Сергей СЕМЕНОВ, начальник ФБУ «Служба морской безопасности»

Кибербезопасность на флоте

Транспортировка грузов морским транспортом и перевозки пассажиров судами – это 90% всего объема международных перевозок[1].

В настоящее время общемировой тенденцией является прогрессирующая цифровизация экономики, которая в полной мере касается морского и речного транспорта. Суда увеличивают габариты, а команды уменьшают численность в связи с все большей автоматизацией процессов. Некоторые бортовые системы получают обновления во время плавания, у команд есть выход в Интернет.

При этом, по мнению ряда специалистов, вопросам информационной безопасности объектов морской и речной транспортной инфраструктуры, морских и речных судов уделяется крайне мало внимания[2].

«Невидимая» отрасль

Согласно отчету ENISA[3] «Analys is of cybersecurity aspects in the maritime sector» от ноября 2011 года[4], «озадаченность вопросами кибербезопасности в морском секторе находится на низком уровне либо вообще отсутствует».

Малую обеспокоенность вопросами, связанными с киберугрозами, отмечают и аналитики компании Cyber Keel, специализирующейся на безопасности морской индустрии. Они отмечают тот факт, что многие занятые в морской сфере привыкли быть частью «практически невидимой» отрасли, незаметной простому обывателю. «Чаще всего, если обычный человек не живет около значительного порта, он не может представить себе действительных масштабов всей индустрии», – говорится в их отчете.

«Зависимость морской индустрии от технологий также представляет риски. Подверженность кибератакам (помимо утраты данных) растет. Уже имел место ряд значимых киберинцидентов, и развитие технологий, включая Интернет и электронную навигацию, означает, что в распоряжении отрасли всего несколько лет, чтобы подготовиться к риску утраты судов в результате кибератак. «Пираты уже злоупотребляют наличием прорех в системе кибербезопасности для планирования кражи конкретных грузов, – говорит капитан Эндрю Кинси, старший консультант по морским рискам AGCS. – При этом нельзя переоценивать значение кибератак. Ведь нельзя же взломать секстант»», – говорится в отчете Allianz о безопасности судоходства за 2015 год[5].

Вопрос актуальности тематики еще осложняется тем, что, по данным Reuters, далеко не вся информация об успешно проведенных атаках получает широкую огласку: часто владельцы бизнеса могут умалчивать ее, опасаясь таких последствий, как потеря имиджа, претензий со стороны клиентов и страховых компаний, начала расследований, проводимых сторонними организациями и государственными органами[6].

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

– AIS (Automatic Identification System) – автоматическая идентификационная система;

– ECDIS (Electronic Chart Display and Information System) – электронно-картографическая навигационно-информационная система. До 2019 года ECDIS должны быть обязательно установлены на всех судах;

– VDR (Voyage Data Recorder) – регистратор данных рейса;

– TOS (Terminal Operating System) – IT-инфраструктура, служащая целям автоматизации процессов, происходящих с грузами в порту. На практике может являться как целостным продуктом конкретного вендора, так и совокупностью систем (в том числе широкого назначения), выполняющих различные задачи;

– CTS (Container Tracking System) – система, позволяющая отслеживать движение контейнеров посредством GPS и реже других каналов передачи данных;

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

Каждая из вышеприведенных систем имеет свои уязвимости и проблемы с точки зрения информационной безопасности[7].

Большое исследование, посвященное безопасности AIS, было проведено исследователями компании Trend Micro. Результаты исследования были представлены на конференции Black Hat Asia 2014. Исследование показало возможность следующих сценариев:

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

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

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

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

– возможность сделать существующее судно «невидимым»;

– создание несуществующих поисково-спасательных вертолетов;

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

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

Морская индустрия активно пользуется спутниковыми технологиями SATCOM (Satellite Communications) 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 исследователем компании Synack Колби Муром был представлен отчет о безопасности систем GPS-трекинга Globalstar. Проведенное исследование показало, что эксплуатация найденных уязвимостей приводит к перехвату и подмене информации или глушению сигнала. В сети Simplex, основанной на радиопередаче, используемой компанией Globalstar для передачи данных между трекерами, спутниками и наземными станциями, отсутствуют механизмы аутентификации и шифрования, обслуживающие работу систем, а механизм передачи данных, работающий только в одну сторону, не представляет возможности валидации переданных данных. Мур уверен, что данная проблема присутствует не только в Globalstar.

Спутниковые системы связи (SATCOM), в том числе связывающие через Интернет суда друг с другом и с «большой землей», также содержат большое количество уязвимостей, сообщается в отчете IO Active. Проверка терминалов спутниковой связи, используемых в судоходстве, выявила такие критические бреши в безопасности, как использование устройствами незащищенных или даже недокументированных протоколов, заведенные «фабрично» учетные записи, возможность эксплуатирования функции сброса пароля, бэкдоры.

Крайне показательный случай компрометации спутниковых систем произошел в июле 2013 года. Студенты из Техасского университета в Остине смогли отклонить от курса яхту стоимостью $80 млн, используя оборудование, цена которого не превышала $3 тыс. С помощью имитатора GPS-сигналов (используются, к примеру, при калибровке оборудования), дублируя сигнал настоящего спутника и постепенно повышая мощность, им удалось «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, исследователям удалось отклонить судно от первоначального курса[8].

Рекомендации от ИМО

Международная морская организация (ИМО), учитывая сложившуюся в сфере информационной безопасности морской отрасли ситуацию, в 2017 году разработала и приняла ряд документов по кибербезопасности.

Приложение № 10 Резолюция КБМ ИМО 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 года.

«Рекомендации по управлению киберрисками в морской отрасли» (Циркуляр КБМ-ФАЛ (MSC-FAL./Circ.3), далее – Рекомендации) отмечают, что кибертехнологии стали необходимыми для эксплуатации и управления множеством систем, важных для безопасности судоходства и защиты морской окружающей среды. Однако уязвимости, создаваемые доступом, соединением или сетевым подключением этих систем, могут привести к киберугрозам, которые необходимо устранить.

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.

Эти риски могут быть обусловлены уязвимостью, обусловленной 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, обслуживание программного обеспечения или разрешения пользователя). Как правило, эти действия вызывают уязвимость (например, устаревшее программное обеспечение или неэффективные брандмауэры) или используют уязвимость в операционной или информационной технологии.

Уязвимости могут быть вызваны недостатками в проектировании, интеграции и/или обслуживании систем, а также недостатками в кибердисциплине. Как правило, в тех случаях, когда уязвимость в оперативной и/или информационной технологии обнаруживается или используется либо непосредственно (например, слабые пароли, приводящие к несанкционированному доступу), либо косвенно (например, отсутствие сегрегации сети), могут иметь место последствия для безопасности, конфиденциальности, целостности и доступности информации. Кроме того, в тех случаях, когда уязвимость эксплуатационных и/или информационных технологий подвергается воздействию или используется, могут возникнуть последствия для безопасности, особенно в тех случаях, когда ставятся под угрозу важнейшие системы (например, навигационный мостик или основные двигательные системы).

Ряд документов по кибербезопасности

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 41I17) 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./Circ.1526
MARITIME CUBER 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)	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./Circ.3)	05.07.2017	«Рекомендации по управлению киберрисками в морской отрасли» Циркуляр КБМ-ФАЛ (MSC-FAL./Circ.3)
THE GUIDELINES ON CYBER SECURITY ONDOARD SHIPS (Version 2.0) 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

[1] *http://www.iccwbo.ru/blog/2016/morskaya-transportirovka-vse-tonkosti-protsessa/*

[2] *В статье использованы материалы из блога компании Positive Technologies «Кибербезопасность на бескрайних морях» от 14 июня 2016 г. https://habrahabr.ru/company/pt/blog/303198/*

[3] *Европейское агентство сетей и информационной безопасности*

[4] *https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1*

[5] *https://www.allianz.ru/ru/press/news/article22445986*

[6] *http://www.reuters.com/article/us-cybersecurity-shipping-idUSBREA3M20820140424*

[7] *Полный анализ смотри в блоге компании Positive Technologies «Кибербезопасность на бескрайних морях» от 14 июня 2016 г. https://habrahabr.ru/company/pt/blog/303198/*

[8] *Иные примеры: http://israelmedia.co.il/tech/piraty-xxi-veka-kak-xakery-ugrozhayut-torgovomu-flotu/; http://news.crewmarket.net/2016/05/rukovodstvo-imo-preduprezhdaet-o-kiber-uyazvimosti-rulevogo-ustrojstva.html; https://moryakukrainy.livejournal.com/3843048.html*

Уязвимые системы

С точки зрения Рекомендаций уязвимые судовые системы могут включать, но не ограничиваться:

– системами ходового мостика;

– системами обработки и управления грузом;

– системами управления двигателями, машинами и энергопитанием;

– системами контроля доступа;

– системами обслуживания и управления пассажирами;

– публичными интернет-сетями судна, предназначенными для использования пассажирами;

– административными системами и сетями;

– системами связи.

Управление рисками традиционно сосредоточено на операциях в физической области, однако большая зависимость от оцифровки, интеграции, автоматизации и сетевых систем обусловила растущую потребность в управлении киберрисками в судоходной отрасли. Быстроменяющиеся 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.

Рекомендации предписывают заинтересованным сторонам принять необходимые меры для защиты судоходства от существующих и возникающих угроз и уязвимостей, связанных с оцифровкой, интеграцией и автоматизацией процессов и систем судоходства.

А как Россия регулирует вопросы информационной безопасности морского и речного транспорта?

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

Федеральный закон от 09.02.2007 № 16-ФЗ «О транспортной безопасности» также вопросы информационной безопасности объектов транспортной инфраструктуры и транспортных средств не регулирует. Вместе с тем киберугрозы можно отнести к актам незаконного вмешательства («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 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.

На первый взгляд складывается впечатление, что в России отсутствует нормативно-правовое регулирование вопросов информационной безопасности, касающихся морского и речного транспорта. Это не совсем верно.

С 1 января 2018 г. вступает в силу Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – Закон).

Закон определяет критическую информационную инфраструктуру как объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов. Под объектами критической информационной инфраструктуры понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры. К субъектам критической информационной инфраструктуры относятся в том числе 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.

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

Законом предусмотрены категорирование и оценка безопасности критической информационной инфраструктуры, реестр значимых объектов критической информационной инфраструктуры.

В соответствии с Законом субъекты критической информационной инфраструктуры обязаны:

– незамедлительно информировать о компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее – компетентный орган);

– оказывать содействие должностным лицам компетентного органа в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов;

– в случае установки на объектах критической информационной инфраструктуры средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность.

Субъекты критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, также обязаны:

1) соблюдать требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленные компетентным органом;

2) выполнять предписания должностных лиц компетентного органа об устранении нарушений в части соблюдения требований по обеспечению безопасности значимого объекта критической информационной инфраструктуры, выданные этими лицами в соответствии со своей компетенцией;

3) реагировать на компьютерные инциденты в порядке, утвержденном компетентным органом, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры;

4) в определенных Законом случаях обеспечивать беспрепятственный доступ должностным лицам компетентного органа, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

В целях обеспечения безопасности значимого объекта критической информационной инфраструктуры субъект критической информационной инфраструктуры в соответствии с требованиями к созданию систем безопасности таких объектов и обеспечению их функционирования, утвержденными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры РФ, создает систему безопасности такого объекта и обеспечивает ее функционирование.

Действия на опережение

Несмотря на то что необходимые подзаконные акты во исполнение Закона еще не изданы, к его требованиям необходимо отнестись со всей серьезностью уже сейчас.

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 сделать предварительный вывод о том, что к критической информационной инфраструктуре транспорта может быть отнесен очень широкий круг объектов, включая судовые, береговые и портовые системы.

Необходимо отметить, что эта проблема коснется всей транспортной сферы, а не только морского и речного транспорта.

На мой взгляд, Минтрансу России, подведомственным федеральным агентствам совместно с транспортным сообществом целесообразно проанализировать складывающуюся ситуацию с обеспечением информационной безопасности транспорта и, на опережение, сформировать свою позицию по данному вопросу. МВР