

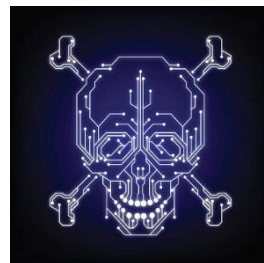
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

№ ИБ 2017-064 от 25.07.2017

Куда: Ваша судоводная компания

Кому: Руководителю и специалистам Вашей судоводной компании

Тема: Информационная безопасность судов
Cyber Security onboard Ships



Уважаемый клиент компании ИБИКОН!

С целью повышения информационной защиты на судах Вашему вниманию предлагается информация по новым требованиям к информационной защите.

Защита информации (Information Security) - сохранение конфиденциальности, целостности и доступности информации.

Существует 3 (три) базовых принципа, которые должна обеспечивать информационная защита:

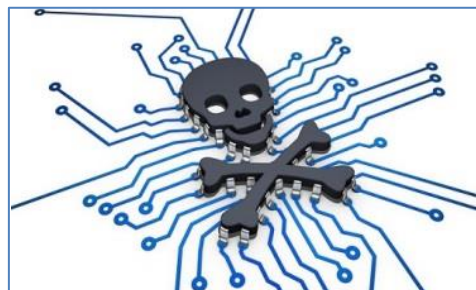
- целостность данных — защита от сбоев, ведущих к потере информации, а также защита от неавторизованного создания или уничтожения данных;
- конфиденциальность информации;
- доступность информации для всех авторизованных пользователей.

Защита информации, задача комплексная, направленная на обеспечение безопасности, реализуемая внедрением системы защиты информации. Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач. Кроме того, проблемы информационной защиты постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем.

При разработке компьютерных систем, выход из строя или ошибки в работе которых, могут привести к тяжелым последствиям, вопросы компьютерной безопасности становятся первоочередными. На сегодняшний день во всем судоводном секторе информационная защита сети становится почти такой же важной, как обеспечение безопасности и охраны на судах.

Примеры рисков, относящихся к информационной защите, включают:

- риски утечки или искажения информации;
- риски отключения электропитания;
- риски кражи или разлива грузов;
- риски изменения курсов судов.



Планы и процедуры судоводной компании по управлению рисками информационной защиты должны быть согласованы с существующими процедурами по управлению рисками, регламентированными кодексами МКУБ и ОСПС.

Дополнительную информацию Вы можете получить, посетив наш сайт www.IBIcon.ru или направив Ваше письмо на наш электронный адрес info@ibicon.ru или связаться с нашим специалистом по телефону: +7 (812) 716 88 56, +7 (812) 716 31 36, +7 (812) 407 10 56 или скайпу: [IbiconSpb](#)

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

№ ИБ 2017-064 от 25.07.2017

Ниже представлен рисунок, показывающий состав функциональных элементов системы информационной защиты:



Данные функциональные элементы должны быть включены в общую систему управления рисками. Они отражают необходимые мероприятия и желаемые результаты эффективного управления информационными рисками в отношении критических систем, задействованных в морских операциях.

Система информационной защиты должна быть задействована на всех уровнях компании от руководства на берегу и до членов экипажа, и интегрирована с системами безопасности и охраны с целью обеспечения эффективности судовых операций.

Дополнительную информацию Вы можете получить, посетив наш сайт www.IBIcon.ru или направив Ваше письмо на наш электронный адрес info@ibicon.ru или связаться с нашим специалистом по телефону: +7 (812) 716 88 56, +7 (812) 716 31 36, +7 (812) 407 10 56 или скайпу: [IbiconSpb](https://www.skype.com/partners/ibicon)

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

№ ИБ 2017-064 от 25.07.2017

Данные являются источником жизненной силы любой организации. Судоходство не сможет функционировать, если данные будут удалены из соответствующих приложений.

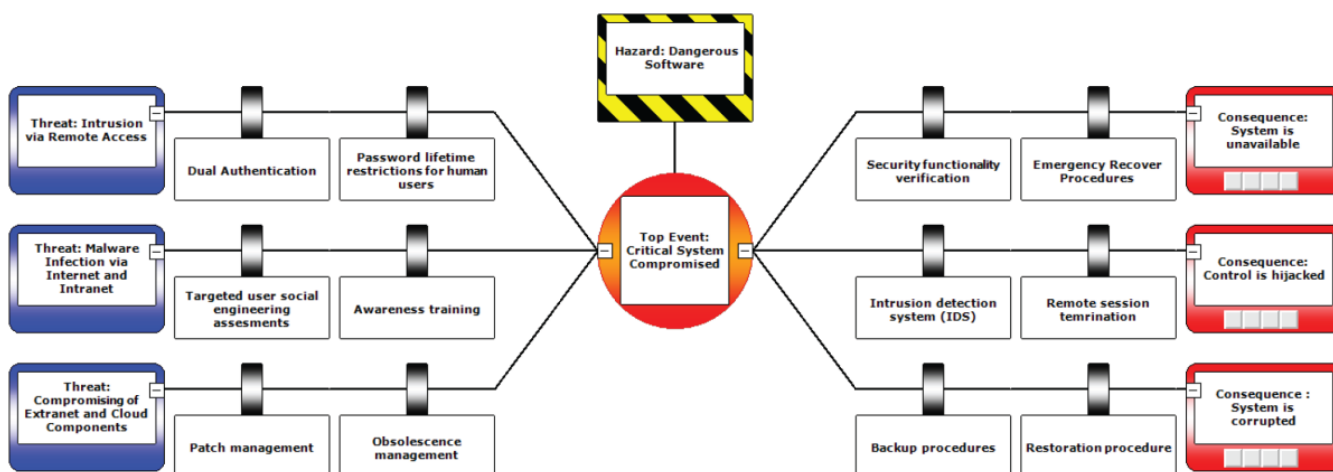
Тем не менее, многие судоходные компании пытаются правильно управлять своими данными, и не знают, какие данные они хранят и действительно ли они необходимы или их уровень качества. Компании должны установить ответственность персонала за хранение и получение данных, которые могут стать основой для принятия управленческих или эксплуатационных решений.

Следующие судовые системы могут быть уязвимы:

- Системы навигационного мостика;
- Грузовые системы;
- Системы движения и энергетического менеджмента;
- Системы управления доступом на судно;
- Системы обслуживания пассажиров;
- Сети общего пользования;
- Системы социального обеспечения экипажа;
- Системы радиосвязи и коммуникации.



Балтийский и Международный Морской Совет (BIMCO - Baltic and International Maritime Council) разработал "Руководство по информационной защите на судах" (The Guidelines on Cyber Security onboard Ships).



В рамках Системы управления безопасностью (СУБ) наша компания предлагает Вам разработку соответствующих планов и судовых процедур по информационной защите на судах (**Cyber Security Management Plan**).

Дополнительную информацию Вы можете получить, посетив наш сайт www.IBIcon.ru или направив Ваше письмо на наш электронный адрес info@ibicon.ru или связаться с нашим специалистом по телефону: +7 (812) 716 88 56, +7 (812) 716 31 36, +7 (812) 407 10 56 или скайпу: *IbiconSpb*