Морская кибербезопасность в России

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

В статье анализируется текущее состояние нормативного правого регулирования морской кибербезопасности в РФ, рассматриваются международные и российские источники права. Прогнозируется вероятность коллизий между различными нормативными правовыми актами в области морской кибербезопасности, подчеркивается необходимость их гармонизации.

Сегодня общемировой тенденцией стала прогрессирующая цифровизация экономики. На морском транспорте активно развивается электронная навигация. Суда увеличиваются, а команды уменьшаются в связи со все большей автоматизацией процессов. Бортовые системы получают обновления во время плавания, у команд есть выход в Интернет.

Предстоит погружение в цифровую среду всех сегментов портового хозяйства. Успешно эксплуатируются полностью автоматические контейнерные терминалы, например голландский Maasvlakte II или китайский Qingdao New Qianwan Container Terminal.

Международная морская организация (ИМО) к уязвимым судовым системам относит следующие **[1]**:

- 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.

С учетом изложенного можно сделать заключение, что судно крайне уязвимо для спланированной кибератаки.

Широко известный и показательный пример компрометации спутниковых систем — случай, произошедший в 2013 г., когда студенты из Техасского университета смогли отклонить от курса яхту стоимостью 80 млн долл. с помощью имитатора GPS-сигналов, цена которого не превышала трех тысяч долларов.

Порты также нуждаются в защите от информационных угроз. Самый гром-

ФОТО: СЕРГЕЙ ТЮРИН

кий инцидент, связанный с портовой кибербезопасностью, произошел в порту Антверпена в 2012 г. Около двух лет системы порта подвергались целевым кибератакам, а в июне 2011 г. хакеры взяли под контроль системы терминала и оперировали погрузками и разгрузками без ведома порта **[2]**. В 2017 г. в результате масштабной вирусной эпидемии NotPetya остановились 17 из 76 грузовых терминалов компании Maersk **[3]**, в 2018 г. кибератакам подверглись порты Барселона и Сан-Диего **[4]**.

Согласно информации израильской компании по интернет-безопасности ThetaRay имел место случай, когда хакеру удалось наклонить плавучую нефтяную вышку в сторону, что привело к ее закрытию **[5]**. В 2010 г. была зафиксирована остановка буровой платформы по пути из Южной Кореи в Бразилию; как оказалось, компьютерные и контрольные системы были переполнены вирусами **[6]**.

Необходимость принятия мер по обеспечению информационной безопасности очевидна на международном и национальном уровне. Международной морской организацией подготовлена третья версия «Руководства по управлению морскими киберрисками» **[7]**. Комитет по безопасности на море ИМО в июне 2017 г. принял резолюцию MSC.428(98) — управление морскими киберрисками в системах управления безопасностью. Резолюция призывает администрации обеспечить учет киберрисков в существующих системах управления безопасностью не позднее первой ежегодной проверки документа компании о соответствии после 1 января 2021 г. Международной организацией по стандартизации и Международной электротехнической комиссией разработан и опубликован Стандарт 27001 по информационным технологиям. Международной морской организацией рекомендованы «Руководство по кибербезопасности на судах», разработанное ведущими морскими транспортными ассоциациями, и «Рамочная программа Национального института стандартов и технологий Соединенных Штатов Америки по совершенствованию критической инфраструктуры кибербезопасности» **[8]**.

1 января 2018 г. вступил в силу Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (ФЗ-187). К объектам критической информационной инфраструктуры ФЗ-187 относит информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры. Содержащиеся в ФЗ-187 определения позволяют сделать предварительное заключение, что к критической информационной инфраструктуре водного транспорта может быть отнесен достаточно широкий круг объектов, включая судовые, береговые и портовые системы.

Проект резолюции XVIII Международной конференции «Терроризм и безопасность на транспорте» (п. 16) призывает федеральные органы исполнительной власти при рассмотрении угроз совершения актов незаконного вмешательства в деятельность объектов транспортной инфраструктуры, при проведении оценки уязвимости и разработке планов обеспечения транспортной безопасности учитывать способы совершения актов незаконного вмешательства с использованием кибератак, вносить необходимые изменения в описание угроз.

Коллизионность норм, регулирующих морскую кибербезопасность

Необходимость обеспечения информационной безопасности водного транспорта, включая морской, на международном и российском уровне признается, отдельные меры принимаются. Однако относительно нормативно-правового регулирования обеспечения информационной безопасности ситуация выглядит более пессимистичной: есть ряд трудноразрешаемых проблем.

В сфере водного транспорта по информационной безопасности не разработаны единый, системный и комплексный подход, унификация требований и правил. Следует обратить внимание на то, что в России нет транспортного отраслевого центра компетенции по информационной безопасности. Ни в положении о Минтрансе России, ни в положении о Росморречфолоте нет ничего об информационной безопасности, в частности и о морской кибербезопасности. Иными словами, формирование единой отраслевой политики в области информационной безопасности не входит в круг задач или обязанностей федеральных органов власти в сфере транспорта.

Можно возразить, что в России вопросы информационной безопасности отнесены к компетенции Федеральной службы по техническому и экспортному контролю (ФСТЭК), которая создает общие, рамочные правила и требования без учета отраслевых особенностей. Вопросы информационной безопасности морского транспорта регулируются международным законодательством и нормами международных отраслевых объединений. Владельцам судов под флагом РФ для успешного бизнеса гораздо важнее соблюсти международные нормы, а не национальные.

В июне нынешнего года в ИМО на 101-й сессии Комитета по безопасности на море обсуждалась 3-я редакция «Руководства по управлению морскими киберрисками». Для выработки позиции делегации РФ по указанному руководству ФСТЭК России не привлекалась. Неизвестно, насколько требования руководства соответствуют российскому подходу к обеспечению информационной безопасности. При этом необходимо напомнить, что через 1,5 года, с 1 января 2021 г., требования Руководства станут обязательными для судов под флагом РФ. Различия в подходах судовладельцам придется узнавать из своего личного опыта. Сходная ситуация с «Руководством по кибербезопасности на судах» **[9]**, разработанным ведущими морскими транспортными ассоциациями. Сейчас инспекторами Международного морского форума нефтяных компаний (OCINF) проверяется выполнение судами норм руководства **[9]**.

Нормы международных организаций и российского законодательства развивались параллельно, без взаимного учета положений. В ближайшее время судовладельцы столкнутся с тем, что им придется одновременно выполнять и требования международных организаций, и положения ФЗ-187. В нормативных правовых актах по информационной безопасности отмечаются различия в понятийном аппарате. Например, в международных документах используется термин «кибербезопасность», в Доктрине информационной безопасности РФ — «информационная безопасность», а в документах ФСТЭК России — «защита информации» и «безопасность критической информационной инфраструктуры». И здесь приведены понятия только верхнего уровня. Есть мнение, что в плане толкования это одно и то же. Однако разница в понятийном аппарате при правоприменении создает практически непреодолимые барьеры в регулировании однотипных и схожих правоотношений. Следовательно, необходимы разработка, параллельное и одновременное функционирования двух систем информационной безопасности. Обоснованность такого утверждения под-

держивается опытом развития транспортной безопасности.

Международная морская организация, рассматривающая кибербезопасность как часть морской безопасности, рекомендует управление в отношении киберрисков осуществлять через естественное расширение существующих методов управления безопасностью мореплавания и безопасностью судна. Однако российское законодательство те или иные составляющие безопасности регулирует разными, не взаимоувязанными нормативными правовыми актами. В результате с позиций российского законодательства, реализация единого и комплексного подхода к обеспечению безопасности судна становится практически невозможной.

Представители ФСТЭК России в публичном выступлении заявили, что меры по обеспечению безопасности критической информационной инфраструктуры могут быть предусмотрены в едином плане обеспечения безопасности объекта критической информационной инфраструктуры. Создается впечатление, что подходы к планированию мер обеспечения информационной безопасности у ИМО и ФСТЭК России сходны. Однако неясно, как ФСТЭК России будет реагировать на запланированные меры по ФЗ-187, если они найдут свое отражение в планах, выполненных согласно требованиям ИМО.

Посмотрим на этот вопрос с позиций транспортной безопасности. Банк данных по угрозам безопасности информации содержит на 14 июня нынешнего года сведения о 213 угрозах и 21 617 уязвимостях программного обеспечения и программно-аппаратных средств **[10]**. Однако законодательство о транспортной безопасности не рассматривает кибератаки в качестве актов незаконного вмешательства, а угрозы их совершения в качестве угроз актов незаконного вмешательства. Порядок разработки планов по обеспечению транспортной безопасности объектов транспортной инфраструктуры и транспортных средств, утвержденный приказом Минтранса России от 11.02.2010 № 34, не предусматривает отражения в планах обеспечения транспортной безопасности сведений о киберугрозах и мерах по защите от них. Получается, что информационная безопасность отделена от транспортной.

Следующий наглядный пример — технические средства обеспечения транспортной безопасности как объект правового регулирования. Обычно их существенный элемент составляют системы и средства видеонаблюдения. Согласно пункту 8 статьи 12.2 Федерального закона от 09.02.2007 № 16-ФЗ «О транспортной безопасности» технические средства обеспечения транспортной безопасности подлежат обязательной сертификации. Требования к функциональным свойствам технических средств обеспечения транспортной безопасности и порядок их сертификации определены постановлением Правительства РФ от 26.09.2016 № 969.

Судовая телевизионная система охранного наблюдения поднадзорна Российскому морскому регистру судоходства и должна отвечать его требованиям, а также иметь сертификат типового одобрения. Она включена в номенклатуру объектов технического наблюдения Регистра (код 0441000, Правила технического наблюдения за постройкой судов и изготовлением материалов и изделий для судов. Т. 1, ч. I: Общие требования по техническому наблюдению). Технические средства судовых (телевизионных) систем охранного наблюдения должны устанавливаться в соответствии с согласованной в Регистре проектной документацией на их установку. Требования к ним для морских судов разработаны и утверждены в разделе 7.2 части IV Правил по оборудованию морских судов. В качестве объекта технического наблюдения Регистр рассматривает также системы внешнего/внутреннего видонаблюдения: видеокамеры (код 11100701), видеотерминалы (код 11100702), щиты, пульты контроля и сигнализации (код 11100703), датчики и другие элементы (код 11100704).

Согласно ФЗ-187 отдельные системы технических средств обеспечения транспортной безопасности и судовые телевизионные системы охранного наблюдения представляют собой объекты правового регулирования. Но с позиций ИМО на них могут распространяться рекомендации «Руководства по управлению морскими киберрисками».

Как все эти требования будут «уживаться», насколько дорого это будет для судовладельцев? Покажет только практический опыт. Необходимо отметить, что под двойное регулирование по информационной безопасности (ИМО и ФЗ-187) попадут и другие системы судна, прежде всего системы автоматизации. Здесь подобраны наиболее наглядные примеры для иллюстрации возможных негативных сценариев. Этими примерами проблемы, конечно, не исчерпываются. Сходные «неувязки» отмечаются и у речного транспорта, портов, береговой инфраструктуры и у транспортной отрасли в целом.

Таким образом, киберугрозы представляют реальную опасность для морского и речного транспорта. Они могут исходить от широкого круга субъектов: криминальных групп, пиратов, террористов, связанных с государствами хакеров. Угрозу представляет несоблюдение требований кибербезопасности персоналом субъектов транспортной инфраструктуры и экипажей судов. В России не сформирован единый подход к нормативно-правовому регулированию морской кибербезопасности. Вопросы обеспечения кибербезопасности морского транспорта одновременно регулируются нормами международного и российского права. Они не увязаны между собой, международные нормы не имплементированы в российское законодательство. К информационным и телекоммуникационным системам, автоматизированным системам управления морскими судами, их элементам и обеспечению их безопасности предъявляются требования, имеющие источники в различных институтах международного и российского права. С учетом изложенного можно прогнозировать неизбежные коллизии правовых норм.

Формирование единой отраслевой политики в области информационной безопасности не входит в круг задач или обязанностей федеральных органов власти в сфере транспорта. Их компетенция в этой области ограничивается подведомственными организациями и учреждениями. Существующие в РФ подходы к обеспечению информационной безопасности не предполагают различий между информационными и телекоммуникационными системами, автоматизированными системами управления, используемыми в различных сферах экономики. Иначе говоря, согласно ФЗ-187 системы медицинского учреждения и морского нефтяного терминала идентичны, критерии к их категорированию и требования к обеспечению их безопасности одинаковы.

Такой подход носит крайне общий характер, и на практике отраслевые особенности придется учитывать. В отсутствие единых отраслевых подходов к обеспечению информационной безопасности субъекты транспортной инфраструктуры и владельцы транспортных средств будут исполнять требования ФЗ-187 на основе собственного их толкования. Складывающуюся ситуацию можно охарактеризовать известным выражением «кто в лес, кто по

ФОТО: СЕРГЕЙ ТЮРИН

дрова». Российское законодательство те или иные составляющие безопасности регулирует разными, не взаимоувязанными нормативными правовыми актами. В результате оказывается, что согласно российскому законодательству реализация единого и комплексного подхода к обеспечению безопасности объекта транспортной инфраструктуры или судна практически невозможна. Если решение прогнозируемых проблем будет сложным и затратным, то для морских судов возникнет дополнительный аргумент в пользу ухода из реестров судов РФ под «удобный» флаг.

Гармонизация правовых норм и упрощение формальностей

Пока отрасль находится в начальной стадии внедрения в жизнь требований по обеспечению информационной безопасности, необходимо организовать работу по гармонизации существующих правовых норм и упрощению формальностей. Отраслевые федеральные органы исполнительной власти некомпетентны в вопросах информационной безопасности, поэтому организацию и осуществление такой работы необходимо взять на себя отраслевым профессиональным объединениям. Хорошим примером служит совместная работа отраслевых международных объединений (BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, OCIMF, IUMI и Всемирного совета судоходства) по разработке «Руководства по кибербезопасности на судах».

В мире активное участие в разработке и руководящих принципов и стандартов, а также рекомендуемых практик по кибербезопасности принимают классификационные общества. В частности, крупнейшее классификационное общество DNV GL в 2016 г. разработало рекомендуемые практики «Управление устойчивостью к кибербезопасности для судов и мобильных морских установок в эксплуатации», а ведущее классификационное общество Японии ClassNK разрабатывает собственные подходы к обеспечению бортовой кибербезопасности для судов. Учитывая изложенное, можно и нужно привлечь к указанной работе Российский морской регистр судоходства. Кроме того, работу по разработке национального подхода к обеспечению морской кибербезопасности необходимо проводить во взаимодействии с ФСТЭК России. Т

Литература

1. Международная морская организация. — URL: http://www.imo.org/en/OurWork/Facilitation/FALCommittee/Facilitation/FAL 41–17 — Table of contents (Secretariat).pdf (Дата обращения 15.06.19).
2. Морская индустрия — лакомый кусок для хакеров // Блог Касперского. — URL: https://www.kaspersky.ru/blog/maritime-cyber-security/7885/ (Дата обращения 15.06.2019).
3. The Untold Story of NotPetya, the Most Devastating Cyberattack in History // Wired. — URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/?src=longreads (Дата обращения 15.06.2019).
4. За одну неделю жертвами кибератак стали сразу два морских порта // Securitylab.ru by Positive Technologies. — URL: https://www.securitylab.ru/news/495727.php (Дата обращения 15.06.2019).
5. Морская отрасль уязвима для атак хакеров // Вести Экономика. — URL: https://www.vestifinance.ru/articles/42174 (Дата обращения 15.06.2019).
6. Морская индустрия — лакомый кусок для хакеров//Блог Касперского. — URL: https://www.kaspersky.ru/blog/maritime-cyber-security/7885/ (Дата обращения 15.06.2019).
7. Международная морская организация. — URL: http://www.imo.org/en/OurWork/Facilitation/FALCommittee/Facilitation/FAL 41–17 — Table of contents (Secretariat).pdf (Дата обращения 15.06.19).
8. Международная морская организация. — URL: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx.
9. Международная палата судоходства. — 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 15.06.19).
10. Банк данных угроз безопасности информации//ФСТЭК России. — URL: https://bdu.fstec.ru/ (Дата обращения 15.06.2019).