Руководство по кибербезопасности на борту судов. Версия 4

Неофициальный перевод
Шевелев В.Я.

Условия использования

Советы и информация, представленные в этой публикации, предназначены исключительно для ознакомления и используются пользователем на свой страх и риск. Мы не даем никаких гарантий или заверений, а также не берем на себя никаких обязательств по проявлению заботы или ответственности со стороны авторов, их членов или сотрудников каких-либо лиц, фирм, корпораций или организаций (которые каким-либо образом были связаны с предоставлением информации или данных, компиляцией или любым переводом, публикацией, или за предоставление данной публикации) за точность любой информации или рекомендаций, приведенных в данной публикации; или за любое упущение в руководстве, или за любые последствия, которые прямо или косвенно являются результатом соблюдения, принятия или доверия к руководству, содержащемуся в данной публикации, даже если это вызвано несоблюдением разумной осторожности в отношении является частью любой из вышеупомянутых сторон.

Оглавление

Цель этого руководства — повысить безопасность моряков, окружающей среды, грузов и судов. Рекомендации призваны помочь в разработке надлежащей стратегии управления киберрисками в соответствии с действующими нормативными актами и передовым опытом на борту судна с упором на рабочие процессы, оборудование, обучение, реагирование на инциденты и управление восстановлением. Судоходство все больше полагается на цифровые решения для выполнения повседневных задач. Быстрое развитие информационных технологий, доступность данных, скорость обработки и передачи данных предоставляют судовладельцам и другим участникам морской отрасли больше возможностей для оптимизации работы, экономии средств, повышения безопасности и более устойчивого ведения бизнеса. Однако эти разработки в значительной степени зависят от расширения возможностей подключения, часто через Интернет, между серверами, ИТ-системами и ОТ-системами, что повышает потенциальные кибер-уязвимости и риски. В рекомендациях объясняется, почему и как следует управлять кибер-рисками в сфере судоходства. Перечислена сопроводительная документация, необходимая для проведения оценки рисков, и описан процесс оценки рисков с объяснением роли каждого компонента киберриска. В этой публикации подчеркивается важность оценки вероятности и угрозы в дополнение к последствиям и уязвимостям при проведении оценки киберрисков. Наконец, в этой публикации даются советы о том, как реагировать на киберинциденты и восстанавливаться после них.

Подходы к управлению киберрисками будут зависеть от компании и судна, но должны соответствовать требованиям соответствующих национальных, международных и государственных норм и правил. В 2017 году Международная морская организация (ИМО) приняла резолюцию MSC.428(98) об управлении киберрисками на море в рамках системы управления безопасностью (СУБ). В резолюции говорится, что утверждённая СУБ должна учитывать управление киберрисками в соответствии с целями и функциональными требованиями (Международного кодекса по управлению безопасностью) ISM. Кроме того, это побуждает администрации обеспечить надлежащее устранение киберрисков в СУБ не позднее первой ежегодной проверки документа о соответствии требованиям (DoC) компании после 1 января 2021 года. В том же году ИМО разработала рекомендации по управлению киберрисками на море, которые содержат общие рекомендации по управлению киберрисками на море для защиты судоходства от существующих и новых киберугроз и уязвимостей. Как также указано в рекомендациях ИМО, эффективное управление киберрисками должно начинаться на уровне высшего руководства. Высшее руководство должно внедрить культуру управления киберрисками на всех уровнях и во всех подразделениях организации и обеспечить целостный и гибкий режим управления киберрисками, который работает непрерывно и постоянно оценивается с помощью эффективных механизмов обратной связи. Помимо резолюции ИМО, при разработке этих рекомендаций также учитывалась структура кибербезопасности Национального института стандартов и технологий США (NIST) версии 1.1 (апрель 2018 г.).

Система кибербезопасности NIST помогает компаниям в их подходе к оценке рисков, помогая им понять эффективный подход к управлению потенциальными киберрисками как внутри компании, так и за ее пределами. В результате применения фреймворка разрабатывается “профиль”, который может помочь определить и расставить приоритеты в действиях по снижению киберрисков. Профиль также может использоваться в качестве инструмента для согласования политических, деловых и технологических решений по управлению рисками. Образцы рамочных профилей находятся в открытом доступе для морских перевозок наливных жидкостей, в открытом море и 1 Системы операционных технологий (OT) включают аппаратное и программное обеспечение, которое отслеживает и/или контролирует физические устройства, процессы и события. Системы информационных технологий (IT) включают аппаратное и программное обеспечение, которое управляет данными (т. е. IT-системы не контролируют физические устройства, процессы или события). 2 MSC-FAL.1/Circ.3 «Руководство по управлению киберрисками на море».

Операции с пассажирскими судами3. Эти профили были созданы Береговой охраной США и Национальным центром передового опыта в области кибербезопасности NIST при участии представителей отрасли. Профили NIST могут использоваться вместе с этими рекомендациями, чтобы помочь отрасли в оценке, определении приоритетов и снижении киберрисков.

Рекомендации также доступны от других ассоциаций, таких как Ассоциация цифровых контейнерных перевозок (DCSA) «Руководство по внедрению DCSA для обеспечения кибербезопасности на судах версии 1.0». Рекомендации DCSA основаны на анализе третьей версии этих рекомендаций и концепции NIST. Хотя целевой аудиторией рекомендаций DCSA является контейнерная отрасль, другие сегменты судоходства также могут найти их полезными для ознакомления.

Международная ассоциация классификационных обществ (IACS) выпустила «Рекомендацию по киберустойчивости (№ 166)». Эта рекомендация объединяет предыдущие 12 рекомендаций IACS, связанных с киберустойчивостью (с № 153 по № 164), и применяется к использованию компьютерных систем, которые обеспечивают функции управления, сигнализации, мониторинга, безопасности или внутренней связи, подпадающие под требования классификационного общества. Рекомендация IACS применяется только к новым судам, но может служить руководством и для существующих судов. Ожидается, что со временем IACS разработает единые требования, которые также будут применяться только к новым судам. Данная публикация не предназначена для того, чтобы служить основой для проведения внешнего аудита или проверки подхода отдельных компаний и судов к управлению киберрисками, и не должна восприниматься как призыв к проведению внешнего аудита или проверке подхода отдельных компаний и судов к управлению киберрисками.

Кибербезопасность и управление рисками

1.1 Характеристики кибербезопасности в морской отрасли Кибербезопасность важна из-за её потенциального влияния на персонал, судно, окружающую среду, компанию и груз. Кибербезопасность связана с защитой ИТ, ОТ, информации и данных
от несанкционированного доступа, манипуляций и сбоев.

Киберинциденты могут возникать в результате, например:

- инцидент, связанный с кибербезопасностью, который влияет на доступность и целостность ОТ, например, повреждение данных о картах, хранящихся в электронной картографической информационно-управляющей системе (ECDIS).
- непреднамеренный сбой системы, возникающий во время обслуживания и установки обновлений программного обеспечения, например, из-за использования зараженного USB-накопителя для завершения обслуживания - потеря или искажение данных внешних датчиков, критически важных для работы судна. Сюда входят, но не ограничиваются ими, глобальные навигационные спутниковые системы (GNSS), в том числе система глобального позиционирования Система (GPS) является наиболее часто используемой.
- сбой системы из-за программных ошибок и/или «багов» - взаимодействие экипажа с попытками фишинга, которые являются наиболее распространенным вектором атак со стороны злоумышленников, что может привести к потере конфиденциальных данных и проникновению вредоносного ПО в бортовые системы.

Морская отрасль обладает рядом характеристик, которые влияют на ее уязвимость к киберинцидентам.

К ним относятся:

- участие нескольких заинтересованных сторон в эксплуатации и фрахтовании судна, что потенциально
приводит к отсутствию ответственности за инфраструктуру ИТ- и ОТ-систем и судовые сети
- использование устаревших ИТ- и ОТ-систем, которые больше не поддерживаются и/или основаны на устаревших операционных системах.
- использование ОТ-систем, которые нельзя обновить или защитить от вирусов из-за проблем с сертификацией.
- суда, которые взаимодействуют онлайн с береговыми службами и другими участниками глобальной цепочки поставок.
- судовое оборудование, которое дистанционно контролируется и к которому осуществляется доступ, например, со стороны производителей или поставщиков услуг.
- обмен критически важной для бизнеса, конфиденциальной и коммерческой информацией с поставщиками услуг на берегу, в том числе с морскими терминалами и стивидорами, а также, в соответствующих случаях, с государственными органами.
- наличие и использование критически важных систем, управляемых компьютером, в которых могут быть установлены не последние обновления или которые могут быть должным образом не защищены, для обеспечения безопасности судна и защиты окружающей среды.

- культура управления киберрисками, которая всё ещё имеет потенциал для улучшения, например, за счёт более формализованного обучения, тренингов и уточнения ролей и обязанностей.
- зачастую система автоматизации состоит из множества подсистем от разных поставщиков, которые интегрируются на верфях с минимальным учётом киберпроблем.

Эти элементы следует учитывать, а соответствующие части включать в политику кибербезопасности компании и СУБ.

Растущее использование комплексного анализа данных, «умных» судов и «промышленного интернета вещей» (IIoT) увеличит объём информации, доступной субъектам угроз, и потенциальную поверхность атаки для киберпреступников. Это требует надёжных подходов к управлению киберрисками.

Управление киберрисками должно быть неотъемлемой частью культуры безопасности компании, способствующей безопасной и эффективной эксплуатации судна, и внедряться на различных уровнях компании, включая высшее руководство на берегу и персонал на борту. Управление киберрисками должно включать в себя:

- определение ролей и обязанностей пользователей, ключевого персонала и руководства как на берегу, так и на борту;
- определение систем, активов, данных и возможностей, нарушение работы которых может создать риски для эксплуатации и безопасности судна;
- внедрение технических и процедурных мер для защиты от киберинцидентов, своевременное обнаружение инцидентов и обеспечение непрерывности операций;

- план действий в чрезвычайных ситуациях, который регулярно отрабатывается.

Некоторые аспекты управления киберрисками могут включать коммерчески важную или конфиденциальную информацию, например, оценку киберрисков и связанные с ней инвентаризации аппаратного и программного обеспечения, а также карты сети. Поэтому компаниям следует надлежащим образом защищать эту информацию и по возможности не включать конфиденциальную информацию в свои СУБ-сообщения.

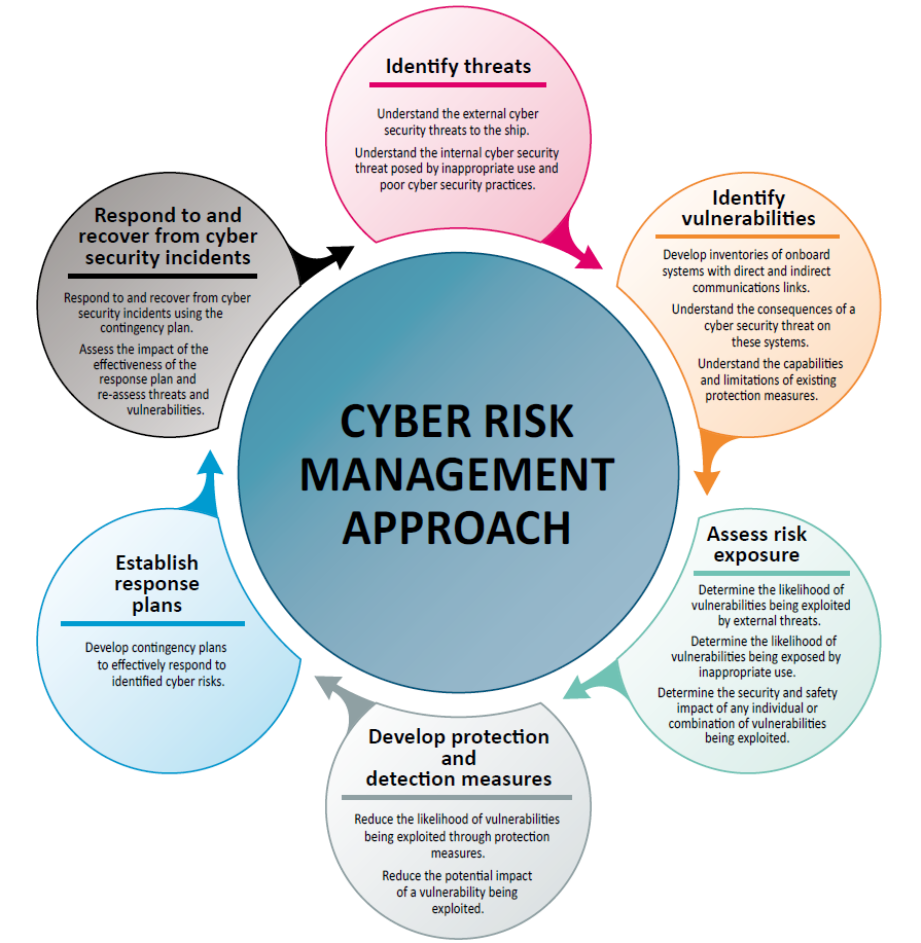

Рисунок 1. Подход к управлению киберрисками, описанный в руководстве.

Разработка, внедрение и поддержка программы управления киберрисками в соответствии с подходом, описанным на рисунке 1, — непростая задача. Поэтому важно, чтобы высшее руководство участвовало в этом процессе на всех этапах, чтобы обеспечить сбалансированность защиты и планирования на случай непредвиденных обстоятельств для управления рисками в допустимых пределах. Такие факторы, как влияние, вероятность, уязвимости, угрозы, возможности, благоприятные условия и намерения злоумышленников, взаимосвязаны (см. рис. 2) и все они важны при оценке риска. Из этого следует, что, если какой-либо из факторов низкий или даже равен нулю, то же самое будет относиться и к риску. Важно подчеркнуть, что оценка риска — это не разовое мероприятие. Ее необходимо повторять через регулярные промежутки времени, чтобы оценить, изменились ли угрозы, уязвимости, вероятности, влияние и риски, а также по-прежнему ли актуальны меры контроля.

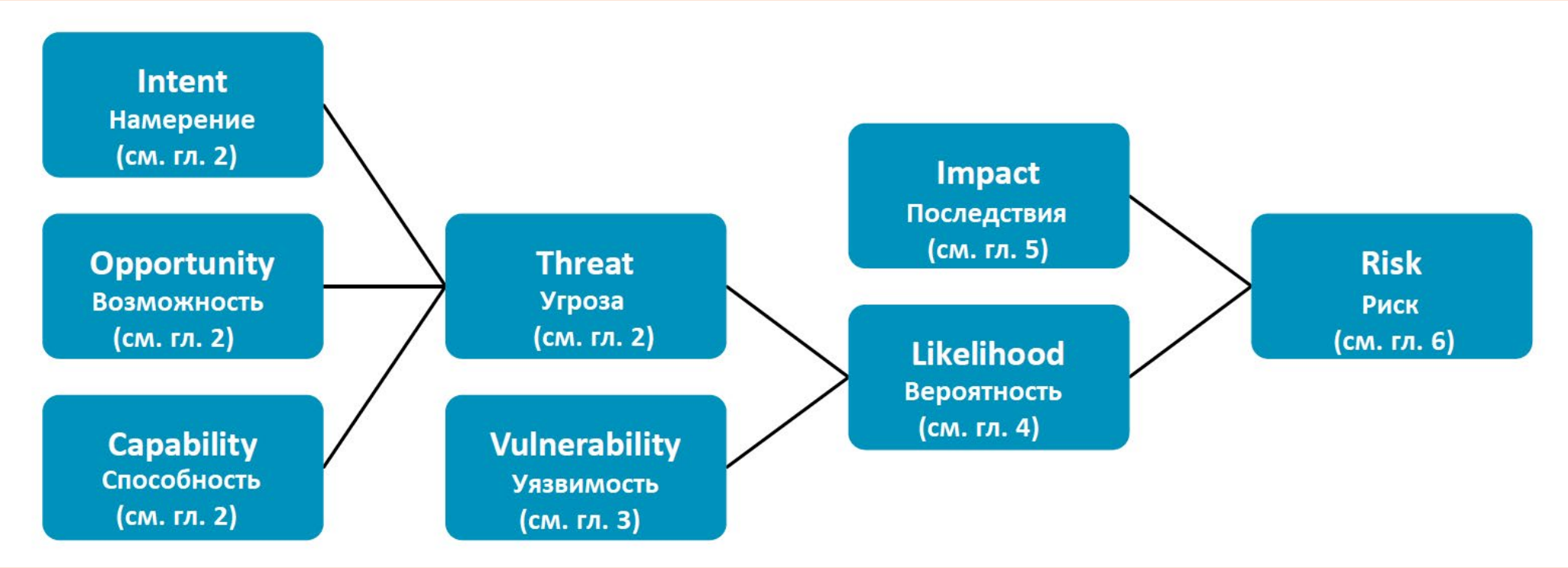

Рисунок 2: Взаимосвязь между различными факторами, влияющими на риск. Линии обозначают умножение, то есть «вероятность» умножается на «воздействие», чтобы получить «риск».

1.2 Участие высшего руководства

В управлении киберрисками на постоянной основе должны участвовать представители высшего руководства компании, а не только, например, сотрудник службы безопасности судна или ИТ-менеджер. Для этого есть несколько причин:

«Некоторые киберрисков имеют широкий спектр разрушительных последствий для безопасности персонала и окружающей среды, а также для производительности и репутации компании.

Таким образом, киберриски — это не просто проблемы безопасности, а бизнес-проблемы, которые требуют участия руководства.

«Инициативы по повышению уровня кибербезопасности и защиты могут повлиять на стандартные бизнес-процессы и операции, сделав их более трудоёмкими и/или дорогостоящими. Поэтому решение о том, как оценить и распределить необходимые ресурсы для снижения рисков до приемлемого уровня остаточного риска, принимает высшее руководство.

«Инициативы, повышающие осведомлённость о кибербезопасности, могут изменить то, как компания взаимодействует с профсоюзами, клиентами, поставщиками и государственными органами, и наложить новые требования на сотрудничество между сторонами». Высшее руководство должно принять решение о том, следует ли вносить изменения в взаимоотношения и как это лучше всего сделать.

Ответы на следующие вопросы могут быть использованы в качестве основы для информирования и привлечения высшего руководства о важности устранения киберрисков на борту судов:

„Какие активы подвержены риску?

„Каковы потенциальные последствия киберинцидента для бизнеса, клиентов, партнеров и заинтересованных сторон?

„ Кто несет конечную ответственность за управление киберрисками?
«Защищены ли ОТ-системы и их рабочая среда от несанкционированного доступа и изменений?
«Есть ли удаленный доступ к ОТ-системам и если да, то как он контролируется и защищается?
«Защищены ли ИТ-системы и контролируется ли доступ к ним?
«Какие передовые методы управления киберрисками используются?
«Каков уровень подготовки персонала, работающего с ИТ- и ОТ-системами, в области киберрисков?
На основе полученных ответов компания должна описать и делегировать полномочия по мере необходимости, а также выделить ресурсы, необходимые для разработки и поддержки подходящих решений на основе результатов оценки рисков.
Рисунок 2. Взаимосвязь между различными факторами, влияющими на риск. Линии обозначают умножение, то есть «вероятность» умножается на «воздействие», чтобы получить «риск».

1.3 Роли, обязанности и задачи

Эффективное управление киберрисками зависит от чёткого распределения обязанностей и задач внутри компании. Управление киберрисками является неотъемлемой частью управления судном и эксплуатации судна, и у разных сотрудников разные роли, обязанности и задачи.

Кроме того, в некоторых компаниях некоторые роли, обязанности и задачи передаются на аутсорсинг третьим лицам.
Различные обязанности и задачи должны быть сопоставлены с должностными инструкциями и/или ролевыми описаниями, содержащимися в СУБ.

Поскольку планирование и реализация управления киберрисками затрагивают всю компанию, в процессе сопоставления может быть полезно уточнить, кто является ответственным лицом, и кто должен оказывать поддержку этому лицу. Например, ИТ-менеджер на судне вполне может быть ответственным за управление киберрисками на судах, но он полагается на поддержку других менеджеров и сотрудников по всей компании, например, сотрудников службы безопасности, охраны труда, обучения, закупок, отдела кадров на судне, экипажа и т. д.

Часто распределение обязанностей и задач будет наиболее эффективным, если оно согласуется с обычной субординацией. Например, при распределении ответственности за соблюдение процедур управления киберрисками на борту судна часто имеет смысл назначить капитана или главного механика.

Задача Роль/лицо	Вклад кибербезопасности в политику безопасности / охраны	Оценка киберрисков в судовых ОТ-системах	Оценка киберрисков в судовых ИТ-системах	Управление ИТ-инфраструктурой судна	Обучение экипажа управлению киберрисками
Управляющий директор	**Ответственный**				
ИТ-менеджер компании	**Поддерживающий**		**Поддерживающий**		
ИТ-менеджер судна	**Поддерживающий**	**Ответственный**	**Ответственный**	**Ответственный**	**Ответственный**
Менеджер по безопасности	**Поддерживающий**	**Поддерживающий**	**Поддерживающий**	**Поддерживающий**	**Поддерживающий**
Менеджер по закупкам	**Поддерживающий**			**Поддерживающий**	
Менеджер по флоту		**Поддерживающий**	**Поддерживающий**	**Поддерживающий**	**Поддерживающий**
Менеджер по обучению			**Поддерживающий**		**Поддерживающий**
Менеджер по персоналу в сфере морских перевозок			**Поддерживающий**		**Ответственный**

Рисунок 3. Пример (неполный) сопоставления ролей, обязанностей и задач в матрице.

Названия должностей и связанные с ними обязанности будут различаться в зависимости от компании. Ответственные лица в сфере ИТ и ОТ должны согласовывать и координировать стратегию управления киберрисками компании.

1.4 Различия между ИТ- и ОТ-системами

В то время как ИТ-системы управляют данными и поддерживают бизнес-функции, ОТ — это аппаратное и программное обеспечение, которое непосредственно контролирует физические устройства и процессы и как таковое является неотъемлемой частью судна и должно функционировать независимо от ИТ-систем на борту. Однако системы могут быть подключены к ИТ-сети для мониторинга производительности, удаленной поддержки и т.д. Такие системы иногда называют относящимися к промышленному интернету вещей (IIOT). В таких случаях необходимо убедиться, что интерфейс как минимум в достаточной степени защищен брандмауэром, а потенциальный уязвимости в ОТ-системах не отображаются в ИТ-сети. Это важно, потому что не всегда возможно или целесообразно обеспечить надлежащий уровень исправлений в ОТ-системах.

ИТ охватывает спектр технологий обработки информации, включая программное обеспечение, аппаратное обеспечение и коммуникационные технологии. Традиционно ОТ и ИТ были разделены, но с развитием интернета ОТ и ИТ сближаются, поскольку исторически автономные системы становятся интегрированными. Нарушение работы ОТ-систем может представлять значительный риск для безопасности персонала на борту, груза, нанести ущерб морской среде и затруднить работу судна.

Аналогичным образом, сбой в работе некоторых ИТ-систем, например, отсутствие немедленного доступа к манифесту опасных грузов, также может привести к опасным ситуациям. Например, в ситуациях, когда на борту судна горит контейнер, информация о содержимом соседних контейнеров имеет решающее значение для эффективного пожаротушения.

Могут быть существенные различия в том, кто занимается закупкой и управлением ОТ-системы в сравнении с ИТ-системами на судне. ИТ-менеджеры обычно не участвуют в покупке ОТ-систем и могут не иметь полного представления о кибербезопасности. В покупке таких систем должен участвовать кто-то, кто знает о влиянии на бортовые системы, но, скорее всего, имеет лишь ограниченные знания о программном обеспечении и управлении киберрисками. Поэтому важно вести диалог с человеком, разбирающимся в кибербезопасности, чтобы учесть киберриски в процессе покупки ОТ-систем.

Обновление программного обеспечения ОТ требует тщательной проверки совместимости и одобрения класса, в отличие от ИТ-программного обеспечения, которое обычно обновляется регулярно. Чтобы получить представление о потенциальных проблемах и разработать необходимую политику и процедуры для обслуживания программного обеспечения, лицу, ответственному за кибербезопасность на борту судна, может быть полезно составить перечень систем ОТ.

1.5 Планы и процедуры

Резолюция MSC.428(98) ИМО определяет острую необходимость повышения осведомлённости об угрозах и уязвимостях, связанных с киберрисками, для обеспечения безопасного и надёжного судоходства, устойчивого к киберрискам. Таким образом, все заинтересованные стороны в сфере морского судоходства должны работать над защитой судоходства от существующих и возникающих киберугроз и уязвимостей. Кроме того, резолюция подтверждает, что система управления безопасностью должна учитывать управление киберрисками в соответствии с целями и функциональными требованиями Кодекса ISM (МКУБ).

101-я сессия Комитета по безопасности на море ИМО (отчет об этом заседании содержится в документе ИМО MSC 101/24) «...согласовала, что аспекты управления киберрисками, в том числе аспекты физической безопасности, связанные с кибербезопасностью, должны быть отражены в планах обеспечения безопасности судов (SSP) в соответствии с Кодексом ISPS (ОСПС);

однако это не следует рассматривать как требование к компании создать отдельную систему управления кибербезопасностью, работающую параллельно с системой управления безопасностью компании (СУБ)».

На том же заседании ИМО также «…подтвердила, что резолюция MSC.428(98) по управлению киберрисками на море в рамках СУБ излагает требования ИМО к администрациям по обеспечению надлежащего учета киберрисков в существующих СУБ

(как определено в Кодексе ПДНВ), подтвержденных одобренным сертификатом соответствия требованиям и управления безопасностью, а также то, что в плане обеспечения безопасности судна следует ссылаться на процедуры управления киберрисками, содержащиеся в СУБ».

Для компании простым способом организации процедур, как того требует Международная морская организация, может быть включение в План обеспечения безопасности судна (SSP) следующего:

- процедур, связанных с физическим доступом к зонам с ИТ- и ОТ-системами;
- ссылки на процедуры кибербезопасности СУБ.

Следует рассмотреть возможность формулирования ссылки таким образом, чтобы ее не нужно было обновлять каждый раз, когда в СУБ вносится изменение, добавляется или удаляется процедура, связанная с кибербезопасностью, поскольку изменения в SSP обычно требуют одобрения государства флага или признанной организации, уполномоченной государством флага.

Соответственно, остальные процедуры по управлению киберрисками должны быть отражены в СУБ, при этом исключая конфиденциальную информацию, такую как документация по системе, описанная в разделе 3.2 настоящих руководящих принципов, которая может быть использована злоумышленниками за пределами компании.

СУБ уже включает процедуры для сообщения о происшествиях или опасных ситуациях и определяет уровни коммуникации и полномочия для принятия решений.

При необходимости в такие процедуры следует внести изменения, чтобы отразить коммуникацию и полномочия в случае киберинцидента. У владельца должен быть определенный ресурс, к которому можно обратиться в случае киберинцидента, а система управления рисками должна включать хорошо продуманный план реагирования на Киберинциденты — см. главу 9.

Дополнительные рекомендации по включению управления киберрисками в систему управления рисками компании можно найти в приложении 2 к этим рекомендациям.

Процедуры системы управления рисками должны учитывать риски, связанные с использованием ИТ и ОТ на борту, с учетом применимых кодексов, руководств и рекомендуемых стандартов. Можно считать, что процедуры, направленные на устранение, например, коммерческих рисков, также включены в СУБ, а не в отдельный документ.

Компания должна рассмотреть вопрос о том, есть ли необходимость в оценке рисков, связанных с конкретным судном, в зависимости от того, настроены ли отдельные суда или группы судов уникальным образом с точки зрения ИТ/ОТ в рамках их флота.

К факторам, которые следует учитывать, относятся, помимо прочего, степень использования ИТ и ОТ на борту, сложность системной интеграции и характер операций. Аналогичным образом следует рассмотреть вопрос о том, можно ли организовать процедуры в СУБ таким образом, чтобы они охватывали весь флот компании, или же для конкретных судов требуются особые процедуры.

Оценка киберрисков и документация по ИТ- и ОТ-системам, описанная в разделе 3.2, считаются конфиденциальной информацией. Хотя не существует нормативных требований, описывающих, как следует хранить эту информацию, рекомендуется хранить и контролировать ее так же, как оценку безопасности судна и план обеспечения безопасности судна.

1.6 Взаимоотношения между судовладельцем и менеджером судна

Владелец документа о соответствии требованиям (DoC) в конечном итоге несет ответственность за управление киберрисками на борту. Если судно находится под управлением третьей стороны, то менеджеру судна рекомендуется достичь соглашения с судовладельцем.

Обеим сторонам следует обратить внимание на разделение обязанностей, согласование ожиданий, согласование конкретных инструкций для менеджера и возможное участие в принятии решений о закупках, а также в бюджетных требованиях.

Помимо требований ISM, такое соглашение должно учитывать дополнительное применимое законодательство, например Общий регламент ЕС по защите данных (GDPR) или специальные правила в области кибербезопасности в других прибрежных государствах, в зависимости от ситуации. Менеджерам и владельцам следует рассмотреть возможность использования этих рекомендаций в качестве основы для открытого обсуждения того, как лучше всего внедрить эффективный режим управления киберрисками.

Соглашения между менеджерами судов и судовладельцами об управлении киберрисками должны быть составлены в письменной форме и подписаны.

1.7 Взаимоотношения между судовладельцем и агентом

Важность этих взаимоотношений делает агента заинтересованной стороной, которая постоянно и одновременно взаимодействует с судовладельцами, операторами, терминалами, поставщиками портовых услуг и государственными контролирующими органами посредством обмена конфиденциальной, финансовой и портовой координационной информацией. Эти взаимоотношения выходят за рамки отношений с поставщиком. Это может принимать разные формы, и особенно в сфере торговли судами-призраками судовладельцам требуется местный представитель (независимый судовой агент), который будет выступать в качестве представителя компании.

Стандарты качества для агентов важны, потому что, как и все остальные компании, агенты также могут стать целью киберпреступников, например, в связи с доставкой ИТ- или ОТ-оборудования на судно. Преступления, связанные с кибертехнологиями, такие как мошенничество с электронными переводами и подставные назначения на суда, а также киберугрозы, такие как программы-вымогатели и хакерские атаки, требуют совместных киберстратегий и расширенных киберотношений между судовладельцами и агентами для снижения таких киберрисков.

ИНЦИДЕНТ:

программа-вымогатель, заразившая сети судовладельца и агента Судовладелец сообщил, что бизнес-сети компании были заражены программой-вымогателем, по-видимому, из-за вложения в фишинговое электронное письмо. Источником программы-вымогателя были два ничего не подозревавших агента в разных портах и в разное время. Пострадали и корабли, но ущерб был ограничен деловыми сетями, в то время как навигация и судоходство не пострадали. В одном случае владелец заплатил выкуп.

Важность этого инцидента заключается в том, что согласованная кибербезопасность в отношениях с надёжными деловыми партнёрами и производителями имеет решающее значение для всех участников цепочки поставок. Отдельные усилия по укреплению собственного бизнеса могут быть доблестными и благими, но их может быть недостаточно. Участники цепочки поставок должны работать сообща и при необходимости обмениваться информацией, чтобы снизить киберриски.

1.8 Взаимоотношения с поставщиками и другими внешними сторонами

Компаниям следует оценивать процессы обеспечения физической безопасности и управления киберрисками при взаимодействии с поставщиками услуг, продавцами и другими внешними сторонами, в том числе государственными органами.

Отсутствие физической и/или кибербезопасности у поставщика, продавца или поставщика услуг может привести к взлому корпоративных ИТ-систем и/или повреждению судовых ОТ/ИТ-систем. Поэтому компании следует рассмотреть возможность заключения соглашений и контрактов с поставщиками/продавцами/поставщиками услуг, в которых определяются требования и ожидания, связанные с кибербезопасностью. Компаниям также следует оценивать процессы управления киберрисками как для новых, так и для существующих контрактов. Существуют общепризнанные стандарты (например, Service Organization Control (SOC) 2 типа 2), но компания также может разработать собственные стандарты.

Процессы, оцениваемые при проверке поставщиков и включаемые в требования к контрактам, могут включать:

- управление безопасностью, в том числе управление субпоставщиками
- производственную/операционную безопасность
- разработку программного обеспечения и архитектуру
- управление активами и киберпреступлениями
- охрана персонала
- защита данных и информации.

Сторона, представляющая владельца судна и/или фрахтователя (принципала) в порту.

Если это предусмотрено, агент несет ответственность перед принципалом за организацию совместно с портом швартовки, всех соответствующих портовых и судовых услуг, удовлетворение потребностей капитана и экипажа, оформление судна в порту и у других

властей (включая подготовку и подачу соответствующей документации), а также за выдачу или получение груза от имени принципала (источник: Конвенция СОЛАС).

Ничто в этих рекомендациях не должно восприниматься как рекомендация к выплате выкупа.

Оценка поставщиков услуг, помимо тех, с которыми у компании есть прямые отношения, может быть сложной задачей, особенно для компаний со множеством прямых поставщиков. Можно рассмотреть возможность привлечения сторонних поставщиков, которые собирают и управляют данными об управлении рисками поставщиков.

Взаимодействие судна и его компании с государственными органами является сложным процессом, охватывающим множество вопросов, начиная от прибытия судна и заканчивая сменой экипажа и подачей предварительных грузовых деклараций. Они также сопряжены с соответствующими трудностями в процессе управления киберрисками. Как правило, эти трудности не могут быть решены так же, как те, с которыми компания сталкивается в своих коммерческих отношениях.

Однако важно, чтобы текущие и будущие коммуникационные связи с государственными органами для предоставления и обмена обязательной информацией оценивались и анализировались в рамках политики компании в области кибербезопасности, а любые проблемы с кибербезопасностью, возникающие в связи с такими связями, доводились до сведения соответствующих органов. Некоторые из этих вопросов рассматриваются далее в разделе 3.4.

В отношении производителей и третьих сторон, включая поставщиков, подрядчиков и поставщиков услуг, следует учитывать следующее:

- желание и способность производителей и поставщиков услуг внедрять эффективные и экономичные методы обеспечения кибербезопасности в своих продуктах и услугах, что может быть продемонстрировано различными способами, например, путем соблюдения Кодекса практики CIRM по киберрискам для поставщиков морского электронного оборудования и услуг и связанных с ним руководящих принципов внедрения.
- Осведомленность производителей и поставщиков услуг в вопросах управления киберрисками и соответствующие процедуры: некоторым компаниям может не хватать обучения по вопросам кибербезопасности и управления в их собственных организациях, и это может создавать дополнительные источники уязвимости, которые могут привести к киберинцидентам. Сторонние поставщики и подрядчики все чаще становятся мишенью для злоумышленников и на протяжении многих лет играли роль в широко освещаемых киберинцидентах. Эти компании должны иметь обновленную политику управления киберрисками, которая включает обучение и процедуры управления доступными ИТ- и ОТ-системами.
- Уровень зрелости процедур управления киберрисками третьей стороны: судовладельцу следует запросить информацию о внутреннем управлении киберсетевой безопасностью и попытаться получить подтверждение управления киберрисками при рассмотрении будущих контрактов и услуг.

Это особенно важно при обеспечении сетевой безопасности, если судно должно взаимодействовать с третьей стороной, такой как морской терминал, стивидорная компания или поставщик ОТ для постоянной поддержки и обслуживания.

ИНЦИДЕНТ:

неизвестный вирус в ECDIS задерживает отправление судна.

Судно-сухогруз нового типа задержалось с отплытием на несколько дней из-за того, что его ECDIS была заражена вирусом. Судно было спроектировано для безбумажной навигации и не имело бумажных карт. Сбой в работе ECDIS, по-видимому, был вызван техническими неполадками и не был признан капитаном и офицерами судна как кибератака. На судно был направлен специалист-технолог, который, потратив значительное время на устранение неполадок, обнаружил, что обе сети ECDIS были заражены вирусом. Вирус был помещён в карантин, и компьютеры ECDIS были восстановлены. Источник и способ заражения в данном случае неизвестны. Задержка в плавании и расходы на ремонт составили сотни тысяч долларов (США).

2. Выявление угроз

2.1 Субъекты угроз

При выявлении угроз компаниям следует учитывать любые конкретные аспекты, связанные с возможностями, шансами и намерениями потенциальных субъектов угроз. Это может включать использование, например, внешнего лица или инсайдера в качестве непреднамеренного посредника, который неосознанно переносит угрозу, например, на заражённой USB-накопителе. После выявления угроз их следует рассматривать наряду с выявленными уязвимостями, чтобы оценить вероятность атаки или инцидента. Вероятность возникновения инцидента в сочетании с его последствиями образует фактор риска.

Организации и отдельные лица могут представлять собой умышленную или даже неумышленную угрозу для безопасности экипажа, окружающей среды и судна. На следующем рисунке приведены примеры субъектов угроз и их возможных мотивов и целей. Список не является исчерпывающим.

Такие субъекты угроз обладают различными навыками и ресурсами, которые могут представлять угрозу для безопасности и охраны судов, а также для способности компании вести свою деятельность:

Группа	Мотивация
Случайные участники.	■ Нет злого умысла, но в результате всё равно наносится непреднамеренный ущерб из-за невезения, недостатка знаний или халатности, например, при подключении заражённого USB-накопителя к бортовым ИТ- или ОТ-системам.
Активисты (в том числе недовольные сотрудники)	■ месть ■ нарушение работы ■ привлечение внимания СМИ ■ ущерб репутации
Преступники	■ финансовая выгода ■ коммерческий шпионаж ■ промышленный шпионаж
Оппортунисты	■ вызов ■ укрепление репутации ■ финансовая выгода
Государства. Государственные организации. Террористы	■ политическая/идеологическая выгода, например, (не)контролируемые сбои в экономике и критически важной национальной инфраструктуре ■ шпионаж ■ финансовая выгода ■ коммерческий шпионаж ■ промышленный шпионаж ■ коммерческая выгода

Рисунок 4: Мотивация и цели участников угроз.

2.2 Типы киберугроз

В целом, существует две категории киберугроз, которые могут повлиять на компании и суда:

- нецелевые атаки, при которых системы и данные компании или судна являются одной из многих потенциальных целей
- целевые атаки, при которых системы и данные компании или судна являются предполагаемой целью или одной из множества целей.

При нецелевых атаках, скорее всего, используются инструменты и методы, доступные в интернете, с помощью которых можно найти, обнаружить и использовать распространённые уязвимости, которые могут существовать в компании и на борту судна. Примеры некоторых инструментов и методов, которые могут использоваться в таких обстоятельствах, включают:

- вредоносное ПО. Вредоносное программное обеспечение, предназначенное для доступа к компьютеру или его повреждения без ведома владельца. Существуют различные типы вредоносного ПО, включая трояны, программы-вымогатели, шпионское ПО, вирусы и черви. Программы-вымогатели шифруют данные в системах до тех пор, пока не будет выплачен выкуп. Вредоносные программы также могут использовать известные недостатки и проблемы в устаревшем/необновленном программном обеспечении для бизнеса.

Термин «эксплойт» обычно относится к использованию программного обеспечения или кода, который предназначен для использования и манипулирования проблемой в другом программном или аппаратном обеспечении компьютера.

Эта проблема может быть, например, ошибкой в коде, уязвимостью системы, неправильным проектированием, сбоем аппаратного обеспечения и/или ошибкой в реализации протокола. Эти уязвимости могут быть использованы удалённо или локально, например, вредоносный код может быть запущен пользователем, иногда по ссылкам, распространяемым во вложениях электронной почты или на вредоносных веб-сайтах.

- Создание «дыры в системе». Создание поддельного веб-сайта или компрометация настоящего веб-сайта для эксплуатации ничего не подозревающих посетителей.
- Сканирование. Случайный поиск в больших частях интернета уязвимостей, которыми можно воспользоваться.
- Типосквоттинг. Также называется перехватом URL-адреса или поддельным URL-адресом. Основан на ошибках, таких как опечатки, которые допускают интернет-пользователи при вводе адреса веб-сайта в веб-браузер. Если пользователь случайно введет неверный адрес веб-сайта, он может быть перенаправлен на альтернативный и зачастую вредоносный веб-сайт.
- Целевые атаки могут быть более изощренными и использовать инструменты и методы, специально созданные для атак на определенную компанию или судно. Примеры инструментов и методов, которые могут использоваться в таких случаях, включают:

• социальную инженерию. Нетехнический метод, используемый потенциальными

киберпреступниками для манипулирования инсайдерами с целью нарушения процедур безопасности, обычно, но не исключительно, посредством взаимодействия через социальные сети.

• Метод перебора. Атака, при которой перебирается множество паролей в надежде в конечном итоге угадать правильный.

Злоумышленник систематически проверяет все возможные пароли, пока не найдет правильный.

• Наполнение учетных данных. Использование ранее скомпрометированных учетных данных или конкретных часто используемых паролей для попытки несанкционированного доступа к системе или приложению.

• Атака типа «отказ в обслуживании» (DoS) препятствует доступу законных и авторизованных пользователей к информации, как правило, путём перегрузки сети данными. Распределённая атака типа «отказ в обслуживании» (DDoS) позволяет контролировать несколько компьютеров и/или серверов для реализации DoS-атаки.

• Фишинг. Отправка электронных писем большому количеству потенциальных жертв с запросом определённой конфиденциальной информации. Электронное письмо может также содержать вредоносное вложение или запрос на посещение поддельного веб-сайта по гиперссылке, включённой в электронное письмо.

• Спин-фишинг. Похож на фишинг, но в этом случае на людей нацелены личные электронные письма, часто содержащие вредоносное ПО или ссылки, которые автоматически загружают вредоносное ПО.

В некоторых случаях сообщения SAT-C используются для создания ощущения знакомства с электронным адресом злоумышленника-отправителя.

• Подрыв цепочки поставок. Атака на компанию или судно путем компрометации оборудования, программного обеспечения или вспомогательных услуг, предоставляемых компании или судну.

Приведенные выше примеры не являются исчерпывающими. Развиваются и другие методы кибератак, такие как выдача себя за законного берегового сотрудника судоходной компании с целью получения ценной информации, которая может быть использована для дальнейшей атаки. Потенциальное количество и сложность инструментов и техник, используемых при кибератаках, продолжают расти и ограничены только изобретательностью организаций и частных лиц, которые их разрабатывают.

2.3 Стадии киберинцидента

В 2019 году в среднем проходило 279 дней с момента взлома сети жертвы до локализации утечки. Однако взлом может оставаться незамеченным в течение многих лет. Этот показатель вырос с 266 дней в 2018 году. Продолжительность подготовки к кибератаке может зависеть от мотивов и целей злоумышленника, а также от устойчивости технических и процедурных средств контроля киберрисков, применяемых компанией, в том числе на борту её судов. При рассмотрении целенаправленных кибератак обычно наблюдаются следующие этапы инцидента:

- Сбор информации/разведка. Для получения информации о потенциальной цели (например, компании, судне или моряке) при подготовке к кибератаке используются открытые/публичные источники, такие как социальные сети. Социальные сети, технические форумы и скрытые свойства веб-сайтов, документов и публикаций могут использоваться для выявления технических, процедурных и физических уязвимостей. Использование открытых/общедоступных источников может дополняться мониторингом (анализом – перехватом) фактических данных, поступающих в компанию или судно и исходящих из них.

- Доставка. Злоумышленники могут попытаться получить доступ к системам и данным компании и судна. Это может быть сделано как внутри компании или судна, так и удаленно через подключение к Интернету.

Примеры методов, используемых для получения доступа, включают:

- *онлайн-сервисы компании, включая системы отслеживания грузов или контейнеров*
- *рассылку сотрудникам электронных писем, содержащих вредоносные файлы или ссылки на вредоносные веб-сайты*
- *предоставление зараженных съемных носителей, например, в рамках обновления программного обеспечения бортовой системы*
- *создание ложных или вводящих в заблуждение веб-сайтов, которые поощряют раскрытие информации об учетной записи пользователя персоналом.*

- Нарушение. Степень, в которой злоумышленник может взломать систему компании или судна, будет зависеть от значимости, обнаруженной злоумышленником уязвимости и выбранного метода атаки. Следует отметить, что взлом может не привести к каким-либо очевидным изменениям в работе оборудования. В зависимости от значимости взлома злоумышленник может:

• вносить изменения, влияющие на работу системы, например прерывать работу или манипулировать информацией, используемой навигационным оборудованием

• получить доступ к важной для работы информации, например к спискам загрузки, или коммерчески значимым данным, например к грузовым манифестам и/или спискам экипажа и пассажиров/посетителей

• получить полный контроль над системой, например над системой управления оборудованием.

- Переключение. Переключение — это метод использования уже скомпрометированной системы для атаки на другие системы в той же сети. На этом этапе атаки злоумышленник использует первую скомпрометированную систему для атаки на недоступные иным способом системы. Злоумышленник обычно нацеливается на наиболее уязвимую часть системы жертвы с самым низким уровнем безопасности.

После получения доступа злоумышленник попытается использовать остальную часть системы. Обычно на этапе перехода злоумышленник может попытаться:

• загрузить в систему инструменты, эксплойты и скрипты для поддержки злоумышленника на новом этапе атаки

• выполнить поиск соседних систем с помощью сканирования или инструментов для отображения сети
• установить постоянные инструменты или кейлоггер для сохранения и поддержания доступа к системе
• выполнить новые атаки на систему.

Мотивация и цели злоумышленника определяют, какое влияние он оказывает на компанию или систему судна и данные. Злоумышленник может изучать системы, расширять доступ и/или обеспечивать себе возможность возвращения в систему, чтобы:

- получить доступ к коммерчески важным или конфиденциальным данным о грузе, экипаже, посетителях и пассажирах
- манипулировать списками экипажа или пассажиров/посетителей, грузовыми манифестами, планами размещения или списками загрузки. Впоследствии это может быть использовано для мошеннической перевозки нелегальных грузов или для облегчения краж
- приводят к полному отказу в обслуживании бизнес- и операционных систем
- способствуют совершению других преступлений, например, пиратству, краже и мошенничеству
- нарушают нормальную работу систем компании и судна, например, удаляя критически важную информацию о прибытии или отправлении или перегружая системы компании
- требуют выкуп за операционные или личные данные.

2.4 Количественная оценка угрозы

Общие соображения

Угроза — это результат возможностей, возможностей и намерений субъекта угрозы причинить вред. Цель количественной оценки угрозы состоит в том, чтобы помочь в количественной оценке вероятности, которая является частью оценки риска, представляющего собой произведение вероятности и последствий. Другими словами, если возможности, условия или намерения субъекта угрозы равны нулю или близки к нулю, угроза и, следовательно, риск будут незначительными.

Угрозы для систем ОТ

В отличие от других областей безопасности, где имеются исторические свидетельства, управление киберрисками усложняется из-за недостатка статистических данных об инцидентах и их последствиях.

Есть основания полагать, что атаки, направленные конкретно против систем ОТ, менее распространены и во многих случаях не предаются огласке. Причинами этого, вероятно, могут быть, например, следующие:

- Большинство систем ОТ в морской отрасли по-прежнему не подключены к сетям с внешним доступом, т.е. подверженность угрозам невелика, и киберпреступники не имеют возможности атаковать.

Однако существуют исключения, например, многие устройства мониторинга (например, устройства, отслеживающие работу двигателя) подключены к Интернету и обычно имеют минимальные средства контроля кибербезопасности, особенно по сравнению с ИТ-системами или даже системами ОТ. Такие системы называются промышленным Интернетом данных.

Интернет вещей (IIoT) и становятся все более интегрированными на борту судов, обеспечивая удаленный мониторинг и подключение систем для большей автоматизации и эффективности операций. Злоумышленники могут сканировать эти системы и использовать их в качестве начальной точки проникновения в корабельную сеть, откуда они могут развернуться, как описано ранее. Таким образом, риски для этих систем важно оценивать, и их не следует упускать из виду.

- Системы ОТ, как правило, не имеют прямого потенциала для экономического вознаграждения киберпреступников.
- Атака на системы ОТ влечет за собой риски для безопасности жертв, что может стать сдерживающим фактором для некоторых киберпреступников.

Несмотря на вышесказанное, не следует недооценивать риски для ОТ-систем. Угрозы, например, связанные с вредоносным ПО, внедряемым через обновления программного обеспечения — как онлайн, так и с помощью ручных процессов, таких как, например, USB-накопители, — или с помощью нерегулируемого или несанкционированного доступа со стороны экипажа, всё ещё могут возникать и, как известно, приводить к сбоям и простоям в работе.

Угрозы для ИТ-систем

Угрозы, связанные с ИТ-системами, как правило, легче поддаются количественной оценке, поскольку существует гораздо больше свидетельств аварий как в целом, так и в частности в морской отрасли. Обычно сбои в работе ИТ-систем не считаются причиной потенциального вреда для людей, окружающей среды, активов или грузов, но не стоит недооценивать угрозы, связанные с ИТ-системами. Недавние примеры из судоходной отрасли показали, что киберинциденты могут нанести ущерб судовождению и управлению грузами, что приводит к значительным финансовым потерям. Кроме того, такие инциденты могут иметь каскадные последствия для безопасности людей, окружающей среды, имущества и грузов, например, когда сбои в работе ИТ-систем приводят к потере контроля над скоропортящимися или опасными грузами.

3. Определите уязвимости

3.1 Распространённые уязвимости

Ниже перечислены распространённые киберуязвимости, которые могут быть обнаружены на борту существующих судов, а также на некоторых новых судах:

- устаревшие и неподдерживаемые операционные системы
- системное программное обеспечение без обновлений
- устаревшее или отсутствующее антивирусное программное обеспечение и защита от вредоносных программ
- недостаточные настройки безопасности и передовые методы, в том числе неэффективное управление сетью и использование учётных записей администраторов по умолчанию и паролей
- бортовые компьютерные сети, в которых отсутствуют меры по защите границ и сегментации сетей
- критически важное для безопасности оборудование или системы, постоянно подключенные к береговой стороне
- недостаточный контроль доступа к киберресурсам, сетям и т. д. для третьих сторон, включая подрядчиков и поставщиков услуг
- персонал, недостаточно обученный и/или квалифицированный для управления киберрисками
- отсутствие, недостаточность или непроработанность планов и процедур на случай непредвиденных обстоятельств.

3.2 Документация по ИТ- и ОТ-системам

Чтобы облегчить каждый этап оценки рисков, ИТ- и ОТ-системы должны быть чётко идентифицированы с указанием документированных обязанностей по управлению и владению в реестре активов, который должен обновляться по мере необходимости. Реестр активов должен включать оценку активов с указанием стоимости актива и затрат на его обслуживание. Рекомендация IACS № 166 по киберустойчивости применима только к новым объектам, однако она может служить руководством при разработке документации, которая может включать:

- перечень взаимодействующих устройств
- инвентаризация сетевых коммуникационных устройств
- логическая карта сетей:
  - IP-адреса
  - не IP-адреса
  - точки доступа, отличные от Ethernet
  - настольные компьютеры и серверы
  - соединители и полевые устройства связи
- инвентаризация программного обеспечения (в некоторых случаях эта инвентаризация является частью системы регистрации программного обеспечения судна)
- инвентаризация сетевых сервисов для каждого оборудования.

Доступны инструменты для управления ИТ-системой, но они не рекомендуются для ОТ-системы, так как целостность ОТ-системы может быть нарушена (если только ею не управляет квалифицированный специалист в тесном сотрудничестве с капитаном, главным инженером и т. д.).
С публикацией МАКО (IACS) «Рекомендаций по киберустойчивости (№ 166)» будущие новые суда могут стать менее уязвимыми.

3.3 Типичные уязвимые системы

Выявление уязвимостей включает в себя анализ приложений, систем и процедур с целью выявления слабых мест, которыми могут воспользоваться потенциальные злоумышленники. Этому могут способствовать внутренние эксперты и/или внешние эксперты, знакомые с морской отраслью и её ключевыми процессами.

ИНЦИДЕНТ:
сбой интегрированной навигационной системы на мостике судна в море.
На судне с интегрированной навигационной системой на мостике в море, в зоне интенсивного движения и плохой видимости, произошёл сбой почти всех навигационных систем. Судно было вынуждено два дня идти по одному радару и запасным бумажным картам, прежде чем прибыть в порт для ремонта. Причиной сбоя всех компьютеров ECDIS была признана устаревшая операционная система. Во время предыдущего захода в порт технический представитель производителя обновил навигационное программное

обеспечение на навигационных компьютерах судна. Однако устаревшие операционные системы не могли запустить программное обеспечение и вышли из строя. Судно было вынуждено оставаться в порту до тех пор, пока не будет установлено новое.

Компьютеры ECDIS могли быть установлены, классификационные инспекторы могли присутствовать, и было выдано уведомление о возможной аварии, как того требовала компания. Задержки привели к значительным расходам, которые понёс судовладелец.

Этот инцидент подчёркивает, что не все сбои в работе компьютеров являются результатом преднамеренной атаки и что устаревшее программное обеспечение подвержено сбоям. Более тщательное тестирование и профилактическое обслуживание программного обеспечения на судне могли бы предотвратить этот инцидент.

Целью оценки корабельной сети, её систем и устройств является выявление любых уязвимостей, которые могут поставить под угрозу или привести к потере конфиденциальности, целостности или доступности данных и систем, необходимых для работы оборудования, системы, сети или даже корабля. Эти уязвимости и слабые места могут относиться к одной из следующих категорий:

- временные уязвимости, такие как дефекты программного обеспечения, устаревшие или не обновлённые системы
- конструктивные особенности, такие как управление доступом или неуправляемые сетевые соединения
- ошибки при внедрении, например, неправильно настроенные брандмауэры
- процедурные или другие ошибки пользователей.

Автономные системы будут менее уязвимы для внешних киберинцидентов по сравнению с системами, подключёнными к неконтролируемым сетям или напрямую к интернету. Более подробно о проектировании сетей и их разделении будет рассказано в Приложении 3.

Следует внимательно изучить, как критически важные системы на борту могут быть подключены к неконтролируемым сетям. Следует учитывать человеческий фактор, так как многие инциденты возникают из-за действий персонала. Бортовые системы могут включать в себя:

- системы управления грузами и погрузкой. Цифровые системы, используемые для погрузки, управления и контроля грузов, в том числе опасных, могут взаимодействовать с различными системами на берегу, в том числе с портами, морскими терминалами и стивидорами. Такие системы могут включать в себя инструменты отслеживания грузов, доступные грузоотправителям через Интернет. Подобные интерфейсы делают системы управления грузами и данные в грузовых декларациях и списках грузов уязвимыми для кибератак.
- Мостовые системы. Растущее использование цифровых сетевых навигационных систем с интерфейсом для подключения к береговым сетям для обновления и предоставления услуг делает такие системы уязвимыми для кибератак. Мостовые системы, не подключенные к другим сетям, могут быть в равной степени уязвимы, поскольку для обновления таких систем с помощью других контролируемых или неконтролируемых сетей часто используются съемные носители.

Кибератаки могут привести к отказу в обслуживании или манипуляциям и, следовательно, могут повлиять на все системы, связанные с навигацией, включая ECDIS, GNSS, AIS, VDR и радар/ARPA.

- Системы управления силовой установкой и механизмами, а также контроля мощности. Использование цифровых систем для мониторинга и управления бортовыми механизмами, силовой установкой и рулевым управлением делает такие системы уязвимыми для кибератак. Уязвимость этих систем может повышаться при использовании в сочетании с дистанционным мониторингом на основе условий эксплуатации и/или при интеграции с навигацией и Коммуникационное оборудование на судах, использующих интегрированные мостовые системы.
- Системы контроля доступа. Цифровые системы, используемые для контроля доступа с целью обеспечения физической безопасности и сохранности судна и его груза, включая системы видеонаблюдения, корабельную охранную сигнализацию и электронные системы «персонала на борту», уязвимы для кибератак.
- Системы обслуживания и управления пассажирами. Цифровые системы, используемые для управления имуществом, доступом на борт и контроля доступа, могут содержать ценные данные о пассажирах. Интеллектуальные устройства (планшеты, портативные сканеры и т. д.) сами по себе являются вектором атаки, поскольку в конечном итоге собранные данные передаются в другие системы.
- Общественные сети, доступные пассажирам.

Фиксированные или беспроводные сети, подключенные к интернету, установленные на борту для удобства пассажиров, например, системы развлечений для гостей, должны считаться неконтролируемыми и не должны быть подключены к критически важным системам безопасности на борту.

- Административные системы и системы жизнеобеспечения экипажа. Бортовые компьютерные сети, используемые для управления судном или обеспечения жизнедеятельности экипажа, особенно уязвимы при предоставлении доступа в Интернет и электронной почты. Этим могут воспользоваться злоумышленники, чтобы получить доступ к бортовым системам и данным.

Эти системы следует считать неконтролируемыми и не подключать к критически важным системам на борту. Программное обеспечение, предоставляемое компаниями по управлению судами или владельцами, также относится к этой категории.

- Системы связи. Наличие подключения к интернету через спутник и/или другие беспроводные каналы связи повышает уязвимость судов, и последние разработки показывают, что, например, сигналы VSAT уязвимы для использования с помощью недорогих готовых продуктов.

Следует рассмотреть системы связи с шифрованием. Механизмы киберзащиты, реализованные поставщиком услуг, должны быть тщательно продуманы, но не следует полагаться только на них для защиты каждой бортовой системы и данных. В эти системы входят каналы связи с государственными органами для передачи необходимой информации о судах и грузах.

Применимые требования к аутентификации и управлению доступом, предъявляемые этими органами, должны строго соблюдаться. Также сюда относятся возможности сбора данных с устройств и анализа данных, прикрепленных к контейнерам, для последующей передачи назначенным получателям на берегу (см. также раздел ниже, посвященный интерфейсу между судном и берегом).

Вышеупомянутые бортовые системы состоят из потенциально уязвимого оборудования, которое следует проверить в ходе оценки. Для оценки уязвимости можно ответить на следующие вопросы по каждой системе:

- Является ли система автономной или она подключена к другим системам?
- Подключена ли система извне, напрямую или через другие системы?
- Есть ли в системе эффективные встроенные меры по снижению рисков, например шифрование?
- Требуется ли для системы регулярное обновление программного обеспечения?
- Требуется ли для работы с системой подключение съемных устройств, например для получения диагностической информации?
- Легко ли получить физический доступ к системе?

3.4 Связь между судном и берегом

Суда становятся всё более интегрированными с береговыми операциями, поскольку цифровая связь используется для ведения бизнеса, управления операциями и поддержания связи с головными офисами. Кроме того, критически важные судовые системы, необходимые для безопасности судоходства, управления энергопотреблением и грузами, становятся всё более цифровыми и подключаются к интернету для выполнения широкого спектра законных функций, таких как:

- мониторинг работы двигателя
- удаленная диагностика
- техническое обслуживание и управление запасными частями
- отслеживание и управление грузами и контейнерами, погрузка и разгрузка, а также планирование размещения
- управление кранами и насосами
- мониторинг систем на предмет соблюдения экологических норм и составление отчетов
- мониторинг эффективности рейса.

Приведенный выше список содержит примеры такого интерфейса и не является исчерпывающим. Вышеупомянутые системы содержат, обрабатывают и обмениваются данными, которые могут представлять интерес для киберпреступников с целью их использования.

Современные технологии могут создавать уязвимости для судов, особенно при небезопасной конструкции сетей и неконтролируемом доступе к Интернету.

Кроме того, береговой и бортовой персонал может не знать, как некоторые производители оборудования и поставщики программного обеспечения обеспечивают удаленный доступ к судовому оборудованию и его сетевой системе. Неизвестный и нескоординированный удаленный доступ к эксплуатируемому судну следует учитывать как важную часть оценки рисков.

Рекомендуется, чтобы компании полностью понимали и документировали, при необходимости, системы OT и IT на судне, а также то, как эти системы взаимодействуют и интегрируются с береговыми службами, в том числе государственными органами, морскими терминалами и стивидорами. Это требует понимания всех компьютерных систем на борту и того, как кибер-инцидент может повлиять на безопасность, работу и бизнес, в том числе на управление грузами и погрузкой.

3.5 Посещение судна

Посещение судов третьими лицами, которым требуется подключение к одному или нескольким компьютерам на борту, также может привести к подключению судна к берегу. Обычно технические специалисты, поставщики, портовые и другие должностные лица, представители морских терминалов, агенты, пилоты и другие технические специалисты поднимаются на борт судна и подключают устройства, такие как ноутбуки и планшеты. Некоторым техническим специалистам может потребоваться использование съемных носителей для обновления компьютеров, загрузки данных и/или выполнения других задач. Также известно, что таможенные служащие и сотрудники портового контроля

поднимаются на борт судна и просят воспользоваться компьютером для «распечатки официальных документов» после того, как вставили неизвестный съёмный носитель.

Иногда невозможно контролировать, у кого есть доступ к бортовым системам, например, во время постановки в сухой док, стоянки или при принятии на борт нового или существующего судна. В таких случаях трудно понять, осталось ли вредоносное ПО в бортовых системах. Рекомендуется удалять конфиденциальные данные с судна и устанавливать их заново по возвращении на судно. По крайней мере, необходимо создавать резервные копии данных. По возможности перед использованием следует проверять системы на наличие вредоносных программ. Системы ОТ следует тестировать, чтобы убедиться, что они работают правильно.

3.6 Удаленный доступ

Некоторые ИТ-системы и системы ОТ доступны удаленно и могут работать при постоянном подключении к Интернету для удаленного мониторинга, сбора данных, обслуживания, обеспечения безопасности. Эти системы могут быть «сторонними системами», при которых подрядчик удалённо контролирует и обслуживает системы. Эти системы могут включать двустороннюю передачу данных и/или только загрузку. Системы и рабочие станции с функциями удалённого управления, доступа или настройки могут быть, например, такими:

- компьютеры и рабочие станции на мостике и в машинном отделении в административной сети судна

- грузы, такие как контейнеры с системами контроля температуры или специализированные грузы, которые отслеживаются удалённо - системы поддержки принятия решений по обеспечению остойчивости
- системы мониторинга напряжений в корпусе
- навигационные системы, включая электронные навигационные карты (ENC), регистраторы данных о рейсе (VDR), системы динамического позиционирования (DP)
- планирование загрузки, размещение и управление грузами
- мониторинг и управление двигателем,
- сети безопасности, такие как системы видеонаблюдения (CCTV)
- специализированные системы, такие как системы для бурения, противовыбросовые системы, системы для подводных установок, системы аварийного отключения (ESD) для газовозов, системы для прокладки и ремонта подводных кабелей.

Судовладелец или оператор должен знать о степени и характере подключения оборудования и учитывать это как важную часть оценки рисков.

3.7 Обслуживание систем и программного обеспечения

ИТ- и ОТ-системы, программное обеспечение и техническое обслуживание могут быть переданы на аутсорсинг сторонним поставщикам услуг, и сама компания может быть не в состоянии проверить уровень безопасности, предоставляемый этими поставщиками.

Некоторые компании используют разных поставщиков, отвечающих за программное обеспечение и проверку кибербезопасности.

В таких случаях следует запрашивать у поставщиков подробную информацию об обновлениях.

ИНЦИДЕНТ:

сбой навигационного компьютера во время лоцманской проводки

Судно находилось под лоцманской проводкой, когда произошел сбой компьютеров ECDIS и судовых. Лоцман находился на мостике.

Сбои в работе компьютеров на короткое время отвлекли вахтенных офицеров, однако пилот и капитан совместными усилиями сосредоточили команду на безопасной навигации с помощью визуальных средств и радара. Когда компьютеры были перезагружены, стало очевидно, что операционные системы были устаревшими и неподдерживаемыми. Капитан сообщил, что эти проблемы с компьютерами возникали часто (он называл их «гремлинами») и что неоднократные запросы на обслуживание от судовладельца игнорировались.

Это наглядный пример того, как простое обслуживание и внимание к судну со стороны руководства могут предотвратить несчастные случаи.

4 Оценка вероятности

4.1 Вероятность как результат воздействия угрозы и уязвимости

Существует тенденция оценивать риски только на основе потенциальных последствий и существующих уязвимостей.

Однако, как уже отмечалось ранее, вероятность возникновения события, связанного с кибербезопасностью, является произведением угрозы и уязвимости. Это также означает, что если один из этих двух факторов практически отсутствует, то и вероятность будет близка к нулю, и это следует учитывать при количественной оценке вероятности.

4.2 Количественная оценка вероятности

В СУБ-сообщении компании обычно содержится матрица оценки рисков, в которой вероятность конкретного события оценивается по пятибалльной шкале. Использование существующей в СУБ шкалы вероятности может быть преимуществом, поскольку использование существующего языка и концепций для описания рисков, связанных с кибербезопасностью, облегчит понимание в масштабах всей компании. Согласованная корпоративная стратегия управления рисками и понимание ее важности имеют решающее значение для обеспечения поддержки высшим руководством эффективных стратегий управления киберрисками на основе результатов оценки рисков.

Один из примеров такой шкалы приведен ниже:

Уровень	Вероятность, описание
1	Никогда не слышал об этом в отрасли. Близко к чему-то невообразимому.
2	Слышал об этом в отрасли, но крайне редко и как о результате цепочки многих неудачных событий.
3	Инцидент, вероятно, произошёл в вашей компании, но из-за неисправного оборудования или неожиданных ошибок вовлечённых людей.
4	Время от времени происходит в вашей компании, как правило, из-за неисправного оборудования или ошибок вовлечённых людей (ошибок, которые время от времени случаются на борту).
5	Это часто случается при выполнении рассматриваемой работы.

Рис. 5. Пример шкалы вероятности из СУБ-сообщения.

В идеальном мире количественная оценка вероятности была бы подкреплена доступом к отраслевой информации об угрозах, связанной с судоходством, на основе отчётов об инцидентах. Однако такая информация об угрозах не всегда доступна, поэтому стоит обратить внимание на другие отрасли, помимо судоходства, поскольку злоумышленники часто используют методы, ранее применявшиеся для атак на одну отрасль, для атак на другую.

Кроме того, зачастую стоит более внимательно изучить факторы угрозы: возможности, условия и намерения. Особенно полезно обратить внимание на намерения, поскольку нулевые намерения будут количественно оценивать потенциальную угрозу как теоретическую и, следовательно, будут иметь лишь небольшую вероятность при сопоставлении (или умножении) с уязвимостью.

5 Оценка воздействия

5.1 Модель конфиденциальности, целостности и доступности CIA

Модель конфиденциальности, целостности и доступности (CIA) обеспечивает основу для оценки последствий:

-утраты конфиденциальности информации, например, несанкционированного доступа и разглашения информации или данных о судне, экипаже, грузе и пассажирах

- потеря целостности, которая может привести к изменению информации и данных, относящихся к безопасной и эффективной эксплуатации судна и управлению им.

- потеря доступности из-за уничтожения информации и данных и/или нарушения работы служб/систем судна.

Относительная важность конфиденциальности, целостности и доступности зависит от использования информации или данных. И наоборот, при оценке уязвимости OT-систем на борту судов, особенно критически важных систем, вместо конфиденциальности может быть уделено внимание доступности и/или целостности.

5.2 Количественная оценка воздействия

СУБ-сообщения компании обычно содержат матрицу оценки рисков, в которой влияние данного события оценивается по пятиступенчатой шкале возрастающих последствий для различных категорий, таких как безопасность персонала, охрана окружающей среды, безопасность грузов, сохранность активов, непрерывность бизнеса, финансовые последствия и репутация компании. Использование существующей шкалы воздействия СУБ может быть преимуществом, поскольку использование существующих формулировок и концепций для описания рисков, связанных с кибербезопасностью, облегчит понимание во всей компании.

Если эта шкала не использовалась для описания последствий, связанных с киберрисками, может потребоваться изменить словесное описание каждого из уровней последствий. Использование такой шкалы также позволяет компании различать разные суда в составе флота в зависимости от их значимости для общей деятельности компании.

Один из примеров такой шкалы приведен ниже:

Уровень	Описание воздействия
1	Отсутствие последствий для здоровья/травм. Отсутствие ущерба для окружающей среды, активов, финансов или репутации компании.
2	Очень незначительное воздействие на здоровье/травмы. Очень незначительный ущерб для окружающей среды, активов, финансов или репутации компании.
3	Незначительное воздействие на здоровье/незначительные травмы. Незначительный ущерб для окружающей среды, активов, финансов или репутации компании.
4	Значительное воздействие на здоровье/относительно серьёзные травмы. Локальный, но серьёзный ущерб окружающей среде, имуществу, финансам или репутации компании.
5	Смертельный исход или необратимые повреждения. Широкомасштабный, значительный ущерб окружающей среде, имуществу, финансам или репутации компании.

Рисунок 6. Пример вербального описания уровней воздействия в СУБ-сообщении.

Существует также несколько других методологий оценки, которые могут помочь определить масштаб последствия кибер-инцидента, например, пример на рисунке 7:

Потенциальное воздействие	Определение	На практике
Низкое	Можно ожидать, что потеря конфиденциальности, целостности или доступности данных окажет ограниченное негативное влияние на компанию и судно, организационные активы или отдельных лиц.	Ограниченный неблагоприятный эффект означает, что нарушение безопасности может: (i) привести к незначительному ущербу для физических лиц; (ii) привести к незначительному финансовому ущербу; (iii) привести к незначительному ущербу для активов организации; или (iv) привести к ухудшению работы судна в такой степени и на такой срок, что организация сможет выполнять свои основные функции, но эффективность этих функций будет заметно снижена.
Умеренное	Можно ожидать, что потеря конфиденциальности,	Существенный неблагоприятный эффект означает, что нарушение безопасности может: (i) привести к значительному ущербу для

	целостности или доступности данных окажет существенное негативное влияние на компанию и судно, активы или отдельных лиц.	физических лиц, не связанному с гибелью людей или серьезными травмами, угрожающими жизни; (ii) привести к значительным финансовым потерям; (iii) привести к значительному ущербу для активов организации; или (iv) привести к значительному ухудшению работы судна в такой степени и на такой срок, что организация сможет выполнять свои основные функции, но эффективность этих функций будет значительно снижена.
Высокое	Можно ожидать, что потеря конфиденциальности, целостности или доступности данных окажет серьёзное или катастрофическое негативное влияние на деятельность	Серьезные или катастрофические негативные последствия означают, что нарушение безопасности может: (i) привести к серьёзному или катастрофическому ущербу для людей, включая гибель или серьёзные травмы, угрожающие жизни; (ii) привести к значительным финансовым потерям;

	компании и судна, активы, окружающую среду или отдельных лиц.	(iii) привести к серьёзному ущербу для окружающей среды и/или активов организации; или (iv) привести к серьёзному ухудшению или потере работоспособности судна в такой степени и на такой срок, что организация не сможет выполнять одну или несколько своих основных функций.

Рис. 7. Потенциальные уровни воздействия при использовании модели CIA.

5.3 «Критическое» оборудование и технические системы

Оценка воздействия должна проводиться для каждой системы на борту.

Для систем ОТ такая оценка воздействия также является частью списка оборудования и технических систем, внезапный выход из строя которых может привести к опасным ситуациям, что требуется в соответствии с пунктом 10.4 Кодекса ISM (часто называемые «критическим» оборудованием и техническими системами).

Потенциальное воздействие на ИТ-системы также должно быть оценено, и, как правило, для этого потребуется участие основных пользователей, которые, в зависимости от функциональности системы, могут быть, например, сотрудниками, занимающимися грузовыми операциями, операционным персоналом, коммерческим и финансовым персоналом и т. д.

Последствия ухудшения работы или потери ИТ-систем могут сильно повлиять на работу судна, соблюдение нормативных требований и даже безопасность, и их не следует недооценивать.

11 Методологий, включая, помимо прочего, ISO/IEC 27005:2018 «Информационные технологии — методы обеспечения безопасности — управление рисками информационной безопасности», COSO «Система управления рисками предприятия» и ISO 31000:2018 «Управление рисками — руководство».

Пример:

Судно оснащено сложной системой управления энергопотреблением. Она состоит из распределительных щитов и систем управления генераторами для автоматического распределения нагрузки, контроля мощности и автоматической синхронизации. Помимо системы управления питанием, **система диспетчерского управления и сбора данных** (**SCADA**) обеспечивает вывод данных и позволяет экипажу контролировать распределение электроэнергии на борту.

SCADA-система (аббр. от англ. supervisory control and data acquisition, диспетчерское управление и сбор данных) — программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте (мониторинг) или управления им.

Основная цель создаваемой с помощью SCADA программы — дать оператору, управляющему технологическим процессом, полную информацию об этом процессе и

необходимые средства для воздействия на него.
Основные задачи SCADA-системы:
сбор данных от датчиков и представление их оператору в удобном для него виде, включая графики изменения параметров во времени;
дистанционное управление исполнительными механизмами;
ввод заданий алгоритмам автоматического управления;
реализация алгоритмов автоматического контроля и управления;
распознавание аварийных ситуаций и информирование оператора о состоянии процесса;
формирование отчётности о ходе процесса и выработке продукции.

Управление питанием важно для безопасности экипажа, судна и груза. Это также оказывает явное воздействие на окружающую среду и финансы, поскольку электроэнергия вырабатывается за счёт использования топлива либо основным двигателем судна (генератором на валу), либо вспомогательными двигателями. Таким образом, киберинцидент, который выводит из строя систему управления питанием или приводит к её сбоям, может поставить под угрозу работу и безопасность судна.
Чтобы снизить риск, компания должна добавить меры защиты, которые минимизируют вероятность такого киберинцидента.
Система SCADA содержит данные датчиков в реальном времени, которые используются на борту для управления питанием.

Он также генерирует данные о потреблении электроэнергии, которые используются судоходной компанией в административных целях. Чтобы определить, происходит ли потенциальное нарушение безопасности данных и информации, следует использовать модель CIA.

Модель CIA (Confidentiality — «конфиденциальность», Integrity — «целостность», Availability — «доступность») используется для обеспечения информационной безопасности IT-инфраструктуры.

Конфиденциальность в этой модели означает защиту данных от посторонних лиц и устройств. Например, подключение к VPN для обмена сообщениями.

Целостность предполагает использование специальных инструментов для защиты исходного вида информации. Например, контроль версий и цифровые подписи помогают отслеживать изменения в документах или коде.

Доступность означает защиту от кибератак, совершённых с целью заблокировать или затруднить доступ к системе и информации. Например, защита от DDoS-атак на сервер.

Также модель CIA может применяться в контексте управления сложными ситуациями, например, в рамках обучения коммуникации и лидерству. В этом случае она помогает определить, какие элементы ситуации можно напрямую контролировать, какие — нельзя, но на них можно повлиять, а с чем нельзя ничего сделать, и научиться с этим жить.

При этом судоходная компания должна определить потенциальное влияние наиболее конфиденциальной информации, которая хранится, обрабатывается или передаётся системой SCADA.

Используя модель CIA, судоходная компания может сделать вывод, что:

- потеря конфиденциальности данных датчиков, полученных системой SCADA, будет иметь незначительные последствия, поскольку датчики находятся в открытом доступе на борту. Однако с точки зрения безопасности важно, чтобы на информацию, передаваемую датчиками, можно было положиться. Поэтому потеря целостности может иметь серьёзные последствия. Если информация не может быть считана, это также будет проблемой с точки зрения безопасности. Таким образом, потеря доступности может иметь серьёзные последствия.
- потеря конфиденциальности информации о потреблении электроэнергии, отправляемой в транспортную компанию для статистических целей, оценивается как потенциальное незначительное воздействие. Также будет незначительное воздействие в случае потери целостности и доступности данных, поскольку они используются только для внутренних целей.

На следующем рисунке показан результат оценки:

SCADA система	Конфиденциальность	Целостность	Доступность	Общее воздействие
Данные датчиков	Низкие	Высокие	Высокие	Высокие
Статистические данные	Низкие	Низкие	Низкие	Низкие

Рисунок 8: Результат оценки CIA системы SCADA.

6. Оценка рисков

6.1 Взаимосвязь между факторами, влияющими на риск

Только после составления обзора угроз (намерений, возможностей и условий), уязвимостей, последствий и вероятности можно проводить оценку рисков. Оценка рисков не является разовым мероприятием и должна повторяться через соответствующие промежутки времени, чтобы результаты оценки рисков оставались актуальными.

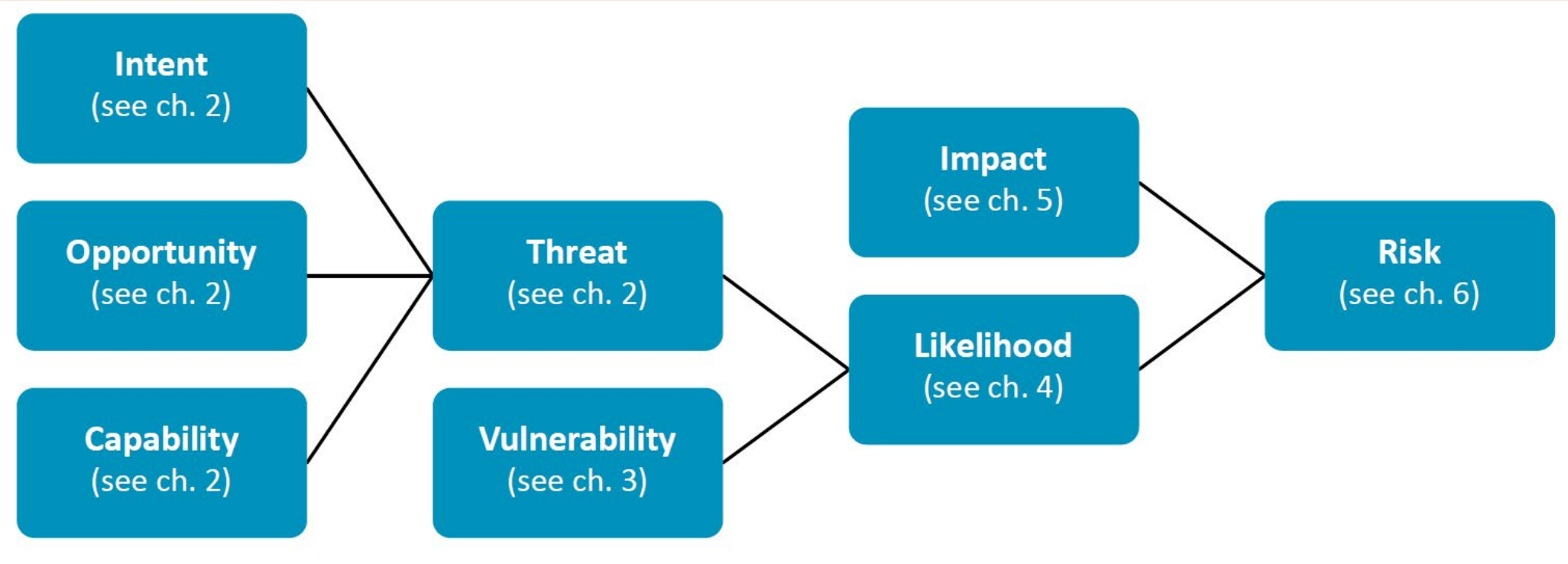

Рисунок 9: Взаимосвязь между различными факторами, влияющими на риск. Линии обозначают умножение, то есть «вероятность» умножается на «воздействие», чтобы получить «риск».

6.2 Четыре этапа оценки рисков

Этап 1: Предварительные мероприятия

Оценка рисков применяется как к существующим судам, так и к новым и бывшим в употреблении судам, поступающим в флот. Оценка киберрисков — сложная задача, требующая детальных знаний об управлении киберрисками, и в некоторых случаях может потребоваться сторонняя поддержка в процессе оценки рисков.

Перед началом оценки киберрисков на борту следует выполнить следующие действия:
- Изучите документацию по ИТ- и ОТ-системам, как описано в разделе 3.2, и оцените потенциальное воздействие, например, с помощью модели CIA (см. 5.1.).
- Определите основных производителей критически важного ИТ- и ОТ-оборудования на борту (в процессе определения следует использовать подход, основанный на оценке рисков).
- Определите точки взаимодействия по вопросам кибербезопасности с наиболее важными производителями и установите с ними рабочие отношения.
- Изучите подробную документацию по техническому обслуживанию и поддержке ИТ- и ОТ-систем на судне.
- Определите договорные требования и обязательства, которые могут быть у судовладельца/судооператора в отношении технического обслуживания и поддержки бортовых сетей и оборудования.

Этап 2: Оценка судна

После оценки всех факторов риска (угроз, уязвимостей, вероятности и последствий) можно приступить к оценке рисков и их снижению. Оценка рисков — это систематическое рассмотрение соответствующих факторов риска.

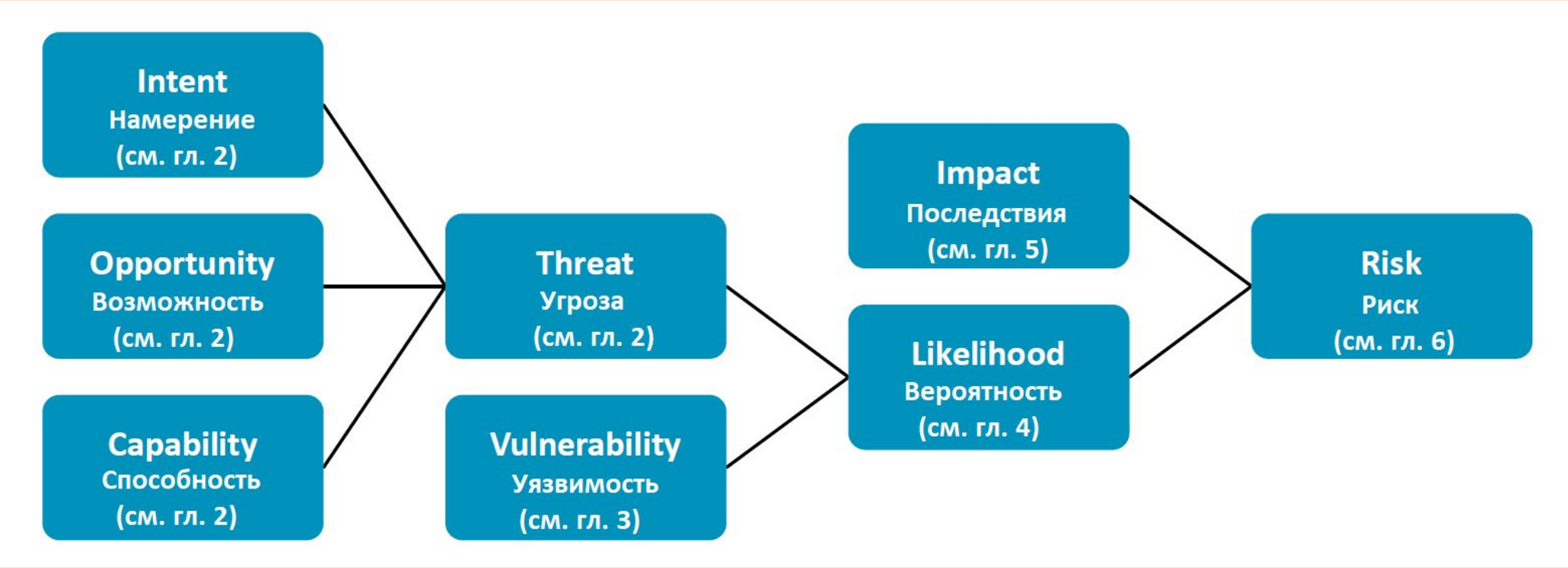

Рисунок 9: Взаимосвязь между различными факторами, влияющими на риск. Линии обозначают умножение, то есть «вероятность» умножается на «воздействие» для получения «риска».

Оценка рисков проводится для каждой системы отдельно и, следовательно, основывается на документации по системе, описанной в разделе 5.2. Для получения точных результатов оценка рисков основывается на знании функциональности систем, потоков данных в систему и из системы, а также на том, как каждая система подключена к другим системам с помощью кабельного или беспроводного соединения.

По этой же причине для оценки рисков, скорее всего, потребуется участие широкого круга сотрудников компании, производителей оборудования и внешних экспертов по кибербезопасности, если это необходимо. Каждое соединение является потенциальной уязвимостью.

Например, подключение к общему сетевому принтеру, доступному через Интернет, сопряжено с риском того, что киберпреступники могут использовать принтер в качестве шлюза для доступа к другим системам, подключенным к принтеру.

Определение и реализация мер по снижению рисков, основанных на оценке рисков, хорошо зарекомендовали себя на всех судах с помощью кодекса ISM и СУБ компании. Однако оценку киберрисков не следует путать с оценкой операционных рисков, обычно проводимой экипажем в соответствии с СУБ.

Оценка киберрисков — более сложная задача, которая, скорее всего, потребует привлечения офисного персонала и, возможно, даже сторонних консультантов в зависимости от уровня сложности.

Чтобы рассчитать риск для конкретной системы, необходимо оценить вероятность и последствия.

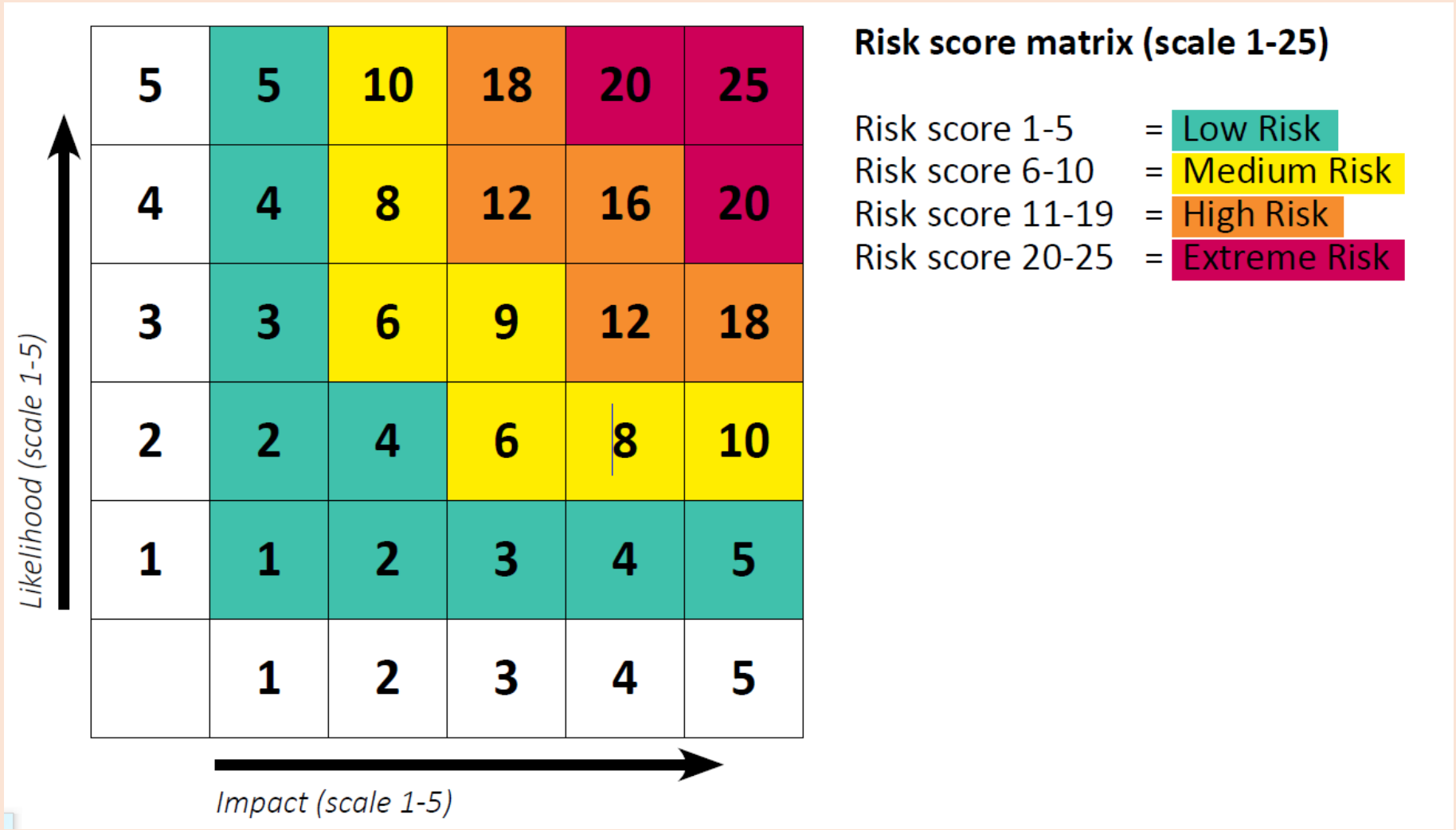

Рис. 10. Пример матрицы оценки рисков компании.

Если рассчитанный первоначальный риск для конкретной системы превышает допустимый в соответствии с критериями принятия рисков компании, риск необходимо снизить, чтобы остаточный риск достиг приемлемого уровня (как показано в следующем примере):

Система	Воздействие	Вероятность	Первоначальный риск	Снижение риска	Остаточный риск
ECDIS	Оценка 5 из-за риска катастрофических событий, таких как посадка на мель и столкновение	Оценка 4 из-за активных USB-портов, использования компьютера для других целей, подключения к административной сети для доступа к общему принтеру, подключения к автоматическому обновлению карт через спутник от надёжного поставщика	**Риск = 5 x 4 = 20**	Защита паролем и ограничение использования ПК только для ECDIS	**Риск = 5 x 3 = 15**
				Отключение от административной сети	**Риск = 5 x 2 = 10**
				Отключение USB-портов	**Риск = 5 x 1 = 5**

Рис. 11. Пример оценки рисков и определения мер по их снижению.

Несмотря на то, что оценка рисков проводится для каждой системы в отдельности, оценка рисков для судна в целом потребует комплексного подхода с учетом того факта, что некоторые потенциальные меры по снижению рисков, предложенные для одной системы, могут повлиять на оценку рисков для других систем. Комплексный подход гарантирует, что меры по снижению рисков будут выбраны в соответствии с их влиянием на различные системы, которые часто связаны между собой, и, конечно, с учётом их экономической эффективности. Различные меры по снижению рисков более подробно описаны в последующих главах настоящего руководства.

. Действия, выполняемые в ходе оценки, могут включать проверку конфигурации всех компьютеров, серверов, маршрутизаторов и технологий кибербезопасности, включая брандмауэры. Они также могут включать проверку всей имеющейся документации по кибербезопасности и процедур для подключённых ИТ- и ОТ-систем и устройств.

Одним из аспектов оценки на борту судна является привлечение экипажа всех уровней, в частности капитана, главного механика и первого помощника. Этот процесс помогает понять, как на борту внедряются ИТ- и ОТ-системы и насколько они могут отличаться от описанных в проектной документации, а также понять, какой уровень киберподготовки должен быть у экипажа судна.

По очевидным причинам выбор мер по снижению рисков зависит от имеющихся ресурсов и характера риска. Некоторые меры по снижению рисков, например изменения в процедурах, могут быть столь же эффективными, как и дорогостоящие технические решения.

Особенно для существующих судов с устаревшими системами внедрение технических решений может быть сложным и дорогостоящим.

Оценка эффективности различных мер по снижению рисков должна быть неотъемлемой частью процесса оценки рисков.

Также можно классифицировать различные меры по снижению рисков, чтобы было проще понять и предоставить рекомендации о том, какие средства контроля использовать и где.

Этап 3: Подведение итогов и составление отчётов

Чтобы соответствовать требованиям Кодекса ISM, оценка рисков должна быть последовательным и актуальным документом, отражающим то, как оцениваются и снижаются риски. Проведение такой оценки рисков часто представляет собой итеративный процесс, в ходе которого различные меры по снижению рисков рассматриваются в разных комбинациях, пока не будет принято решение об оптимальном составе мер по снижению рисков, учитывающем законодательные требования, допустимый уровень риска, осуществимость, эффективность и стоимость.

Если оценка рисков проводится сторонней организацией (например, если в штате нет достаточного количества специалистов), то первоначальный отчёт сторонней организации, скорее всего, будет промежуточным отчётом, в котором содержатся рекомендации. После рассмотрения рекомендаций и принятия окончательного решения это должно быть отражено в окончательной оценке рисков.

Первоначальная оценка киберрисков сторонней организацией может включать, например, следующее:

- краткое изложение — обзор результатов, рекомендаций и общего уровня безопасности оцениваемого судна
- технические выводы — описание обнаруженных уязвимостей, вероятность их использования, денежные затраты на их использование, влияние на экипаж, судно и окружающую среду, а также

соответствующие рекомендации по техническому исправлению и смягчению последствий

- приоритетный список действий — расставленные приоритеты должны отражать эффективность меры, затраты, применимость и т. д. Важно, чтобы этот список был полным и включал все доступные варианты, а не представлял собой перечень услуг и продуктов, которые сторонний специалист по оценке рисков, если применимо, хотел бы продать.
- дополнительные данные — дополнение, содержащее технические подробности всех ключевых выводов и всесторонний анализ критических уязвимостей. В этот раздел также следует включить образцы данных, полученных в ходе тестирования на проникновение, если таковые имеются, и критические уязвимости или уязвимости с высоким уровнем риска.
- приложения — записи о проведённых мероприятиях и инструментах, использованных группой по оценке киберрисков.

Этап 4: отчёт производителя

После того как судовладелец получит возможность ознакомиться с результатами, обсудить и оценить их, часть результатов может быть отправлена производителям затронутых систем для снижения или устранения рисков. Любые выявленные уязвимости, например, любая выявленная киберуязвимость в заводской стандартной конфигурации критически важной системы или компонента, могут быть дополнительно проанализированы при поддержке внешних экспертов, которые должны работать с контактным лицом производителя по вопросам кибербезопасности, чтобы обеспечить полное понимание рисков и технических аспектов проблемы. Эта вспомогательная деятельность направлена на то, чтобы любой план устранения уязвимостей, разработанный производителем, был комплексным и определял правильное решение для устранения уязвимостей.

6.3 Оценка рисков третьей стороной

В зависимости от возможностей компании по проведению точной оценки рисков может быть рассмотрена возможность привлечения помощи третьих лиц.

Оценка рисков третьей стороной может также включать тесты на проникновение в критически важную ИТ-инфраструктуру, чтобы определить, соответствует ли фактический уровень защиты желаемому уровню, указанному в стратегии кибербезопасности компании.

Такие тесты могут имитировать инциденты с использованием как IT-систем, так и социальной инженерии и, при желании, даже физического проникновения за периметр безопасности объекта. Эти тесты называются активными тестами, поскольку они предполагают доступ к программному обеспечению и его потенциальную установку в систему.

Это может быть уместно только для ИТ-систем. Если риск для ОТ-систем во время тестирования на проникновение неприемлем, следует рассмотреть возможность пассивного тестирования. Пассивные методы основаны на сканировании данных, передаваемых системой, для выявления уязвимостей. Как правило, не следует предпринимать попыток активного доступа к системе или внедрения в нее программного обеспечения.

Оценка рисков сторонними организациями — это ценный способ интеграции специализированных навыков и опыта в области для выполнения различных задач в рамках общих усилий по управлению и устранению киберрисков. Такие оценки также полезны для компаний с ограниченными кадровыми ресурсами, поскольку позволяют проводить объективную и прозрачную оценку киберрисков. Выбор сторонних организаций для оказания помощи в этих мероприятиях также позволяет заинтересованным сторонам получить информацию с разных точек зрения и провести комплексную проверку, что дает им возможность делать осознанный и уверенный выбор.

Хотя тестирование на проникновение рассматривается как способ определения того, могут ли сети и системы быть скомпрометированы, существует множество других способов, которые также позволяют получить представление об окружении собственной организации и парка оборудования. Эти услуги могут включать в себя обнаружение и инвентаризацию активов в сетях, чтобы помочь судовладельцам и операторам понять, что подключено, где и с кем. Третьи стороны также могут проводить анализ и проектирование архитектуры сети, чтобы понять и проверить текущую структуру, а также определить, где можно внести улучшения экономически эффективными и разумными способами. Оценка уязвимостей может проводиться как более глубокое и широкое исследование, включая даже пассивное сканирование сети. Тестирование на проникновение является интрузивной процедурой, сопряжено с большим риском, в значительной степени дороже и требует понимания сетей и инвентаризируемых активов. Тестирование на проникновение следует проводить только в особых случаях и при необходимости технических действий. Как и в случае с любой другой услугой, руководящим должностным лицам и береговому персоналу важно координировать эти действия в целях безопасности и выбирать сторонние службы, знакомые с флотом и имеющие опыт.

7. Разработка мер защиты

7.1 Защита по принципу «глубокой» и «широкой» обороны

Важно защищать критически важные системы и данные с помощью многоуровневых мер защиты, которые учитывают роль персонала, процедур и технологий, чтобы:

- повысить вероятность обнаружения киберинцидента
- максимально эффективно использовать ресурсы, необходимые для защиты конфиденциальности, целостности и доступности данных в ИТ- и ОТ-системах.

Для подключенных ОТ-систем на борту должно требоваться более одной технической и/или процедурной меры защиты. Периферийные средства защиты, такие как брандмауэры, важны для предотвращения нежелательногодоступа к системам, но этого может быть недостаточно для борьбы с внутренними угрозами.

Такой подход к многоуровневой защите предполагает сочетание:

- физической безопасности судна в соответствии с планом обеспечения безопасности судна (SSP);
- защиты сетей, включая эффективную сегментацию;
- обнаружения вторжений
- использование брандмауэра
- периодическое сканирование и тестирование на уязвимости
- внесение программного обеспечения в белый список
- контроль доступа и пользователей
- контроль управления конфигурацией и изменениями

- соответствующие процедуры, касающиеся использования съемных носителей и политики паролей
- осведомленность персонала о кибербезопасности и понимание рисков для себя и отрасли
- понимание и знакомство с соответствующими процедурами, включая реагирование на инциденты.

Политика и процедуры компании должны способствовать обеспечению кибербезопасности в рамках общего подхода к управлению рисками в сфере безопасности. Сложность и потенциальная устойчивость киберугроз означают, что следует рассматривать подход «глубокой защиты». Оборудование и данные, защищенные несколькими уровнями мер безопасности, более устойчивы к киберинцидентам.

Широкая защита

При разработке интеграции между системами следует учитывать модель границ доверия, согласно которой системы группируются в те, между которыми доверие подразумевается (например, рабочие станции пользователей), и те, между которыми доверие должно быть явным (между компьютерами-мостами и корпоративными сетями). Для больших или сложных сетей следует рассматривать моделирование угроз как деятельность, направленную на понимание того, где между системами следует внедрять технические средства контроля для обеспечения защиты по широкому спектру.

Однако на борту судов, где уровень интеграции между ИТ- и ОТ-системами может быть высоким, эшелонированная защита работает только в том случае, если технические и процедурные меры защиты применяются на нескольких уровнях во всех уязвимых и интегрированных системах. Это «эшелонированная защита», которая используется для предотвращения использования уязвимостей одной системы для обхода мер защиты другой системы.

Углубленная и комплексная защита — это взаимодополняющие подходы, которые при совместном применении создают основу для комплексного реагирования на киберриски. Необходимо расставить приоритеты в области контроля кибербезопасности, уделяя особое внимание в первую очередь тем мерам или сочетанию мер, которые приносят наибольшую пользу. Конечно, все системы могут быть защищены, но в некоторых случаях затраты времени и денег намного превышают риск заражения как таковой.

7.2 Технические меры защиты

Меры по защите от киберрисков могут быть техническими и направленными на обеспечение того, чтобы бортовые системы были спроектированы и сконфигурированы таким образом, чтобы быть устойчивыми к киберинцидентам. Необходимо рассмотреть возможность внедрения технических средств контроля, которые являются практичными и экономически эффективными, особенно на существующих судах.

Следует отметить, что внедрение технических средств контроля — это не разовая процедура.

После внедрения их необходимо поддерживать в актуальном состоянии, чтобы избежать риска сбоя.

Центр интернет-безопасности (CIS) предоставляет рекомендации по мерам, которые можно использовать для устранения уязвимостей в сфере кибербезопасности. Меры защиты представляют собой список критически важных средств контроля безопасности (CSC), которые отбираются и проверяются с целью обеспечения эффективного подхода к оценке и улучшению защиты компаний. CSC включают в себя как технические, так и процедурные аспекты.

Приведенные ниже примеры CSC были выбраны как наиболее подходящие для оборудования и данных на борту судов.

Ограничение и контроль сетевых портов, протоколов и служб Списки доступа к сетевым системам могут использоваться для реализации политики безопасности компании. Это помогает обеспечить, чтобы через контролируемую сеть или подсеть разрешался только соответствующий трафик в соответствии с политикой управления этой сетью или подсетью.

Рекомендуется защищать маршрутизаторы от инцидентов и закрывать неиспользуемые порты, чтобы предотвратить несанкционированный доступ к системам или данным.

Настройка сетевых устройств, таких как брандмауэры, маршрутизаторы и коммутаторы

Следует определить, какие системы следует подключать к контролируемым или неконтролируемым сетям.

Контролируемые сети предназначены для предотвращения любых угроз безопасности, исходящих от подключенных устройств, с помощью брандмауэров, шлюзов безопасности, маршрутизаторов и коммутаторов. Неконтролируемые сети могут представлять опасность из-за отсутствия контроля за трафиком данных и должны быть изолированы от контролируемых сетей, поскольку прямое подключение к Интернету делает их очень уязвимыми для проникновения вредоносных программ. Например:

-сети, которые имеют решающее значение для функционирования самого судна, должны контролироваться. Важно, чтобы эти системы имели высокий уровень безопасности.

- Сети, предоставляющие поставщикам удалённый доступ к навигационному и другому программному обеспечению ОТ-систем на борту, также должны контролироваться. Может потребоваться разрешить поставщикам загружать обновления системы или выполнять удалённое обслуживание в этих сетях. Внешние точки доступа к таким соединениям на берегу должны быть защищены от несанкционированного доступа.

- Системы хранения грузов, планирования загрузки и управления грузами и контейнерами должны контролироваться.

Таким образом, те системы, которые выполняют обязательную передачу данных о судне государственным органам.

- другие сети, такие как сети гостевого доступа, могут быть неконтролируемыми, например, те, которые связаны с развлечениями пассажиров или частным доступом в Интернет для экипажа. Как правило, любая беспроводная сеть должна считаться неконтролируемой.

Разработка мер защиты

Эффективное разделение систем на основе необходимого доступа и уровней доверия — одна из наиболее успешных стратегий предотвращения киберинцидентов. Эффективно разделённые сети могут значительно затруднить доступ злоумышленников к системам судна и являются одним из наиболее эффективных методов предотвращения распространения вредоносного ПО. Бортовые сети должны быть разделены брандмауэрами для создания безопасных зон. Конфигурации брандмауэров следует регулярно проверять на наличие несанкционированных изменений. Чем меньше каналов связи и устройств в зоне, тем безопаснее системы и данные в этой зоне. Конфиденциальные и критически важные системы должны находиться в наиболее защищенной зоне. Дополнительную информацию о судовых сетях см. в приложении 3 к настоящим рекомендациям, а также в стандарте ISO/IEC 62443 и рекомендации IACS № 166 по киберустойчивости.

ИНЦИДЕНТ:

заражение вредоносным ПО морских ИТ-систем и ОТ-систем

Корабль был оснащён системой управления питанием, которую можно было подключить к интернету для обновления программного обеспечения и установки исправлений, удалённой диагностики, сбора данных и удалённого управления. Корабль был построен недавно, но эта система не была подключена к интернету по умолчанию.

ИТ-отдел компании принял решение посетить корабль и провести сканирование уязвимостей, чтобы определить, есть ли в системе признаки заражения и безопасно ли подключение. Команда обнаружила дремлющего червя, который мог активироваться, как только система была подключена к Интернету, и это имело бы серьезные последствия. Инцидент подчеркивает, что даже системы с воздушными зазорами могут быть скомпрометированы, и подчеркивает важность упреждающего управления киберрисками.

Судовладелец уведомил производителя об обнаружении и запросил процедуры по удалению вируса-червя. Судовладелец заявил, что до обнаружения на борту судна находился специалист по техническому обслуживанию.

Предполагалось, что заражение потенциально могло быть вызвано этим специалистом.

Червь распространялся через USB-устройства в запущенном процессе, который выполнял программу в памяти.

Эта программа была разработана для связи с сервером управления и контроля для получения следующего набора инструкций. Она могла даже создавать файлы и папки.

Компания обратилась к специалистам по кибербезопасности для проведения криминалистической экспертизы и устранения последствий. Было установлено, что все серверы, связанные с оборудованием, были заражены и что вирус находился в системе незамеченным в течение 875 дней.

Инструменты сканирования удалили вирус.

Анализ показал, что поставщиком услуг действительно был червь, который внедрил вредоносное ПО в систему судна через USB-накопитель во время установки программного обеспечения.
Анализ также показал, что этот червь работал в системной памяти и активно выходил в Интернет с сервера. Поскольку червь был загружен в память, он мог влиять на производительность сервера и систем, подключенных к Интернету.

Физическая безопасность

Физическая безопасность иногда является самой простой, дешёвой и очевидной формой киберзащиты. Это центральный аспект управления киберрисками, и эффективная стратегия эшелонированной защиты должна быть направлена на то, чтобы обеспечить невозможность обхода мер физического контроля. Зоны, содержащие чувствительные компоненты OT или IT-систем, должны быть надёжно заблокированы, критически важное для безопасности оборудование и кабельные трассы должны быть защищены от несанкционированного доступа, а физический доступ к чувствительному пользовательскому оборудованию (например, к открытым USB-портам на мостовых системах) должен быть ограничен. В плане обеспечения безопасности судна такие зоны будут определены как зоны ограниченного доступа в соответствии с разделом 9.4.1 части A Кодекса ISPS с учетом рекомендаций, изложенных в части B Кодекса. Это особенно актуально для мест, которые обычно не освещаются в порту, например, мостика.

Спутниковая связь и радиосвязь

Кибербезопасность радио- и спутниковой связи должна рассматриваться совместно с поставщиком услуг. В связи с этим при определении требований к защите бортовой сети следует учитывать характеристики спутниковой связи.

Спутниковый терминал обычно имеет незащищённый порт локальной сети для подключения к судовой сети, что оставляет открытыми различные варианты защиты в зависимости от угрозы.

Защита от прослушивания обычно осуществляется с помощью подключения к виртуальной частной сети (VPN) или зашифрованных протоколов. В то время как защита от взлома, перехвата и других видов атак может быть достигнута с помощью других средств, таких как соглашение о безопасности с поставщиком услуг, подключение через защищённый сервер на берегу, например, принадлежащий компании, или бортовой брандмауэр.

Одним из важных аспектов кибербезопасности является обеспечение невидимости спутникового терминала. Этого можно добиться, отключив такие функции, как «страница удалённого администрирования» и «переадресация портов». Отключение обычно можно выполнить в меню настроек терминала.

При установлении соединения между навигационными и управляющими системами судна и поставщиками услуг на берегу следует учитывать, как предотвратить несанкционированный доступ к бортовым системам. Рекомендуется не публиковать общедоступный IP-адрес и не маршрутизировать его напрямую на судно из интернета.

Соединения из интернета должны проходить через береговую сеть и брандмауэр для маршрутизации и контроля доступа. Во-вторых, необходимо тщательно отслеживать исходящие соединения, исходящие из судовых сетей, сетей управления или сетей, подключенных к сетям управления (т. е. обратные туннельные соединения).

Ответственность за подключение к сети лежит на партнере по распределению. Ответственность за окончательную маршрутизацию пользовательского трафика от точки доступа к интернету до конечного пункта назначения на борту («последняя миля») лежит на судовладельце. Пользовательский трафик направляется через коммуникационное оборудование для дальнейшей передачи на борту. В точке доступа к этому трафику необходимо обеспечить безопасность данных, брандмауэр и выделенное соединение «последней мили».

При использовании виртуальной частной сети (VPN) трафик данных должен быть зашифрован в соответствии с международным стандартом. Кроме того, перед серверами и компьютерами, подключёнными к сетям (на берегу или на борту), должен быть установлен брандмауэр. Партнер по дистрибуции должен проконсультировать по поводу маршрутизации и типа подключения, наиболее подходящих для конкретного трафика. Фильтрация (проверка/блокировка) трафика на берегу также является вопросом, который решается между судовладельцем и партнёром по дистрибуции. Для достижения достаточного уровня защиты необходимы как фильтрация трафика на берегу, так и брандмауэры/шлюзы для проверки/блокировки безопасности на судне.

Производители терминалов спутниковой связи и другого коммуникационного оборудования могут предоставлять интерфейсы управления с программным обеспечением для контроля безопасности, которые доступны по сети.

В основном это веб-интерфейсы. При оценке безопасности судовой установки следует учитывать защиту таких интерфейсов. Примеры защиты административных интерфейсов включают ограничение доступа к таким интерфейсам из сетей, будь то веб-интерфейсы или командная строка, а также полное отключение ненужных интерфейсов, которые используются только при первоначальной настройке. Как и в случае с другими системами, следует надлежащим образом управлять паролями, например, пароли по умолчанию, которые часто известны преступникам, следует менять.

Управление беспроводным доступом

Беспроводной доступ к сетям на судне должен быть ограничен соответствующими авторизованными устройствами и защищён с помощью надёжного ключа шифрования, который регулярно меняется. Для управления беспроводным доступом можно рассмотреть следующие варианты:

- использование корпоративных систем аутентификации с асимметричным шифрованием и изоляцией сетей с помощью соответствующих выделенных точек беспроводного доступа (например, гостевые сети, изолированные от административных сетей)
- внедрение систем, таких как беспроводная IPS, которые могут перехватывать неавторизованные точки беспроводного доступа или мошеннические устройства.

Использование контроля доступа к сети (NAC) для профилирования устройств (корпоративных или личных) и управления доступом к беспроводной сети эффективно для управления доступом

- защита физического соединения между устройствами беспроводного доступа и сетью, такими как сетевые разъемы, сетевые стойки и т. д., для предотвращения несанкционированного доступа мошеннических устройств.

Безопасная конфигурация аппаратного и программного обеспечения

Профили пользователей должны быть ограничены таким образом, чтобы компьютеры, рабочие станции или серверы можно было использовать только для тех целей, для которых они предназначены. Профили пользователей не должны позволять пользователям изменять системы или устанавливать и запускать новые программы.

Защита электронной почты и веб-браузера

Любая защита электронной почты и веб-браузера должна:

- защищать береговых и судовых сотрудников от потенциальной социальной инженерии
- предотвращать использование электронной почты для получения конфиденциальной информации
- убедитесь, что обмен конфиденциальной информацией по электронной почте или с помощью голосовой связи защищен надлежащим образом, чтобы обеспечить конфиденциальность и целостность данных, например, с помощью шифрования

- предотвратите выполнение вредоносных сценариев веб-браузерами и почтовыми клиентами.

Для безопасной передачи электронной почты рекомендуется использовать электронные письма в формате zip или зашифрованные файлы, при необходимости отключите гиперссылки в системе электронной почты, избегайте использования общих адресов электронной почты и убедитесь, что в системе настроены учетные записи пользователей.

Безопасность прикладного программного обеспечения (управление исправлениями)

Для бортовых систем следует предоставлять обновления безопасности, и рекомендуется разработать план обновления программного и аппаратного обеспечения. Обновления безопасности следует включать в периодический цикл технического обслуживания, и рекомендуется уделять особое внимание оборудованию, используемому для разделения виртуальных сетей (VLAN) и межсетевых экранов. Эти обновления или исправления следует применять правильно и своевременно, чтобы устранить любые уязвимости в системе до того, как они будут использованы и станут доступны хакерам. Некоторые исправления могут быть сложными и дорогостоящими.

В OT-системах необходимо согласовывать все программное и аппаратное обеспечение, а также проводить тщательные тесты после установки для проверки целостности. В других случаях исправления безопасности могут быть неприменимы без частичной или полной модернизации аппаратного обеспечения системы. По этим причинам OT-системы обновляются не так часто или не обновляются вовсе.

Перед установкой исправлений важно оценить совместимость и потенциальное влияние на работу ОТ-систем. Если критически важное исправление не может быть установлено, следует рассмотреть альтернативные меры, чтобы гарантировать, что уязвимости не будут раскрыты в более крупных ИТ-сетях или, в конечном итоге, в интернете. Это может быть сочетание физической защиты, ограничения доступа к сети и применения методов виртуального исправления ошибок.

7.3 Процедурные меры защиты

Меры защиты также могут быть процедурными и должны быть предусмотрены политикой компании, процедурами управления безопасностью, процедурами обеспечения безопасности и контролем доступа. Как и в случае со всеми другими мерами контроля, следует применять только те процедурные меры контроля, которые являются практичными и экономически эффективными. Процедурные меры контроля направлены на то, чтобы персонал использовал бортовые системы надлежащим образом. Планы и процедуры, содержащие конфиденциальную информацию, должны храниться в секрете и обрабатываться в соответствии с политикой компании.

Примерами процедурных мер могут быть:

Обучение и повышение осведомлённости

Обучение и повышение осведомлённости являются ключевыми вспомогательными элементами эффективного подхода к управлению киберрисками, описанного в этих рекомендациях.

Следует учитывать внутреннюю киберугрозу. Персонал играет ключевую роль в защите ИТ- и ОТ-систем, но может проявлять небрежность, например, используя съёмные носители для передачи данных между системами без мер предосторожности против передачи вредоносного ПО.

Обучение и повышение осведомлённости должны соответствовать необходимым уровням для:

- судового персонала, включая капитана, офицеров и членов экипажа
- берегового персонала, который поддерживает управление, погрузку, хранение и эксплуатацию судна.

Конвенция ПДНВ требует от компаний обеспечить, чтобы моряки были ознакомлены “[...] со всеми судовыми механизмами, установками, оборудованием, процедурами и характеристиками судов, которые имеют отношение к их повседневным или аварийным обязанностям”, и чтобы “[...] экипаж судна мог эффективно координировать их действия в аварийной ситуации и в чрезвычайных ситуациях". выполнение функций, жизненно важных для обеспечения безопасности, защиты или смягчения последствий загрязнения”. Управление, при необходимости, киберрисками подпадает под действие конвенции ПДНВ.

В дополнение к ознакомительному обучению моряков, предусмотренному конвенцией ПДНВ, для всего судового персонала в соответствии с его ролью должна быть разработана программа повышения осведомлённости, охватывающая, например, некоторые из следующих вопросов:

- риски, связанные с электронной почтой, и способы безопасного поведения. Примерами являются фишинговые атаки, когда пользователь переходит по ссылке на вредоносный сайт или открывает вредоносное вложение
- риски, связанные с использованием интернета, в том числе социальных сетей, чатов и облачных хранилищ, где перемещение данных менее контролируется и отслеживается
- риски, связанные с общедоступными данными геолокации персонала и судна
- риски, связанные с использованием собственных устройств. На этих устройствах могут отсутствовать обновления безопасности и средства контроля, такие как антивирусные программы, и они могут переносить риски на среду, к которой подключены
- риски, связанные с установкой и обслуживанием программного обеспечения на оборудовании компании с использованием заражённого оборудования (съемных носителей) или программного обеспечения (заражённого пакета)
- риски, связанные с ненадлежащими методами обеспечения безопасности программного обеспечения и данных, когда не выполняются антивирусные проверки или проверка подлинности
- защита пользовательской информации, паролей и цифровых сертификатов
- киберриски, связанные с физическим присутствием сотрудников, не являющихся сотрудниками компании, например, когда сторонние специалисты работают с оборудованием без надзора
- обнаружение подозрительной активности или устройств и способы сообщения о возможном киберинциденте.

Примерами могут служить странные подключения, которые обычно не наблюдаются, или подключение неизвестного устройства к корабельной сети
- осведомлённость о последствиях или влиянии киберинцидентов на безопасность и работу судна
- понимание того, как выполнять профилактическое обслуживание, такое как антивирусная и антишпионская защита,
установка обновлений, резервное копирование, планирование и тестирование реагирования на инциденты
- процедуры защиты от рисков, связанных с использованием съёмных носителей данных поставщиками услуг, перед подключением к системам судна.
Кроме того, персонал должен быть осведомлён о том, что наличие антивирусного программного обеспечения не отменяет необходимости в надёжных процедурах безопасности, например, в контроле использования всех съёмных носителей.
Кроме того, соответствующий персонал должен знать признаки того, что компьютер был взломан. К ним могут относиться следующие:
- система не отвечает или отвечает медленно
- неожиданные изменения паролей или блокировка авторизованных пользователей в системе
- неожиданные ошибки в программах, в том числе некорректная работа или неожиданное выполнение программ

- неожиданные или внезапные изменения доступного дискового пространства или памяти
- неожиданное возвращение электронных писем
- непредвиденные проблемы с подключением к сети
- частые сбои системы
- аномальная активность жесткого диска или процессора
- непредвиденные изменения в браузере, программном обеспечении или настройках пользователя, включая разрешения.

Назначенный персонал должен уметь разбираться в отчетах систем обнаружения вторжений, если они используются.

Этот список не является исчерпывающим и предназначен для повышения осведомленности о потенциальных признаках, которые следует рассматривать как возможные киберинциденты.

Эти рекомендации предполагают, что другие основные участники цепочки поставок, такие как фрахтователи, классификационные общества и поставщики услуг, будут внедрять передовые методы обеспечения кибербезопасности и проводить обучение. Владельцам и операторам рекомендуется проверять уровень готовности к обеспечению кибербезопасности своих сторонних поставщиков, в том числе морских терминалов и стивидоров, в рамках процедур поиска поставщиков таких услуг.

Доступ к компьютеру для посетителей

Доступ к компьютерам на борту должен быть ограничен для таких посетителей, как представители власти, технические специалисты, агенты, сотрудники портов и терминалов, а также представители владельцев. Несанкционированный доступ к конфиденциальным компьютерам должен быть запрещён. Если доступ к сети для посетителя необходим и разрешён, то он должен быть ограничен с точки зрения прав пользователя и осуществляться под наблюдением. Доступ к определённым сетям для технического обслуживания должен быть одобрен и согласован в соответствии с надлежащими процедурами, описанными компанией/судовладельцем.
Если посетителю требуется доступ к компьютеру и принтеру, следует использовать отдельный компьютер, изолированный от всех контролируемых сетей. Чтобы избежать несанкционированного доступа, на всех других физически доступных компьютерах и сетевых портах следует установить блокираторы съемных носителей.

ИНЦИДЕНТ:

Доступ инспектора по бункеровке к административной сети судна

Сухогруз в порту только что завершил операции по бункеровке. Инспектор по бункеровке поднялся на борт судна и запросил разрешение на доступ к компьютеру в машинном отделении, чтобы распечатать документы для подписи. Инженер-строитель вставил USB-накопитель в компьютер и непреднамеренно внедрил вредоносное ПО в административную сеть судна.

Вредоносное ПО оставалось незамеченным до тех пор, пока на судне не была проведена киберэкспертиза, а также после того, как экипаж сообщил о «компьютерной проблеме», затронувшей рабочие сети.
Это подчёркивает необходимость процедур по предотвращению или ограничению использования USB-устройств на борту, в том числе принадлежащих посетителям.

Личные устройства экипажа

Должны быть предусмотрены процедуры, предоставляющие экипажу инструкции по использованию ИТ-устройств в личных и развлекательных целях. Это должно включать в себя использование судовых сетей связи для личных целей, таких как Skype, электронная почта, игры, потоковое видео, без угрозы для критически важных ИТ- или ОТ-систем.

Обновление и обслуживание программного обеспечения

Аппаратное или программное обеспечение, которое больше не поддерживается производителем или разработчиком программного обеспечения, не получать обновления для устранения потенциальных уязвимостей. По этой причине использование аппаратного и программного обеспечения, которое больше не поддерживается, должно быть тщательно оценено компанией в рамках оценки киберрисков.

Соответствующее аппаратное и программное обеспечение на борту должно быть обновлено, чтобы обеспечить достаточный уровень безопасности.

Для своевременного обновления программного обеспечения могут потребоваться специальные процедуры с учетом типа судна, скорости подключения к интернету, времени в море и т. д. Программное обеспечение включает в себя операционные системы компьютеров, которые также должны обновляться. Кроме того, ряд маршрутизаторов, коммутаторов и брандмауэров, а также различные ОТ-устройства будут работать под управлением собственных прошивок, которые могут требовать регулярных обновлений, что должно быть отражено в процедурных требованиях.

Эффективное обслуживание программного обеспечения зависит от выявления, планирования и выполнения мер, необходимых для поддержки работ по обслуживанию на протяжении всего жизненного цикла программного обеспечения. Был разработан отраслевой стандарт, помогающий обеспечить безопасное обслуживание программного обеспечения. В нем определены требования ко всем заинтересованным сторонам, участвующим в обслуживании программного обеспечения судового оборудования и связанных с ним интегрированных систем. Стандарт охватывает обслуживание программного обеспечения на борту, на берегу и удаленно.

Управление антивирусными и вредоносными программами

Необходимо постоянно обновлять программные средства сканирования, используемые для обнаружения вредоносных программ и борьбы с ними. Необходимо установить процедурные требования для обеспечения своевременного распространения обновлений на судах и обновления всех соответствующих компьютеров на борту.

Удаленный доступ

Необходимо разработать политику и процедуры для контроля удаленного доступа к бортовым ИТ- и ОТ -системам. Необходимо четко определить, у кого есть разрешение на доступ, когда они могут получить доступ и к чему они могут получить доступ. Любые процедуры удаленного доступа должны предусматривать тесную координацию с капитаном судна и другим ключевым старшим персоналом судна.

Все случаи удаленного доступа должны регистрироваться для проверки в случае сбоев в работе ИТ- или ОТ -систем. Системы, требующие удаленного доступа, должны быть четко определены, периодически контролироваться и пересматриваться.

Использование прав администратора

Доступ к информации должен быть разрешен только соответствующему уполномоченному персоналу.

Права администратора обеспечивают полный доступ к настройкам конфигурации системы и всем данным. Пользователи, входящие в систему с правами администратора, могут облегчить использование существующих уязвимостей. Права администратора должны предоставляться только соответствующим образом обученному персоналу, которому в рамках его роли в компании или на борту необходимо входить в систему с использованием этих прав. В любом случае использование прав администратора всегда должно быть ограничено функциями, требующими такого доступа.

Права пользователя должны быть отозваны, если он больше не находится на борту. Учетные записи пользователей не должны передаваться от одного пользователя к другому с использованием общих имен пользователей. Аналогичные правила должны применяться к любому береговому персоналу, имеющему удаленный доступ к системам на судах, когда они меняют свои роли и больше не нуждаются в доступе.

В бизнес-среде, например в судоходстве, доступ к бортовым системам предоставляется различным участникам. Поставщики и подрядчики представляют собой риск, поскольку они часто обладают как глубокими знаниями о работе судна, так и полным доступом к системам.

Многофакторная аутентификация (MFA) и пароли

Для защиты доступа к конфиденциальным данным и критически важным системам следует разработать надёжную политику паролей в сочетании с многофакторной аутентификацией. Многофакторную аутентификацию следует использовать как можно шире, то есть на всех соответствующих уровнях. Чтобы снизить вероятность атаки методом перебора, пароли должны быть надёжными и могут генерироваться как пользователем, так и системой. Политика компании должна учитывать тот факт, что слишком сложные пароли, которые приходится часто менять, могут быть записаны на листке бумаги и храниться рядом с компьютером. Пароли следует дополнять использованием многофакторной аутентификации, которая основана на том, что у вас есть, например, токене или устройстве, и на том, что вы знаете, например, пароле, и на том, чем вы являетесь, например, отпечатке пальца на телефоне.

При использовании многофакторной аутентификации риск компрометации пароля снижается, поскольку токен или устройство не будут находиться во владении злоумышленника, которому удастся получить пароль.

ИНЦИДЕНТ:

главный сервер приложений заражен программой-вымогателем

Заражение главного сервера приложений судна программой-вымогателем привело к полному сбою в работе ИТ -инфраструктуры. Программа-вымогатель зашифровала все важные файлы на сервере, в результате чего конфиденциальные данные были потеряны,

а приложения, необходимые для административных операций судна, оказались непригодными для использования. Инцидент повторялся даже после полного восстановления сервера приложений.

Основной причиной заражения была неправильная политика паролей, которая позволила злоумышленникам успешно взломать службы удаленного управления. ИТ-отдел компании отключил незарегистрированного пользователя и ввёл политику надёжных паролей в системах судна, чтобы устранить последствия инцидента.

Контроль физических и съёмных носителей

При передаче данных из неконтролируемых систем в контролируемые системы существует риск заражения вредоносным ПО.

Съёмные носители могут использоваться для обхода уровней защиты и атак на системы, которые в противном случае не подключены к интернету. Важна чёткая политика использования таких устройств хранения данных. Она должна гарантировать, что устройства хранения данных обычно не используются для передачи информации между неконтролируемыми и контролируемыми системами.

Однако бывают ситуации, когда использование таких устройств хранения данных неизбежно, например, при обслуживании программного обеспечения. В таких случаях должна быть предусмотрена процедура проверки съёмных носителей на наличие вредоносного ПО и/или проверки легитимности программного обеспечения с помощью цифровых подписей и водяных знаков.

Правила и процедуры, касающиеся использования съёмных носителей, должны включать требование о сканировании любого съёмного носителя на компьютере, который не подключён к контролируемым сетям судна. Если сканирование съёмного носителя на борту, например, ноутбука специалиста по техническому обслуживанию, невозможно, то сканирование может быть выполнено до посадки на судно. Компаниям следует рассмотреть возможность уведомления портов и терминалов о требовании сканирования съёмных носителей перед загрузкой файлов в систему судна. Такое сканирование должно выполняться при передаче файлов, например:

- грузовые документы и планы погрузки, например, файлы BAPLIE для контейнеровозов
- национальные, таможенные и портовые формы
- формы для бункеровки и смазочных масел

- судовые запасы и список провизии
- файлы для обновления программного обеспечения
- файлы для технического обслуживания.

Этот список содержит примеры и не является исчерпывающим. По возможности файлы и формы должны передаваться в электронном виде или загружаться напрямую из надёжного источника без использования съёмных носителей.

Утилизация оборудования, включая уничтожение данных

Устаревшее оборудование может содержать коммерчески важные или конфиденциальные данные. Прежде чем выбрасывать оборудование, компания должна разработать процедуру, которая обеспечит
надлежащее уничтожение данных, хранящихся в устаревшем оборудовании, и невозможность их восстановления, например, с помощью дегауссирующего устройства в соответствии с инструкциями производителя.

8. Разработка мер по обнаружению

8.1 Обнаружение, блокировка и оповещения

Обнаружение вторжений и заражений является важнейшей частью управления киберрисками. Необходимо установить и контролировать базовые параметры работы сети и ожидаемые потоки данных для пользователей и систем, чтобы можно было установить пороговые значения оповещений о киберинцидентах.

Ключевым моментом здесь будет определение ролей и обязанностей по обнаружению, чтобы обеспечить подотчётность.

Кроме того, компания может внедрить систему обнаружения вторжений (IDS) или Система предотвращения вторжений (IPS) в сеть или как часть брандмауэра. Некоторые из их основных функций включают выявление угроз/вредоносных действий и кода, а затем ведение журнала, составление отчётов и попытки заблокировать действия. Более подробную информацию о IDS и IPS можно найти в Приложении 3 к этим рекомендациям. Соответствующий персонал на борту должен уметь понимать оповещения и их последствия. Информация об обнаруженных инцидентах должна быть направлена лицу или поставщику услуг, которые отвечают за реагирование на такого рода оповещения.

8.2 Обнаружение вредоносного ПО

Программное обеспечение для сканирования, способное автоматически обнаруживать и устранять вредоносные программы в системах на борту, должно быть обновлено и управляться.

В целом, компьютеры на борту должны быть защищены на том же уровне, что и офисные компьютеры на берегу. На всех персональных и рабочих компьютерах на борту должны быть установлены, поддерживаться и обновляться антивирусные программы и программы для защиты от вредоносного ПО. Это снизит риск того, что эти компьютеры станут векторами атак на серверы и другие компьютеры в сети судна.

При принятии решения о том, стоит ли полагаться на эти методы защиты, необходимо учитывать, как часто будет обновляться программное обеспечение для сканирования.

9 Разработка планов на случай непредвиденных обстоятельств

Необходимо разработать план реагирования на соответствующие непредвиденные обстоятельства, и все планы должны храниться в печатном виде на случай полной потери к ним электронного доступа. При разработке планов действий в чрезвычайных ситуациях для реализации на борту судов важно понимать значимость любого киберинцидента с точки зрения безопасности и соответствующим образом расставлять приоритеты в действиях по реагированию. Это можно сделать только совместно с командой берегового персонала.

Любой киберинцидент следует оценивать с точки зрения его влияния на операции, активы и т. д. В большинстве случаев, за исключением систем планирования и управления загрузкой, потеря ИТ-систем на борту, в том числе утечка конфиденциальной информации, является проблемой непрерывности бизнес-процессов и, как правило, не оказывает немедленного существенного влияния на безопасную эксплуатацию судна. В случае киберинцидента, затрагивающего только ИТ-системы, приоритетной задачей может быть уведомление уполномоченных лиц в компании-судовладельце или эксплуатирующей компании для немедленного реагирования и незамедлительного выполнения плана расследования и восстановления. Этот назначенный персонал должен быть доступен капитану в случае такого инцидента.

Потеря систем ОТ может оказать значительное и немедленное влияние на безопасную эксплуатацию судна.

Если в результате киберинцидента системы ОТ будут потеряны или выйдут из строя, необходимо будет принять эффективные меры для обеспечения немедленной безопасности экипажа, судна, груза и защиты морской среды. В целом, соответствующие планы действий в чрезвычайных ситуациях, связанных с киберинцидентами, в том числе с потерей критически важных систем и необходимостью использования альтернативных режимов работы, должны быть включены в соответствующие оперативные и аварийные процедуры, предусмотренные в СУБ. В идеале некоторые из существующих процедур, предусмотренных в СУБ судна, уже будут охватывать такие киберинциденты. Однако киберинциденты могут привести к множественным сбоям, в результате которых одновременно отключится несколько систем. При планировании действий в чрезвычайных ситуациях следует учитывать такие инциденты.

Ниже приведён примерный неполный список киберинцидентов, которые должны быть учтены в планах действий в чрезвычайных ситуациях на борту.

Возможно, большинство из этих инцидентов уже учтены в процедурах компании по действиям в чрезвычайных ситуациях на борту в соответствии с главой 8 Кодекса ISM (готовность к чрезвычайным ситуациям).

- потеря работоспособности электронного навигационного оборудования или потеря целостности данных, связанных с навигацией

- потеря работоспособности или целостности внешних источников данных, включая, помимо прочего, GNSS
- потеря связи с берегом, в том числе, но не ограничиваясь этим, отсутствие связи по Глобальной системе связи при бедствии и для обеспечения безопасности на море (GMDSS)
- потеря работоспособности промышленных систем управления, в том числе двигательных, вспомогательных и других критически важных систем, а также потеря целостности управления данными и контроля
- заражение вирусом-вымогателем или отказ в обслуживании.

Кроме того, важно обеспечить, чтобы потеря оборудования или достоверной информации из-за кибер-инцидента не сделала существующие планы и процедуры реагирования на чрезвычайные ситуации неэффективными. Планы реагирования на чрезвычайные ситуации и связанная с ними информация должны включать средства связи и управление эскалацией, чтобы обеспечить доступ к необходимой береговой поддержке, и должны быть доступны в неэлектронной форме, поскольку некоторые виды кибер-инцидентов могут включать удаление данных и отключение каналов связи.

Планы действий в чрезвычайных ситуациях должны быть тщательно разработаны, а простой и назначенный персонал на берегу должен быть интегрирован с судном на случай киберинцидента. Капитан и назначенные офицеры должны быть ознакомлены с этим планом для проведения тренировок и периодического ознакомления с ним.

Отключение ОТ от берегового сетевого подключения

Соединения между береговыми и техническими системами могут быть актуальны в широком спектре применений, таких как мониторинг производительности, профилактическое техническое обслуживание и удаленная поддержка, и это лишь некоторые из них.

Общим для этих систем является то, что они не являются строго необходимыми для безопасной эксплуатации судна.

Однако они представляют собой потенциальный вектор атаки на системы, которые необходимы для безопасной эксплуатации судна. Поэтому важно оценить, когда эти подключения разрешены и при каких обстоятельствах. Необходимо разработать планы, определяющие, когда такие ОТ-системы следует временно отключать от берегового сетевого подключения для обеспечения безопасной работы судна. Отключение поможет предотвратить возможность злоумышленника манипулировать критически важными системами или получить прямой контроль над системой. Отключение также может быть выполнено для предотвращения распространения вредоносного ПО между сегментами сети.

Для эффективного отключения береговых подключений важно, чтобы сеть и службы подключения были спроектированы таким образом, чтобы сети можно было быстро физически изолировать, отсоединив один сетевой кабель (например, окрашенный в необычный цвет) или отключив брандмауэр. Эту схему и процедуру ответственный береговой персонал должен предоставить капитану.

Также следует провести обучение, чтобы помочь капитану и офицерам разобраться в киберугрозах. Экипаж также должен быть обучен управлению судном в случае отключения ОТ. Эти воздействия должны быть заранее известны, протестированы, а процедуры разработаны для каждого судна.

10. Реагирование на инциденты, связанные с кибербезопасностью, и восстановление после них

10.1 Эффективное реагирование

Отправной точкой для эффективного реагирования является план реагирования, охватывающий соответствующие непредвиденные обстоятельства.

Однако маловероятно, что планы реагирования в конечном итоге будут соответствовать сценарию киберинцидента по мере его развития. Вот почему важно регулярно отрабатывать план реагирования и разрабатывать непредвиденные обстоятельства в соответствии с полученными знаниями об угрозах, уязвимостях и последствиях. Для большинства судов планы действий в чрезвычайных ситуациях уже предусмотрены в соответствии с требованиями Кодекса ISM 1.4.5.

Для устранения последствий киберинцидентов потребуется активное реагирование, чтобы вернуть судно в рабочее состояние. Если, например, ECDIS заражена вредоносным ПО, запуск резервной ECDIS может привести к другому киберинциденту.

Поэтому рекомендуется составить и отрепетировать план реагирования на инциденты с подробным описанием ролей и обязанностей, каналов связи и основных действий.

В некоторых случаях реагирование на киберинцидент может выходить за рамки компетенции сотрудников на борту или в головном офисе из-за сложности или серьёзности таких инцидентов. В таких случаях следует обращаться за помощью к внешним экспертам, которые помогут с выполнением различных функций, таких как сетевая активность, аномальное поведение подключённых устройств или обнаружение незарегистрированных устройств, несанкционированный или несогласованный доступ поставщиков к критически важным системам, а также с реагированием и восстановлением (например, с криминалистическим анализом и очисткой после инцидента).

По возможности следует использовать информацию о ранее выявленных киберинцидентах (как в собственном флоте, так и в других флотах) для улучшения планов реагирования на все инциденты на всех судах компании, а также для разработки информационной стратегии реагирования на такие инциденты.

10.2 Четыре этапа реагирования на инциденты

По определению NIST, существует четыре ключевых этапа реагирования на инциденты:

1. Подготовка
2. Обнаружение и анализ
3. Локализация и устранение
4. Восстановление после инцидента.

Этап 1, подготовка:

В соответствии с предыдущими рекомендациями в этом руководстве:
- определите критически важные компоненты на судне, их приоритетность и расположение
- обеспечьте регулярное резервное копирование всех соответствующих данных
- определите единые точки отказа и при необходимости определите обходные пути
- составьте план реагирования на инцидент и регулярно его отрабатывайте План должен включать в себя роли и обязанности экипажа и персонала на берегу, а также рекомендации по чёткой коммуникации. Вплане также должны быть подробно описаны процессы восстановления критически важных сетей и данных, если это необходимо.

Этап 2. Обнаружение и анализ:

Чтобы обеспечить надлежащее реагирование, группа реагирования должна по возможности выяснить:
- как произошёл инцидент
- какие ИТ- и/или ОТ-системы были затронуты и каким образом
- в какой степени затронуты коммерческие и/или операционные данные
- в какой степени сохраняется угроза для ИТ- и ОТ-систем.

Этап 3. Локализация и устранение:

Локализация вспышки инцидента — критически важная задача, требующая времени. По возможности удалите устройство из сети. Если это невозможно, то важно изолировать устройство от его VLAN или локальной сети и убедиться, что между сетями действует пограничный контроль.

Кроме того, - проверьте, не изменились ли правила брандмауэра. Опытный злоумышленник может открыть сетевые порты. Если системы подключены к интернету / VSAT, отключите порты управления удалённым доступом.

- Убедитесь, что антивирусные и антишпионские программы обновлены до последней версии.
- Сделайте полный образ диска всех затронутых систем. Храните его в надежном месте в соответствии с цепочкой хранения для проведения криминалистической экспертизы на берегу. Процесс создания цепочки хранения включает в себя идентификацию, маркировку, запись, обработку, транспортировку, контроль доступа и надежное хранение образа диска.
- Рассмотрите возможность создания дампов памяти (образов оперативной памяти), так как это важно для криминалистической экспертизы. Обратите внимание,

что перезагрузка или выключение компьютера приведёт к потере энергозависимых данных, таких как оперативная память, поэтому при устранении угроз следует обратиться за советом к экспертам.

Этап 4, восстановление после инцидента:

- Восстановление систем и данных: после первоначальной оценки последствий киберинцидента ИТ-системы и ОТ-системы и данные должны быть очищены, восстановлены и, насколько это возможно, приведены в рабочее состояние путём устранения угроз из системы и восстановления программного обеспечения. Содержание плана восстановления описано в разделе 10.3.

- Расследование инцидента: чтобы понять причины и последствия киберинцидента, компания должна провести расследование, при необходимости с привлечением внешнего эксперта. Информация, полученная в результате расследования, сыграет важную роль в предотвращении возможного повторения инцидента. Расследование киберинцидентов описано в разделе 10.5.
- Предотвратить повторное возникновение: учитывая результаты упомянутого выше расследования, следует рассмотреть возможность принятия мер по устранению любых недостатков в технических и/или процедурных мерах защиты в соответствии с процедурами компании по реализации корректирующих мер.

Если киберинцидент является сложным, например, если ИТ- и/или ОТ-системы не могут быть возвращены к нормальной работе, может потребоваться инициировать план восстановления наряду с планами действий в чрезвычайных ситуациях на борту.

В этом случае группа реагирования должна быть в состоянии предоставить рекомендации по:

- следует ли отключать или продолжать использовать ИТ- или ОТ-системы для защиты данных
- следует ли отключать определенные каналы связи судна с берегом и каковы могут быть последствия таких действий
- надлежащее использование любых инструментов восстановления, предусмотренных предустановленным программным обеспечением безопасности

- степень, в которой инцидент повлиял на ИТ- или ОТ-системы, выходя за рамки возможностей существующих планов восстановления. Как объясняется в разделе 7.3, обучение и повышение осведомлённости являются ключевыми вспомогательными элементами эффективного подхода к управлению киберрисками. Поэтому важно, чтобы соответствующий персонал на борту судна и на берегу регулярно проводил учения по кибербезопасности.

10.3 План восстановления

Планы восстановления в печатном виде на борту и на берегу должны быть доступны персоналу, отвечающему за кибербезопасность и оказывающему помощь при киберинцидентах. Цель плана — обеспечить восстановление систем и данных, необходимых для возвращения ИТ- и ОТ-систем в рабочее состояние.

Чтобы обеспечить безопасность персонала на борту, в плане следует уделить приоритетное внимание эксплуатации и навигации судна. Детализация и сложность плана восстановления будут зависеть от типа судна и установленных на нем информационных, технических и других систем.

Группа реагирования на инциденты должна тщательно взвесить последствия действий по восстановлению (таких как очистка дисков), которые могут привести к уничтожению доказательств, которые могли бы предоставить ценную информацию о причинах инцидента.

Там, где это уместно, следует заручиться профессиональной поддержкой в реагировании на киберинциденты, чтобы помочь сохранить доказательства и одновременно восстановить работоспособность.

Как объясняется в разделе 7.2, возможность восстановления данных является ценной мерой технической защиты.

Возможности восстановления данных обычно реализуются в виде программного резервного копирования ИТ-данных. Наличие программного резервного копирования на борту или на берегу должно обеспечивать восстановление ИТ-систем до рабочего состояния после киберинцидента. Поскольку программы-вымогатели и черви исторически распространялись и на резервные устройства, следует также рассмотреть возможность использования автономных резервных копий.

Восстановление ОТ может быть более сложным, особенно если нет доступных резервных систем, и может потребоваться помощь с берега. Информация о том, где и кем может быть оказана такая помощь, должна быть частью плана восстановления, например, путем перехода в порт для получения помощи от сервисного инженера.

Если на борту есть квалифицированный персонал, можно выполнить более обширную диагностику и восстановление. В противном случае план восстановления будет ограничен получением быстрого доступа к технической поддержке.

Важно, чтобы компании часто тестировали свои процедуры восстановления и взаимодействие между судном и берегом при реагировании на киберинциденты.

10.4 Возможность восстановления данных

Возможность восстановления данных — это способность восстановить систему и/или данные из защищенной копии или образа, что позволяет восстановить чистую систему. Для обеспечения восстановления после киберинцидента должны быть доступны основные средства резервного копирования информации и программного обеспечения.

Необходимо установить периоды хранения и сценарии восстановления, чтобы определить, какие критически важные системы нуждаются в быстром восстановлении для снижения последствий. Системы, к которым предъявляются высокие требования к доступности данных, должны быть отказоустойчивыми. Системы ОТ, которые жизненно важны для безопасной навигации и эксплуатации судна, должны иметь резервные системы, позволяющие судну быстро и безопасно восстановить навигационные и эксплуатационные возможности после киберинцидента.

10.5 Расследование киберинцидентов

Расследование киберинцидента может предоставить ценную информацию о том, как была использована уязвимость. Компании должны по возможности расследовать киберинциденты, затрагивающие ИТ и ОТ на борту, в соответствии с внутренними процедурами. Для детального расследования может потребоваться внешняя экспертная поддержка.

Если требуется внешняя поддержка, полный образ диска, созданный на этапе локализации, может быть передан команде, проводящей расследование.

Если обеспечить надлежащее хранение вещественных доказательств, то любые полученные судебно-медицинские доказательства будут допустимы в суде, поскольку процесс их получения демонстрирует, что с доказательствами не производились манипуляции.

Информация, полученная в ходе расследования, может быть использована для улучшения технических и процессуальных мер защиты на борту и на берегу. Она также может помочь морской отрасли в целом лучше понимать морские киберриски. Любое расследование должно привести к следующим результатам:

- более глубокое понимание потенциальных киберрисков, с которыми сталкивается морская отрасль как на борту, так и на берегу;
- выявление извлечённых уроков, в том числе совершенствование обучения для повышения осведомлённости;
- обновление технических и процедурных мер защиты для предотвращения повторных инцидентов.

10.6 Ущерб, возникший в результате киберинцидента

По мере того, как риски, связанные с кибербезопасностью, становятся частью общей картины рисков, морские страховщики также сталкиваются с растущим спросом на страховые продукты и услуги, защищающие от этих рисков.

Оценка рисков и их снижение имеют первостепенное значение и являются предварительным условием для предоставления страховой защиты.

Киберинциденты могут привести к экономическим потерям или затратам на восстановление утраченных данных. Как правило, они не застрахованы, но для защиты от этого риска в настоящее время доступны автономные страховые продукты от программ-вымогателей как на морском, так и на не морском страховых рынках. Ограниченные данные о частоте, серьезности потерь или вероятности физического ущерба, а также о потенциальной возможности столкнуться с системным риском по-прежнему являются проблемой для андеррайтеров.

Успешный киберинцидент может повлечь за собой несколько последствий, связанных со страхованием: гибель людей, травмы, загрязнение окружающей среды, утрата/повреждение груза, погрузочно-разгрузочного оборудования или имущества, прерывание коммерческой деятельности, обязательства, потеря производительности, потеря данных, потеря репутации и, возможно, любой косвенный ущерб. Исследование, проведённое Lloyd’s of London, показывает, что риски, связанные с киберинцидентами, быстро развиваются и могут стать системным риском, поэтому не существует универсального подхода к мониторингу и количественной оценке этого риска. Таким образом, риски, связанные с киберинцидентами, регулярно страхуются при наличии соответствующих мер контроля, а совокупные риски и лимиты надлежащим образом отслеживаются.

Компании должны быть в состоянии продемонстрировать, что они действуют с разумной осмотрительностью в отношении управления киберрисками и защиты судна от любого ущерба, который может возникнуть в результате киберинцидента.

Покрытие ущерба имуществу

Страховые решения, покрывающие ущерб, возникающий в результате киберрисков в целом и киберинцидентов в частности, должны разрабатываться в каждой отдельной компании. Текущее положение дел можно охарактеризовать следующим образом:

- Некоторые местные страховые рынки по-прежнему выпускают необязательные рекомендации для определенных видов деятельности, исключая ущерб, связанный с киберрисками. Исторически сложилось так, что наиболее широко используемым исключением является CL380 для злонамеренных киберинцидентов (оговорка об исключении кибератак Института). Оно используется во всех морских отраслях и видах деятельности (грузовые перевозки, энергетика, превышение убытков, корпус судна, ответственность, специализированные и военные перевозки). Другим широко используемым исключением является оговорка об исключении кибератак Американского института (1/06/2015).
- Другие рыночные решения могут либо прямо страховать риск, либо — во всех полисах страхования рисков — не исключать риск и предоставлять «молчаливое покрытие» (т. е. киберриски покрываются договором без прямого упоминания). Однако следует отметить, что подход с «молчаливым покрытием» становится все более распространенным. На основе CREST, руководства по реагированию на инциденты кибербезопасности, подвергаются тщательному анализу.

- Наконец, так называемые решения «обратного выкупа» могут включать риск при определенных предварительных условиях и за дополнительную плату, согласованную сторонами. «Обратный выкуп» означает, что риск исключается из договора, но есть возможность снова включить в договор дополнительное киберстрахование при определенных условиях и за дополнительную плату.

Компаниям рекомендуется заранее уточнить у своих страховых компаний/брокеров, покрывает ли их полис убытки, вызванные киберпреступлениями и/или киберинцидентами.

Были опубликованы рекомендации для рынка, в которых морским страховым компаниям рекомендуется задавать вопросы о том, насколько компания осведомлена о киберрисках и о нетехнических процедурах. Поэтому компаниям следует ожидать запроса от страховых компаний о нетехнической информации, касающейся их подхода к управлению киберрисками.

Покрытие ответственности

Рекомендуется связаться с P&I Club для получения подробной информации о страховом покрытии, предоставляемом судовладельцам и фрахтователям в отношении ответственности перед третьими лицами (и связанных с этим расходов), возникающих в связи с эксплуатацией судов.

Инцидент, вызванный, например, неисправностью навигационных или механических систем судна в результате преступного деяния или случайного киберинцидента, сам по себе не является основанием для какого-либо исключения из обычного страхового покрытия

P&I. В случае подачи иска, связанного с киберинцидентом, истцы могут попытаться доказать, что иск был подан в результате недостаточного уровня кибербезопасности. Таким образом, это ещё раз подчёркивает важность того, чтобы компании могли продемонстрировать, что они действуют с должной осмотрительностью в отношении управления киберрисками и защиты судна.

Следует отметить, что многие убытки, которые могут возникнуть в результате киберинцидента, не являются обязательствами перед третьими лицами, возникающими в связи с эксплуатацией судна, и поэтому не покрываются страховкой P&I. Например, финансовые потери, вызванные программами-вымогателями, или затраты на восстановление зашифрованных данных не будут указаны в страховом покрытии.

Однако следует отметить, что обычное покрытие обязательств в рамках P&I не распространяется на военный риск, а киберинциденты в контексте военного или террористического риска, как правило, не покрываются.

ПРИЛОЖЕНИЕ 1 Целевые системы, оборудование и технологии

В этом приложении приводится краткое описание потенциально уязвимых систем и данных на борту судов, чтобы помочь компаниям оценить подверженность киберрискам.

Уязвимые системы, оборудование и технологии
могут включать, например,
системы связи

- интегрированные системы связи
- оборудование спутниковой связи
- оборудование передачи голоса по интернет-протоколам (VOIP)
- беспроводные сети (WLAN)
- системы громкой связи и общей сигнализации
- системы, используемые для передачи обязательной информации государственным органам.

Мостовые системы

- интегрированная навигационная система
- системы позиционирования (GPS и т. д.)
- электронная система отображения карт (ECDIS)
- системы динамического позиционирования (DP)
- системы, взаимодействующие с электронными навигационными системами и силовыми/рулевыми системами
- система автоматической идентификации (AIS)

- Глобальная морская система связи при бедствии и для обеспечения безопасности (GMDSS)
- радиолокационное оборудование
- регистраторы данных о рейсе (VDR)
- система навигационной сигнализации на мостике (BNWAS)
- системы сигнализации безопасности на судне (SSAS).

Системы управления движением, механизмами и мощностью
- регулятор двигателя
- система управления мощностью
- интегрированная система управления
- система сигнализации
- система контроля за трюмной водой
- система очистки воды
- мониторинг выбросов
- мониторинг систем отопления, вентиляции и кондиционирования воздуха
- системы контроля повреждений
- другие системы мониторинга и сбора данных, например, пожарная сигнализация.

Системы контроля доступа
- системы наблюдения, такие как сеть видеонаблюдения
- электронные системы «персонала на борту».

Системы управления грузом
- Грузовой диспетчерский пункт (ГДП) и его оборудование
- бортовые погрузочные компьютеры и компьютеры, используемые для обмена информацией о погрузке и обновлениями плана погрузки
с морским терминалом и стивидорной компанией
- системы дистанционного отслеживания и измерения грузов и контейнеров
- система индикации уровня
- система дистанционного управления клапанами
- системы балластной воды
- системы мониторинга рефрижераторов
- система сигнализации о попадании воды.
Системы обслуживания и управления пассажирами и посетителями
- Система управления имуществом (PMS)
- системы управления судном (часто включающие электронные медицинские карты)
- финансовые системы
- системы доступа на борт для пассажиров/посетителей/моряков
- системы поддержки инфраструктуры, такие как система доменных имён (DNS) и системы аутентификации/
авторизации пользователей.
- системы управления инцидентами.

Сети, доступные пассажирам

- пассажирский Wi-Fi или доступ в Интернет по локальной сети (LAN), например, для бортового персонала, который может подключать свои собственные устройства
- развлекательные системы для гостей.

Системы базовой инфраструктуры

- шлюзы безопасности"

" маршрутизаторы "

- коммутаторы "
- брандмауэры
- Виртуальные частные сети (VPN)
- Виртуальные локальные сети (VLAN)
- системы предотвращения вторжений
- системы регистрации событий, связанных с безопасностью.

Административные системы и системы обеспечения жизнедеятельности экипажа

- административные системы
- доступ экипажа к Wi-Fi или локальной сети, например, когда члены экипажа могут подключать свои устройства.

ПРИЛОЖЕНИЕ 2. Управление киберрисками и система управления безопасностью

В резолюции MSC.428(98) ИМО четко указано, что утвержденная СУБП должна учитывать управление киберрисками при выполнении целей и функциональных требований Кодекса ISM.

Руководство, содержащееся в Руководстве по управлению киберрисками на море (MSC-FAL.1/Circ.3), содержит рекомендации высокого уровня относительно элементов надлежащего подхода к внедрению управления киберрисками. Руководство, приведенное в этом приложении, разработано для того, чтобы предоставить минимальный набор мер, которые всем компаниям следует рассмотреть для внедрения с целью управления киберрисками в рамках утвержденного СУБ-сообщения.

Идентификация

ПРИЛОЖЕНИЕ 3. Бортовые сети

Безопасность сети зависит от ИТ/ОТД, установленных на борту судна, и эффективности политики компании, основанной на результатах оценки рисков. Управление точками входа и физической сетью на существующем судне может быть ограничено, поскольку при строительстве судна не было учтено управление киберрисками. Рекомендуется планировать расположение сети и управление сетью для всех новых судов.

Прямая связь между неконтролируемой и контролируемой сетями должна быть предотвращена.

Кроме того, следует добавить несколько мер защиты:

- реализовать разделение сетей и/или управление трафиком
- управлять протоколами шифрования для обеспечения надлежащего уровня конфиденциальности и коммерческой связи
- управлять использованием сертификатов для проверки происхождения документов с цифровой подписью, программного обеспечения или услуг.

В целом, только оборудование или системы, которым необходимо взаимодействовать друг с другом по сети, должны иметь такую возможность. Основным принципом должно быть то, что объединение оборудования или систем в сеть определяется эксплуатационными потребностями.

Физическая компоновка

Необходимо тщательно продумать физическую структуру сети.

Важно учитывать физическое расположение основных сетевых устройств, включая серверы, коммутаторы, брандмауэры и кабели. Это поможет ограничить доступ и обеспечить физическую безопасность при установке сети и контроле точек входа в сеть.

Управление сетью

Любая сетевая структура должна включать инфраструктуру для администрирования и управления сетью. Это может включать установку программного обеспечения для управления сетью на выделенных рабочих станциях и серверах, обеспечивающих общий доступ к файлам, электронную почту и другие сетевые сервисы.

Сегментация сети

Бортовые сети, как правило, должны выполнять следующие основные функции (нередко сети еще более разделены):

- необходимая связь между оборудованием ОТ, а также настройка и мониторинг оборудования ОТ
- административные задачи на борту, включая электронную почту и обмен файлами или папками, связанными, например, с управлением судном, грузовыми операциями, техническим управлением и т.д. (ИТ-сети)
- доступ в Интернет для отдыха экипажа и/или пассажиров/посетителей.

Эффективная сегментация сети является ключевым аспектом «многоуровневой защиты». ОТ, ИТ и общедоступные сети должны быть разделены или сегментированы с помощью соответствующих мер защиты.

При необходимости можно рассмотреть возможность дальнейшей сегментации между навигационными системами, инженерными системами и системами управления грузом. Используемые меры защиты могут включать, помимо прочего, соответствующую комбинацию следующих мер:

- межсетевой экран между бортовой сетью и Интернетом
- сетевые коммутаторы между каждым сегментом сети
- внутренние брандмауэры между каждым сегментом сети
- виртуальные локальные сети (VLAN) для размещения отдельных сегментов.

Кроме того, каждый сегмент должен иметь собственный диапазон адресов интернет-протокола (IP). Сегментация сети не отменяет необходимости в том, чтобы системы в каждом сегменте были настроены с использованием соответствующих средств контроля доступа к сети, программных брандмауэров и средств обнаружения вредоносных программ.

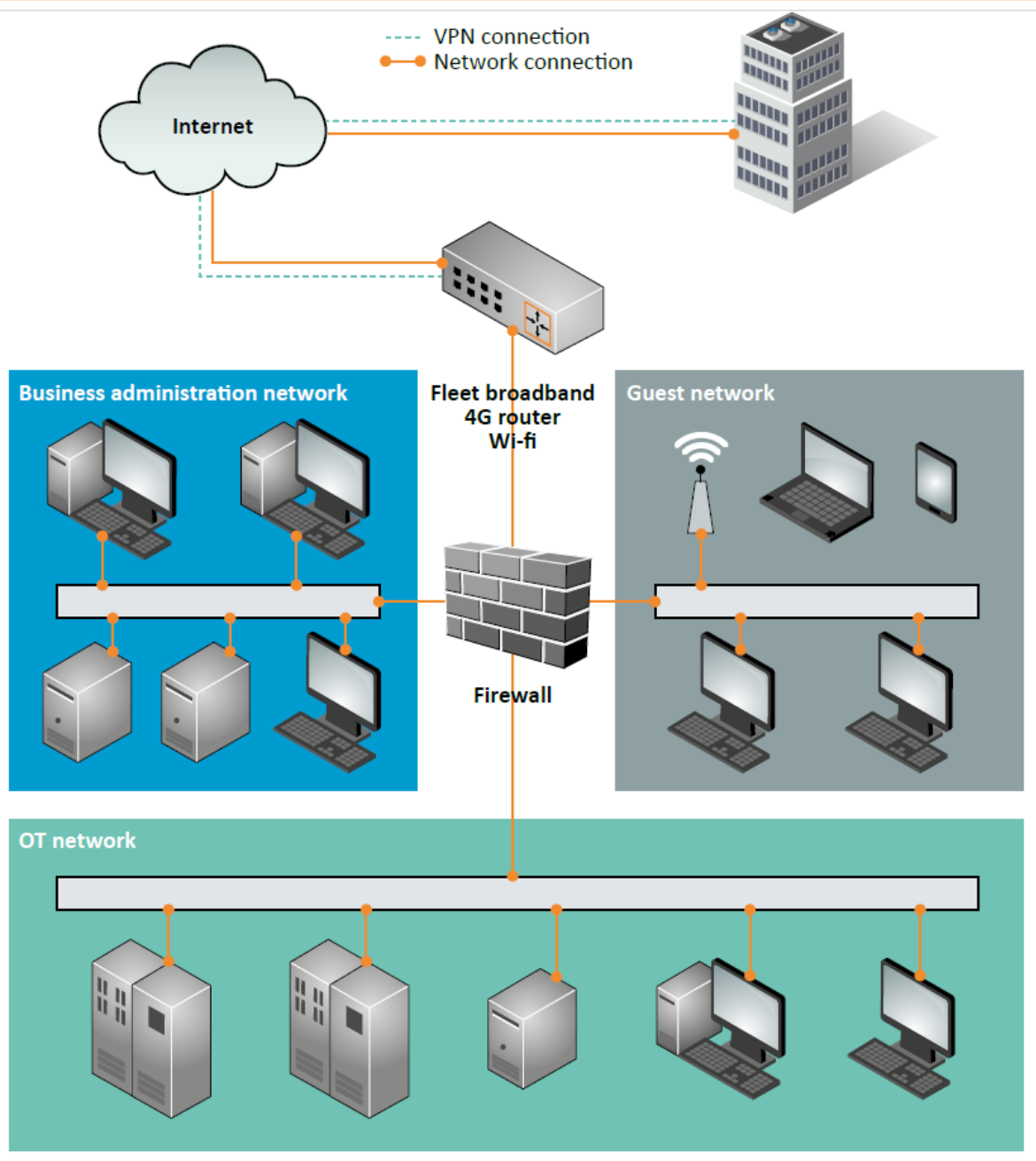

Рис. 12. Пример бортовой сети.

Интернет
Сеть бизнес-администрирования
OT-сеть
VPN-подключение
Сетевое подключение
Широкополосная гостевая сеть
Маршрутизатор 4G
Wi-Fi
Брандмауэр

В приведенном выше примере сеть сегментирована с помощью брандмауэра по периметру, который поддерживает три виртуальные локальные сети:

1. Сеть OT, содержащая оборудование и системы, выполняющие критически важные функции.
2. ИТ-сеть, содержащая оборудование и системы, выполняющие административные или бизнес-функции.
3. Сеть для экипажа и гостей, обеспечивающая неконтролируемый доступ в Интернет.

Необходимо продумать, как максимально повысить безопасность самих коммутаторов. Для достижения наивысшего уровня безопасности в каждой сети должен использоваться отдельный аппаратный коммутатор. Это сведёт к минимуму вероятность того, что злоумышленник сможет переключаться между сетями из-за неправильной настройки или получив доступ к конфигурации коммутатора.

Правильно настроенный и подходящий брандмауэр является важным элементом надлежащей сегментации сетевой установки. Бортовая установка должна быть защищена как минимум периферийным брандмауэром для контроля трафика между Интернетом и бортовой сетью. Чтобы предотвратить непреднамеренное общение, брандмауэр по умолчанию должен быть настроен на запрет всех видов общения.

На основе этой конфигурации следует внедрить правила. Правила должны быть разработаны таким образом, чтобы разрешить передачу трафика данных, необходимого для предполагаемой работы этой сети.

Например, если определенная конечная точка получает обновления из Интернета, правило должно позволять конкретной конечной точке подключаться к серверу, обслуживающему конкретную службу обновления.

Не рекомендуется включать общий доступ в Интернет к указанной конечной точке для получения обновлений.

Неконтролируемым сетям, таким как сеть экипажа или пассажиров, не следует разрешать какое-либо взаимодействие с контролируемыми сетями. Неконтролируемую сеть следует считать такой же небезопасной, как и Интернет, поскольку устройства, подключающиеся к ней, не управляются, их статус безопасности (антивирус, обновления и т. д.) неизвестен, а их пользователи могут действовать злонамеренно, намеренно или непреднамеренно.

Мониторинг активности данных

При мониторинге и управлении системами важно знать о состоянии сетей и выявлять любой несанкционированный трафик данных.

Ведение журнала должно быть реализовано в брандмауэре и, в идеале, во всех устройствах, подключенных к сети, чтобы в случае взлома ответственное лицо могло отследить источник и способ совершения инцидента. Это поможет защитить сеть от подобных инцидентов в будущем.

Система обнаружения вторжений (IDS) или система защиты от вторжений (IPS) может в режиме реального времени оповещать системного администратора о любых инцидентах в сетевых системах. Система IDS и IPS анализирует трафик данных, точки входа или и то, и другое, чтобы выявлять известные угрозы или отклонять трафик, который не соответствует политике безопасности. Система IPS должна соответствовать последним отраслевым рекомендациям и стандартам.

Рекомендуется разместить датчик в сегменте, выходящем в Интернет, поскольку общедоступные серверы являются видимой целью для злоумышленников. Другой датчик следует разместить за брандмауэром для мониторинга трафика между Интернетом и внутренней сетью. Датчик IDS/IPS также может быть размещён в сегменте удалённого доступа, например в виртуальной частной сети (VPN).

Меры защиты

Меры защиты должны быть реализованы таким образом, чтобы поддерживать целостность системы как при нормальной работе, так и во время кибератак. В каждой бортовой сети есть несколько конечных устройств, таких как рабочие станции, серверы, маршрутизаторы, модули ввода и вывода, датчики и т. д. Конечные устройства очень важны, поскольку они контролируют работу и безопасность системы.

Один продукт, технология или решение для обеспечения безопасности не могут сами по себе обеспечить адекватную защиту системы.
Желательно использовать многоуровневую стратегию, включающую два (или более) различных перекрывающихся механизма безопасности, чтобы свести к минимуму последствия сбоя любого из механизмов (см. раздел 7.1 «Глубокая защита»).
Кроме того, эффективная стратегия глубокой защиты требует глубокого понимания возможных направлений атак на систему. Они могут включать:
- «черные ходы» и уязвимости в сетевом периметре и инструментах
- уязвимости в часто используемых протоколах
- уязвимые конечные устройства и датчики
- незащищённые базы данных.

Безопасная рабочая среда может быть создана с помощью, изолированной от сетей и компьютеров тестовой среды, которая обеспечивает дополнительную защиту от киберугроз за счёт изоляции исполняемого программного обеспечения от базовой операционной системы. Это предотвращает несанкционированный доступ к операционным системам, на которых работает программное обеспечение. «Песочница» позволяет запускать программное обеспечение в соответствии с определённым набором правил, что обеспечивает контроль над процессами и компьютерными ресурсами. Таким образом, «песочница» помогает предотвратить воздействие вредоносного, неисправного или ненадёжного программного обеспечения на остальную часть системы.

ПРИЛОЖЕНИЕ 4 Глоссарий

Контроль доступа (Access control) — это выборочное ограничение возможностей и средств связи с системой или иного взаимодействия с ней, использования системных ресурсов для обработки информации, получения сведений об информации, содержащейся в системе, или управления компонентами и функциями системы.

«Черный ход» (Back door) — это секретный метод обхода обычной аутентификации и проверки при доступе к системе. «Черный ход» иногда создается в скрытых частях самой системы или устанавливается с помощью отдельного программного обеспечения.

Использование собственных устройств (Bring your own device - BYOD) позволяет сотрудникам брать с собой на борт личные устройства (ноутбуки, планшеты и смартфоны) и использовать их для доступа к конфиденциальной информации и приложениям для работы.

Цепочка хранения (Chain of custody) — это хронологическая документация или бумажный след, в котором фиксируется последовательность хранения, контроля, передачи, анализа и утилизации вещественных или электронных доказательств.

Кибератака (Cyber attack) — это любой вид наступательных действий, нацеленных на ИТ- и ОТ-системы, компьютерные сети,

и/или персональные компьютерные устройства, а также на попытки скомпрометировать, уничтожить или получить доступ к системам и данным компании и судна.

Киберинцидент (Cyber incident) — это событие, которое фактически или потенциально приводит к неблагоприятным последствиям для

бортовой системы, сети и компьютера или для информации, которую они обрабатывают, хранят или передают,
и которое может потребовать ответных действий для смягчения последствий.
Управление киберрисками (Cyber risk management) — это процесс выявления, анализа, оценки и информирования о рисках, связанных с кибербезопасностью, а также принятия, предотвращения, передачи или снижения их до приемлемого уровня с учётом затрат и выгод от действий, предпринимаемых заинтересованными сторонами.
Киберсистема (Cyber system) — это любая комбинация объектов, оборудования, персонала, процедур и средств связи, объединённых для предоставления киберсервисов. Примерами могут служить бизнес-системы, системы управления и системы контроля доступа.
Комплексная защита (Defence in breadth) — это запланированный, систематический комплекс мероприятий, направленных на выявление, устранение и уменьшение уязвимостей, которые могут быть использованы в ИТ-системах, сетях и оборудовании на каждом этапе жизненного цикла системы,
сети или подкомпонента. На борту судов этот подход, как правило, фокусируется на проектировании сети, системной интеграции, эксплуатации и техническом обслуживании.
Комплексная защита— это подход, при котором используются уровни независимых технических и процедурных мер для защиты ИТ и других объектов на борту.
Цифровизация (Digitisation) — это преобразование аналоговой информации в цифровую.
Цифровизация — это то, как цифровой мир влияет на людей и работу.

Исполняемое программное обеспечение включает в себя инструкции для компьютера по выполнению определённых задач в соответствии с закодированными инструкциями.
Брандмауэр (Firewall) — это логическая или физическая преграда, предназначенная для предотвращения несанкционированного доступа к ИТ-инфраструктуре и информации.
Микропрограмма (Firmware) — это встроенное в электронные устройства программное обеспечение, которое обеспечивает управление, мониторинг и обработку данных в инженерных продуктах и системах. Обычно они являются автономными и не доступен для манипуляций пользователя.
Ошибка (Flaw) — это непреднамеренная функциональность в программном обеспечении.
Промышленный интернет вещей (Industrial Internet of Things - IIoT) — это применение контрольно-измерительных приборов и подключенных датчиков и других устройств в машинах и транспортных средствах в транспортной, энергетической и промышленной отраслях.
Информационные технологии (Information Technology - IT) охватывают спектр технологий для хранения и обработки данных, включая программное обеспечение, аппаратное обеспечение и коммуникационные технологии.
Система обнаружения вторжений (Intrusion Detection System - IDS) — это устройство или программное приложение, которое отслеживает действия в сети или системе на предмет вредоносных действий или нарушений политики и отправляет отчёты на станцию управления.

Система предотвращения вторжений (Intrusion Prevention System - IPS), также известная как система обнаружения и предотвращения вторжений (Intrusion Detection and Prevention Systems - IDPS), — это устройства сетевой безопасности, которые отслеживают действия в сети и/или системе на предмет вредоносных действий.

Локальная сеть (Local Area Network - LAN) — это компьютерная сеть, которая соединяет компьютеры в пределах ограниченной территории, например дома, на корабле или в офисном здании, с помощью сетевых средств.

Вредоносное ПО (Malware) — это общий термин для обозначения различных вредоносных программ, которые могут заражать компьютерные системы и влиять на их производительность.

Производитель (Manufacturer) — это организация, производящая судовое оборудование и связанное с ним программное обеспечение.

Операционные технологии (Operational technology - OT) включают аппаратное и программное обеспечение, которое непосредственно контролирует физические устройства и процессы, как правило, на борту.

Исправления (Patches) — это программное обеспечение, предназначенное для обновления программного обеспечения или вспомогательных данных с целью улучшения программного обеспечения или устранения уязвимостей в системе безопасности и других ошибок в операционных системах или приложениях.

Фишинг (Phishing) — это процесс обмана получателей с целью получения конфиденциальной информации от третьей стороны.

Принцип наименьших привилегий (Principle of least privilege) — это ограничение прав учётных записей пользователей только теми правами, которые необходимы для функционирования.

Восстановление (Recovery) — это действия после инцидента, необходимые для восстановления основных служб и операций в краткосрочной и среднесрочной перспективе и полного восстановления всех возможностей в долгосрочной перспективе.

Съёмные носители (Removable media) — это собирательный термин для всех способов хранения и передачи данных между компьютерами. Сюда входят ноутбуки, USB-накопители, компакт-диски, DVD-диски и дискеты.

Оценка рисков (Risk assessment) — это процесс сбора информации и присвоения значений рискам в качестве основы для принятия решений о приоритетах и разработки или сравнения вариантов действий.

Управление рисками (Risk management) — это процесс выявления, анализа, оценки и информирования о рисках, а также принятия, предотвращения, передачи или контроля рисков до приемлемого уровня с учётом сопутствующих затрат и выгод от любых предпринятых действий.

«Песочница» (Sandbox) — это изолированная среда, в которой программа может выполняться без влияния на базовую систему (компьютер или операционную систему) и любые другие приложения. «Песочница» часто используется при выполнении ненадёжного программного обеспечения.

Поставщик услуг (Service provider) — это компания или физическое лицо, которое предоставляет и выполняет обслуживание программного обеспечения.

Социальная инженерия (Social engineering) — это метод, используемый для получения доступа к системам путём обмана человека с целью получения конфиденциальной информации.

Белый список программного обеспечения (Software whitelisting) — это перечень программного обеспечения, которое присутствует и активно в ИТ- или ОТ-системе.

Типоскеттинг (Typosquatting), также называемый захватом URL-адреса или поддельным URL-адресом, основан на ошибках, таких как опечатки, которые допускают интернет-пользователи при вводе адреса веб-сайта в веб-браузер. Если пользователь случайно введет неверный адрес веб-сайта, он может быть перенаправлен на альтернативный и зачастую вредоносный веб-сайт.

Виртуальная локальная сеть (Virtual Local Area Network - VLAN) — это логическая группировка сетевых узлов. Виртуальная локальная сеть позволяет географически разнесённым сетевым узлам взаимодействовать так, как если бы они физически находились в одной сети.

Виртуальная частная сеть (Virtual Private Network - VPN) позволяет пользователям отправлять и получать данные через общие или общедоступные сети так, как если бы их вычислительные устройства были напрямую подключены к частной сети, тем самым используя преимущества функциональности, безопасности и политик управления частной сети.

Вирус (Virus) — это скрытый, самовоспроизводящийся фрагмент компьютерного программного обеспечения, который вредоносно заражает и управляет работой компьютерной программы или системы.

Wi-Fi (Wi-Fi) — это все виды связи на коротких расстояниях, которые используют электромагнитный спектр для отправки и/ или получения информации без проводов.