



Назначение:

Мультимедийный обучающий модуль (МОМ) предназначен для проведения подготовки по программе «Ознакомительная подготовка по кибербезопасности для членов экипажей морских судов» (Maritime Cyber Security Awareness).

Растущая техническая сложность судов и использование ими услуг, предоставляемых через Интернет, делают судовые системы все более уязвимыми перед кибератаками.

Международная морская организация (ИМО) разработала руководящие принципы, которые предоставляют рекомендации по управлению рисками для защиты от текущих и возникающих угроз кибербезопасности (IMO MSC-FAL.1/Circ.3, 05.07.2017., «GUIDELINES ON MARITIME CYBER RISK MANAGEMENT»).

Кибер-риски должны надлежащим образом учитываться в системах управления безопасностью (СУБ) Компании не позднее первой ежегодной проверки документа о соответствии МКУБ после 1 января 2021 года.

Судовой экипаж играет важную роль в защите судовых информационных систем и оборудования, поэтому обучение и повышение осведомленности являются ключевым элементом эффективного подхода к кибербезопасности.

Что такое мультимедийный обучающий модуль?

МОМ представлен в виде электронного учебника. Размещенный в нем теоретический материал сопровождается рисунками и схемами. Для самостоятельной проверки знаний в МОМ включены разделы тестирования. МОМ может быть установлен на одном компьютере или по сетевой лицензии на всех компьютерах, объединенных одной локальной сетью.

Содержание:

- Введение
- Общая терминология в области кибербезопасности
- Категории и типы кибератак
- Этапы кибератаки
- Кибербезопасность
- Ключевые организационные меры обеспечения кибербезопасности, которые необходимо соблюдать всем членам экипажа
- Признаки того, что компьютер скомпрометирован
- Процедуры действий в случае кибер-инцидента
- Приложение 1. Уязвимые судовые системы и оборудование

Целевая аудитория

Палубная команда –
Управление

Палубная команда –
Эксплуатация

Палубная команда –
Вспомогательный

Машинная команда–
Управление

Машинная команда–
Эксплуатация

Машинная команда–
Вспомогательный

Тип судна

Все типы



Нормативная база

- IMO MSC-FAL.1/Circ.3, 05.07.2017., «GUIDELINES ON MARITIME CYBER RISK MANAGEMENT» (Рекомендации по управлению рисками для защиты от текущих и возникающих угроз кибербезопасности).
- Кодекс ОСПС



МУЛЬТИМЕДИЙНЫЙ ОБУЧАЮЩИЙ МОДУЛЬ ОЗНАКОМИТЕЛЬНАЯ ПОДГОТОВКА ПО КИБЕРБЕЗОПАСНОСТИ ДЛЯ ЧЛЕНОВ ЭКИПАЖЕЙ МОРСКИХ СУДОВ

Тема 1. Введение.

1. ВВЕДЕНИЕ

Растущая техническая сложность судов и использование ими услуг, предоставляемых через Интернет, делают судовые системы все более уязвимыми перед рисками.

Пояснение

Приставка «Кибер» (Cyber), как правило используется, чтобы присвоить слову значение чего-то относящегося к компьютерным и цифровым технологиям.



Слайд: 01/130

МУЛЬТИМЕДИЙНЫЙ ОБУЧАЮЩИЙ МОДУЛЬ ОЗНАКОМИТЕЛЬНАЯ ПОДГОТОВКА ПО КИБЕРБЕЗОПАСНОСТИ ДЛЯ ЧЛЕНОВ ЭКИПАЖЕЙ МОРСКИХ СУДОВ

Тема 2. Общая терминология в области кибербезопасности.

- Кибербезопасность
- Кибер-инцидент
- Киберпространство
- Киберсистема
- Ключ шифрования
- Контроль доступа
- Операционная технология (OT)

- функция открытой системы, обеспечивающая технологию безопасности, которая разрешает или запрещает доступ к определенным типам данных, основанная на учетных данных субъекта, которому нужен доступ, и объекта данных, являющегося целью доступа.

Иными словами - доступ к защищенной информации должен быть ограничен, чтобы только люди, которые имеют право доступа, могли получать эту информацию.

Слайд: 02/130

МУЛЬТИМЕДИЙНЫЙ ОБУЧАЮЩИЙ МОДУЛЬ ОЗНАКОМИТЕЛЬНАЯ ПОДГОТОВКА ПО КИБЕРБЕЗОПАСНОСТИ ДЛЯ ЧЛЕНОВ ЭКИПАЖЕЙ МОРСКИХ СУДОВ

Тема 3. Категории и типы кибератак.

Направленный фишинг (spear phishing) - фишинг - атака, проводимая против конкретных субъектов, в отличие от обычной, которая проводится путем массовой рассылки писем. Целевые пользователи получают тщательно разработанные фишинговые сообщения, - заставляющие их ввести конфиденциальные персональные данные (логины и пароли), которые дают доступ к корпоративным сетям или базам данных с важной информацией. Помимо запроса учетных данных, целевые фишинговые письма могут также содержать вредоносное ПО.

Пример фишинг - атаки.

При направленном фишинге киберпреступник пытается использовать в электронном сообщении максимально возможную копию личной данных жертвы. Например, злоумышленник выйдет по таким открытым сервисам, как Facebook, и другим сетевым источникам данных, чтобы иметь возможность обращаться к получателю по имени с целью возникновения у пользователя уверенности в законности происхождения сообщения и склонению его к нажатию на фишинговую ссылку, привязанную к письму.

После нажатия на ссылку открывается фальшивая страница, на которой пользователь вводит



Слайд: 03/130

МУЛЬТИМЕДИЙНЫЙ ОБУЧАЮЩИЙ МОДУЛЬ ОЗНАКОМИТЕЛЬНАЯ ПОДГОТОВКА ПО КИБЕРБЕЗОПАСНОСТИ ДЛЯ ЧЛЕНОВ ЭКИПАЖЕЙ МОРСКИХ СУДОВ

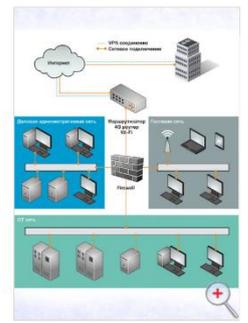
Тема 5. Кибербезопасность.

Технические меры

Используемые на судне меры защиты могут включать соответствующие комбинации следующей:

- межсетевые экраны между бортовой сетью и Интернетом;
- сетевые коммутаторы между каждым сегментом сети;
- внутренние межсетевые экраны между каждым сегментом сети;
- виртуальные локальные сети (VLAN) для размещения отдельных сегментов.

Кроме того, каждый сегмент должен иметь собственные адреса интернет-протокола (IP). Сегментация сети не устраняет необходимость применения мер безопасности в каждом сегменте с помощью соответствующих средств контроля доступа и брандмауэров.



Слайд: 05/130

МУЛЬТИМЕДИЙНЫЙ ОБУЧАЮЩИЙ МОДУЛЬ ОЗНАКОМИТЕЛЬНАЯ ПОДГОТОВКА ПО КИБЕРБЕЗОПАСНОСТИ ДЛЯ ЧЛЕНОВ ЭКИПАЖЕЙ МОРСКИХ СУДОВ

Тема 6. Ключевые организационные меры обеспечения кибербезопасности, которые необходимо соблюдать всем членам экипажа.

Меры безопасности, связанные с использованием социальных сетей:

- Будьте осторожны при использовании социальных сетей.
- Внимательно изучите и выберите параметры конфиденциальности.
- Не выкладывайте в сеть рабочие документы и не общайтесь служебными сообщениями.
- Не обсуждайте детали своей рабочей деятельности.
- Не размещайте сообщения или комментарии, которые могут считаться дискредитирующими, истинными, клеветническими или угрожающими для других.
- Будьте осторожны при загрузке приложений с сайтов социальных сетей



Слайд: 06/130

МУЛЬТИМЕДИЙНЫЙ ОБУЧАЮЩИЙ МОДУЛЬ ОЗНАКОМИТЕЛЬНАЯ ПОДГОТОВКА ПО КИБЕРБЕЗОПАСНОСТИ ДЛЯ ЧЛЕНОВ ЭКИПАЖЕЙ МОРСКИХ СУДОВ

Задачи для самопроверки



Текст вопроса:

Какими международными нормативными документами регламентируется необходимость разработки судовых планов и процедур по управлению кибер-рисками?

Выберите все правильные варианты

- ПДНВ
- МКУВ
- ОСПС
- ИАМСАР

Попыток: 1

Слайд: 07/130