RMT consulting
+7 (914) 345-63-36, info@rmtcons.com, www.rmtcons.com
Квалификация, опыт и технологии для безопасного судоходства

Информационный бюллетень *RMT ИБ-24/20 (03.12.2020)*

Требования к обеспечению кибербезопасности в СУБ Компании

Уважаемые коллеги!

С 01.01.2021 г. вступает в силу требование ИМО о том, что киберриски должны быть учтены в СУБ судоходной компании. Соответствие этим требованиям будет проверяться при первом ежегодном освидетельствовании СУБ Компании после этой даты.

Это требование регламентировано следующими документами:

1. Резолюция ИМО MSC.428(98) от 16.06.2017 г. «Управление киберрисками в морской отрасли в рамках систем управления безопасностью».
2. Циркулярное письмо ИМО MSC-FAL.1/Circ.3 от 05.07.2017 г. «Руководство по управлению киберрисками в морской отрасли».

Требования к судам под флагом Российской Федерации регламентированы Руководством РС НД № 2-030101-040.

В отношении учета киберрисков в СУБ компании говорится следующее:

Доказательством того, что вопросы управления кибербезопасностью учтены в СУБ и находятся в управляемых условиях можно считать следующее:

1. Компанией проведена оценка рисков, связанных с кибератаками или киберинцидентами, для обеспечения бесперебойной работы своих береговых подразделений и судов в соответствии с процедурами оценки рисков установленными в СУБ.
2. Управление киберрисками начинается на уровне высшего руководства. В компании внедрена культура понимания киберрисков на всех уровнях организации для обеспечения гибкого режима устойчивости к кибератакам и киберинцидентам. Высшее руководство понимает важность оценки и управления киберрисками.
3. Компания разработала принципы защиты от кибератак и киберинцидентов, таких как отключение, взлом, внедрение вредоносных программ, блокировка компьютерных систем и т.д. на основе оценки рисков. Эти принципы могут быть представлены в виде функциональных элементов, которые должны применяться на практике, работать непрерывно и одновременно в рамках внедренной системы управления, а именно:

- Определены кадровые решения по управлению кибербезопасностью. Распределены функции и обязанности персонала по использованию и обслуживанию, установлена система доступа и правила использования.
- Определены данные и ресурсы, при сбое в работе которых возникают риски, связанные с выполнением судовых операций.

- Разработаны защитные меры, включая меры немедленного реагирования на случаи сбоев в работе компьютеризированных систем для обеспечения непрерывности выполнения морских операций.
- Разработаны и реализованы меры для своевременного обнаружения сбоев в работе компьютеризированных систем.
- Разработаны и внедрены мероприятия по восстановлению выполнения судовых операций альтернативными методами в случае сбоев в работе компьютеризированных систем.
- Определены меры по резервному копированию и восстановлению компьютеризированных систем в случае нарушения их работы.

Интеграция необходимых мер для управления кибербезопасностью в СУБ компании может быть реализована через следующие элементы СУБ:

1. Цели:

Компания должна установить, что цели интеграции системы управления кибербезопасностью соответствуют целям МКУБ, а именно обеспечению безопасности на море, предотвращению несчастных случаев или гибели людей и предотвращению нанесения вреда окружающей среде, в частности морской среде, и имуществу.

2. Политика:

Высшее руководство компании должно оценить и, в случае актуальности проблемы кибератак и киберинцидентов в рамках эксплуатации судов, признать необходимость изменения СУБ компании для внедрения процессов кибербезопасности. Политика в области управления безопасностью может быть пересмотрена с учетом проблем кибератак и киберинцидентов и необходимости принятия ответных мер. Кибербезопасность, наряду с другими вопросами управления безопасностью, должна стать предметом регулирования со стороны высшего руководства и обязательной для исполнения судовым и береговым персоналом.

3. Ответственность компании:

Главная ответственность в области кибербезопасности остается за высшим руководством. Может быть рассмотрен вопрос о назначении в компании ответственного за управление кибербезопасностью, защиту от кибератак и киберинцидентов, а также ответственного за оказание помощи капитану в выполнении судовых задач и обязанностей, связанных с применением IT и OT.

4. Соответствие требованиям:

В отношении кибербезопасности компания должна соблюдать обязательные для выполнения международные и национальные требования, а также должны быть оценены и приняты во внимание применимые кодексы, рекомендации и руководства ИМО, Морских Администраций, классификационных обществ и организаций морской индустрии. Это, в свою очередь, должно оказать помощь в формировании основы для оценки рисков и изменении СУБ компании.

5. Оценка риска:

С помощью установленных в СУБ процедур по оценке рисков должны быть определены основные риски, связанные с кибератаками и киберинцидентами, и способы защиты от негативных последствий. Если не существует эквивалентной системы, то для систематической оценки можно использовать подход, изложенный соответствующих стандартах ИСО и ГОСТ Р.

Результаты оценки рисков и меры по защите от кибератак и киберинцидентов должны быть учтены в СУБ компании. **Это могут быть процедуры, инструкции, руководства и т.д.** Все принятые изменения в СУБ должны быть проведены в соответствии с процедурами компании и доведены до сведения соответствующего берегового и судового персонала.

6. Капитан:

В СУБ должны быть определены требования к квалификации капитана в области IT и OT, чтобы он был способен выполнять возложенные на него обязанности связанные с его должностью.

7. Поддержка со стороны берегового подразделения компании:

Должна быть определена береговая структура поддержки капитана и судна в случаях необходимости:

- Реагирования на кибератаки.
- Реагирования на последствия киберинцидентов.
- Восстановления работоспособности компьютеризированных систем.

8. Ресурсы и персонал; квалификация; доступ к компьютеризированным системам:

При приеме на работу новый судовой персонал и сотрудники береговых подразделений должны ознакомиться с правилами компании в области кибербезопасности. Должны быть распределены обязанности и разработаны инструкции для всех лиц, имеющих задачи по кибербезопасности, а также для персонала, использующего судовые компьютеризированные системы каким-либо способом.

Компания должна разработать и внедрить меры по ограничению как физического, так и логического доступа к информационным ресурсам и компьютеризированным системам, а также меры по использованию съемных носителей информации и подключению других компьютеризированных систем.

В случае необходимости должны быть предусмотрены мероприятия по ознакомлению, обучению и совершенствованию навыков судового и берегового персонала на регулярной основе. СУБ может содержать план обучения и повышения квалификации, а также требования к квалификации для занятия той или иной позиции.

9. Готовность к аварийным ситуациям:

Для судов и береговых подразделений компании в СУБ должны быть предусмотрены планы действий в чрезвычайных ситуациях при возникновении кибератак и киберинцидентов. Также должны быть предусмотрены проведения учений и тренировок по вопросам действий в чрезвычайных ситуациях при возникновении кибератак и киберинцидентов;

10. Обслуживание и ремонт:

В систему технического обслуживания и ремонта судовых механизмов и устройств должны быть добавлены меры безопасности, которые должны соблюдаться при обслуживании и ремонте компьютеризированных систем. Эти меры должны быть определены на основании оценки рисков.

В СУБ должны быть установлены критерии по выбору поставщиков услуг.

11. Отчеты:

С целью совершенствования системы сообщения о кибератаках и киберинцидентах должны направляться в ответственные подразделения компании для оценки, анализа и разработки корректирующих действий в соответствии с процедурами, установленными в СУБ.

12. Проверка, анализ и оценка, осуществляемая компанией; документация:

Как правило, СУБ устанавливает применимые требования к ведению и доступности документации. При составлении документации в области кибербезопасности, возможно, необходимо будет предусмотреть ограничения в области публичного доступа к информации доступной только ограниченной группе лиц на борту и/или на берегу, например, представление прав администратора, управление паролями, резервное копирование и восстановление и т.д.

Интегрированная в СУБ компании Система управления кибербезопасностью, ее функционирование и эффективность должны периодически проверяться и оцениваться компанией в соответствии с требованиями, установленными МКУБ.

Управление кибербезопасностью является постоянно изменяющимся процессом, который может претерпевать изменения в зависимости от внешних обстоятельств, поэтому одноразовая установка процедур управления кибербезопасностью и внедрение защитных средств не могут рассматриваться как достаточные. Компания должна учитывать постоянные изменения и выявленные недостатки в собственной системе и обеспечивать обновление оценки рисков и СУБ, инициируя тем самым непрерывный процесс улучшения.

Требования некоторых администраций «удобных» флагов:

Флаг	Нормативный документ	Примечания
Антигуа и Барбуда	CIRCULAR 2020-005	Стандартные требования ИМО
Багамские острова	MARINE NOTICE 95	Стандартные требования ИМО
Белиз	---	---
Кипр	Circular No. 04/2020	Стандартные требования ИМО
Либерия	Marine security advisory 02/2019	Стандартные требования ИМО
Мальта	Technical Notice SLS.34	Стандартные требования ИМО. В форме рекомендации
Маршалловы острова	MN-2-011-13 Sep/2020, No. 2-11-16 Rev. Oct/2020	Стандартные требования ИМО
Монголия	---	---
Панама	Merchant Marine Circular MMC-354	Стандартные требования ИМО. Процедуры управления киберрисками рекомендуется внедрять в качестве дополнения к существующим требованиям по управлению рисками безопасности согласно МКУБ и МК ОСПС.
Сьерра Леоне	---	---
Того	Circular no. 0049C/TG/11/20	Стандартные требования ИМО

Комментарии и рекомендации

1. Соответствие СУБ Компании требованиям ИМО в отношении учета киберрисков будет проверяться инспектором КО при первом ежегодном освидетельствовании СУБ Компании.

При этом соответствующие процедуры уже должны быть включены в СУБ и иметь определенную «обкатку» на практике.

Рекомендуем внести соответствующие положения в СУБ заблаговременно, но, в любом случае, не позднее 3 месяцев до даты планируемого освидетельствования. Кроме того, если промежуточное освидетельствование СУБ судна Компании выпадает на более раннее время, чем ежегодное освидетельствование СУБ Компании, то рекомендуем учитывать именно эту дату для начала заблаговременного внедрения в практику новой процедуры СУБ.

2. Приверженность Компании обеспечению кибербезопасности должна быть подтверждена Политикой в области кибербезопасности.

Эта Политика может быть представлена в виде отдельного документа, или интегрирована в существующую Политику безопасности (согласно МКУБ).

Рекомендуем оформить Политику обеспечения кибербезопасности отдельным документом, и, при желании, сделать краткое упоминание о соответствующей цели в Политики безопасности. Внесение изменений в Политику безопасности предполагает регистрацию ее новой версии и последующее информирование КО при освидетельствовании СУБ Компании и / или судна.

3. Требования к обеспечению кибербезопасности затрагивают все аспекты деятельности Компании и эксплуатации судна. Поэтому киберриски должны быть учтены путем эффективной интеграции требований во все соответствующие процедуры СУБ.

Рекомендуем оформлять процедуру обеспечения кибербезопасности в СУБ не только в виде отдельно разработанной процедуры, но и внесением изменений и ссылок во все соответствующие процедуры СУБ. Такими процедурами, например, являются: техническое обслуживание и ремонт; снабжение судов; подбор и подготовка персонала; выбор подрядчика и другие.

4. Включение развернутой и подробной процедуры в СУБ увеличивает вероятность последующего внесения изменений, а, соответственно, и их последующего согласования с РС.

Рекомендуем включать в процедуры СУБ только самые основные положения, а более подробные сведения и инструкции выносить в отдельные руководства и планы, на которые давать ссылки в тексе процедуры.

5. Процедура оценки киберрисков, несмотря на определенную схожесть с процедурой оценки эксплуатационных рисков (которая уже есть в СУБ), имеет и принципиальные отличия. Например, такие, что киберпреступник целенаправленно проводит кибератаку с целью причинения вреда. В то время как, эксплуатационные риски в большинстве случаев возникают непреднамеренно, при определенном негативном стечении обстоятельств. Кроме того, вероятность киберриска, в отличие от вероятности эксплуатационного риска, не может традиционно основываться на статистике прошлых инцидентов. Поскольку статистика киберрисков в настоящее время еще очень скудна. Поэтому для определения вероятности киберриска необходимо учитывать такие факторы как актив кибербезопасности, источник киберугрозы и оценка киберуязвимости.

Рекомендуем разработать процедуру управления киберрисками с учетом соответствующих стандартов ИСО и/или ГОСТ Р, при этом она должна коррелировать с существующей в Компании процедурой управления (эксплуатационных) рисков, или, как минимум, ей не противоречить.