Морская кибербезопасность: новые угрозы и зарубежный опыт

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

В статье представлены краткий анализ киберугроз со стороны государств, роль стран Запада в создании основ международного нормативного регулирования морской кибербезопасности и место классификационных и страховых обществ в обеспечении последней.

Эта статья — продолжение предыдущих статей, посвященных вопросам морской кибербезопасности **[1; 2]**. Постараюсь осветить здесь темы, вопросы и факты, ранее мной не затронутые.

Киберугрозы со стороны государств — актуальная реальность

Если еще недавно судоходные компании, морские порты и терминалы в качестве основной киберугрозы рассматривали деятельность преступников-одиночек или организованных преступных групп, то сейчас на передний план выходит угроза кибератак со стороны государств.

25 сентября 2020 г. глава британского Стратегического командования генерал Патрик Сандерс, которого называют самым высокопоставленным кибергенералом Британии, заявил The Guardian, что Великобритания обладает способностью «нарушать, разрушать и уничтожать» критическую инфраструктуру своих врагов в будущем киберконфликте. Уничтожение ключевой инфраструктуры может подразумевать нанесение удара по коммуникациям, телефонным или энергетическим сетям противника в ходе войны. При этом Патрик Сандерс отнес Россию к враждебным государствам **[3; 4]**.

На мой взгляд, заявление Патрика Сандерса примечательно тем, что оно на данный момент завершает ряд прозвучавших в последнее время заявлений руководителей ведущих стран мира или их вооруженных и специальных сил, где акцент делается на кибернападении, а не на киберзащите. При этом транспортная инфраструктура и коммуникации, в том числе морского транспорта, обозначены в качестве целей кибердаров и объектов кибератак. Причем оговорки о «будущей» кибервойне не должны успокаивать и вселять уверенность в том, что в мирное время государства станут воздерживаться от использования кибероружия друг против друга, ведь никаких общепризнанных норм и договоренностей касательно ведения таких войн

в настоящий момент нет. В предыдущие годы был зафиксирован ряд кибератак на морской транспорт, которые связывают с государствами. В 2020 г. также имеется пример кибератаки на порт — иранский терминал Шахид-Раджаи, ее ассоциируют с киберподразделениями Израиля.

Осознание угрозы кибервойн и их последствий у мирового сообщества есть. В частности, 25 сентября 2020 г. Владимир Путин сделал заявление, в котором назвал риск возникновения масштабной конфронтации в цифровой сфере одним из основных стратегических вызовов современности. Обращаясь ко всем странам, включая США, он предложил выйти на заключение глобальной договоренности о принятии политического обязательства государствами касательно ненанесения первыми удара с использованием информационно-коммуникационных технологий друг против друга **[5]**.

Однако надеяться на то, что в ближайшее время на международном уровне будут достигнуты какие-либо взаимообязывающие договоренности, рассчитывать не стоит. Это в первую очередь связано с тем, что ведущие страны мира имеют лидирующий киберпотенциал и рассматривают его в качестве серьезного аргумента при решении внешнеполитических и внешнеэкономических задач.

То, что субъектами кибератаки, в том числе на морской транспорт, могут выступать государства, для морской отрасли не новость. В рекомендованном Международной морской организацией в 2017 г. Руководстве по кибербезопасности на борту судов, разработанном ведущими отраслевыми объединениями, государства уже названы одним из субъектов кибератак. Но если ранее кибератаки на транспорт со стороны государств воспринимались скорее как гипотетические, то сейчас они всё больше и больше становятся реальностью. Притом государства обладают финансовым, научным и человеческим потенциалом, который несравним с потенциалом преступных групп. Это очень тревожный знак для всей морской отрасли.

Будем надеяться, что громкие и грозные заявления политиков останутся в области политики и за ними не последуют кибервойны на просторах Мирового океана. В первую очередь такая надежда связана не с миролюбием ведущих государств планеты, а с тем огромным значением морского транспорта, который он имеет для мировой экономики.

Роль западных наработок

Дабы лучше понять историю развития темы морской кибербезопасности, необходимо акцентировать внимание на том, что отнюдь не резолюция Комитета по безопасности на море Международной морской организации (КБМ ИМО) MSC.428(98) «Управление морскими киберрисками в системах управления безопасностью», принятая в июне 2017 г., послужила отправной точкой развития отраслевого нормативного регулирования морской кибербезопасности **[6]**.

Отправной точкой для формирования принципов, определяющих практику кибербезопасности на море, стала канадско-американская рекомендация, которую поддержал в ноябре 2014 г. КБМ ИМО. Но и до этого момента рядом западных стран была проведена определенная работа в данном направлении.

Так, Европейское агентство сетевой и информационной безопасности (ENISA) еще в ноябре 2011 г. опубликовало результаты анализа аспектов кибербезопасности в морском секторе **[7]**. Тогда ENISA констатировала, что осведомленность о потребностях и вызовах кибербезопасности в морском секторе низка или вообще отсутствует.

Выработанные на основе анализа рекомендации высокого уровня предусматривали в том числе необходимость рассмотрения Международной морской организацией — совместно с Европейской комиссией и государствами-членами ИМО — вопроса о согласовании и гармонизации международной и европейской политики, связанной с этим сектором, особенно в отношении кибербезопасности.

Дорожная карта, предусмотренная анализом, включила в себя необходимость определить и внедрить целостный, основанный на рисках подход к решению проблемы морской кибербезопасности; разработать стандарты и обеспечить соблюдение нормативных актов, гарантирующих кибербезопасность в морском секторе; создать центры обмена информацией и анализа на национальном и европейском уровнях; согласовать и гармонизировать международную и европейскую политику в области морской кибербезопасности; принять надлежащие меры для включения требований кибербезопасности в существующую нормативную базу, применимую к морскому сектору.

Береговая охрана Соединенных Штатов (USCG) опубликовала свой руководящий документ по киберстратегии в июне 2015 г. В этом документе формулируется ви́дение работы агентства в киберпространстве, излагаются цели и задачи по трем заявленным стратегическим приоритетам: защита киберпространства, стимулирование операций и защита инфраструктуры. В декабре 2016 г. USCG опубликовала письмо о политике кибербезопасности, касающееся критериев и процесса сообщения о подозрительной деятельности и нарушении безопасности, а также добавила кибербезопасность в список элементов, охватываемых законом «О безопасности морского транспорта» 2002 г. В соответствии с ним, за нарушение киберготовности может назначаться наказание в виде штрафа в размере до 25 тыс. долл. США **[8]**.

Документы о морской кибербезопасности разработаны и внедряются властями США, Великобритании, Евросоюза, Дании, Норвегии и Сингапура. Естественно, список не исчерпывающий. При этом часть из них, например руководство «Кибербезопасность портов и портовых систем» лондонского Инженерно-технологического института, созданное при поддержке Минтранса Великобритании и Минобороны Великобритании, и их Свод правил кибербезопасности для судов написаны или раньше, или одновременно с резолюцией КБМ ИМО MSC.428(98).

Многие негосударственные и отраслевые организации также начали работы в области морской кибербезопасности еще до выхода указанной резолюции. Например, Руководство по кибербезопасности на борту судов, написанное BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO и IUMI, опубликовано в январе 2016 г. Международная ассоциация классификационных обществ (МАКО, IASC) в июне 2016 г. создала панель киберсистем.

В то же время, о чем я писал в предыдущих статьях, в Российской Федерации до сих пор не принималось документов, касающихся отраслевого регулирования вопросов морской кибер- или информационной безопасности: как на государственном уровне, так и на негосударственном. Сведений о состоянии кибер- или информационной безопасности морской отрасли в открытом доступе нет.

Сейчас можно с уверенностью говорить о том, что в ближайшее время морская отрасль России в целом, и в первую очередь российские судоходные компании, при обеспечении морской кибербезопасности будут руководствоваться международными требованиями и рекомендациями, инициаторами и разработ-

чиками которых были США, Великобритания и страны ЕС.

Об имеющихся проблемах, связанных с гармонизацией международных норм в области морской кибербезопасности и российских норм в области информационной безопасности, я писал в предыдущих статьях.

Место классификационных и страховых обществ

В соответствии с общепринятым международным подходом, рекомендации по обеспечению морской кибербезопасности касаются как эксплуатации судна, так и его проектирования и строительства. Одна из основ такого подхода — вышеупомянутая резолюция КБМ ИМО MSC.428(98), в которой содержится призыв ускорить работу по защите судоходства от текущих и возникающих киберугроз и уязвимостей, адресованный в том числе классификационным обществам, производителям оборудования, поставщикам услуг и всем другим заинтересованным сторонам морской отрасли.

В частности, Международная ассоциация классификационных обществ в апреле 2020 г. опубликовала Рекомендацию по киберустойчивости (№ 166), объединившую предыдущие 12 рекомендаций, относящихся к киберустойчивости (№ 153–164). Это результат работы основанной МАКО в июне 2016 г. панели киберсистем.

Рекомендация подготовлена с учетом резолюции МАКО UR E22 «Использование и применение бортовых компьютерных систем» и распространяется на компьютерные системы, которые обеспечивают функции контроля, сигнализации, мониторинга, безопасности или внутренней связи и подчиняются требованиям МАКО.

Рекомендация предназначена для судов, строящихся по контракту после публикации документа. Она касается технических аспектов проектирования, строительства и испытаний. Рекомендация может использоваться в качестве справочного материала для судов, уже находившихся в эксплуатации до ее публикации.

Рекомендация применяется к бортовым системам операционных технологий (ОТ) и другим системам, которые подключены к бортовым системам ОТ таким образом, что он может повлиять на их работу (это определяется оценкой риска). Она также касается оборудования, которое может оказывать влияние на безопасность человека, безопасность судна или морскую среду, как это определено требованиями Международной конвенции по охране человеческой жизни на море и Международной конвенции по предотвращению загрязнения с судов. При оценке рисков следует учитывать требования МАКО и национального органа исполнительной власти.

В марте 2020 г. классификационное общество DNV GL впервые в отрасли провело проверку кибербезопасности большого пассажирского судна, которое стало первым, добившимся соответствия требованиям в рамках интегрированной системы кибербезопасности DNV GL **[9]**.

Тип кибербезопасности был утвержден DNV GL в 2017 г., а в следующем году добавлено обозначение класса кибербезопасности: Cyber Secure **[10]**. Эта классификация, разработанная DNV GL, устанавливает общепризнанные требования к эксплуатируемым и строящимся судам, а также к морским установкам, для различных сегментов и уровней безопасности.

Обозначение класса Cyber Secure включает три различных квалификатора:

• *Cyber Secure (Basic)*. Устранены наиболее критические уязвимости. Создана система управления кибербезопасностью для обеспечения безопасной эксплуатации судна и соответствия предстоящим требованиям резолюции ИМО MSC.428 (98);

• *Cyber Secure (Essential)*. Включает в себя все вышеприведенные требования начального уровня, но кроме того, более детально изучаются системы управления обеспечения контроля безопасности/возможности согласно профилю безопасности 1 (профиль уровня безопасности 1 в соответствии с IEC62443). Он в первую очередь предназначен для сложных в эксплуатации судов. На этом уровне кибербезопасность внедряется в существующие процедуры и системы, направленные на установление адекватного уровня безопасности;

• *Cyber Secure (Advanced)*. Охватывает ту же область, что и Essential, но с повышенным уровнем охраны (профиль безопасности 3). Он в первую очередь предназначен для сложных новостроек и для обеспечения защиты от преднамеренных нарушений с использованием сложных средств и специальных навыков системы управления.

• *Cyber Secure (+)* охватывает дополнительные системы, которые не входят в сферу действия трех вы-

шеуказанных квалификаторов, но которые можно комбинировать с любым из них. Обозначение *(+)* позволяет владельцу подключать себе дополнительные системы. Оно свидетельствует, что устранены угрозы, а кроме того, оценены и защищены дополнительные системы, которые особенно значимы для операций и не входят в стандартный набор основных и важных функций, таких как грузовые системы, развлекательные системы, IT-системы и системы бурения.

Ведущее классификационное общество ClassNK в июле 2020 г. выпустило уже вторую редакцию Руководства по проектированию кибербезопасности на борту судов, касающегося новостроек и предназначенного для верфей и судовладельцев **[11]**. Издание определяет меры контроля и структуру для реализации таких мер, которые были дополнены международными стандартами кибербезопасности для промышленных систем контроля серии IEC62443 и последними рекомендациями по киберустойчивости для новых судов, опубликованными МАКО.

Кроме того, ClassNK ввело требования касательно добавления обозначений классов к классификационным кодам, связанным с кибербезопасностью. В руководство также включены современные передовые практики верфей и судовладельцев с позиции определения компьютерных систем, которые следует защитить от киберинцидентов, и построения сетей для их защиты.

18 сентября классификационное общество Корейский регистр судоходства (KR) провело первое в мире присвоение класса кибербезопасности (CS Ready) крупному газовозу (принадлежащему компании Hyundai Heavy Industries) **[12]**. Это произошло после завершения документальных и полевых инспекций. Класс CS Ready присваивается вновь построенным судам, и для его получения необходимо успешно пройти 49 пунктов инспекции в общей сложности по 12 категориям, включая управление рисками и активами, реагирование на киберинциденты и восстановление после них.

Также KR проводит сертификацию по морской кибербезопасности в отношении компании или судна с системой менеджмента кибербезопасности. Соответствие требованиям кибербезопасности для компании или существующего судна разделено на три уровня (CS1, CS2 и CS3) в соответствии со зрелостью кибербезопасности и состоит из 35 зон и 144 пунктов обследования. Кроме того, KR проводит освидетельствование оборудования на соответствие требованиям кибербезопасности **[13]**.

Приведенные примеры хорошо иллюстрируют роль зарубежных классификационных обществ в обеспечении морской кибербезопасности, начиная с этапа строительства судна. К сожалению, на момент написания статьи открытая информация о деятельности Российского морского регистра судоходства по обеспечению морской кибер- или информационной безопасности отсутствовала на его сайте.

Большое внимание вопросам морской кибербезопасности уделяют и страховые общества и компании. Так, Международный союз морского страхования (IUMI) участвовал в разработке Руководства по кибербезопасности на борту судов, начиная с первого издания. IUMI входит — в числе отраслевых партнеров — в совместную с МАКО рабочую группу по киберсистемам.

Опубликованная 24 августа 2020 г. Стратегическая программа Международного союза морского страхования содержит раздел «Киберриски» **[14]**. В данном разделе отмечается, что страхование рисков, связанных с единичными атаками вымогателей, теперь доступно как на морском, так и на неморском рынке страхования. Однако косвенный ущерб корпусу судна, грузу и обязательствам перед третьими лицами в результате кибератаки на борту судна или морской плавучей платформы представляет собой иной и более дорогостоящий риск. Успешная кибератака может повлечь за собой несколько последствий, имеющих отношение к страхованию: гибель людей, телесные повреждения, загрязнение окружающей среды, потеря имущества, прерывание бизнеса, потеря производства, потеря данных и потеря репутации. С точки зрения грузовых перевозок особую озабоченность вызывают потенциальные риски и последствия кибератак, направленных на беспилотные грузовые автоколонны и мегаузлы. Ограниченность данных о частоте атак, серьезности потерь и вероятности физического ущерба — проблема для страховщиков.

По оценкам Лондонского Ллойда, ущерб от кибератак в морской отрасли может оцениваться в 200 млрд долл. США. При низком уровне страхования только 10 % убытков от кибератак будет покрыто страховкой **[15]**.

Надеюсь, что примеры положительного зарубежного опыта позволят России в кратчайшие сроки сформировать передовую морскую отраслевую систему кибербезопасности, избежав ошибок и неэффективных решений. Т

Литература:

1. Семенов С. А. Кибербезопасность морского и речного транспорта // Транспорт РФ. 2018. № 1 (74). С. 43–46.
2. Семенов С. А. Морская кибербезопасность в России // Там же. 2019. № 3 (82). С. 11–14.
3. URL: russian.rt.com/inotv/2020–09–26/Guardian-London-rabotaet-nad-kiberoruzhiem (дата обращения: 10.10.2020).
4. URL: www.theguardian.com/technology/2020/sep/25/britain-has-offensive-cyberwar-capability-top-general-admits (дата обращения: 10.10.2020).
5. URL: kremlin.ru/events/president/news/64086 (дата обращения: 10.10.2020).
6. URL: www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution MSC.428(98).pdf (дата обращения: 10.10.2020).
7. URL: www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport (дата обращения: 10.10.2020).
8. URL: iumi.com/document/view/3Cyber_risks__5f43bcc573736.pdf (дата обращения: 10.10.2020).
9. URL: safety4sea.com/dnv-gl-awards-first-cyber-security-verification-to-a-ship (дата обращения: 10.10.2020).
10. URL: www.dnvgl.com/services/cyber-secure-class-notation-124600 (дата обращения: 10.10.2020).
11. URL: safety4sea.com/classnk-issues-second-edition-of-guidelines-for-designing-cyber-security-onboard-ships (дата обращения: 10.10.2020).
12. URL: safety4sea.com/kr-launches-worlds-first-cyber-cecurity-notation-for-very-large-lpg-carrier (дата обращения: 10.10.2020).
13. URL:www.krs.co.kr/download/download.aspx?path=%2fboard%2f13071 %2fKR+MARITIME+CYBER+SECURITY+NEWS+Vol.+029_EN.pdf&filename=KR+MARITIME+CYBER+SECURITY+NEWS+Vol.+029_EN.pdf (дата обращения: 10.10.2020).
14. URL: iumi.com/document/view/3Cyber_risks__5f43bcc573736.pdf (дата обращения: 10.10.2020).
15. URL: safety4sea.com/covid-19-response-is-a-lesson-learned-for-future-cyber-attacks (дата обращения: 10.10.2020).