АНАЛИЗ ПРОБЛЕМ И ПУТИ РОБОТИЗАЦИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРИМЕНИТЕЛЬНО К ОБЪЕКТАМ МОРСКОЙ ТЕХНИКИ И МОРСКИМ ТРАНСПОРТНЫМ СИСТЕМАМ

К. В. Балицкая (Санкт-Петербург)

Актуальность темы. Морские автоматизированные системы управления (АСУ) в зависимости от своего предназначения содержат в себе информацию, поступающую с различных подсистем, отвечающих за перемещение тех или иных объектов, различные характеристики, данные датчиков, локационные данные и содержат в себе параметрически заданные алгоритмы выполнения поставленных задач. АСУ – как информационная сеть, аккумулирующая и хранящая в себе данные необходимые для жизнеспособности и правильного функционирования объекта управления при использовании на критически важных объектах инфраструктуры, таких как морские транспортные системы, морские порты, подвержена опасности нарушения своей целостности, доступности и конфиденциальности, т.е. нарушению состояния информационной безопасности.

Формулировка проблемы. Особенностью покушения на информационные ресурсы объектов морской техники является их неотслеживаемость на длительном временном промежутке воздействия оказываемой атаки. Нарушение информационной безопасности на море оказывает влияние на стабильность работы и репутацию отдельных корпораций, финансовое благополучие отрасли, а также может нанести непоправимый вред окружающей среде. Морской сектор является основным игроком в глобальной торговой инфраструктуре и транспорте. Доставка товаров по морю, транспортные перевозки, представляют собой уникальную проблему кибербезопасности из-за участия в обмене информацией большого количества стран с различной политикой и ресурсами по обеспечению информационной безопасности на море. Стандартные навигационные системы, такие как системы глобального позиционирования (GPS), системы автоматической идентификации (AIS) и системы отображения электронных карт и информации (ECDIS), повысили физическую безопасность благодаря международному регулированию. Тем не менее, с их технологическими достижениями возникает новая угроза атаки, благодаря которой злоумышленники, например, подменяют данные маршрута и перенаправляют суда по ложному пути следования [1].

Одной из основных угроз безопасности на море является отсутствие подготовки экипажа в области информационной безопасности (ИБ). Низкая осведомленность членов экипажа об использовании их собственных устройств в связи с частотой возникновения уже обзавелась собственной аббревиатурой («Принесите свое собственное устройство» или BYOD). Подключение своих устройств к системам кораблей для их зарядки может привести к появлению вредоносного ПО.

В 2017 году в судоходной отрасли произошел один из самых крупномасштабных инцидентов нападения на информационные ресурсы международной судоходной компании Maersk, в результате которого большая часть компьютерной сети компании была заражена вредоносным ПО «WannaCry NotPetya», что по данным, предоставленным Maersk, нанесло ущерб в размере 300 миллионов долларов [1], и положило начало информационной борьбе в среде, где национальные границы не имеют значения, и где сопутствующий ущерб наносится по неизвестной логике и несет непредсказуемые и жестокие последствия.

Постановка задачи. На сегодняшний день политика большинства стран в связи с высокой степенью актуальности проблемы и масштабом ущерба от ее реализации,

направлена на повышение защищенности критической информационной инфраструктуры (к которой непосредственно отнесен морской транспортный сектор) и устойчивости ее функционирования [2-3]. Обеспечение состояния защищенности от внутренних и внешних угроз систем управления безопасностью объектов морской техники неразрывно связано с возможностью своевременной оценки рисков и способностью АСУ противостоять известным угрозам ИБ, а также предупреждать возможность появления инцидентов ИБ на основе имеющейся аналитики системы. Аналитические данные АСУ объекта морской техники должны обладать свойствами полноты, достоверности и формироваться в режиме реального времени.

Неотъемлемой частью АСУ объекта морской техники является человек, оператор подсистемы, специалист ИБ, принимающий решения и расследующий инциденты нарушения режима ИБ. Одними из ключевых задач целеполагания специалиста, обеспечивающего ИБ являются:

1. расследование инцидентов нарушения ИБ, выяснение цели нарушителя;
2. контроль за соблюдением политики разграничения доступа, контроль за использованием информации, содержащейся на внутренних носителях, перемещаемой на/с внешних носителей;
3. организационно-распорядительная работа с документацией по фиксации инцидентов на бумаге для дальнейшего анализа и доработки системы ИБ;
4. восстановление хронологии событий, привлекшей к инциденту;
5. восстановление данных из теневой копии.

Практически все задачи, связанные с обнаружением, предупреждением и нейтрализацией угроз, имеют целый ряд общих признаков. Любая физическая среда, любое пространство, подвергаемое процедуре мониторинга, обладают определенными интегральными параметрами и характеристиками в «спокойном» состоянии. Возникновение каких-либо угроз или потенциально опасных процессов в этих пространствах непременно ведут к изменению их характеристик, появлению возмущений в системе, которые поддаются фиксации и анализу, для последующего формирования противодействия. При этом эпицентр бедствия может наблюдаться не в момент возникновения угрозы, а как следствие неверного и/или несвоевременного управленческого решения по нейтрализации угрозы.

Критерии, обеспечивающие защищенность объекта критической информационной инфраструктуры, подразумевают наличие системы мониторинга состояния защищенности объекта морской инфраструктуры [4], а также наличия высокой квалификации и осведомленности каждого сотрудника в области текущего состояния ИБ.

Новизна предложений. Для реализации задачи обеспечения защищенности АСУ объекта морской техники и морских транспортных систем предлагается минимизация влияния негативного «человеческого фактора» при формировании управленческих решений, и увеличение эффективности функционирования АСУ посредством роботизации управления. Роботизация управления морскими АСУ будет достигаться за счет автоматического формирования в системе решений по ликвидации инцидентов, формированию упреждающих уведомлений о потенциальных зонах риска, за счет возможности реагирования на инцидент в автоматическом режиме в соответствии с выбранной политикой, оставляя за специалистом АСУ задачу целеполагания.

При формировании и внедрении политик ИБ предлагается использование метода оценки интегрированных (агрегированных) показателей уровня информационной защищенности по каждому возможному каналу нарушения состояния защищенности значимой информации, в том числе, методом квалиметрической оценки качества [5].

Заключение. В связи с усложнением технологических решений, используемых в морской отрасли, необходимостью постоянного поиска верных решений по реагированию на возникающие угрозы информационной безопасности эффект влияния человеческого фактора возрастает от совокупности объема информации, которой необходимо свободно владеть лицу, принимающему решения, до влияния стрессовых факторов в сложной ситуации, требующей незамедлительного действия. С точки зрения психологических возможностей человека по концентрации внимания – человек способен отслеживать лишь семь визуальных объектов одновременно, что значительно меньше числа объектов управления АС.

Сложность построения эффективной системы управления информационной безопасностью на объектах морской техники неразрывно связана с системой формирования адекватных контрмер на актуальные угрозы. Необходимость интеграционного подхода к управлению морской АС определяется сложностью самого объекта и степенью взаимозависимости параметров, обеспечивающих его функционирование. Это, в свою очередь, обуславливает необходимость реализации единого и своевременного управленческого решения, обеспечивающего оптимальное поведение объекта управления в условиях внешних воздействий и внутреннего развития. Обеспечение вышеуказанных условий может быть достигнуто только при условии взаимной согласованности во времени процессов управления каждым объектом, входящим в АС, а также ускоренного совершенствования и развития морских АСУ.

Литература

1. The Marine Express, Inmarsat strengthen cyber security for Maritime December. – [Электронный ресурс] URL: http://themarineexpress.com/the-marine-express-december (дата обращения: 11.06.2019).
2. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (зарегистрирован в Минюсте России 26 марта 2018 г. № 50524). Опубликован 26 марта 2018 г.
3. Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
4. **Алексеев А.В., Соловьев С.Н., Москаленко В.А., Сус Г.Н., Ушакова Н.П., Каганский М.А.** Мониторинг процессов и информационная поддержка обеспечения безопасности объектов морской техники // Сборник материалов X Научно-практической конференции «Актуальные проблемы профессиональной подготовки командиров кораблей и специалистов ВМФ», 30 мая 2017 г. СПб, ВИ ДПО ВУНЦ ВМФ «ВМА», С. 120-126.
5. **Алексеев А.В., Орлов К.М.** Квалиметрическая оценка подсистем визуализации и обработки информации корабельных автоматизированных систем управления // Состояние, проблемы и перспективы разработки корабельных информационно-управляющих комплексов (эффективность, надежность, экономика). Сб. докладов научно-технической конференции. М.: ОАО «Концерн «Моринформсистема-Агат», 2011.