СЕТЕВАЯ УГРОЗА:

КАК ЗАЩИТИТЬ МОРСКИЕ СУДА ОТ КИБЕРАТАК?

С ХАКЕРСКИМИ АТАКАМИ НА МОРСКИЕ СУДА ВЕДЕТСЯ БОРЬБА КАК НА МЕЖГОСУДАРСТВЕННОМ, ТАК И НА ЛОКАЛЬНОМ УРОВНЯХ. БЕЗ ДОЛЖНОГО УРОВНЯ ЗАЩИТЫ СУДНА МОЖЕТ БЫТЬ ПОТЕРЯН НЕ ТОЛЬКО ГРУЗ, НО И ПОСТАВЛЕНА ПОД УГРОЗУ ЖИЗНЬ И БЕЗОПАСНОСТЬ ПАССАЖИРОВ И ЭКИПАЖА.

Network threat: How to protect sea vessels from cyber-attacks? There is a struggle with hacker attacks on sea vessels, both at the interstate and local levels. Without the proper level of protection of the ship, the cargo may be lost, and life and safety of passengers and crew can be under the threat.

Сергей СЕМЕНОВ,
начальник ФБУ «Служба морской безопасности»

Sergey SEMENOV,
Head of Maritime Security Service

Транспортировка грузов морским транспортом и перевозки пассажиров судами, по данным Международной торговой палаты, составляют 90% всего объема международных перевозок. При этом общемировая тенденция цифровизации экономики не обошла стороной и эту сферу. Суда увеличиваются, а команды уменьшаются в связи со все большей автоматизацией процессов. Некоторые бортовые системы получают обновления во время плавания, у команд есть выход в интернет. При этом, по данным Европейского агентства по сетевой и информационной безопасности (ENISA), вопросам информационной безопасности объектов морской и речной транспортной инфраструктуры, морских и речных судов уделяется крайне мало внимания.

Согласно отчету агентства “Analysis of cyber security aspects in the maritime sector” от ноября 2011 года, «озадаченность вопросами кибербезопасности в морском секторе находится на низком уровне либо вообще отсутствует». Недостаточную обеспокоенность вопросами, связанными с киберугрозами, отмечают и аналитики компании CyberKeel, специализирующейся на безопасности морской индустрии.

Подверженность кибератакам объектов морской индустрии растет. Имел место ряд значимых киберинцидентов, которые в совокупности с тем, как развиваются технологии, включая интернет и электронную навигацию, означают, что в распоряжении отрасли всего несколько лет, чтобы подготовиться и предусмотреть защиту от угрозы потери целых судов в результате кибератак. Зарубежные специалисты констатируют, что пираты уже злоупотребляют наличием прорех в системе кибербезопаности для планирования кражи конкретных грузов, сообщается в отчете Allianz о безопасности судоходства за 2015 год.

Вопрос актуальности тематики осложняется еще и тем, что, согласно данным исследования агентства Reuters, далеко не вся информация об успешно проведенных атаках получает широкую огласку. Часто владельцы бизнеса могут умалчивать ее, опасаясь потери имиджа, претензий со стороны клиентов и страховых компаний, начала расследований, проводимых сторонними организациями и государственными органами, и т. д.

УЯЗВИМОСТИ СИСТЕМ

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

AIS (Automatic Identification System) – автоматическую идентификационную систему;

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

VDR (Voyage Data Recorder) – регистратор данных рейса;

TOS (Terminal Operating System) – IT-инфраструктуру, служащую 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) – систему, позволяющую 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 комбинированно. Кроме сигнала бедствия некоторые EPIRB могут также передавать информацию о судне (при синхронизации с AIS).

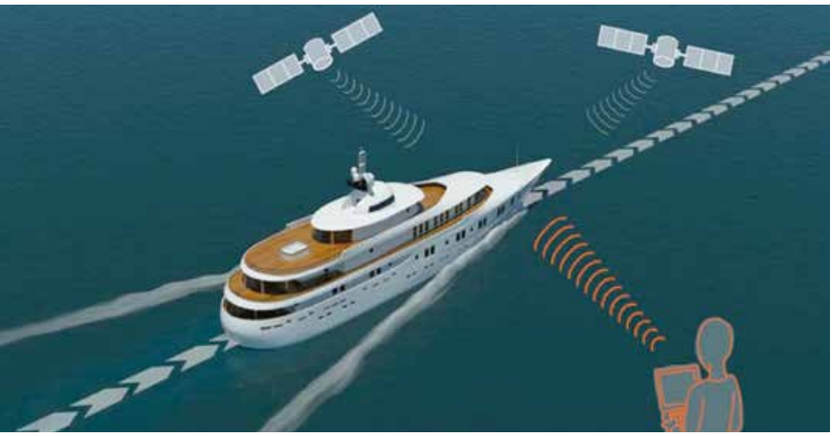
Каждая из вышеприведенных систем, считают специалисты, имеет свои уязвимости и проблемы с точки зрения информационной безопасности.

Так, большое исследование, посвященное безопасности AIS, было проведено исследователями компании Trend Micro, которое показало, что хакеры имеют возможность использовать следующие сценарии взлома:

- 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.

Остаются уязвимыми для атак хакеров системы GPS-трекинга, которыми активно пользуется морская индустрия.

На конференции Black Hat USA 2015 исследователь компании Synack Колби Мур представил отчет о безопасности систем GPS-трекинга Globalstar. Исследование показало, что эксплуатация найденных уязвимостей приводит к перехвату и подмене информации или даже к глушению сигнала. В сети Simplex, основанной на радиопередаче, используемой компанией Globalstar для передачи



Уязвимости могут быть вызваны недостатками в проектировании, интеграции и/или обслуживании систем, а также недостатками в кибердисциплине

данных между трекерами, спутниками и наземными станциями, вообще 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.

О большом количестве уязвимостей в спутниковых системах связи (SATCOM), в том числе связывающих через интернет суда друг с другом и с «большой землей», сообщается и в отчете компании IOActive. 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.

Один из показательных случаев компрометации спутниковых систем произошел в июле 2013 года. Тогда студенты из Техасского университета в Остине смогли отклонить от курса яхту стоимостью 80 млн долларов, используя оборудование, цена которого не превышала 3 тыс. долларов. 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.

МЕЖДУНАРОДНОЕ РЕГУЛИРОВАНИЕ

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

Приложение № 10 Резолюции КБМ ИМО MSC.428(98) настоятельно рекомендует администрациям включить киберриски в системы 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 множества систем, необходимых для безопасности судоходства и защиты морской окружающей среды. Однако уязвимости, создаваемые доступом, соединением или сетевым подключением этих систем, могут привести к киберугрозам.

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 из-за неадекватной работы, интеграции, обслуживания и разработки киберсистем, а также преднамеренными и непреднамеренными киберугрозами.

УГРОЗЫ И УЯЗВИМОСТИ

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 напрямую влияют на уязвимость (например, устаревшее программное обеспечение или неэффективные брандмауэры) или используют уязвимость в операционной или информационной технологии.

С другой стороны, уязвимости могут быть вызваны недостатками в проектировании, интеграции и/или обслуживании систем, а также недостатками в кибердисциплине. 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.

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).

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 си-

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) 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 98th 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 companies	05.07.2017	«Рекомендации по кибербезопасности на судах» (Редакция 2.0) Разработаны и поддерживаются мировыми судоходными компаниями

стем привела к росту потребности 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 ввести управление в отношении киберрисков путем естественного расширения существующих методов управления безопасностью мореплавания и безопасностью судов.

ПОМЕХИ И ЗАКОНОДАТЕЛЬСТВО

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

Федеральный закон от 09.02.2007 № 16-ФЗ «О транспортной безопасности» также не регулирует вопросы информационной безопасности объектов транспортной инфраструктуры и транспортных средств.

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 России от 05.03.2010 № 52, ФСБ России № 112, МВД России № 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.

Может показаться, что в России отсутствует нормативное правовое регулирование вопросов информационной безопасности, касающихся морского и речного транспорта. Однако это не совсем так.

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

Под объектами критической информационной инфраструктуры (далее – КИИ) понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ. К субъектам КИИ относятся в том числе российские юридические лица и 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 входят подразделения и должностные лица субъектов КИИ, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и в реагировании на компьютерные инциденты.

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

Кроме того, в соответствии с законом субъекты КИИ обязаны:

- незамедлительно информировать о компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ 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 КИИ 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 КИИ, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты КИИ, также обязаны:

1) соблюдать требования по обеспечению безопасности значимых объектов КИИ, установленные компетентным органом;

2) выполнять предписания должностных лиц компетентного органа об устранении нарушений в части соблюдения требований по обеспечению безопасности значимого объекта КИИ, 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 КИИ;

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

ОБЪЕКТЫ РЕГУЛИРОВАНИЯ

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

Содержащиеся в Законе определения позволяют сделать предварительный вывод о том, что к КИИ 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. Также к категории КИИ с большой долей вероятности будут отнесены многие системы технических средств обеспечения транспортной безопасности.

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

Кибертехнологии необходимы для безопасности судоходства и защиты морской окружающей среды. Однако уязвимости, создаваемые доступом, могут привести к киберугрозам