, означает, что в распоряжении специалистов отрасли всего несколько лет, чтобы подготовиться к риску утраты судов в результате кибератак. «Пираты уже злоупотребляют наличием прорех в системе кибербезопаности для планирования кражи конкретных грузов», — сказал капитан Эндрю Кинси, старший консультант по морским рискам AGCS. При этом не стоит переоценивать значение кибератак: «Нельзя же взломать секстант».

Сотрудники компании Positive Technologies к основным специфическим для морского транспорта информационным системам и технологиям относят:

- Automatic Identification System (AIS) — автоматическую идентификационную систему;
- Electronic Chart Display and Information System (ECDIS) — электронно-картографическую навигационно-информационную систему; до 2019 г. ECDIS должны быть установлены на всех судах;
- Voyage Data Recorder (VDR) — регистратор данных рейса;
- Terminal Operating System (TOS) — IT-инфраструктуру, служащую целям автоматизации процессов, происходящих с грузами в порту; на практике бывает целостным продуктом конкретного вендора или совокупностью систем (возможно, и широкого назначения), выполняющих различные задачи;
- Container Tracking System (CTS) — систему, позволяющую отслеживать движение контейнеров посредством GPS и (реже) других каналов передачи данных;

Документы по кибербезопасности, принятые в 2017 г.

Название документа (оригинал)	Дата принятия	Название документа (перевод)
GUIDELINES ON MARITIME CYBER RISK MANAGEMENT Annex 1 (Report of the FAL on its 41st session – FAL 41/17) **[7]** On Guidelines on maritime cyber risk management, superseding the interim guidelines cjntained in MSC.1/ Circ.1526	07.04.2017	Рекомендации по управлению киберрисками в морской отрасли. Приложение № 1 отчета о работе Комитета по упрощению формальностей (ФАЛ) на 41-й сессии – документ ФАЛ 41/17) О новой редакции Рекомендаций по управлению морскими киберрисками, заменяющей предыдущую редакцию, которая дана в циркуляре MSC.1/Circ.1526
MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS Resolution MSC.428(98) Annex 10 (Report of the MSC jn ins 98-th session – MSC 98/23/Add.1) **[8]**	30.06.2017	Управление киберрисками в системах управления безопасности морской отрасли. Резолюция (КБМ) MSC.428(98) Приложение № 10 отчета о работе КБМ на 98-й сессии – документ MSC 98/23/Add.1
GUIDELINES ON MARITIME CYBER RISK MANAGEMENT (MSC-FAL.1/Circ.3) **[9]** (см. п. 12 Литературы)	05.07.2017	Рекомендации по управлению киберрисками в морской отрасли. Циркуляр КБМ-ФАЛ (MSC-FAL.1/Circ.3)
THE GUIDELINES ON CYBER SECURITY ONDOARD SHIPS (Version 2.0) **[10]** Produced and supported by the world leading shipping compaines.	05.07.2017	Рекомендации по кибербезопасности на судах (Редакция 2.0). Разработаны и поддерживаются мировыми судоходными компаниями.

• Emergency Position Indicating Radio Beacon (EPIRB) — аварийный радиобуй, передатчик, подающий при активации сигнал бедствия; в зависимости от технологии исполнения, передача сигнала может осуществляться через спутник, в диапазоне УКВ или же комбинированно; некоторые EPIRB кроме сигнала бедствия могут передавать информацию о судне (при синхронизации с AIS).

Каждая из приведенных систем так или иначе уязвима в плане информационной безопасности **[5]**.

Результаты исследования безопасности AIS, проведенного сотрудниками компании Trend Micro, были представлены на конференции Black Hat Asia 2014. Предложены следующие возможные сценарии нарушения безопасности:

• изменение данных о судне, включая его местоположение, курс, информацию о грузе, скорость и имя;

• создание «кораблей-призраков», опознаваемых другими судами как настоящее судно, в любой локации мира;

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

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

• «превращение» существующего судна в невидимое;

• создание несуществующих поисково-спасательных вертолетов;

• фальсификация сигналов EPIRB, активирующих тревогу на находящихся поблизости судах;

• проведение DoS-атаки на всю систему путем инициирования увеличения частоты передачи AIS-сообщений.

Морская индустрия активно использует спутниковые технологии Satellite Communications (SATCOM) для доступа в Интернет, связи судно – судно и судно – суша, GPS/DGPS для определения местоположения и навигации, а также отслеживания перевозимых грузов.

На конференции Black Hat USA 2015 сотрудник компании Synack K. Myp представил отчет о безопасности систем GPS-трекинга Globalstar. Вследствие уязвимости систем можно осуществить перехват и подмену информации или глушение сигнала. В сети Simplex, основанной на радиопередаче, которую компания Globalstar использует для передачи данных между трекерами, спутниками и наземными станциями, не предусмотрены механизмы аутентификации и шифрования, невозможна валидация переданных данных. Мур уверен, что такая проблема отмечается не только в Globalstar.

В отчете IOActive сообщается, что спутниковые системы (SATCOM), в частности связывающие через Интернет суда друг с другом и с «большой землей», также весьма уязвимы. При проверке терминалов спутниковой связи, используемых в судоходстве, выявлены такие критические бреши в безопасности, как использование устройствами незащищенных или даже недокументированных протоколов, заведенные «фабрично» учетные записи, возможность эксплуатирования функции сброса пароля, бэкдоры.

Показательный случай компрометации спутниковых систем произошел в июле 2013 г. Студенты Техасского университета смогли отклонить от курса яхту стоимостью 80 млн долл. с помощью оборудования, цена которого не превышала 3 тыс долл. Дублируя сигнал настоящего спутника с помощью имитатора GPS-сигналов (используются, к примеру, при калибровке оборудования) и постепенно повышая мощность, они смогли «убедить» навигационную систему судна принимать сообщения спуфингового устройства и отбрасывать сигнал настоящего спутника как помехи. После того как навигационная система начала ориентироваться по данным двух спутников и атакующего устройства, судно удалось отклонить от первоначального курса **[6]**.

Требования Международной морской организации

С учетом сложившейся в сфере информационной безопасности ситуации Международная морская организация (ИМО) в 2017 г. разработала и приняла ряд документов по кибербезопасности в морской отрасли (*таблица*).

Приложение № 10 Резолюции (КБМ) MSC.428(98) настоятельно рекомендует администрациям обеспечить надлежащее рассмотрение киберрисков в системах управления безопасностью не позднее первой ежегодной верификации Документа о соответствии компании после 1 января 2021 г.

В Рекомендациях по управлению киберрисками в морской отрасли (далее Рекомендации) отмечается, что кибертехнологии стали необходимыми для эксплуатации и управления множеством систем, важных для безопасности судоходства и защиты морской окружающей среды. Однако вследствие уязвимости, создаваемой доступом, соединением или сетевым подключением этих систем, могут появиться киберугрозы, которые необходимо устранять.

Рекомендации определяют морские киберугрозы как риски технологическому ресурсу со стороны потенциальных обстоятельств или событий, которые могут привести к сбоям в перевозке грузов и пассажиров, безопасности мореплавания или безопасности судна, в связи с повреждением, утратой или компрометацией связанных с судоходством информации или систем. Риски могут быть обусловлены уязвимостью, связанной с неадекватной работой, интеграцией, обслуживанием и разработкой киберсистем, а также преднамеренными и непреднамеренными киберугрозами.

Угрозы представляют собой вредоносные действия (например, взлом или внедрение вредоносных программ) или непреднамеренные последствия доброкачественных действий (например, обслуживания программного обеспечения или разрешения пользователя). Как правило, эти действия приводят к уязвимости (например, устаревшее программное обеспечение или неэффективные брандмауэры) или используют уязвимость в операционной или информационной технологии.

В Рекомендациях указано, что уязвимые судовые системы могут включать (но не ограничиваются указанным):

- системы ходового мостика;
- системы обработки и управления грузом;
- системы управления двигателями, машинами и энергопитанием;
- системы контроля доступа;
- системы обслуживания и управления пассажирами;
- публичные Интернет-сети судна, предназначенные для использования пассажирами;
- административные системы и сети;
- системы связи.

Управление рисками традиционно сосредоточено на операциях в физической области, однако зависимость от оцифровки, интеграции, автоматизации и сетевых систем обусловила растущую потребность в управлении киберрисками в судоходной отрасли. Быстро меняющиеся информационные технологии и угрозы затрудняют устранение киберрисков только на основе технических стандартов. В связи с этим Рекомендациями предлагается управление в отношении киберрисков через естественное расширение существующих методов управления безопасностью мореплавания и безопасностью судна.

Информационная безопасность водного транспорта в России

Кодекс торгового мореплавания **[11]**, Кодекс внутреннего водного транспорта РФ **[12]**, Федеральный закон от 08.11.2007 № 261-ФЗ «О морских портах в Российской Федерации» **[13]**, иные исследованные подзаконные акты в области морского и речного транспорта не содержат норм, регулирующих вопросы информационной безопасности морского и речного транспорта.

В Федеральном законе от 09.02.2007 № 16-ФЗ «О транспортной безопасности» **[14]** также не рассматриваются вопросы информационной безопасности объектов транспортной инфраструктуры и транспортных средств. Вместе с тем киберугрозы можно отнести к актам незаконного вмешательства. Стоит напомнить, что акт незаконного вмешательства определяется как противоправное действие (бездействие), в том числе террористический акт, угрожающее безопасной деятельности транспортного комплекса, повлекшее за собой причинение вреда жизни и здоровью людей, материальный ущерб либо создавшее угрозу наступления таких последствий. Однако приказом Минтранса РФ от 05.03.2010 № 52, ФСБ РФ № 112, МВД РФ № 134 **[15]** в перечень потенциальных угроз совершения актов незаконного вмешательства в деятельность объектов транспортной инфраструктуры и транспортных средств включены только угрозы, связанные с физическим воздействием на объекты транспортной инфраструктуры и транспортные средства.

Может сложиться впечатление, что в России не разработаны обязательные для водного транспорта требования по информационной безопасности. Однако это не совсем верно.

С 1 января 2018 г. вступил в силу Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее Закон), который определяет критическую информационную инфраструктуру (КИИ) как объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов **[16]**. Под объектами КИИ понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ. К субъектам КИИ относятся, в частности, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере транспорта.

Законом предусмотрены категорирование и оценка безопасности КИИ, а также реестр ее значимых объектов.

В государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ включаются подразделения и должностные лица субъектов КИИ, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и в реагировании на компьютерные инциденты.

В целях обеспечения безопасности значимого объекта КИИ субъект КИИ, согласно требованиям к созданию систем безопасности таких объектов и обеспечению их функционирования, которые утверждены федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ РФ, создает систему

безопасности такого объекта и обеспечивает ее функционирование.

В заключение нужно отметить следующее. К требованиям закона необходимо отнестись со всей серьезностью. Исходя из опыта реализации новых законов, в частности в сфере транспортной безопасности, можно прогнозировать, что вступление в силу Закона может повлечь увеличение бюрократических процедур, количества обязательных для субъекта транспортной инфраструктуры и/или транспортного средства документов, объема контрольных и надзорных мероприятий. Содержащиеся в Законе определения позволяют представить, что к КИИ транспорта может быть отнесен весьма широкий круг объектов, включая судовые, береговые и портовые системы.

Нормы ИМО рекомендуют осуществлять управление в отношении киберрисков через естественное расширение существующих методов управления безопасностью мореплавания и безопасностью судна. Однако российское законодательство различные вопросы безопасности регулирует отдельными, не взаимосвязанными нормативными правовыми актами, и реализация комплексного подхода к обеспечению безопасности объекта водного транспорта становится практически невозможной.

С учетом сказанного можно легко прогнозировать ситуацию в отсутствие интеграции норм ИМО по кибербезопасности и российского законодательства в сфере информационной безопасности. У судовладельцев и субъектов морской и речной транспортной инфраструктуры возникнет обязанность соблюдать как международное (ИМО), так и российской законодательство. Иными словами, потребуется обеспечить параллельное и одновременное функционирование двух систем информационной безопасности.

Необходимо отметить, что эта проблема коснется всей транспортной сферы, а не только морского и речного транспорта. На наш взгляд, Минтрансу России, подведомственным федеральным агентствам совместно с транспортным сообществом целесообразно проанализировать ситуацию с обеспечением информационной безопасности транспорта и сформировать определенную позицию по данному вопросу.

Литература

1. Морская транспортировка//Международная торговая палата — Всемирная ассоциация бизнеса: [сайт]. URL: http://www.iccwbo.ru/blog/2016/morskaya-transportirovka-vse-tonkosti-protsessa/ (дата обращения 17.12.17).
2. Кибербезопасность на бескрайних морях: [блог]//Positive Technologies. Хабрхабр: [сайт]. URL: https://habrahabr.ru/company/pt/blog/303198/ (дата обращения 17.12.17).
3. Кибербезопасность на бескрайних морях: [блог]//Positive Technologies. Хабрхабр: [сайт]. URL: https://habrahabr.ru/company/pt/blog/303198/ (дата обращения 17.12.17).
4. Allianz проанализировал безопасность судоходства в мире//Allianz: [сайт]. URL: https://www.allianz.ru/ru/press/news/article22445986 (дата обращения 17.12.17).
5. Кибербезопасность на бескрайних морях: [блог]//Positive Technologies. Хабрхабр: [сайт]. URL: https://habrahabr.ru/company/pt/blog/303198/ (дата обращения 17.12.17).
6. См.: Пираты XXI века: как хакеры угрожают торговому флоту//IsraelMedia: [сайт]. URL: http://israelmedia.co.il/tech/piraty-xxi-veka-kak-xakery-ugrozhayut-torgovomu-flotu/ (дата обращения 17.12.17); Руководство IMO предупреждает о кибер-уязвимости рулевого устройства//Crewmarket.net: [сайт]. URL: http://news.crewmarket.net/2016/05/rukovodstvo-imo-preduprezhdaet-o-kiber-uyazvimosti-rulevogo-ustrojstva.html (дата обращения 17.12.17); Кибербезопасность находится в руках моряков. Моряк Украины: [блог].//Livejournal: [сайт]. URL: https://moryakukrainy.livejournal.com/3843048.html (дата обращения 17.12.17).
7. Международная морская организация: [сайт]. URL: http://www.imo.org/en/OurWork/Facilitation/FALCommittee/Facilitation/FAL 41-17 — Table of contents (Secretariat).pdf (дата обращения 19.12.17).
8. Международная морская организация: [сайт]. URL: http://www.imo.org/en/OurWork/Security/WestAfrica/Documents/Resolution MSC.428(98) — Maritime Cyber Risk Management in Safety Management Systems.pdf (дата обращения 19.12.17).
9. Международная морская организация: [сайт]. URL: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3 — Guidelines On Maritime Cyber Risk Management (Secretariat).pdf (дата обращения 19.12.17).
10. Международная палата судоходства: [сайт]. URL: http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16 (дата обращения 19.12.17).
11. «Кодекс торгового мореплавания Российской Федерации» от 30.04.1999 № 81-ФЗ (ред. от 18.07.2017). [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_22916/ (дата обращения 19.12.17).
12. «Кодекс внутреннего водного транспорта Российской Федерации» от 07.03.2001 № 24-ФЗ (ред. от 01.07.2017). [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_30650/ (дата обращения 19.12.17).
13. Федеральный закон от 08.11.2007 № 261-ФЗ (ред. от 18.07.2017) «О морских портах в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации». [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_72390/ (дата обращения 19.12.17).
14. Федеральный закон от 09.02.2007 № 16-ФЗ (ред. от 06.07.2016) «О транспортной безопасности» (с изм. и доп., вступ. в силу с 21.12.2016). [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_66069/ (дата обращения 19.12.17.)
15. Приказ Минтранса РФ, ФСБ РФ и МВД РФ от 5 марта 2010 г. № 52/112/134
16. «Об утверждении Перечня потенциальных угроз совершения актов незаконного вмешательства в деятельность объектов транспортной инфраструктуры и транспортных средств». [Электронный ресурс] URL: http://ivo.garant.ru/#/document/12174831/paragraph/2:1 (дата обращения 19.12.17).
17. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 19.12.17).