Сергей Семенов, начальник ФБУ «Служба морской безопасности»

Морская кибербезопасность — ситуация, проблемы и риски

Комитет по безопасности на море Международной морской организации (ИМО) в июне 2017 г. принял резолюцию MSC.428(98) — Управление морскими киберрисками в системах управления безопасностью. Резолюция призывает администрации обеспечить учет киберрисков в системах управления безопасностью судов после 1 января 2021 г.

Несмотря на многолетнее внимание ИМО, сфера морской кибербезопасности остается отчасти латентной. Владельцы бизнеса часто скрывают информацию об успешно проведенных в отношении них кибератаках, опасаясь таких последствий, как потеря имиджа, претензии со стороны клиентов и страховых компаний, расследования, проводимые сторонними организациями и государственными органами.

Но все же анализ СМИ позволяет описать текущее состояние морской кибербезопасности и привести ряд интересных примеров. Так, в 2017 г. вирусом *NotPetya* были заражены 17 из 76 грузовых терминалов компании Maersk. Ущерб составил около 300 млн евро. В 2018 г. кибератакам подверглись порты Барселона и Сан-Диего. 9 мая 2020 г. иранский терминал Шахид Раджаи испытал на себе кибератаку, которую предположительно провел Израиль. В 2020 г. кибератакам дважды подверглась австралийская логистическая группа компаний *Toll Group*. В апреле 2020 г. от кибератаки пострадала крупнейшая судоходная контейнерная компания *Mediterranean Shipping*. В середине мая в результате кибератаки были зашифрованы приблизительно 370 (20%) рабочих станций и 20 (10%) серверов компании *Anglo-Eastern*.

Израильская компания *Naval Dome*, специализирующаяся в области морской кибербезопасности, провела серию успешных демонстрационных кибератак на морские суда. В результате атак «хакерами» были изменены сведения о местоположении судна, введен в заблуждение дисплей РЛС, включалось и выключалось судовое оборудование, были взяты под контроль системы управления топливом, рулевое управление и балластная система. Видеоролик о результатах кибератаки доступен на сайте компании.

Около 64% опрошенных в 2020 г. журналом *Safety at Sea* и организацией *BIMCO* в рамках опроса о морской кибербезопасности заявили, что их компании имеют план обеспечения непрерывности деятельности в случае киберинцидента. Полученный в ходе опроса процент кажется существенным. Однако это доля только среди тех, кто согласился принять участие в опросе.

По оценкам Лондонского Ллойда, ущерб от кибератак в морской отрасли оценивается в 200 млрд долларов. При низком уровне страхования примерно только 10% убытков от кибератак будет покрыто страховкой.

Основным трендом последнего времени является то, что кибератаки все чаще являются частью и инструментом общего по замыслу преступления, а не самодостаточным преступлением. Злоумышленники все меньше заинтересованы только в краже данных из корпоративных *IT-систем*. Сейчас они активно пытаются понять, как взять под контроль

эксплуатационные сети и системы судов, обозначаемые термином *operational technology*. По мнению экспертов журнала *Maritime Executive*, эволюция морского пиратства может привести к тому, что пираты смогут захватывать командные и контрольные системы судна.

Белая книга по кибербезопасности Международной ассоциации портов и гаваней акцентирует внимание на том, что судно само по себе также может представлять угрозу для портового объекта.

По мнению Британской ассоциации портов, глобальный рынок кибербезопасности вырастет с 144 млрд фунтов стерлингов до 182 млрд фунтов стерлингов к 2021 г.

Вышеприведенные факты опубликованы на иностранных тематических информационных ресурсах, где теме морской кибербезопасности уделяется серьезное внимание. Мониторинг позволяет констатировать, что с 1 мая только на четырех англоязычных интернет-ресурсах было опубликовано более 20 статей на тему морской кибербезопасности. При этом 5 из них были посвящены выпуску различных международных и национальных рекомендаций по кибербезопасности. В одной сообщалось о внесении в сенат США законопроекта об усилении морской кибербезопасности. В другой — о создании портами США некоммерческого центра кибербезопасности.

Документы о морской кибербезопасности разработаны и внедряются властями США, Великобритании, Евросоюза, Дании, Норвегии и Сингапура. Естественно, список не исчерпывающий. При этом «Руководство по внедрению системы кибербезопасности в транспортном секторе» Министерства внутренней безопасности США опубликовано в 2015 г., Руководство «Кибербезопасность портов и портовых систем» Лондонского Инженерно-технологического института при поддержке Минтранса Великобритании и Минобороны Великобритании — в 2016 г., а их «Свод правил кибербезопасности для судов» — в 2017 г.

В июле 2017 г. Международная морская организация рекомендовала «Руководство по кибербезопасности на борту судов», разработанное ведущими судоходными компаниями мира.

С января 2018 г. Международный морской форум нефтяных компаний (*OCIMF*) сделал оценку кибербезопасности в рамках Программы самооценки и управления танкерами обязательной частью коммерческих контрактов.

Классификационное общество *DNV GL* с 2017 г. предоставляет услугу по утверждению типа кибербезопасности судна, а в 2018 г. разработало обозначение класса кибербезопасности связанного с уровнем охраны.

Стоит обратить внимание на то, что за рубежом регулирование морской кибербезопасности осуществляется в рамках отраслевого подхода, путем дополнения рекомендаций Международной морской организации национальными требованиями и рекомендациями.

Морская информационная безопасность в России

В России морская информационная безопасность не является актуальной темой для отрасли. Русскоязычных публикаций по этой теме практически нет, осведомленность в среднем находится на зачаточном уровне.

Несмотря на то, что Россия, являясь членом Международной морской организации, участвовала в обсуждении и приеме ее документов о морской кибербезопасности, каких-либо действий как правительство-член или администрация флага Россия не предпринимала и не предпринимает.

Обращаю внимание на то, что циркуляром ИМО, в принятии которого участвовала и Россия, рекомендуется «Рамочная структура для улучшения кибербезопасности критически важной инфраструктуры» Национального института стандартов и технологий США. Вышеупомянутое «Руководство по кибербезопасности на борту судов» также разработано при участии Национального института стандартов и технологий США и Береговой охраны США.

Не исключено, что морская отрасль России, включая суда под Государственным флагом Российской Федерации в части, касающейся морской кибербезопасности, будет руководствоваться рекомендациями государственных структур США.

Специальное нормативное правовое регулирование морской информационной безопасности Российской Федерацией не осуществляется, доктринальные документы (например, Морская доктрина Российской Федерации) данный вопрос не затрагивают.

Функция выработки государственной политики и нормативно-правового регулирования в сфере информационной безопасности к компетенции Минтранса России не относится. К задачам созданного в 2019 г. Департамента цифровой трансформации Минтранса относится проведение единой технической политики, организация и координация работ по информационной безопасности и технической защите информации только в министерстве.

Правительством Российской Федерации полномочия в сфере морской информационной безопасности на Росморречфлот также не возложены.

К специальному законодательству по противодействию киберугрозам, принятому Российской Федерацией, можно отнести институт права, сформированный Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» (от 26.07.2017 № 187-ФЗ). Однако данный закон является универсальным и общим для всех отраслей экономики и не учитывают специфику транспорта в целом и отдельных видов транспорта, в частности, морского. Он в первую очередь нацелен на защиту значимых объектов критической информационной инфраструктуры, к которым относит исчерпывающий перечень объектов: информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления. Для закона не имеет существенного значения, в какой отрасли, на каком объекте используются вышеуказанные сети и системы. Закон рассматривает в качестве объектов защиты именно сами сети и системы, а не объекты, которыми они эксплуатируются. Международный же подход нацелен на защиту именно судна или портового средства.

В этом, наверно, главное отличие международного подхода от российского. Другим отличием является то, что для российского законодательства ключевое значение имеет значимость защищаемого объекта, которая рассматривается как основание для защиты. Объекты, не относящиеся к значимым объектам критической информационной инфраструктуры, вообще выпадают из правового регулирования ФЗ-187. Международные же рекомендации распространяются на все суда и портовые средства, но реализуются в части, их касающейся.

Требования ФЗ-187 не увязаны с отраслевыми подходами и требованиями к обеспечению иных видов морской безопасности. Они не содержат практических руководств. Без адаптации и компетентного разъяснения их сложно использовать на практике, на конкретном судне или портовом средстве.

Также международные документы в качестве объектов киберзащиты выделяют *IT*-системы и *OT*-системы, причем рассматриваются они во взаимосвязи и взаимодействии. Наиболее подходящим российским термином для описания *OT*-систем может быть автоматизированные системы управления технологическими процессами. ФСТЭК приказом № 31 2014 г. утверждены требования к таким АСУ. Но данные требования имеют цель защитить информацию, обрабатываемую АСУ. И они распространяются только на АСУ на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность. Какие-либо отраслевые особенности в требованиях отсутствуют.

Серьезной проблемой для комплексного подхода к морской кибербезопасности в Российской Федерации является создание единого понятийного аппарата.

Выше был приведен пример, связанный с отсутствием однозначного синонима к англоязычному термину «*operational technology*», занимающего ключевое положение в международных рекомендациях. Также в русском языке термины «кибербезопасность» и «информационная безопасность» не являются синонимами. Нет единства в терминологии и в российских документах.

«Доктрина информационной безопасности Российской Федерации» использует термины «информационная безопасность» и «обеспечение информационной безопасности», ФЗ-187 — «безопасность критической информационной инфраструктуры», а ФСТЭК России — «обеспечение защиты информации».

«Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг.» вводит понятие «индустриальный интернет», под которым понимает концепцию построения информационных и коммуникационных инфраструктур на основе подключения к информационно-телекоммуникационной сети Интернет промышленных устройств, оборудования, датчиков, сенсоров, систем управления технологическими процессами, а также интеграции данных программно-аппаратных средств между собой без участия человека. Ни в «Доктрине информационной безопасности», ни ФЗ-187, ни в документах ФСТЭК данное понятие не найдено. Не ясно, можно ли отнести, например, АСУ ТП и *OT*-системы судов и портов к индустриальному интернету. Есть ли у него особенности киберзащиты?

Наличие разнообразной и не взаимоувязанной терминологии не способствует осведомленности морской отрасли о кибербугрозах и ее эффективной киберзащите.

До 1 января 2021 года меньше 6 месяцев

С 1 января 2021 г. морские администрации ряда стран начнут проверки заходящих в их порты судов на предмет выполнения рекомендаций ИМО по кибербезопасности. Как было отмечено в начале статьи, резолюция ИМО MSC.428(98) призывает администрации обеспечить учет киберрисков в системах управления безопасностью судов. Однако во исполнение резолюции российская сторона вообще ничего не сделала. Вопрос пущен на самотек. Далеко не все судовладельцы и операторы судов знают, что делать и, самое главное, не понимают как.

Отсюда можно сделать логический вывод о том, что у судов под Государственным флагом Российской Федерации в иностранных портах, начиная с 1 января 2021 г., могут возникнуть риски санкций за невыполнение рекомендаций ИМО по кибербезопасности. Невыполнение рекомендаций по кибербезопасности может послужить причиной отказа российскому судну в коммерческом контракте со стороны фрахтователя. Тарифные ставки страхования морских грузов, вероятно, будут отличаться для судов, выполняющих и не выполняющих рекомендации по кибербезопасности, что может снизить конкурентную способность российского флота.

С 2021 г. киберинциденты на интерфейсе судно/порт будут рассматриваться через призму рекомендаций по кибербезопасности. В результате наши порты могут признаваться небезопасными с точки зрения кибербезопасности (аналогия с перечнем небезопасных с точки зрения охраны портов) и судам, заходящим в такие порты России или побывавшим в них, будут рекомендоваться повышенные меры кибербезопасности. Соответственно, это повлияет на экономическую привлекательность портов и стоимость перевозок из и в них. Кроме того, невыполнение РФ международных норм может служить поводом для санкций как в отношении РФ — члена ИМО, так и портов РФ.

Случаи кибератак на судовые системы через интерфейс судно/порт могут послужить поводом для как финансовых претензий, так и политических. В этой связи заголовок в СМИ о том, что Россия организует кибератаки на суда, вероятно, в мире скептически воспринят не будет.

Выше были приведены примеры кибератак на зарубежные порты.

Вместе с тем, о состоянии информационной безопасности даже в ведущих российских портах ничего не известно. А ведь успешная кибератака на порт сразу ведет к многомиллионным убыткам.

Киберинциденты могут негативно влиять не только на имидж конкретного российского порта или компании, но и на имидж России как государства — члена ИМО.

Также обращаю внимание на то, что морская кибербезопасность не заканчивается на том, чтобы вписать несколько строк в существующую систему управления безопасностью судна. Рекомендуемое ИМО «Руководство по кибербезопасности на борту судов» определяет следующий круг субъектов кибератак:

- активисты (включая недовольных сотрудников);
- преступники;
- оппортунисты;
- государства;
- спонсируемые государством организации;
- террористы.

Если против первой категории СУБ еще как-то помочь может, то для защиты от всех остальных категорий она защитить не способна. Необходима более серьезная система мер.

В частности, за рубежом наблюдается консенсус об отношении оценки кибербезопасности и плана кибербезопасности к другим документам. План кибербезопасности для судна должен являться приложением к плану охраны судна. У иностранных специалистов есть консенсус и в отношении того, что роль должностного лица, ответственного за охрану, должна эволюционировать так, чтобы охватить вопросы кибербезопасности.

На мой взгляд, к вышеперечисленным рискам необходимо отнестись серьезно. Лучше заранее принять меры по их предупреждению, чем дожидаться стимула в виде кибератаки или санкций.

Дата публикации: 8 сентября 2020 г.

Источник: РСМД https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/morskaya-kiberbezopasnost-situatsiya-problemy-i-riski/