Cybersecurity as an element of maritime transport security

The approaches to ensuring cybersecurity in Russian and international law differ significantly, which can cause a number of problems. It is necessary to organize the work on harmonization of the existing legal norms and simplification of formalities with the industry organizations and the relevant public authorities engaged.

Кибербезопасность как элемент ТБ на морском транспорте

Сергей СЕМЕНОВ,
начальник Федерального бюджетного учреждения «Служба морской безопасности»

Sergey SEMENOV,
Head of Maritime Security Service

ПОДХОДЫ К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ В РОССИЙСКОМ И МЕЖДУНАРОДНОМ ЗАКОНОДАТЕЛЬСТВЕ СУЩЕСТВЕННО ОТЛИЧАЮТСЯ, ЧТО МОЖЕТ СТАТЬ ПРИЧИНОЙ РЯДА ПРОБЛЕМ. НЕОБХОДИМО ОРГАНИЗОВАТЬ РАБОТУ ПО ГАРМОНИЗАЦИИ СУЩЕСТВУЮЩИХ ПРАВОВЫХ НОРМ И УПРОЩЕНИЮ ФОРМАЛЬНОСТЕЙ С УЧАСТИЕМ ОТРАСЛЕВЫХ ОРГАНИЗАЦИЙ И ПРОФИЛЬНЫХ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ.

Растущая цифровизация всех отраслей экономики в полной мере касается и морского транспорта. Активно развивается электронная навигация, происходит все большая автоматизация процессов. Бортовые системы получают обновления во время плавания. У команд есть возможность выходить в Интернет.

Со временем все сегменты портового хозяйства будут затронуты цифровизацией. Уже сейчас успешно эксплуатируются полностью автоматические контейнерные терминалы, например голландский Maasvlakte II или китайский Qingdao New Qianwan Container Terminal.

Цифровизация имеет свои преимущества, благодаря которым цифровые системы получают все большее распространение. Но кроме несомненных выгод она несет и риски, связанные с обеспечением информационной безопасности (далее – ИБ).

СЦЕНАРИИ КИБЕРАТАК НА СУДОВЫЕ СИСТЕМЫ

Специалисты по ИБ выделяют следующие возможные сценарии кибератак на судовые системы:

- изменение данных о судне, включающих его местоположение, курс, информацию о грузе, скорость и название;
- создание «кораблей-призраков», опознаваемых другими судами в качестве настоящего судна 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 аварийного радиобуя, активирующих тревогу на находящихся поблизости судах;
- возможность проведения DoS-атаки на всю систему путем инициирования увеличения частоты передачи сообщений автоматической идентификационной системы.

В качестве примера таких кибератак можно привести широко известный случай, произошедший в 2013 году, когда студенты из Техасского университета смогли отклонить от курса яхту стоимостью в 80 млн долл. с помощью имитатора GPS-сигналов, цена которого не превышала 3 тыс. долл.

По мнению ряда экспертов, основной причиной столкновения эсминцев ВМС США «Фитцджеральд» и «Мак-Кейн» с гражданскими судами в 2017 году могла стать кибератака на навигационные системы гражданских судов.

Ситуацию с обеспечением кибербезопасности на морских судах в целом можно оценить как неудовлетворительную. Согласно отчету британской компании FutureNautics, в 2018 году 43% экипажей отплыли на судах, зараженных вредоносными программами. Только 15% моряков прошли обучение по кибербезопасности.

УЯЗВИМОСТИ В СУДОВЫХ СИСТЕМАХ

Международная морская организация к уязвимым судовым системам относит:

1. Системы ходового мостика.
2. Системы обработки и управления грузом.
3. Системы управления двигателями, машинами и энергопитанием.
4. Системы контроля доступа.
6. Системы обслуживания и управления пассажирами.
7. Публичные Интернет-сети судна, предназначенные для использования пассажирами.
8. Административные системы и сети.
9. Системы связи.

Таким образом, судно крайне уязвимо перед спланированной кибератакой.

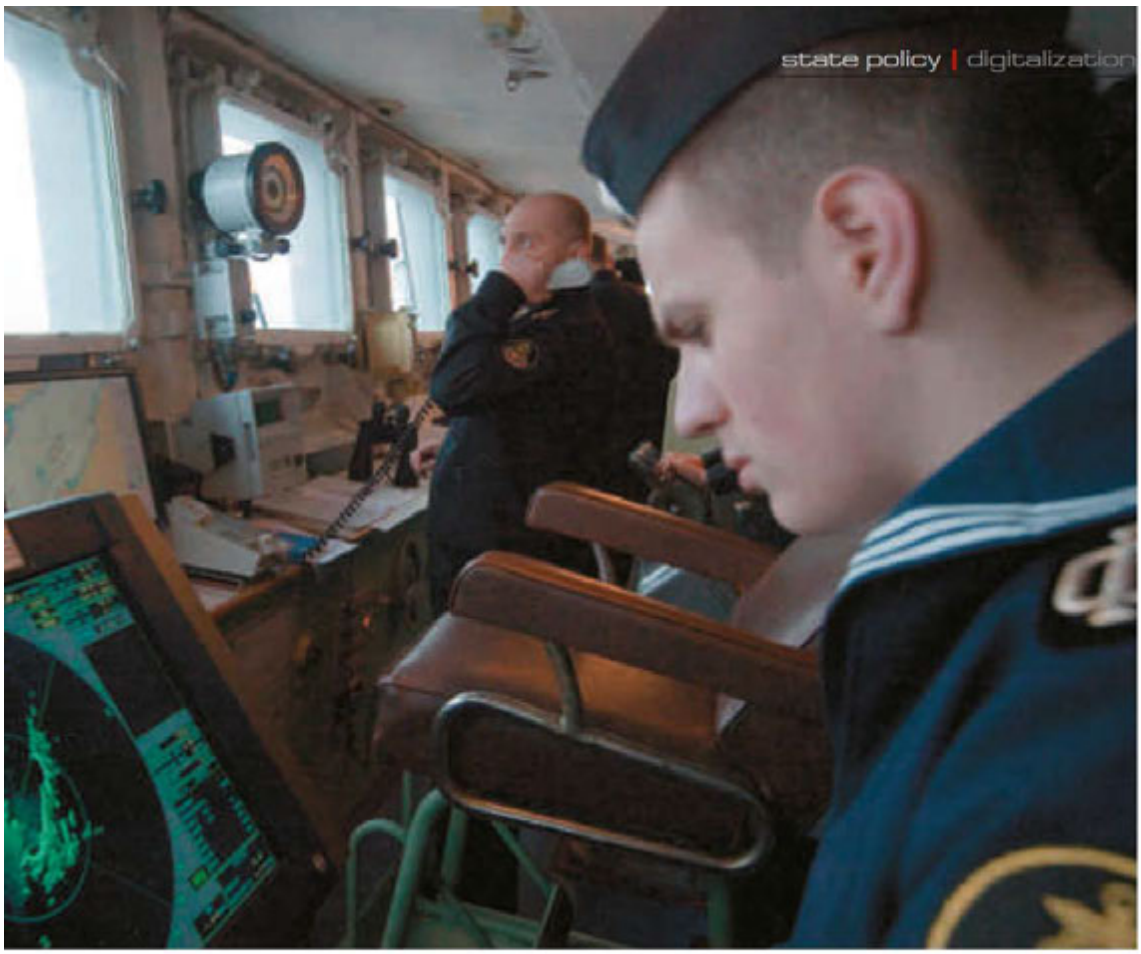
Законодательство о ТБ не рассматривает кибератаки в качестве АНВ, а угрозы их совершения – в качестве угроз АНВ

ПОРТЫ И ИНФОРМАЦИОННЫЕ УГРОЗЫ

Не только суда, но и порты необходимо защищать от информационных угроз. Неоднократные случаи кибератак на портовые системы подтверждают это.

Самый знаменитый инцидент, связанный с портовой кибербезопасностью, произошел в порту Антверпена в 2012 году. Около двух лет системы порта подвергались целевым кибератакам, организованным наркокартелем. Предположительно еще в июне 2011 года хакеры взяли под контроль системы терминала и оперировали погрузками и разгрузками без ведома порта.

В 2017 году в результате масштабной вирусной эпидемии NotPetya оста-



новилось 17 из 76 грузовых терминалов компании Maersk.

В 2018 году подверглись кибератакам порты Барселона и Сан-Диего.

В 2010 году на буровой платформе по пути из Южной Кореи в Бразилию вредоносное программное обеспечение привело к остановке систем судна. Компьютерные и контрольные системы были переполнены вирусами.

В практике израильской компании по интернет-безопасности ThetaRay имел место случай, когда хакеру удалось наклонить плавучую нефтяную вышку в сторону, заставив ее закрыться.

Для обеспечения ИБ как морских судов, так и портов необходимо принимать соответствующие меры как на международном, так и на национальном уровне.

МЕЖДУНАРОДНЫЕ ОРГАНИЗАЦИИ И КИБЕРРИСКИ

В июне 2017 года Комитет по безопасности на море принял резолюцию MSC.428(98) – управление морскими киберрисками в системах управления безопасностью. Резолюция призывает администрации обеспечить надлежащий учет киберрисков в существующих системах управления безопасностью не позднее первой ежегодной проверки документа компании о соответствии после 1 января 2021 года.

Международной организацией по стандартизации и Международной электротехнической комиссией разработан и опубликован Стандарт 27001 по информационным технологиям.

Международная морская организация (ИМО) подготовила уже третью версию «Руководства по управлению морскими киберрисками». Кроме того, этой организацией рекомендовано «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».

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РОССИИ

1 января 2018 года вступил в силу Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № ФЗ-187. Этот закон относит к объектам критической информационной инфраструктуры (далее – ИИ) информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической ИИ. Таким образом, к критической ИИ 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» (пункт 16) призывает федеральные органы исполнительной власти при рассмотрении угроз совершения актов незаконного вмешательства (далее – АНВ) в деятельность объектов транспортной инфраструктуры (далее – ТИ) при проведении оценки уязвимости и разработке планов обеспечения транспортной безопасности (далее – ТБ) учитывать способы совершения АНВ с использованием кибератак и внести соответствующие изменения в описание угроз.

В Российской Федерации отсутствует транспортный отраслевой центр компетенции по ИБ

Можно сделать вывод, что проблема обеспечения ИБ водного транспорта, включая морской, признается на международном и российском уровне, и для ее обеспечения принимаются отдельные меры. Но в плоскости нормативно-правового регулирования обеспечения ИБ существует ряд трудно разрешаемых проблем. В частности, отсутствует единый, системный и комплексный подход, унификация требований и правил.

РАЗЛИЧИЯ В ПОДХОДАХ

В Российской Федерации отсутствует транспортный отраслевой центр компетенции по ИБ. Ни в положении о Минтрансе России, ни в положении о Росморречфлоте нет ничего об ИБ в целом и о морской кибербезопасности в частности. То есть формирование единой отраслевой политики в области ИБ не является задачей или обязанностью федеральных органов власти в сфере транспорта. Федеральная служба по техническому и экспортному контролю (далее – ФСТЭК) создает общие, рамочные правила и требования в области ИБ без учета отраслевых особенностей. Важной особенностью морского транспорта является то, что вопросы ИБ регулируются также и международным законодательством, и нормами международных отраслевых объединений. Причем для бизнеса гораздо важнее соблюдение международных, а не национальных норм законодательства.

В июне 2019 года на 101-й сессии Комитета по безопасности на море обсуждалась уже 3-я редакция «Руководства по управлению морскими киберрисками» (далее – Руководство). Позиция делегации Российской Федерации по данному Руководству была выработана без участия ФСТЭК. Неизвестно, насколько его требования соответствуют тому подходу к обеспечению ИБ, который существует в РФ. С 1 января 2021 года требования Руководства становятся обязательными для судов под флагом Российской Федерации. Поэтому о различиях в подходах судовладельцы будут узнавать по факту.

Похожая ситуация сложилась и с «Руководством по кибербезопасности на судах», разработанным ведущими морскими транспортными ассоциациями. Инспектора Международного морского форума нефтяных компаний (OCIMF) уже начали проверять выполнение норм этого руководства.

Таким образом, нормы международных организаций и российского законодательства развивались и продолжают развиваться параллельно. В ближайшее время судовладельцы столкнутся с тем, что им придется одновременно выполнять и требования международных организаций, и ФЗ-187.

НЕСОГЛАСОВАННОСТЬ ПОНЯТИЙНЫХ АППАРАТОВ

Понятийный аппарат в нормативно-правовых актах международных организаций и российском законодательстве существенно различается. Так, в международных документах используется термин «кибербезопасность», в Доктрине информационной безопасности Российской Федерации – «информационная безопасность», а в документах ФСТЭК – «защита информации» и «безопасность критической информационной инфраструктуры». И это только понятия верхнего уровня.

Хотя может показаться, что с точки зрения толкования это одно и то же, разница в понятийном аппарате при правоприменении создает практически непреодолимые барьеры в регулировании однотипных и схожих правоотношений. Следствием этого станет необходимость разработки двух систем ИБ, которые будут функционировать параллельно.

Так, Международная морская организация рекомендует осуществлять управление в отношении киберрисков через естественное расширение существующих методов управления безопасностью мореплавания и безопасностью судна. Кибербезопасность рассматривается как часть морской безопасности. Российское законодательство регулирует различные аспекты безопасности разными, не взаимосвязанными нормативными правовыми актами. В результате, с точки зрения российского законодательства, реализация единого и комплексного подхода к обеспечению безопасности судна практически невозможна.

Позиция ФСТЭК, высказанная публично, заключается в том, что меры по обеспечению безопасности критической ИИ могут быть предусмотрены в едином плане обеспечения безопасности объекта критической ИИ. Как видим, подходы к планированию мер обеспечения информационной безопасности у ИМО и ФСТЭК схожи. Однако пока неясно, как ФСТЭК будет реагировать на запланированные меры по ФЗ-187, если они найдут свое отражение в планах, выполненных в соответствии с требованиями ИМО.

С точки зрения обеспечения ТБ различия в позициях могут стать причиной возникновения рисков для судов и портовой инфраструктуры. Банк данных угроз безопасности информации по состоянию на 30 апреля 2019 года содержит сведения о 213 угрозах и 21 237 уязвимостях программного обеспечения и программно-аппаратных средств. Однако законодательство о ТБ вообще не рассматривает кибератаки в качестве АНВ, а угрозы их совершения – в качестве угроз АНВ.

Порядок разработки планов обеспечения ТБ объектов ТИ и транспортных средств (далее – ТС), утвержденный приказом Минтранса России от 11 февраля 2010 года № 34, не предусматривает отражения в планах обеспечения ТБ сведений о киберугрозах и мерах по защите от них.

То есть ИБ – отдельно, а ТБ – отдельно.

ТСОТБ И ПРАВОВОЕ РЕГУЛИРОВАНИЕ

Еще один пример рассогласованности связан с техническими средствами

обеспечения транспортной безопасности (далее – ТСОТБ). Существенным элементом ТСОТБ являются системы и средства видеонаблюдения.

В соответствии с пунктом 8 ст. 12.2. Федерального закона «О транспортной безопасности» от 09 февраля 2007 года ФЗ-16 ТСОТБ подлежат обязательной сертификации. Требования к функциональным свойствам ТСОТБ и порядок их сертификации определены Постановлением Правительства РФ от 26 сентября 2016 года № 969.

Судовая телевизионная система охранного наблюдения является подтерминалы (код 11100702), щиты, пульты контроля и сигнализации (код 11100703) и датчики и другие элементы (код 11100704).

С точки зрения ФЗ-187 отдельные системы ТСОТБ и судовые телевизионные системы охранного наблюдения являются его объектами правового регулирования, а с точки зрения ИМО на них могут распространяться рекомендации «Руководства по управлению морскими киберрисками».

То, насколько все эти требования будут уживаться вместе и насколько мо организовать работу по гармонизации существующих правовых норм и упрощению формальностей. В связи с тем, что отраслевые федеральные органы исполнительной власти некомпетентны в вопросах ИБ, организацию и осуществление этой работы необходимо взять на себя отраслевым профессиональным объединениям. Хорошим примером здесь может послужить совместная работа отраслевых международных объединений (BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, OCIMF, IUMI и Всемир-

надзорной Российскому Морскому Регистру Судоходства и должна отвечать его требованиям, а также иметь сертификат типового одобрения. Она включена в номенклатуру объектов технического наблюдения Регистра (код 044000, Правила технического наблюдения за постройкой судов и изготовлением материалов и изделий для судов. Т 1, часть 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 видеонаблюдения: видеокамеры (код 11100701), видеоэто будет дорого для судовладельцев, покажет только практический опыт.

Необходимо также отметить, что под двойное регулирование по ИБ (ИМО и ФЗ-187) попадут и другие системы судна, прежде всего системы автоматизации.

РАБОТА НАД ПОЛИТИКОЙ КИБЕРБЕЗОПАСНОСТИ В РОССИИ

Приведенные выше примеры иллюстрируют возможные негативные сценарии, которые приведут к разного рода сложностям. Схожие проблемы есть и у речного транспорта, портов, береговой инфраструктуры, да и в целом у транспортной отрасли. Если на практике их решение будет сложным и затратным, то для морских судов возникнет дополнительный аргумент в пользу ухода из реестров судов Российской Федерации под «удобный флаг».

Пока отрасль находится в самом начале пути по внедрению требований по обеспечению ИБ, необходиного совета судоходства) по разработке «Руководства по кибербезопасности на судах».

Активное участие в разработке рекомендуемых практик, руководящих принципов и стандартов по кибербезопасности принимают классификационные общества. В частности, крупнейшее классификационное общество DNV GL в 2016 году разработало рекомендуемые практики «Управление устойчивостью к кибербезопасности для судов и мобильных морских установок в эксплуатации», а ведущее классификационное общество Японии ClassNK разрабатывает свои подходы к обеспечению бортовой кибербезопасности для судов. Учитывая это, Российский Морской Регистр Судоходства можно и нужно привлечь к данной работе. Сама работа по разработке национального подхода к обеспечению морской кибербезопасности должна проводиться в непосредственном взаимодействии со ФСТЭК.