МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТУ ВНУТРІШНІХ СПРАВ
Кафедра кримінального аналізу та інформаційних технологій

В. Г. ПЯДИШЕВ, Г.В. ФОРОС

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТА ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В ЗАБЕЗПЕЧЕННІ МОРСЬКОЇ БЕЗПЕКИ

Навчально-методичні рекомендації
до вивчення навчальної дисципліни

для здобувачів вищої освіти освітнього ступеня «доктор філософії»
у галузі знань 26 «Цивільна безпека»
спеціальність 262 «Правоохоронна діяльність»

2025 рік

Схвалено та рекомендовано до друку
Кафедрою кримінального аналізу та інформаційних технологій ОДУВС
(протокол № 2 від 30.01.2025 р.)

Автори:
Володимир ПЯДИШЕВ – професор кафедри кримінального аналізу та інформаційних технологій, д.ю.н., професор
Ганна ФОРОС – завідувачка кафедри кримінального аналізу та інформаційних технологій, к.ю.н., доцент

Рецензенти:
Карен ІСМАЙЛОВ – заступник начальника 5-го відділу (інформаційних технологій та програмування в південному регіоні) (м. Одеса) 3-го управління (інформаційних технологій та програмування) Департаменту кіберполіції Національної поліції України, підполковник поліції, кандидат юридичних наук, доцент
Дмитро АФОНІН – завідувач науково-дослідної лабораторії з актуальних питань кримінального аналізу ННІПФПКП НПУ, кандидат юридичних наук, доцент

Використання сучасних інформаційних та телекомунікаційних технологій в забезпеченні морської безпеки: навчально-методичні рекомендації для здобувачів вищої освіти освітнього ступеня «доктор філософії» у галузі знань 26 «Цивільна безпека» спеціальність 262 «Правоохоронна діяльність» /уклад. В. Г. Пядишев, Г.В. Форос. Одеса: ОДУВС, 2025, 42 с.

ЗМІСТ

1. ПОЯСНЮВАЛЬНА ЗАПИСКА

З давнини судноплавство є найбільш економічним засобом транспортування. Сьогодні воно також є одним із найбільш поширених засобів транспортування. Саме судноплавство є єдиною міжнародною галуззю, яка зробила можливою глобалізацію. Матеріали «Конференції ООН з торгівлі та розвитку» свідчать, що 90% світової торгівлі здійснюється саме водним транспортом. Розвиток останнього супроводжується двома основними патогенними факторами: 1) піратством і збройним пограбуванням і 2) морським тероризмом. Спосіб роботи судноплавства та темпи його зростання роблять його дуже легкою мішенню. Отже, створення безпечного середовища стає великим викликом для світової спільноти.

Доведено, що сьогодні найбільшу загрозу безпеці морського транспорту становлять кіберзагрози, оскільки кібертехнології, проникаючи в усі аспекти управління, приносять із собою вразливості до кіберзагроз, що, можуть впливати на всі аспекти управлінської діяльності від управління персоналом до управління судном. До морської безпеки у повному обсязі відноситься й кібербезпека морських портів. Отже, необхідно ознайомитися з організацією забезпечення інформаційної безпеки морського судна, зі вразливими об'єктами судна, із засобами забезпечення інформаційної безпеки судна, з концептуальною моделлю безпеки судна. Необхідно також опанувати сучасний підхід до захисту та базові принципи забезпечення інформаційного захисту судна.

Морська безпека містить багато компонентів, жоден з яких не є другорядним. Навігаційну безпеку радари для автоматичного супроводу цілей забезпечують через можливість автоматичного пошуку та супроводу цілей. Але існує проблема виявлення малих цілей, яку вирішують встановленням інфрачервоних камер. Велике значення має застосування систем автоматичної ідентифікації. Перевірка людей, що потрапляють на борт, найсучаснішими технічними засобами стає в один ряд з ідентифікацією ворожого судна. Одночасно застосування контейнерів отримало неймовірний розмах через свою зручність і важливість. Їх навчилися використовувати у своїх цілях також й злочинці. Тому вдосконалення систем сканування та відстеження контейнерів посідає окреме місце у боротьбі з піратством і тероризмом. Також важливим є безпосередній захист суден і акваторій найсучаснішими засобами.

Час не залишається на місті. Виникають і отримують своє застосування новітні технології. Наприклад, технологія блокчейн вже застосовується злочинцями, і морські правоохоронці не мають права відставати. Також застосування штучного інтелекту та машинного навчання вже працюють для підвищення якості виявлення загроз небезпек у морі. Але цим не вичерпано арсенал сучасних засобів, до яких відносяться також аналіз даних, прогнозне моделювання та квантові обчислення, що сьогодні працюють для підвищення ефективності морської безпеки.

Програму вивчення навчальної дисципліни «Використання сучасних інформаційних та телекомунікаційних технологій в забезпеченні морської

безпеки» складено відповідно до освітньо-професійної підготовки в галузі знань 26 «Цивільна безпека» та спеціальності 262 «Правоохоронна діяльність». «Використання сучасних інформаційних та телекомунікаційних технологій в забезпеченні морської безпеки» є навчальною дисципліною, що надає базові теоретичні знання та практичні навички з питань застосування сучасних інформаційних та телекомунікаційних технологій в забезпеченні морської безпеки.

Зміст навчальної дисципліни «Використання сучасних інформаційних та телекомунікаційних технологій в забезпеченні морської безпеки» охоплює теоретичні питання стосовно морської безпеки та (загальний огляд та визначення); класифікації загроз морській безпеці; загальний огляд кібербезпеки (атрибути кібербезпеки, вразливі місця та загрози, кібератаки); специфіку організації забезпечення інформаційної безпеки морського судна та кібербезпеки морських портів; базові знання про застосування технологій у навігаційній безпеці; базові знання про застосування технологій у перевірці персоналу, пасажирів та контейнерів, а також у безпосередньому захисті суден і акваторій; організацію застосування у морській безпеці найновітніших технологій: блокчейн, штучного інтелекту, машинного навчання та інтернету речей, аналізу даних, прогнозного моделювання та квантових обчислень.

Метою навчальної дисципліни «Використання сучасних інформаційних та телекомунікаційних технологій в забезпеченні морської безпеки» є формування у здобувачів вищої освіти компетентності з морської безпеки, пов’язаної з використанням інформаційних технологій, розкриття сутнісних аспектів застосування інформаційних та інших технологій у навігаційній безпеці, у захисті суден та портів, ознайомлення з можливостями застосування у морській безпеці, найновітніших інформаційних технологій, таких як блокчейн, штучний інтелект, машинне навчання, інтернету речей, аналіз даних, прогнозне моделювання та квантові обчислення.

Завданнями навчальної дисципліни «Використання сучасних інформаційних та телекомунікаційних технологій в забезпеченні морської безпеки» є формування теоретичної бази знань щодо загальних загроз морській безпеці – для кваліфікованого та ефективного використання сучасних інформаційно-комунікаційних технологій в організації морської безпеки; розвинення уміння щодо організації забезпечення інформаційної безпеки морського судна з урахуванням його вразливих об’єктів; розвинення уміння орієнтуватися у найсучасніших інформаційних та телекомунікаційних технологіях стосовно їх застосування в організації морської безпеки.

Засвоївши програму навчальної дисципліни «Використання сучасних інформаційних та телекомунікаційних технологій в забезпеченні морської безпеки», здобувачі вищої освіти мають бути здатними:

- вирішувати професійні завдання з урахуванням досягнень теорії та практики застосування інформаційних та телекомунікаційних технологій в забезпеченні безпеки морського судна й порту,
- володіти основними професійними компетенціями, а саме: вміння

використовувати сучасні інформаційні та телекомунікаційні технології при виявленні вразливих об’єктів судна та загроз, при встановленні доцільних засобів забезпечення інформаційної безпеки судна, при плануванні та організації заходів щодо загального забезпечення морської безпеки;

- здійснювати моніторинг, збір та аналіз новітньої наукової, правової та технічної інформації що може бути застосована у забезпеченні морської безпеки.

Перелік компетентностей, формування яких забезпечує вивчення навчальної дисципліни (з ОПП).

Загальні компетентності: ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області та розуміння професійної діяльності. ЗК4. Здатність використовувати інформаційні та комунікаційні технології. ЗК11. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі

Спеціальні компетентності: СК6. Здатність аналізувати та систематизувати одержані результати, формулювати аргументовані висновки та рекомендації. СК9. Здатність ефективно застосовувати сучасні техніку і технології захисту людини, матеріальних цінностей і суспільних відносин від проявів криміногенної обстановки та обґрунтовувати вибір засобів та систем захисту людини і суспільних відносин. СК13. Здатність забезпечувати охорону об’єктів державної власності, державну охорону органів державної влади України та безпеку взятих під захист осіб, охорону фізичних осіб та об’єктів приватної і комунальної власності. СК14. Здатність до використання технічних приладів та спеціальних засобів, інформаційно-пошукових систем та баз даних. СК18. Здатність забезпечувати кібербезпеку, економічну та інформаційну безпеку держави, об’єктів критичної інфраструктури.

Результати навчання: РН1. Розуміти історичний, економічний, технологічний і культурний контексти розвитку правоохоронної діяльності. РН14. Здійснювати пошук та аналіз новітньої інформації у сфері правоохоронної діяльності, мати навички саморозвитку та самоосвіти протягом життя, підвищення професійної майстерності, вивчення та використання передового досвіду у сфері правоохоронної діяльності. РН17. Використовувати основні методи та засоби забезпечення правопорядку в державі, дотримуватись прав і свобод людини і громадянина, попередження та припинення нелегальної (незаконної) міграції та інших загроз національної безпеки держави (кібербезпеку, економічну та інформаційну безпеку, тощо). РН18. Застосовувати штатне озброєння підрозділу (вогнепальну зброю, спеціальні засоби, засоби фізичної сили); інформаційні системи, інформаційні технології, технології захисту даних, методи обробки, накопичення та оцінювання інформації, інформаційно-аналітичної роботи, бази даних (в тому числі міжвідомчі та міжнародні), оперативні та оперативно-технічні засоби, здійснення оперативно-розшукової діяльності.

Міждисциплінарні зв’язки: дана навчальна дисципліна тісно пов’язана й логічно доповнює такі навчальні дисципліни, як «Методологія наукового

пізнання», «Міжнародно-правове регулювання морської безпеки», «Проблеми службово-бойової діяльності правоохоронних органів на об’єктах водної інфраструктури», «Іноземна мова професійного спрямування». Успішне її вивчення вимагає від здобувачів вищої освіти знання різних міжнародних та національних нормативних актів, а також цілого комплексу спеціальних знань, що були придбані в перелічених навчальних дисциплінах.

2. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Використання сучасних інформаційних та телекомунікаційних технологій в забезпеченні морської безпеки»

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна</td><td>заочна</td></tr>
<tr><td rowspan="2">Кількість кредитів– 3</td><td>Галузь знань
26 «Цивільна безпека»</td><td colspan="2" rowspan="2">Вибіркова</td></tr>
<tr><td rowspan="5">Спеціальність
262 «Правоохоронна діяльність»</td></tr>
<tr><td rowspan="4">Загальна кількість годин – 90</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">1 й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td colspan="2">2 й</td></tr>
<tr><td colspan="2" rowspan="8">Освітній ступінь:
«доктор філософії»</td><td colspan="2">Лекції</td></tr>
<tr><td>12 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Практичні (семінарські)</td></tr>
<tr><td>28 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>50 год.</td><td>82 год.</td></tr>
<tr><td colspan="2">Вид контролю</td></tr>
<tr><td colspan="2">Залік</td></tr>
</table>

Тематичний план

Назва змістових модулів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі				с.р.	усього	у тому числі				с.р.
		л	с	п	інд			л	с	п	інд	
1	2	3	4	5	6	7	8	9	10	11	12	13
Тема № 1. Загальні поняття про морську безпеку	12	2	4			6	10					10
Тема № 2. Загальні підходи до кібербезпеки морських суден та портів	20	2	6			12	22	2	2			18
Тема №3. Застосування технологій у навігаційній безпеці	14	2	4			8	20	2	2			16
Тема № 4. Безпосередня робота	16	2	**6**			8	14					14

по захисту суден і акваторій												
Тема № 5. Новітні технології у морській безпеці (частина 1).	14	2	4			8	12					12
Тема № 6. Новітні технології у морській безпеці (частина 2).	14	2	4			8	12					12
Усього годин	90	12	28			50	90	4	4			82

3. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема № 1 Загальні поняття про морську безпеку

Міжнародна морська організація, як орган сприяння технічній допомозі забезпечення безпеки та захисту морського середовища. Загальний огляд морської безпеки. Приклади терористичних атак на морські судна. Визначення стосовно морської безпеки.

Ризики морської безпеки. Нестабільні вантажі. Нелегальне застосування морського транспорту. Незаконне транспортування зброї масового знищення, вибухових речовин, незаконних матеріалів і контрабанди, впровадження терористів на судна.

Піратство а морський тероризм. Визначення піратства, його розвиток, особливості сьогодення, географія та перспективи. Відмінності морського тероризму від піратства. Виникнення зв'язку між ними.

Кримінальне та регулятивне право в міжнародно-правовій базі безпеки на морі. Майбутній розвиток міжнародної правової бази стосовно морської безпеки

Теоретичні знання: у наслідку вивчення даної теми здобувачі вищої освіти повинні знати поняття «морська безпека», «Міжнародна морська організація», «піратство», «морський тероризм», «Міжнародна конвенція з охорони людського життя на морі», «Міжнародний кодекс безпеки суден і портових засобів», класифікацію загроз морській безпеці, причини необхідності посилення морської безпеки, класифікацію піратства, коротку історію морського тероризму, структуру кримінального та регулятивного права в міжнародно-правовій базі безпеки на морі.

Практичні навички: при вивченні даної теми необхідно вміти надати характеристику морським злочинам, що становлять загрозу безпеці на морі, розрізняти морське піратство і морський тероризм, характеризувати призначення Типового національного закону про акти піратства та порушення морського права.

Методичні рекомендації

У процесі вивчення даної теми здобувачі вищої освіти повинні засвоїти, що віками судноплавство було вразливим до різноманітних морських злочинів. Галузь рік за роком піддається різноманітним морським злочинам. Зокрема, загрози для морської галузі спостерігалися під час ірано-іракської війни. Протягом 1980-1988 років мішенями були численні кораблі та морська інфраструктура. Викрадення Фронтом звільнення Палестини 7 жовтня 1985 року італійського круїзного лайнера Achille Lauro, що перевозив 400 пасажирів, і вбивство 69-річного Леона Клінгхоффера, американця єврея, показало відсутність безпеки в галузі. Цей інцидент викликав занепокоєння держав-членів Міжнародної морської організації, оскільки він забрав численні людські життя.

Необхідно зазначити, що перш, ніж братися за це визначення, слід зауважити, що український термін «безпека» перекладається на англійську двома термінами, які містять досить різний сенс:

- «security» – захист від зовнішньої загрози;
- «safety» – запобігання нещасним випадкам.

У дисципліні, що пропонується, ми будемо застосовувати термін «морська безпека» само у сенсі «security» – захист від зовнішньої загрози. Отже, «морську безпеку» визначають різними способами, деякі з яких наведені нижче. Хоукс (1993) визначає морську безпеку як «заходи, що вживаються власниками, операторами та адміністраторами суден, портових споруд, морських установок та інших морських організацій або закладів для захисту від... будь-якого ворожого втручання в законні операції».

За словами Стівена М. Джонса (2006), безпека на морі – це «стан судноплавної компанії/судна/екіпажу/порту, відчуття безпеки або безпека судноплавної компанії/судна/екіпажу/порту від таких загроз. як тероризм, піратство та інша злочинна діяльність».

Меджіа (2007) визначає морську безпеку як: «стан вільності від загрози протизаконних дій, таких як піратство, збройне пограбування, тероризм або будь-яка інша форма насильства проти суден, екіпажів, пасажирів, портових споруд, морських установок та інших цілей у морі або у прибережних районах.

Окремо слід підкреслити, що певні вантажі, що перевозяться, є дуже нестабільними, саме їхній зміст створює високу ступінь небезпеки. Наприклад, СПГ (зріджений природний газ) є дуже летким за своєю природою, і якщо його піддати займанню, це призведе до сильного вибуху, який охопить територію, площа якої в деяких випадках може досягати одного квадратного кілометра («Тероризм танкерів СПГ», 2007). Тому деякі автори назвали танкери зі СПГ «плаваючими бомбами» (Центр розвідки тероризму та повстанців, 2007). Найджел Вілсон (2008) цитує Управління звітності уряду США (GAO), яке повідомляє, що ланцюг постачання СПГ є вразливим до атак смертників із завантажених вибухівкою човнів, атак із застосуванням зброї на відстані та збройних нападів.

При самостійні підготовці слід звернути увагу, що сьогодні загрози безпеці на морі становить певний перелік морських злочинів, серед яких перші місця посідають піратство та збройне пограбування суден. Слід звернути увагу на особливості сучасного піратства, його складові, зброю, що використовується, географічний розподіл.

Семінарське заняття № 1- 2 години

Учбові питання:

1. Загальний огляд морської безпеки
2. Визначення стосовно морської безпеки
3. Побоювання та факти стосовно морської безпеки.
4. Основні загрози морській безпеці

Тематика рефератних повідомлень:

1. Значення морського транспорту для глобальної економіки.
2. Роль Міжнародної морської організації в організації безпеки на морі.
3. Сучасні визначення поняття «морська безпека».
4. Найвідоміші інциденти на морі.

Питання для самоконтролю:

1. Який вид транспорту у світі перевозить більшість вантажів?
2. Яка організація була створена для сприяння технічній допомозі у забезпеченні безпеки та захисту морського середовища?
3. Чому на морське судно проникнути простіше, ніж на авіалайнер?
4. Стосовно морського транспорту що визначає англійське слово «security»?
5. Стосовно водного транспорту що визначає англійське слово «safety»?
6. Що слід розуміти під морською безпекою?
7. Які є основні ризики морської безпеки
8. Якою є мета морського тероризму?
9. Які два злочини становлять найбільшу загрозу безпеці на морі.
10. Що було метою піратства у минулих століттях?
11. Що є метою піратства у 21 столітті?

Семінарське заняття № 2 – 2 години

Учбові питання:

1. Піратство та збройне пограбування суден.
2. Морський тероризм.
3. Міжнародна правова база стосовно морської безпеки.
4. Перспективи розвитку міжнародної правової бази стосовно морської безпеки.

Тематика рефератних повідомлень:

1. Особливості сучасного морського тероризму.
2. Відмінності морського тероризму та піратства.
3. Що поєднує піратство і морський тероризм.
4. Міжнародні конвенції стосовно дій на морі.

Питання для самоконтролю:

1. Що входить до арсеналу дій морського тероризму?
2. Якої площу може охопити результат вибуху зрідженого природного газу?
3. Найнебезпечніший варіант незаконного вантажу на водному транспорті?
4. Яким роком датується «Конвенції про відкрите море»?
5. Яким роком датується UNCLOS (Конвенція ООН з морського права)?
6. Що є основним мотивом нападу на судна у Південно-Східній Азії?
7. Що є основним мотивом нападу на судна поруч із Сомалі?
8. У чому полягає призначення міжнародної конвенції SOLAS?
9. У чому полягає призначення міжнародної конвенції UNCLOS)?

Тема № 2. Загальні підходи до кібербезпеки морських суден та портів

Кібербезпека (загальний огляд). Атрибути кібербезпеки: конфіденційність, цілісність і доступність). Чотири стовпи побудови ефективної та цілісної кібербезпеки: люди, процеси, технології, фізичні аспекти. Вразливі місця та загрози. Вразливість інформаційної системи. Загроза діяльності або активам. Подія загрози. Рівень впливу загрозливої події. Суб'єкти загрози. Кібератаки на системи інформаційних технологій на системи операційних технологій, або фізичні активи. Зловмисник кібератаки. Вектори атаки. Варіанти кібератак. Просунута стійка загроза. Задні двері. Шкідливе програмне забезпечення. Фішинг. Програми-вимагачі. Соціальна інженерія. Віруси. Хробаки.

Організація забезпечення інформаційної безпеки морського судна. Вразливі об'єкти судна. Засоби забезпечення інформаційної безпеки судна. Критичні системи судна. Причини неможливості забезпечення абсолютної безпеки судна. Концептуальна модель безпеки судна. Поняття «середовища безпеки» та його значення. Причини неможливості раптового забезпечення безпеки при виникненні проблеми. Сучасний підхід до захисту та базові принципи забезпечення інформаційного захисту судна. Три напрями заходів забезпечення безпеки конфіденційної інформації. Два базові принципи забезпечення інформаційного захисту. Зміст плану захисту інформаційної безпеки судна.

Кібербезпека морських портів. Порти – критична інфраструктура. Порти – критична інформаційна інфраструктура. Вплив (наслідки) збою порту. П'ять потенційних небезпек, пов'язаних із порушенням роботи порту: перевантаження, економіка, навколишнє середовище, геополітика та безпека. Порти та кібербезпека. Порт як кіберфізичне середовище. Інформаційні технології та операційні технології, як елементи кіберфізичного середовища. Атрибути кібербезпеки портів. Сценарії кібератак на порти

Теоретичні знання: у наслідку вивчення даної теми здобувачі вищої освіти повинні знати поняття «кібербезпека», «атрибути кібербезпеки», «вразливість», «загроза», «суб'єкт загрози», «кібератаки», «зловмисник», «вектор атаки», класифікацію суб'єктів загрози, класифікацію шкідливого програмного забезпечення, склад інформації, яку надають інформаційні системи судна, склад основних систем судна, вразливих перед кібератаками, концептуальну модель безпеки судна, основні напрями заходів для забезпечення безпеки конфіденційної інформації на судні, склад атрибутів у моделі кібербезпеки портів,

Практичні навички: по вивченні даної теми необхідно вміти надати визначення та характеризувати кібербезпеку, розрізняти різні варіанти кібератак, визначати вразливі об'єкти судна, визначати основні напрями забезпечення безпеки конфіденційної інформації на судні, визначати основні напрями порушень роботи порту.

Методичні рекомендації

При вивчення даної теми слід зосередитися на сутності кібербезпеки, як такої, а також на її ролі у підтримці морської безпеки. Отже, Кібербезпека –це захист інформаційних систем (апаратного забезпечення, програмного забезпечення та пов'язаної інфраструктури), даних у них і послуг, які вони надають, від несанкціонованого доступу, шкоди чи неправильного використання. Це включає навмисне заподіяння шкоди системним оператором або випадкову шкоду внаслідок недотримання процедур безпеки. Критично важливі інформаційні активи, «перлини» організації, мають величезну цінність і можуть мати серйозні наслідки для бізнесу, якщо їх зламати. Заходи кібербезпеки мають захистити ці перлини корони від низки низьких злочинів і проблем національної безпеки. Це досягається завдяки розумінню вразливостей і загроз для бізнесу. Проаналізуємо основні властивості кібербезпеки інформаційних систем, які є важливими для запобігання використанню вразливостей загрозами, які призводять до кібератаку морському секторі.

Слід пам'ятати, що бажані характеристики захищеної системи складає тріада атрибутів КЦД (конфіденційність, цілісність і доступність).

Також необхідно зосередитися на наступних чинниках кііерзагроз судну.

Вразливість—це слабке місце в інформаційній системі, її процедурах безпеки, внутрішньому контролі або реалізації, які можуть бути використані загрозою. Багато поширених вразливостей стосуються апаратного забезпечення, програмного забезпечення, мереж, персоналу та організацій

Більшість вразливостей інформаційної системи пов'язано із засобами контролю безпеки, які або не були застосовані (навмисно чи ненавмисно),або були застосовані, але зберігають деякі слабкі місця. Організаціям може знадобитися з часом переоцінити існуючі засоби контролю безпеки, щоб визначити їх ефективність.

Загроза—це обставина або подія, яка потенційно може негативно вплинути на діяльність та активи організації, окремих осіб, інші організації чи країну через несанкціонований доступ, знищення, розкриття, модифікацію або відмову в обслуговуванні інформаційної системи. Загрози можуть бути навмисними, випадковими, нецільовими або цілеспрямованими.

Подія загрози – це ситуація або подія, спричинена загрозою, яка має потенціал несприятливого впливу. Коли виникає загроза, вона стає інцидентом, який може поставити під загрозу конфіденційність, цілісність або доступність інформаційної системи або стати порушенням політик безпеки, процедур або їх використання.

Рівень впливу загрозливої події —це величина шкоди, яку можна очікувати в результаті наслідків неавторизованого розкриття, модифікації, знищення або втрати інформації чи втрати доступності інформаційної системи.

Організації можуть відчувати вплив несприятливих подій на рівні інформаційної системи (наприклад, невиконання вимог), на бізнес-рівні (наприклад, невиконання бізнес-цілей) і на рівні організації (наприклад,

невиконання юридичних або нормативні вимоги, що шкодить репутації або відносинам).

Суб'єкт загрози – це фізична чи юридична особа, яка реалізує загрозу кібербезпеці, і є відповідальною за інцидент, і може бути внутрішньою або зовнішньою щодо організації. Суб'єкти загрози мають різноманітні мотивації та можливості, які вимагають використання різних методів зменшення та контролю ризику. Деякі суб'єкти мотивовані фінансовою вигодою, тоді як інші мотивовані політичними, ідеологічними чи релігійними мотивами.

Протягом самостійної роботи слід розглянути чинники та варіанти кібератак, вразливі об'єкти судна, а також засоби забезпечення інформаційної безпеки судна.

Семінарське заняття № 3 – 2 години

Учбові питання:

1. Атрибути кібербезпеки.
2. Вразливі місця та загрози.
3. Кібератаки.

Тематика рефератних повідомлень:

1. Кібератаки та їхній вплив на морську безпеку..
2. Вектори кібератаки.
3. Найсучасніші кібератаки
4. Шкідливе програмне забезпечення та його роль на морську безпеку

Питання для самоконтролю:

1. Надайте визначення поняття «вразливість кіберсистеми».
2. Надайте визначення поняття «загроза».
3. Охарактеризуйте поняття «кібратака»
4. Надайте визначення поняття «вектор атаки».
5. Що означає поняття «бекдор» стосовно кібербезпеки?
6. Охарактеризуйте таке шкідливе програмне забезпечення, як «вірус»?
7. У чому полягає сутність троянських програм?
8. Як застосовуються програми-вимагачі?
9. Яким чином працюють шпигунські програми?

Семінарське заняття № 4 – 2 години

Учбові питання:

1. Вразливі об'єкти судна
2. Засоби забезпечення інформаційної безпеки судна
3. Концептуальна модель безпеки судна.
4. Сучасний підхід до захисту та базові принципи забезпечення інформаційного захисту судна

Тематика рефератних повідомлень:

1. Критичні системи судна, відмова яких небезпечна для нього.
2. Чому абсолютний захист інформаційної системи судна недоцільний.
3. Середовище безпеки», як найважливішій фактор при побудові формальної

моделі безпеки судна.
4. Правила розробки інформаційного захисту судна.

Питання для самоконтролю:

1. Перелічить основні системи вантажного судна, що є вразливими для кібератак.
2. Яку інформацію надають сучасні суднові інформаційні системи:
3. У чому полягає основний недолік сучасних систем управління морськими транспортними суднами
4. Чому недоцільно намагатися забезпечити абсолютну інформаціну безпеку? судна
5. Що входить до складу концептуальної моделі безпеки судна?
6. Для побудови формальної моделі безпеки судна яке значення має порняття «середовище безпеки»?
7. У чому полягає сучасний підхід до інформаційного захисту судна?
8. Що входить до базових принципів забезпечення інформаційного захисту судна?

Семінарське заняття № 5 – 2 години

Учбові питання:

1. Важливість портів
2. Порти та кібербезпека
3. Сценарії кібератакна порти

Тематика рефератних повідомлень:

1. *Порти як критична інфраструктура держави.*
2. Роль безпеки портів у підтримці життєздатності держави
3. Порт як кіберфізичне середовище.
4. Атрибути кібербезпеки портів

Питання для самоконтролю:

1. Чом порти сильно вразливі до кіберзагроз?
2. Поясніть, чому порти як критична інформаці йна інфраструктура
3. Поясніть, які п’ять потенційних небезпек, пов’язані із порушенням роботи порту.
4. Доведіть, що порт є кіберфізичним середовищем.
5. Як розмір порту впливає на його вразливість та чому?
6. Які є основні та додаткові атрибути кібербезпеки порту?
7. Які сценарії кібератак на порти ви вважаєте найважливішими?
8. У чому полягала сутність кібератаки Maersk NotPetya?
9. У чому полягала сутність кібератаки на порт Антверпена протягом 2011-2013 років?

Тема № 3. Застосування технологій у навігаційній безпеці

Ефективність впровадження заходів безпеки на морі. Роль Міжнародного кодексу безпеки суден і портових засобів (ISPS). Роль взаємодії між морською адміністрацією та правоохоронними органами у навігаційній системі.

Технології, прийняті для забезпечення навігаційної безпеки (SOLAS). Автоматична радіолокаційна допомога (ARPA): особливості автоматичного пошуку. Причини обмежень застосування. Засоби подолання обмежень. Призначення та застосування інфрачервоних камер на допомогу ARPA. Система автоматичної ідентифікації (AIS). Сутність роботи AIS. Інформація, яку надає AIS. Ідентифікація небезпечних цілей за допомогою AIS. Недоліки ARPA, що усуваються за допомогою AIS. Небезпека підключення AIS до Інтернету.

Інтегрована система мосту або інтегровані навігаційні системи. Елементи, що входять до інтегрованих навігаційних систем. Переваги інтегрованих навігаційних систем. Ситуації, в яких корисні інтегровані навігаційні системи. Далека ідентифікація та відстеження (LRIT – Long-range identification and tracking). Типи суден, на які встановлюється система LRIT. Інформація, що передається за допомогою системи LRIT. Ситуації, в яких систему слід вимикати. Порівняння можливостей AIS та LRIT.

Питання безпеки судноплавства. Автоматизована система стеження, що використовується на суднах та у службах руху суден (VTS). Зони, в яких встановлюється система VTS. Основні функції системи VTS. Інфраструктура, за допомогою якої забезпечується система VTS. Причини зниження ефективності системи VTS. Система дистанційного керування морськими транспортними засобами (ROV). Ситуації, у яких доцільно застосування система дистанційного керування морськими транспортними засобами.

Теоретичні знання: у наслідку вивчення даної теми здобувачі вищої освіти повинні знати поняття «Міжнародна конвенція з охорони людського життя на морі (SOLAS)», знати призначення, принцип роботи та можливості автоматичної радіолокаційної допомоги ARPA, системи автоматичної ідентифікації AIS, системи далекої ідентифікація та відстеження LRIT, призначення та загальні параметри інтегрованої навігаційної системи, служби забезпечення руху суден (Vessel Traffic Service – VT)S, системи дистанційного керування морськими транспортними засобами (ROV).

Практичні навички: по вивченні даної теми необхідно вміти надати характеристику ініціативі Міжнародної морської адміністрації (IMO) щодо запровадження добровільної схеми аудиту держав-членів IMO, охарактеризувати можливості систем APRA, AIS, інтегрованої системи мосту та системи далекої ідентифікації та відстеження (LRIT).

Методичні рекомендації

При вивченні даної теми необхідно зазначити, що Інструменти IMO, які набувають чинності, повинні бути включені державами-членами у свої

національні закони для забезпечення виконання. Ступінь дотримання вимог різниться від країни до країни. Прийнявши інструмент, деякі країни впроваджують його ефективно на пріоритетній основі, тоді як інші можуть не застосовувати його настільки ефективно. Причини можуть бути різними – від економічних обмежень до професійної компетентності. Після того, як інструмент буде включено в національну правову систему, його потрібно впровадити на землі, тобто в морському секторі. Кодекс ISPS вимагає вжиття заходів урядам, що укладає контракт, компаніями та судном. Для суден можливо перевірити стан готовності через державний портовий контроль. Однак не існує механізму, який би гарантував, що заходи, прийняті державою-членом, є адекватними та відповідають цілям кодексу. Слід зазначити, що для досягнення цілей кодексу Європейський Союз оприлюднив директиви щодо проведення комісійних інспекцій з питань морської безпеки (Європейський Союз, 2005, 10 червня). Ця ініціатива призведе до стандартизації заходів, прийнятих для безпеки на морі серед держав-членів. Крім того, ініціатива ІМО щодо запровадження добровільної схеми аудиту держав-членів ІМО є шляхом уперед до впровадження стандартизації у світі та сприятиме безпеці на морі ("Схема аудиту в процесі", 2007, лютий). Саме «воля» та співпраця держав-членів можуть зробити судноплавство безпечним. Діяльність контролю держави порту державами-членами ІМО щодо ліквідації небезпечних суден дала значні результати. Таким чином, необхідно розпочати подібну співпрацю, щоб ліквідувати кораблі, які займаються незаконною діяльністю та загрожують безпеці на морі.

Слід зазначити, що в більшості країн світу морська адміністрація є правоохоронним органом у морському судноплавстві в порту, тоді як у морі є іншим органом. Крім того, обидва вони знаходяться у віданні різних міністерств. Таким чином, адекватна взаємодія між двома відомствами є важливою для ефективної реалізації морської безпеки. Однак на практиці так не буває.

Результати опитування також вказують на те, що правоохоронний орган є іншою організацією в їхніх країнах і існує неадекватна взаємодія між морською адміністрацією та правоохоронними органами в їхній державі прапора, на що необхідно звернути увагу державам-членам.

Протягом самостійної роботи слід детальніше ознайомитись зі влаштуванням засобів автоматичної радіолокаційної допомоги, систем автоматичної ідентифікації, а також усвідомити сутність інтегрованої системи мосту.

Семінарське заняття № 6 – 2 години

Учбові питання:

1. Автоматична радіолокаційна допомога (ARPA)
2. Система автоматичної ідентифікації (AIS)
3. Інтегрована система мосту або інтегровані навігаційні системи
4. Далека ідентифікація та відстеження (LRIT)

Тематика рефератних повідомлень:
1. Кодекс ISPS та його вплив на морську безпеку.
2. Взаємодія між морською адміністрацією та правоохоронними органами в різних державах
3. Найсучасніші технології радіолокаційної допомоги у морі.

Питання для самоконтролю:
1. Чим доповнюють радіолокаційні засоби для виявлення малих цілей?
2. Як у порту можна перевірити стан радіолоаційної готовності судна?.
3. Які можливості надає система ARPA?
4. Які обмеження система ARPA має при виявленні цілей?
5. Яким чином можна подолати деякі обмеження система ARPA?
6. Яким чином інфрачервоні камери сприяють підвищенню безпеки судна?
7. У чому полягає основна функція AIS?
8. Яку інформацію передає система AIS?
9. Які недоліки системи ARPA усуває система AIS?

Семінарське заняття № 7 – 2 години

Учбові питання:
1. Служби забезпечення руху суден
2. Система дистанційного керування морськими транспортними засобами (ROV).

Тематика рефератних повідомлень:
1. Інфраструктура та інші засоби для постійного контролювання руху суден.
2. Служби забезпечення руху суден
3. Забезпечення ефективності служб забезпечення руху суден.
4. Сучасні системи дистанційного керування морськими транспортними засобами.

Питання для самоконтролю:
1. Які засоби дозволяють фіксувати малі цілі на воді?
2. У чому допомагає система AIS?
3. Які організаційно-правові проблеми заважають безпеці на морі?
4. У чому полягає ідея створення охоронного кільця за допомогою APRA?
5. Які дії система здійснює автоматично після виявлення судна поблизу?
6. Які умови сильно погіршують ефективність роботи радара?
7. Чим обумовлена наявність сліпої зони щодо роботи бортового радара?
8. Які переваги (можливості) надає інтегрована навігаційна система?
9. Що входить до складу інтегрованої навігаційної системи мосту?

Тема № 4. Безпосередня робота по захисту суден і акваторій

Перевірка персоналу та пасажирів. Причини необхідності перевірки та ідентифікації персоналу та пасажирів. Безпечна система огляду людей SPO-20. Відмінність перевірки людей у засобах повітряного та водного транспорту. Особливості безпечної системи огляду людей SPO-20. Принцип її роботи.

Робота з контейнерами. Сканування контейнерів, як наслідок Міжнародного кодексу з охорони суден та портових засобів (ISPS). Політика роботи з контейнерами та її причини. Проблеми здійснення 100%-го сканування контейнерів. Небезпеки, пов'язані з несканованими контейнерами. Методи ядерного виявлення та складного програмного забезпечення – перспективні технології для забезпечення швидкого сканування контейнерів. Відстеження контейнерів. Кримінальні причини відстеження руху контейнерів. Можливості розширеного пристрою безпеки контейнерів (ACSD) щодо відстеження контейнерів та несанкціонованих дій з ними. Необхідні перспективи розвитку систем сканування контейнерів. Шляхи застосування нанотехнологій у скануванні та відстеженні руху контейнерів.

Безпосередній захист суден і акваторій. Антитерористична система виявлення водолазів Cerberus360. Принцип дії та застосування. Захист судна електричними огорожами Тактико-технічні та експлуатаційні особливості захисної системи Secure-Ship. Висотний безпілотний літальний апарат (БПЛА) тривалої дії. Тактико-технічні та експлуатаційні особливості БПЛА Zephir та можливості його застосування для забезпечення морської безпеки. Переваги патрулювання чутливих зон за допомогою безпілотних надводних суден. Причини необхідності спостереження за портами і каналами. Проблеми та шляхи здійснення спостереження за портами і каналами.

Теоретичні знання: у наслідку вивчення даної теми здобувачі вищої освіти повинні знати призначення та принципи перевірки персоналу та пасажирів, принцип роботи безпечної системи огляду людей SPO-20, призначення та принципи перевірки морських контейнерів, призначення та принципи відстеження шляху контейнерів, особливості застосування нанотехнологій у забезпеченні безпеки контейнерів, основні принципи безпосереднього захисту суден та акваторій.

Практичні навички: по вивченні даної теми необхідно вміти обґрунтувати необхідність перевірки персоналу та пасажирів з точки зору морської безпеки, охарактеризувати безпечну система огляду людей SPO-20, обґрунтувати можливість злочинного використання контейнерів, охарактеризувати можливості пристрою безпеки контейнерів ACSD.

Методичні рекомендації

При вивченні даної теми слід звернути увагу, що морська безпека містить багато компонентів, жоден з яких не є другоряндним. У час, коли новітні технічні засоби надають неймовірні можливості окремому пасажирові або члену екіпажу, перевірка людей, що потрапбяють на борт, найсучаснішими технічними засобами стає в один ряд з ідентифікацією ворожого судна. Одночасно застосування контейнерів отримало неймовірний розмах через совю зручність. Але їх навчилися використовувати у своїх цілях також й злочинці. Тому окреме місце у бборотьбі з піратством і тереризмом посідає вдосконалення систем сканування та відстеження контейнерів. На тлі цього

безпосередній захист суден і акваторій найсучаснішими засобами сприймається цілком природно.

Важливо, що з експоненційним зростанням морського сектору також значно зросла взаємодія людини з об’єктами та суднами. Морський транспорт є найдоступнішим і найрозкішнішим засобом транспортування, Тому важливо мати контроль доступу та ретельно перевіряти облікові дані персоналу. Схема посвідчення особи транспортного працівника (TWIC), започаткована урядом США, є позитивним кроком у галузі безпеки на морі. Ідентифікаційна картка містить біометричні дані, такі як відбитки пальців, особи. Міжнародна організація праці (МОП) також прийняла переглянуту Конвенцію про посвідчення особи моряків (SID) (Конвенція № 185) у червні 2003 року для запобігання актам тероризму, які загрожують безпеці пасажирів і екіпажів і безпеці суден. SID також включає біометричну технологію 66 (Міжнародна організація праці, 2004). Біометрична автентифікація широко використовується для конфіденційних і важливих питань. Його корисність можна побачити в таких програмах, як доступ до робочої станції, мережі та домену, єдиний вхід, вхід у програму, захист даних, віддалений доступ до ресурсів, безпека транзакцій та веб-безпека. Він також ефективно використовується в захищених електронних банках, правоохоронних органах, паспортних програмах, водійських правах і фінансових операціях ("Біометрія"). Ініціативи TWIC ID-картки та SID стануть чудовим стримуючим засобом для злочинців, які мають намір вторгнутися, скориставшись великомасштабним переміщенням персоналу, і стануть життєво важливою ідентифікацією для підтвердження повноважень справжніх людей, пов’язаних із промисловістю.

Оскільки морський транспорт є найбільш економічним і комфортним засобом транспортування, кількість пасажирів, які користуються цими зручностями, постійно зростає, як видно з даних, зібраних судноплавними компаніями. Пасажири, які подорожують круїзними та пасажирськими лайнерами, перевіряються на 100%, оскільки їх кількість невелика порівняно з поромами. Через характер поромних переправ виникли труднощі, оскільки вони мобілізують масове населення за короткий час для швидкого повернення, що становить велику загрозу безпеці на морі.Отже, важливою є перевірка персоналу і пасажирів.

Не менш важливою є й перевірка контейнерів. Кодекс ISPS набув чинності 1 липня 2004 року, і мета цього кодексу полягала у «встановленні міжнародної структури, яка передбачає співпрацю між договірними урядами, урядовими установами, місцевими адміністраціями та судноплавством і портовою галуззю для виявлення/оцінки загроз безпеці та вжиття превентивних заходів, заходи безпеки, що впливають на судна або портові засоби, що використовуються в міжнародній торгівлі» (Міжнародний кодекс безпеки суден і портів (ISPS), 2002 р., стор. iii). Кодекс окреслив комплексні заходи щодо підвищення безпеки суден і портових засобів на основі управління ризиками. Це вимагає проведення аналізу ризиків і впровадження необхідних заходів для запобігання або пом'якшення наслідків у разі порушення безпеки на морі. Щоб

відповідати вимогам Кодексу, були прийняті різні технології для підвищення безпеки на морі. Можливості цих технологій обговорюються нижче.

При самостійній роботі необхідно приділити увагу сучасним методам перевірки контейнерів, впровадженню політики SOS: «Відправлятися контейнери лише за умови сканування». Сканування контейнерів стало неминучим у зв'язку зі зростанням міжнародного тероризму та відповідними вимогами безпеки на морі. На сьогоднішній день технологія сканування не розвинулася настільки, щоб встигати за обсягом вантажу та швидкістю його обробки.

Семінарське заняття № 8 – 2 години

Учбові питання:

1. Перевірка та ідентифікація персоналу.
2. Безпечна система огляду людей SPO-20.

Тематика рефератних повідомлень:

1. Міжнародна рада круїзних ліній та її роль у підвищені морської безпеки.
2. Сучасні засоби перевірки персоналу морського транспорту.
3. Сучасні засоби перевірки пасажирів.
4. Міжнародний кодекс безпеки суден і портів (ISPS) та його роль у підвищені морської безпеки.

Питання для самоконтролю:

1. Чому проблеми скринінгу людей на морському транспорті найвищі?
2. З якими потенційними загрозами пов'язана необхідність ретельної перевірки персоналу?
3. Які параметри посвідчення особи моряка (SID) гарантують, що документ належить саме тій людині, яка його надає?
4. Які особливі проблеми виникають при перевірці пасажирів на поромних переправах?
5. У чому полягають призначення та можливості системи SPO-20?
6. Яку конвенцію (номер) прийняла Міжнародна організація праці про посвідчення осіб моряків?
7. Яку кількість пасажирів (приблизно) перевозить морський транспорт щорічно?
8. Яка організація веде підрахунок кількості осіб у світі, що користуються морським транспортом у якості пасажирів?
9. Скільки відсотків пасажирів, які подорожують круїзними та пасажирськими лайнерами, перевіряються?

Семінарське заняття № 9 – 2 години

Учбові питання:

1. Сканування контейнерів.
2. Відстеження контейнерів
3. Технологія NANO – шлях вперед у безпеці контейнерів

Тематика рефератних повідомлень:

1. Міжнародний кодекс безпеки суден і портів (ISPS), призначення, дата набуття чинності та особливості.
2. Сучасні особливості морських контейнерних перевезень.
3. Перспективні методи і засоби швидкісного здійснення перевірок морських контейнерів.

Питання для самоконтролю:

1. Скільки відсотків вантажів сьогодні перевантажуються морем?
2. Скільки контейнерів (приблизно) перебуває в океанах одночасно?
3. Які вимоги ставить Управлінням митної та прикордонної служби США (стосовно контейнерів) для посилення безпеки на морі?
4. Скільки відсотків багажу піддаються скануванню у сфері авіаційних перевезень?
5. Які саме напрями (заходи) окреслив Міжнародний кодекс безпеки суден і портів (ISPS) щодо підвищення безпеки суден і портових засобів ?
6. Які соціально-політичні явища останнього часу спонукають стрімко підвищити відсоток перевірок морських контейнерів?
7. Які проблеми може викликати спроба здійснювати стовідсоткову перевірку морських контейнерів?
8. Яким чином можна вирішити протиріччя поміж питаннями 7 і 8?
9. Яка технологія вважається перспективною щодо підвищення швидкості перевірок морських контейнерів?
10. У чому полягає сутність та перспективи застосування нано-технологій для перевірки морських контейнерів?

Семінарське заняття № 10 – 2 години

Учбові питання:

1. Антитерористична система виявлення водолазів Cerberus360
2. Захист судна електричними огорожами
3. Висотний безпілотний літальний апарат (БПЛА) тривалої дії
4. Патрулювання чутливих зон за допомогою безпілотного надводного судна
5. Спостереження за портом і каналом.

Тематика рефератних повідомлень:

1. Методи виявлення та протидії водолазам терористам в оточенні судна.
2. Забезпечення безпеки суден за допомогою електричних огорож.
3. Застосування безпілотних летальних апаратів для здійснення безпкки акваторій.
4. Безпілотні надводні судна у патрулюванні чутливих зон акваторій.
5. Сучасні засоби спостережень за портами і каналами.

Питання для самоконтролю:

1. Якими є призначення та характеристики сонару Cerberus 360?
2. Якими є призначення та параметри та засобу Secure-Ship?
3. Які додаткові засоби підключаються для підвищення ефективності засобу Secure-Ship?

4. Якими є призначення та параметри БПЛА Zephyr?

5. Які є способи керування безпілотними надводними суднами, що здійснюють патрулювання?

6. Чому вважається, що загроза для судноплавства у вузьких каналах і в портових районах є високою?

7. За допомогою яких пристроїв зазвичай здійснюється спостереження ситуації у портах і каналах?

8. Застосування терористами яких засобів погіршує можливості спостереження за ситуацією у портах і каналах?

Тема № 5. Новітні технології у морській безпеці (частина 1)
(Застосування блокчейн, штучного інтелекту машинного навчання та інтернету речей у морській безпеці)

Сутність технології блокчейн. Особливості транзакцій у блокчейн.

Перспективи застосування блокчейн у морській сфері: надійна реєстрація судна, якісний моніторинг та відстеження суден, покращений обмін даними між зацікавленими сторонами, оптимізація паперової роботи, підвищення ефективності аналітичної роботи. Застосування блокчейн у морській безпеці. Автентифікації та верифікації морських активів і документів. Управління ланцюгами поставок. Сприяння безпечним та ефективним транзакціям у морській галузі. Підвищення кібербезпеки в морській галузі.

Сутність штучного інтелекту та машинного навчання. Застосування ШІ та машинного навчання в морській безпеці. Ідентифікація загроз та прогнозування майбутніх ризиків. Виявлення підозрюваних суден (піратство, контрабанда). Застосування штучного інтелекту сумісно з блокчейн та інтернетом речей – для виявлення загроз та порушень безпеки. Аналіз даних і прогнозне моделювання для визначення тенденцій та закономірностей розвитку порушень безпеки та прийняття рішень на основі актуальної інформації в реальному часі.

Сутність інтернету речей (IoT). Застосування інтернету речей (IoT) у морській безпеці. Переваги, що надає інтеграція IoT для морської безпеки: безпрецедентне підключення між пристроями, що дозволяє збирати дані в реальному часі, аналізувати та реагувати, покращення обізнаності про ситуацію, покращення прогнозної аналітики та можливостей реагування. Можливості для морської безпнеки, що надає поєднання пристроїв IoT з алгоритмами штучного інтелекту та машинного навчання. Удосконалення моніторингу та спостереження за допомогою Інтернету речей у морській безпеці Проблеми, що супроводжують впровадження IoT до безпеки на морі – підвищення можливостей злому.

Теоретичні знання: у наслідку вивчення даної теми здобувачі вищої освіти повинні знати поняття «блокчейн», «штучний інтелект», «машинне навчання», «Інтернет речей», а також напрями та принципи застосування зазначених новітніх технологій у морській безпеці.

Практичні навички: при вивченні даної теми необхідно вміти надати характеристику технологіям блокчейн, штучного інтелекту, машинного навчання та інтернету речей, а також обґрунтувати доцільність їх застосування для підвищення рівня морської безпеки.

Методичні рекомендації

При вивченні цієї теми слід пам’ятати, що новітні технології постійно виникають і отримують своє застосування. Тому служби з організації безпеки знаходяться у постійних перегонах зі злочинним світом у застосуванні зазначених технологій. Технологія блокчейн вже застосовується злочинцями, і морські правоохоронці не мають права відставати. Також застосування штучного інтелекту та машинного навчання вже працює для підвищення якості виявлення загроз небезпек у морі, а інтернет речей допомагає у вдосконаленні моніторингу та спостереження.

У сфері морської безпеки технологія блокчейн має великі перспективи. Вона може підвищити ефективність, прозорість і безпеку різних процесів і систем. Наприклад, використовуючи блокчейн, зацікавлені сторони морської безпеки можуть створити безпечнийі незмінний запис про власність, реєстрацію та історію експлуатації судна. Це може суттєво зменшити ризик викрадення ідентифікаційних даних судна, шахрайства та несанкціонованого доступу. Крім того, технологія блокчейн може забезпечити безпечний та ефективний обмін даними між різними зацікавленими сторонами в екосистемі морської безпеки. Це може полегшити відстеження та моніторинг суден, вантажів і портових операцій у режимі реального часу, підвищуючи обізнаність про ситуацію та можливості реагування. Крім того, блокчейн може оптимізувати складну документацію та паперову роботу, пов’язану з міжнародною торгівлею, зменшуючи адміністративне навантаження та підвищуючи безпеку ланцюжка постачання.

Отже, слід вникнути в особливості блокчейн, яка, будучи децентралізованою та прозорою бухгалтерською книгою, пропонує численні застосування для посилення заходів безпеки в морській галузі, як от:

1)Автентифікація та верифікація морських активів і документів;

2)Управління ланцюгами поставок;

3)Сприяння безпечним та ефективним транзакціям у морській галузі;

4)Підвищення кібербезпеки в морській галузі.

Слід також мати на увазі, що одночасно штучний інтелект (ШІ) і машинне навчання стали ключовими технологіями, які революціонізують різні сектори, включаючи безпеку на морі. ШІ означає розробку комп’ютерних систем, які можуть виконувати завдання, які зазвичай потребують людського інтелекту. З іншого боку, машинне навчання —це підмножина штучного інтелекту, яка зосереджена на тому, щоб дозволити комп’ютерам навчатися та вдосконалюватисяна основідосвіду без явного програмування.Ці технології мають потенціал для підвищення ефективності операцій з безпеки на морі. Одним із важливих застосувань ШІ та машинного навчання в морській безпеці

є використання інтелектуальних систем спостереження. Ще одна сфера, де штучний інтелект і машинне навчання можуть мати значний вплив, — це виявлення аномалій.

Семінарське заняття № 11 – 2 години

Учбові питання:

1. Застосування Blockchain у морській безпеці.
2. Застосування ШІ та машинного навчання в морській безпеці.
3. Підвищення ефективності виявлення загроз і реагування на них за допомогою ШІ та машинного навчання.

Тематика рефератних повідомлень:

1. Застосування ШІ та машинного навчання в морській безпеці для здійснення спостереження.
2. Застосування ШІ та машинного навчання в морській безпеці для виявлення аномалій.
3. Здійснення прогнозного моделювання та аналізу даних з використанням ШІ та машинного навчання.
4. Здійснення ідентифікації суден, що відхиляються від нормальної поведінки або беруть участь у незаконній діяльності, за допомогою ШІ та машинного навчання.

Питання для самоконтролю:

1. У чому полягає сутність технології блокчейн?
2. Чому сприяє використання блокчейн, коли зацікавлені сторони морської безпеки створюють безпечний і незмінний запис про власність, реєстрацію та історію експлуатації судна?
3. Яким чином за допомогою блокчейн полегшується відстеження та моніторинг суден, вантажів і портових операцій у режимі реального часу?
4. Яким чином застосування блокчейн може зменшити адміністративне навантаження та підвищити безпеку ланцюжка постачання?
5. Яким чином застосування блокчейн сприяє автентифікації та верифікації морських активів і документів?
6. Яким чином застосування блокчейн сприяє управлінню ланцюгами поставок?
7. Як за допомогою блокчейн можна сприяти безпечним та ефективним транзакціям у морській галузі?
8. Як здійснити підвищення кібербезпеки в морській галузі за допомогою блокчейн?
9. У яких сферах морської безпеки штучний інтелект успішно застосовується сумісно з машинним навчанням?

Семінарське заняття № 12 – 2 години

Учбові питання:

1.Вступ до IoT у морській безпеці.
2. Застосування інтернету речей у морській безпеці.
3.Удосконалення моніторингу та спостереження за допомогою Інтернету речей

у морській безпеці.

Тематика рефератних повідомлень:

1. Сутність застосування інтернету речей у морській безпеці.
2. Технологія здійснення моніторингу і спостереження за суднами та морською інфраструктурою за допомогою інтернету речей.
3. Роль технології інтернету речей у впровадженні розумних портів.
4. Виклики, що супроводжують впровадження інтернету речей у безпеку на морі.

Питання для самоконтролю:

1. Які потреби зробили Інтернет речей потужним інструментом у морській безпеці?
2. Яким чином організується моніторинг і спостереження за суднами та морською інфраструктурою за допомогою Інтернету речей?
3. Як фізично розташовується інтернет речей для організації морської безпеки?
4. У чому полягає революція, яку здійснив інтернет речей у морській безпеці?
5. Яким чином та які переваги може надати поєднання блокчейн та інтернету речей для морської безпеки?
6. Які саме аспекти забезпечує інтернет речей при створенні «розумних портів»?
7. Які можливості надає інтернет речей щодо відстеження вантоажіві?
8. Які проблеми виникають при впровадженні інтернету речей у безпеку на морі?

Тема № 6. Новітні технології у морській безпеці (частина 2).
(Перспективи застосування аналізу даних, прогнозного моделювання та квантових обчислень у системі морської безпеки)

Сутність аналітики даних. Сутність прогнозного моделювання. Сутність квантових обчислень. Кубіти та суперпозиція. Квантові обчислення та криптографія. Квантові обчислення та технологія блокчейн, штучний інтелект (AI), машинне навчання та Інтернет речей (IoT).

Особливості квантових обчислень, важливі для застосування у морській безпеці. Принцип криптографії на базі квантових обчислень. Протоколи квантового розподілу ключів. Квантові обчислення підвищення ефективності морських операцій. Квантові обчислення та оптимізація морської логістики та управління ланцюгом поставок. Квантові алгоритми для оптимізації маршрутизації та планування суден, мінімізації споживання палива, скорочення викидів парникових газів і підвищення загальної ефективності роботи. Квантові обчислення та розширення можливостей систем морського спостереження.

Квантові обчислення у розвитку морської кібербезпеки. Квантові алгоритми для виявлення та оцінки вразливості для захисту критичної морської інфраструктури. Алгоритми квантового машинного навчання – для виявлення аномалій і виявлення потенційних порушень безпеки. Вразливість до атак шифрування, заснованого на асиметричному алгоритмі RSA (Rivest, Shamir и Adleman), при застосуванні класичних комп’ютерів. Перевага квантових

обчислень – прискорення шифрування через паралельні обчислення завдяки концепції квантової суперпозиції. Підвищення ефективності ідентифікації кіберзагроз через прискорення шифрування через аналіз великої кількості даних в реальному часі.

Теоретичні знання: у наслідку вивчення даної теми здобувачі вищої освіти повинні знати поняття «аналіз даних», «прогнозне моделювання», «квантові обчислення», переваги застосування квантових обчислень, сфери діяльності у забезпеченні морської безпеки, які можуть бути здійснені завдяки квантовим обчисленням.

Практичні навички: по вивченні даної теми необхідно вміти надати характеристику технологіям «аналіз даних» і «прогнозне моделювання» та охарактеризувати можливості покращення оцінки ризиків і прийняття рішення за їх допомогою, обґрунтувати перспективи застосування квантових обчислень для підвищення рівня морської безпеки.

Методичні рекомендації

При вивченні даної теми у першу чергу слід звернути увагу на те, що аналітика даних передбачає вилучення значущої інформації з великих і складних наборів даних, яких у морській галузі дуже багато. Використовуючи вдосконалені алгоритми та статистичні методи, аналітика даних дозволяє ідентифікувати моделі, тенденції та аномалії, які інакше було б важко виявити. У сфері морської безпеки ця технологія відіграє вирішальну роль у виявленні потенційних загроз, прогнозуванні майбутніх ризиків та оптимізації заходів безпеки.

Не слід обходити увагою й прогнозне моделювання, яке використовує історичні дані для створення моделей, які можуть прогнозувати майбутні події чи результати з певним ступенем точності. Аналізуючи минулі інциденти та фактори, що їх спричинили, прогностичні моделі можуть допомагати фахівцям із морської безпеки приймати обґрунтовані рішення та вживати профілактичних заходів для запобігання порушенням безпеки. У цьому підрозділі будуть розглянуті різні техніки та методології, що використовуються в прогнозному моделюванні, такі як регресійний аналіз, аналіз часових рядів і алгоритми машинного навчання. Тут доводиться повернутися до блокчейну, штучного інтелекту, машинне навчання та Інтернету речей, але у даному випадку – для подальшого розширення можливостей аналітики даних і прогнозного моделювання. Аналітика даних передбачає систематичний аналіз величезних обсягів даних для виявлення закономірностей, тенденцій і аномалій. У контексті морської безпеки це може виявитися неоціненним у прогнозуванні та запобіганні порушенням безпеки, забезпеченні безперебійного руху товарів і послуг у міжнародних водах.

Слід мати на увазі, що, використовуючи технологію блокчейн, фахівці з морської безпеки можуть безпечно збирати та зберігати дані, пов’язані з маршрутами судноплавства, вантажними маніфестами та відстеженням суден. Потім ці дані можна проаналізувати за допомогою інструментів аналітики

даних для виявлення будь-яких підозрілих дій або розбіжностей, що дозволить своєчасно втручатися та запобігати потенційним загрозам безпеці.

Розглянутий у попередній темі Інтернет речей, завдяки інтеграції пристроїв, таких як датчики та камери на суднах і в портах, фахівці з морської безпеки можуть збирати дані в режимі реального часу про різні параметри, такі як розташування судна, температура та статус вантажу. Потім ці дані можна проаналізувати за допомогою аналізу даних, щоб виявити будь-які аномалії або порушення безпеки. Отже аналітика даних і прогнозне моделювання стали незамінними інструментами безпеки на морі.

Окремої уваги слід приділити квантовим обчисленням. Останні пропонують неперевершену обчислювальну потужність, дозволяючи професіоналам із морської безпеки аналізувати величезні обсяги даних у режимі реального часу. Це може значно підвищити ефективність і точність систем виявлення загроз і реагування на них, роблячи морські операції більш безпечними та надійними. Квантові обчислення використовують принципи квантової механіки, які керують поведінкою частинок у найменшому масштабі. На відміну від класичних комп'ютерів, які використовують біти для зберігання та обробки інформації, квантові комп'ютери використовують квантові біти або кубіти. Кубіти можуть існувати в кількох станах одночасно завдяки властивості, яка називається суперпозиція. Ця унікальна характеристика дозволяє квантовим комп'ютерам виконувати складні обчислення та вирішувати проблеми, які виходять за межі можливостей класичних комп'ютерів. Квантові обчислення також можуть сприяти розвитку розглянутих вище нових технологій безпеки на морі, такихяк технологія блокчейн, штучний інтелект і машинне навчання, а також Інтернет речей. Отже, квантові обчислення є трансформаційною технологією, яка має потенціал революціонізувати різні аспекти морської безпеки.

Семінарське заняття № 13 – 2 години

Учбові питання:

1. Аналіз даних та прогнозне моделювання
2. Застосування ШІ та машинного навчання в морській безпеці
3. Покращення оцінки ризиків і прийняття рішень за допомогою прогнозного моделювання

Тематика рефератних повідомлень:

1. Використання штучного інтелекту та машинного навчання для аналізу історичних та виявлення закономірностей, як ознак ризиків безпеці.
2. Прогнозне моделювання у сфері морської безпеки.
3. Застосування прогнозного моделювання для ідентифікації та запобігання загрозам морської безпеки.
4. Прогнозне моделювання у виявленні шахрайства та незаконних дій, пов'язаних з морським транспортом.
5. Аналіз даних та морська безпека.

Питання для самоконтролю:

1. У чому полягає сутність аналітики даних?

2. Яким чином поєднання можливостей блокчейн та інструментів аналітики сприятиме своєчасному втручанню та запобіганню потенційних загроза безпеці?

3. Яким чином застосування технології інтернету речей на суднах у поєднанні з аналітикою сприятиме виявленню критичних аномалій та порушень умов безпеки?

4. Яким чином застосування квантових обчислень може підвищити ефективність і точність систем виявлення загроз і реагування на них?

5. У чому полягає сутність прогнозного моделювання?

6. Яким чином прогнозне моделювання допомагає оптимізувати розподіл ресурсів, а також планувати реагування?

7. Яким чином застосування прогнозного моделювання сприяє ефективному зменшенню ризиків ?

8. Яким чином прогнозне моделювання сприяє виявленню шахрайства та незаконних дій?

Семінарське заняття № 14 – 2 години

Учбові питання:

1.Вступ до квантових обчислень.

2.Потенційне застосування квантових обчислень у морській безпеці.

3.Покращення шифрування та кібербезпеки за допомогою квантових обчислень.

4. Майбутні напрямки досліджень і розробок.

Тематика рефератних повідомлень:

1. Криптографія на підставі квантових обчислень у забезпеченні морської безпеки

2. Квантові обчислення в оптимізації морської логістики та управлінні ланцюгом поставок.

3. Квантові обчислення у вдосконаленні морського спостереження.

для самоконтролю:

1. У чому полягає сутність квантових обчислень? На яких принципах вони ґрунтуються?

2. У якому сенсі квантові комп’ютери ламають традиційні алгоритми шифрування?

3. Покращення яких технологій може здійснюватись на підставі квантових обчислень?

4. Які сфери інформаційної діяльності можуть бути вдосконалені через застосування квантових обчислень?

5. Яким чином квантові обчислення можуть покращити морську логістику?

6. Як саме квантові обчислення можуть сприяти оптимізації маршрутизації та суден?

7. Яким чином квантові обчислення можуть розширити можливості систем морського спостереження?

8. Які небезпеки, зазвичай, підлягають спостереженню у сфері морської безпеки?

4. ПЕРЕЛІК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Конституція України: Закон України від 28.06.1996. № 254к/96. Дата оновлення: 01.01.2020. URL:. https://zakon.rada.gov.ua
2. Кодекс торговельного мореплавства України від 21 жовтня 1997 року N 590/97-ВР. Дата оновлення: 10.10.2024. URL: https://ips.ligazakon.net.
3. Про інформацію Закон України від 02.10.1992 № 2657-12. Дата оновлення: 01.01.2023. URL: https://zakon.rada.gov.ua
4. Про Національну програму інформатизації: закон України від 04.02.1998 № 74/98-ВР. URL: https://zakon.rada.gov.ua
5. Про морські порти України: Закон України від 4 липня 2013 року N 406-VII.
6. Про науково-технічну інформацію: Закон України від 25.06.1993 № 3322-XII URL: https://zakon.rada.gov.ua
7. Закон України « Про хмарні послуги» від 17.02.2022 № 2075-IX**.** URL: https://zakon.rada.gov.ua/laws
8. Закон України «Про захист персональних даних» від 01.06.2010 № 742297-17. URL: http://zakon.rada.gov.ua/laws
9. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017. № 2163- VIII. URL: http://zakon.rada.gov.ua/laws
10. Блінцов О.В. Проблеми забезпечення інформаційної безпеки на водному транспорті в сучасних умовах. Сучасні проблеми інформаційної безпеки на транспорті. *ІІ всеукраїнська науково-технічна конференція з міжнародною участю* URL: web-site: conference.nuos.edu.ua
11. Бурячок В.Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект. Підручник За загальною редакцією доктора технічних наук, професора В. Б. Толубка. Київ:ДУТ.2015. 288с.
12. Волянська Я.Б., Калініченко Є.В., Логінов О.В. Використання інформаційних технологій на водному транспорті та перспективи їх розвитку. *Scientific Notes of Taurida National V I Vernadsky University Series Economy and Management* 33(72)(3): August 2022. 99-105
13. Грохольський В.Л., Ісмайлов К.Ю., Форос Г.В. Науково-практичний коментар до Закону України «Про основні засади забезпечення кібербезпеки України» / за заг. ред. д. ю. н., проф. В. Л. Грохольського. Одеса. ОДУВС, 2020. 142 с.
14. Євтушевська О.А. Інформаційна безпека як елемент підвищення ефективності комплексного контролю підприємств водного транспорту. *Зовнішня торгівля: економіка, фінанси, право. Науковий журнал. Серія: Економічні науки. ISSN* 1028-7507 №5-6. 2015. С. 82-83
15. Карпенко О.О. Аналіз досвіду використання інформаційно-комунікаційних технологій у портах світу. *Економіка і суспільство*. Випуск # 15 / 2018. С. 130-137.

16. Кульбацький А.А. Підвищення ефективності судноводіння на водних шляхах України з застосуванням сучасних інформаційних технологій. Дисертація на здоб. ступеня канд. техн. наук. *НУ «Одеська морська академія»*. Одеса. 2021. 292 с. URL : http://onma.edu.ua/wp-content/uploads/2016/09/dysser-1-1a.pdf (дата звернення: 07.05.2023).
17. Мельник О.М., Волошин А.О., Онищенко О.А. Організація забезпечення інформаційної безпеки морського судна. *Збірник наукових праць Українського державного університету залізничного транспорту*. 2022, Вип. 201. С. 69-78.
18. Пядишев В.Г, Питання вдосконалення кібербезпеки морського транспорту. *Морська безпека та оборона* №1, 2023. С. 52-59.
19. Слюсаренко А.І.Впровадження та вплив кібер-безпеки на сучасне технічне обслуговування обладнання суден і судноплавних компаній. Λόγοσ.online (2020). Сайт. URL:https://www.ukrlogos.in.ua/10.11232-2663-4139.10.16.html
20. Трофіменкоа.О.,Майданевич С.В., Войчсенко Т.О., Дорофєєва З.Я. Деякі проблемні питання впровадження стандартів кібербезпеки на морському транспорті. *Водний транспорт №1 (37)2023*. С. 87-94.
21. A Comprehensive Guide to Maritime Cybersecurity. URL: https://www.missionsecure.com/maritime-security-perspectives-for-a-comprehensive-approach
22. Cybercrime Emerges as New Maritime Security Threat. *ADF-Magazine.Com*. Dec 5, 2023. Site. URL: https://adf-magazine.com/2023/12/cybercrime-emerges-as-new-maritime-security-threat
23. Cybersecurity for the maritime industry. *Maritime-Cybersecurity.Com*. Site. URL : https://www.maritime-cybersecurity.com/ (дата звернення: 07.05.2023).
24. DNV Maritime Cyber Priority 2023: Shipping faces 5 major cyber security challenges. The Editorial Team June in Cyber Security. *Safety4Sea*. 7, 2023. Site. URL: https://safety4sea.com/dnv-maritime-cyber-priority-2023-shipping-faces-5-major-cyber-security-challenges
25. Farrell R. Maritime Terrorism: Focusing on the Probable. *Naval War College Review, Vol. 60, No. 3* (Summer 2007), pp. 46-60 (15 pages). Site. URL: https://www.jstor.org/stable/26396848?seq=1
26. Guide to Ship Cybersecurity. Last updated on Feb 26, 2023. Blog. Site. URL: https://www.mitags.org/guide-ship-cybersecurity
27. Hack the Port. Maritime & Control Systems. *SCADAfence. Cybersecurity Con.*2022. 16p.
28. Hayes, Christopher R. Maritime cybersecurity-the future of national security.*Commons.Wikimedia.Org*. Site. URL : https://commons.wikimedia.org/wiki/File:Maritime_cybersecurity-_the_future_of_national_security_(IA_maritimecybersec1094549484).pdf

29. Maritime cyber security. *Dnv.Com*. Site. URL:https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/index.html
30. Pandey S., Chandra M. Advancements in Maritime Security: Exploring Emerging Technologies. *Amazon Inc. September 2023*). Site. URL: https://www.researchgate.net/publication/373682954_Advancements_in_Maritime_Security_Exploring_Emerging_Technologies. (дата звернення: 07.05.2023).
31. The importance of cybersecurity in the maritime industry. *Marine-Digital.Com*. Site. URL: https://marine-digital.com/article_importance_of_cybersecurity
32. Timlen T. Maritime terrorism effectively suppressed in Asia. *RiskIntelligence.EU. 22 August 2023*. Site. URL: https://www.riskintelligence.eu/analyst-briefings/maritime-terrorism-effectively-suppressed-in-asia

5. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ ОСВІТНЬОЇ ДІЯЛЬНОСТІ

Система оцінювання передбачає накопичення 100 балів із кожної навчальної дисципліни, які перераховуються в національну шкалу та шкалу оцінювання ЄКТС.

Оцінювання результатів вивчення навчальної дисципліни у формі заліку.

Підсумковий контроль у формі заліку проводиться після проведення всіх видів занять передбачених робочою навчальною програмою відповідної освітньої компоненти.

Оцінювання здійснюється за результатами накопичених балів з аудиторної та самостійної робіт.

Результати навчання з аудиторної роботи обчислюються за таким алгоритмом:

- результат аудиторної роботи визначається, як середній бал помножений на коефіцієнт 16 та заокруглюється до цілого балу за математичними правилами (до 0,4 включно – до попереднього цілого числа, 0,5 і більше – до наступного цілого числа);

- середній бал дорівнює сумі усіх одержаних позитивних оцінок (балів) поділених на відповідну кількість, при цьому:

а. мінімальна кількість оцінок має складати не менше 1/3 (33 %) від загальної можливої кількості занять (семінарських, практичних, лабораторних) передбачених робочою навчальною програмою навчальної дисципліни. Якщо 1/3 (33 %) від кількості занять складає дробове число, то до розрахунку береться наступне ціле число;

б. якщо кількість отриманих оцінок менша за 1/3 (33 %), то кожна недостаюча оцінка враховується, як «нуль» балів;

в. кількість позитивних оцінок, які перевищують визначену мінімальнодопустиму («додаткових») враховуються з коефіцієнтом 0,5, такий коефіцієнт застосовується з метою мотивування здобувачів вищої освіти до покращення результатів оцінювання за аудиторну роботу;

г. невідпрацьовані «незадовільні» оцінки та пропущені заняття враховуються як «нуль» балів;

д. відпрацювання усіх «незадовільних» оцінок та пропущених занять не є обов’язковим.

У випадку, якщо за результатами оцінювання аудиторної роботи сума накопичувальних балів перевищує 80, то здобувачу вищої освіти нараховується максимально допустимий результат – 80 балів.

Формула розрахунку:

$$РАР = \frac{СОБ}{МКО + КДО*0,5+КНО} * 16$$

де:

- РАР – результат аудиторної роботи;

- СОБ – сума отриманих оцінок у балах;
- МКО – мінімальна кількість оцінок (1/3 (33 %) від кількості семінарських, практичних, лабораторних занять передбачених робочою навчальною програмою навчальної дисципліни). При цьому, якщо МКО складає дробове число, то до розрахунку береться наступне ціле число;
- КДО – кількість «додаткових» оцінок – оцінок, що перевищують МКО;
- КНО – кількість невідпрацьованих «незадовільних» оцінок та невідпрацьованих пропущених занять.

Загальна кількість балів за самостійну роботу визначається, як сума отриманих балів за виконання видів робіт, передбачених робочою навчальною програмою навчальної дисципліни.

Підсумкова кількість балів отриманих під час складання заліку визначається, як сума отриманих балів за аудиторну (максимум 80 балів) та самостійну роботу (максимум 20 балів.

Поточний контроль		**Підсумковий контроль (ПК)**
Аудиторна робота (РАР) (семінарські/практичні заняття та контрольні заходи)	**Самостійна робота (РСР)**	ЗАЛІК (З)
≤ 80	≤20	
≤ 100		
Підсумкова кількість балів = РАР+РСР ≤ 100		

У разі, якщо здобувач вищої освіти під час складання заліку отримав менше 60 балів – «не зараховано» він ліквідовує академічну заборгованість за окремим графіком на вище визначених умовах.

Такий здобувач повинен покращити результати поточного контролю (відпрацювати пропущені заняття та/або незадовільні оцінки, відпрацювати тему для одержання оцінки, виконати самостійну роботу тощо) до моменту ліквідації академічної заборгованості.

У разі повторного не складання заліку ліквідація академічної заборгованості здійснюється перед комісією без врахування результатів навчання отриманих за результатами аудиторної та самостійної роботи за 100 бальною шкалою. При ліквідації академічної заборгованості перед комісією здобувач вищої освіти може одержати не більше 70 балів.

Здобувач вищої освіти, як додатковий здобуток може отримати додаткові бали, при цьому загальна сума накопичувальних балів не повинна перевищувати 100:

- за наукову роботу в межах навчальної дисципліни до 10-ти балів;
- за проходження тренінгу за тематикою навчальної дисципліни та отриманні сертифікату до 5-ти балів.

З метою підвищення поточного рейтингу успішності здобувач вищої освіти має право перескладати аудиторну та самостійну роботу відповідно до

графіка, встановленого науково-педагогічним працівником до підсумкового контролю, і не більше двох пропусків та/або незадовільних оцінок з однієї навчальної дисципліни в один робочий день.

Відсутність здобувача вищої освіти на підсумковому контролі без поважної причини, прирівнюється до незадовільної оцінки. Такий здобувач вищої освіти має право скласти підсумковий контроль під час ліквідації академічної заборгованості, визначеної окремим графіком.

Здобувач вищої освіти зобов'язаний попередити деканат про свою можливу відсутність на підсумковому контролі до його початку. Здобувач вищої освіти, який був відсутній на підсумковому контролі з поважних причин, які підтверджені відповідними документами, за рішенням декана факультету (директора інституту, керівника відділу докторантури та аспірантури) може скласти пропущений підсумковий контроль у визначений час.

Здобувач вищої освіти, який за результатами поточного та підсумкового контролю сумарно накопичив менше 60-ти балів, допускається до повторного перескладання підсумкового контролю після закінчення екзаменаційної сесії, але до початку наступного семестру чи атестації.

Критерії оцінювання знань на заліку

Оцінка «відмінно»/ A – виставляється, якщо здобувач вищої освіти має глибокі і системні знання, вміє узагальнювати теоретичний матеріал, співвідносити загальні знання з конкретними ситуаціями; оволодів навиками аналізу, моделювання та адекватного оцінювання ситуації; обізнаний з науковими працями вітчизняних та зарубіжних фахівців в цій галузі; матеріал викладає логічно, послідовно, переконливо і аргументовано.

Оцінка «добре»/ B,C – виставляється, якщо здобувач вищої освіти показав достатній рівень знання курсу; надав правильні, але не зовсім повні визначення термінів; засвоїв основи аналітичного методу; допускає незначні неточності в розкритті окремих теоретичних положень.

Оцінка «задовільно»/ D, E – виставляється, якщо здобувач вищої освіти в цілому засвоїв теоретичний матеріал курсу навчальної дисципліни, але декламує із деякими упущеннями при визначенні основних явищ та процесів; намагається висловити своє ставлення до проблемних питань, хоча і не зовсім аргументовано; вміє аналізувати набуті теоретичні знання і співвідносити їх з конкретними ситуаціями; викладає матеріал непослідовно, неточно, з наявними помилками.

Оцінка «незадовільно»/ FX,F – виставляється, якщо здобувач вищої освіти виявив слабкі (відсутні) знання теоретичного матеріалу навчальної дисципліни; не зміг дати визначення основних категорій та явищ; відсутні знання основних норм і визначень; матеріал викладається непослідовно, нелогічно, фрагментарно та з допущенням помилок.

Оцінка «зараховано» / A, B, C, D, E – виставляється, якщо здобувач вищої освіти виявив достатньо повні знання матеріалу навчальної дисципліни; вміє узагальнювати теоретичний матеріал, співвідносити загальні знання з конкретними ситуаціями, дає правильні, хоча і не завжди повні відповіді на

оставлені запитання; припускається помилок у розкритті окремих теоретичних положень, норм та визначень.

Оцінка «не зараховано»/ FX,F – виставляється, якщо здобувач вищої освіти виявив слабкі знання; не зміг дати визначення основних термінів та понять; викладає матеріал непослідовно, нелогічно, фрагментарно, неточно, стисло; відсутня переконливість у викладенні матеріалу.

Шкала оцінювання: національна та ECTS

<table>
<tr><th>За внутрішньою шкалою закладу вищої освіти в балах</th><th colspan="2">За шкалою ECTS /За національною шкалою</th></tr>
<tr><td></td><td colspan="2">Вноситься до відомості</td></tr>
<tr><td></td><td>Екзамен</td><td>залік</td></tr>
<tr><td>90 – 100</td><td>A/Відмінно</td><td rowspan="5">A,B,C,D,E/Зараховано</td></tr>
<tr><td>82-89</td><td>B/Добре</td></tr>
<tr><td>75-81</td><td>C/Добре</td></tr>
<tr><td>64-74</td><td>D/Задовільно</td></tr>
<tr><td>60-63</td><td>E/Задовільно</td></tr>
<tr><td rowspan="2">35-59</td><td>FX/Незадовільно</td><td>FX/Не зараховано</td></tr>
<tr><td colspan="2">з можливістю повторного складання</td></tr>
<tr><td rowspan="2">0-34</td><td>F/Незадовільно</td><td>F/Не зараховано</td></tr>
<tr><td colspan="2">з обов’язковим повторним курсом</td></tr>
</table>

6. ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ

1. Надайте визначення поняття «безпека на морі».
2. Який сенс має англомовний термін «security»?
3. Який сенс має англомовний термін «safety»?
4. Які версії терміну «безпека на морі» вам відомі?
5. Які ризики морській безпеці вам відомі?
6. Які вантажі створюють високий рівень небезпеки на морі?
7. Для яких нелегальних цілей використовувались цивільні морські судна?
8. Яку площу може охопити вибух судна зі зрідженим природним газом?
9. Перелічить та поясніть атрибути кібербезпеки.
10. Поясніть вразливі місця та загрози з точки зору кібербезпеки.
11. Перелічить відомі Вам способи кібератак.
12. Які вектори кібератак вам відомі?
13. Перелічить відомі вам вразливі об’єкти судна.
14. Засоби забезпечення інформаційної безпеки судна.
15. У чому полягає концептуальна модель безпеки судна?
16. У чому полягає сучасний підхід до захисту та базові принципи забезпечення інформаційного захисту судна?
17. Обґрунтуйте важливість портів.
18. Поясніть поняття порту як кіберфізичного середовища.
19. Порти та кібербезпека.
20. Які сценарії кібератак на порти Вам відомі?
21. Поясніть призначення кодексу ISPS.

22. Який орган є правоохоронним органом в порту у морському судноплавстві в більшості країн світу?
23. Поясніть можливості системи автоматичної радіолокаційної допомоги (ARPA).
24. Поясніть призначення та можливості системи автоматичної ідентифікації (AIS).
25. Поясніть призначення та можливості інтегрованої система мосту або інтегрованої навігаційної системи
26. Поясніть, як здійснюється далека ідентифікація та відстеження за допомогою LRIT.
27. Поясніть сутність та задачі служби безпеки руху суден.
28. Поясніть сутність та задачі системи дистанційного керування морськими транспортними засобами (ROV).
29. Поясніть призначення та сутність перевірки та ідентифікації персоналу.
30. Поясніть призначення та сутність перевірки та ідентифікації пасажирів.
31. Поясніть роботу безпечної система огляду людей SPO-20.
32. Поясніть, як сучасними методами здійснюється сканування контейнерів.
33. Поясніть, як сучасними методами здійснюється відстеження контейнерів.
34. Поясніть сутність технології NANO у забезхпеченні безпеки контейнерів.
35. Поясніть роботу антитерористичної системи виявлення водолазів Cerberus360.
36. Поясніть роботу захисту судна електричними огорожами.
37. Надайте основні характеристики висотного безпілотного літального апарату (БПЛА) тривалої дії.
38. Опишіть патрулювання чутливих зон за допомогою безпілотного надводного судна танадайте його зарактеристики.
39. Поясніть сучасні методи спостереження за портом і каналом.
40. Поясніть сутність технології блокчейн.
41. Опишіть можливості застосування Blockchain у морській безпеці.
42. Поясніть сутність штучного інтелекту.
43. Поясніть сутність машинного навчання.
44. За якими напрямами передбачається застосування ШІ в морській безпеці?
45. За якими напрямами передбачається застосування машинного навчання в морській безпеці?
46. Як забезпечується покращення виявлення загроз і реагування за допомогою ШІ та машинного навчання?
47. Поясніть сутність Інтернету речей (IoT).
48. Поясніть застосування Інтернету речей (IoT) у морській безпеці.
49. Поясніть сутність удосконалення моніторингу та спостереження за допомогою Інтернету речей у морській безпеці.
50. Поясніть сутність прогнозного моделювання.
51. Поясніть сутність аналізу даних.
52. Поясніть застосування ШІ в морській безпеці.
53. Поясніть застосування машинного навчання в морській безпеці.

54. Поясніть сутність покращення оцінки ризиків і прийняття рішень за допомогою прогнозного моделювання.
55. Поясніть сутність прогнозного моделювання.
56. Поясніть сутність квантових обчислень.
57. Поясніть потенційне застосування квантових обчислень у морській безпеці.
58. Обґрунтуйте покращення шифрування та кібербезпеки за допомогою квантових обчислень.
59. Визначить майбутні напрямки досліджень і розробок.
60. Що означає термін «Доступність інформаційного ресурсу»?
61. Що з погляду морської безпеки означає термін «Загроза»?
62. Як слід тлумачити термін «Вектори атаки»?
63. Як слід тлумачити термін «Критична інфраструктура»?
64. Які компоненти сьогодні офіційно складають поняття «Морська злочинність»?
65. Надайте визначення поняття «Піратство» з точки зору морської безпеки.
66. Що означає термін «Тріада КЦД» і який сенс він має з точки зору кібербезпеки?
67. Який зміст поняття «Подія загрози» з точки зору морської безпеки?
68. Як Ви розумієте поняття «Нанотехнології»?
69. В якій сфері морської безпеки передбачається застосування нанотехнологій?

7. ГЛОСАРІЙ

Аналіз даних – процес отримання необроблених даних і подальшого перетворення їх на інформацію

Безпека на морі – стан судноплавної компанії/судна/екіпажу/порту, відчуття безпеки або безпека судноплавної компанії/судна/екіпажу/порту від таких загроз. як тероризм, піратство та інша злочинна діяльність.

Блокчейн (англ. blockchain) —технологія розподіленого цифрового реєстру, що використовується для зберігання та перевірки даних транзакцій. Це ланцюжок блоків, кожен з яких містить інформацію про транзакції, які відбулися, а також криптографічний ключ, який зв'язує його з попереднім блоком.

Вектори атаки – це шляхи для отримання доступу до цілі, які використовують зловмисники.

Вразливі об'єкти судна ***(з*** погляду кібербезпеки) – різні системи судна, що керуються та контролюються відповідним програмним забезпеченням, інформаційними системами.

Вразливість – це слабке місце в інформаційній системі, її процедурах безпеки, внутрішньому контролі або реалізації, які можуть бути використані загрозою.

Доступність – властивість інформаційного ресурсу, яка полягає в тому,

що користувач та/або процес, який володіє відповідними повноваженнями, може використовувати цей ресурс відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого (прийнятного) інтервалу часу.

Загроза – це обставина або подія, яка потенційно може негативно вплинути на діяльність та активи організації, окремих осіб, інші організації чи країну через несанкціонований доступ, знищення, розкриття, модифікацію або відмову в обслуговуванні інформаційної системи. Загрози можуть бути

Збройне пограбування суден – незаконний акт насильства або затримання, або погрози або крадіжки, спрямовані проти судна, людей або майна на борту. Це може бути і в межах національної юрисдикції держави, і в інших випадках, передбачених міжнародним правом.

Зловмисник – це сторона, яка атакує хост, мережу чи інші IT-ресурси.

ЗМЗ – зброї масового знищення.

ЗМІ (Засоби масової інформації) – різновид медіа, орієнтований на одночасне передавання інформації великим групам людей.

Інформаційна інфраструктура (англ. information infrastructure) – комплекс програмно-технічних засобів, організаційних систем та нормативних баз, який забезпечує організацію взаємодії інформаційних потоків, функціонування та розвиток засобів інформаційної взаємодії та інформаційного простору країни або організації.

Квантові обчислення – тип обчислень, що діє не за стандартними математичними алгоритмами, а використовує переваги квантових механічних явищ,

КІ (Критична інфраструктура) – це сукупність об'єктів та систем, які є надзвичайно важливими для функціонування суспільства та економіки країни. У разі їхнього порушення або руйнування може мати значний негативний вплив на безпеку, економіку, здоров'я та життя людей.

Кібератака — спроба реалізації інформаційної загрози.

Кібербезпека –це захист інформаційних систем (апаратного забезпечення, програмного забезпечення та пов’язаної інфраструктури), даних у них і послуг, які вони надають, від несанкціонованого доступу, шкоди чи неправильного використання.

Конфіденційність – (від латинського confidentia - довіра) - це властивість інформації або даних, яка характеризується необхідністю запобігти їх розголошенню або витоку. Це означає, що доступ до такої інформації має бути обмежений, і доступ до неї повинні мати лише ті особи, які мають на це право.

Машинне навчання – галузь штучного інтелекту, що зосереджена на розробці алгоритмів, здатних вчитися на даних і покращувати свою продуктивність без явного програмування.

Міжнародне морське публічне право –регламентує відносини між державами з питань використання світового океану.

Моделювання – метод пізнання та дослідження, що передбачає створення і вивчення моделей реальних об'єктів, явищ або процесів.

Моніторинг – система систематичного спостереження за певними явищами, процесами або об'єктами з метою виявлення їхніх змін, тенденцій та закономірностей.

Морська безпека – сукупність заходів, спрямованих на забезпечення захисту людського життя, здоров'я, майна та навколишнього середовища на морі, а також сталого розвитку морської та річкової держави

Морська злочинність – охоплює широкий спектр злочинної діяльності, що вчиняється на морі або пов'язана з морем, і є значною загрозою для світової торгівлі та міжнародної безпеки. Ці злочини включають піратство, незаконний риболовний промисел, контрабанду та тероризм.

Морське право (міжнародне морське право) — підгалузь міжнародного приватного права, що регулює майнові відносини, ускладнені іноземним елементом, що виникають у процесі міжнародного економічного обороту та пов'язані з використанням моря.

Морський транспорт – будь-яке судно, здатне пересуватися водною поверхнею (морів, океанів і прилеглих акваторій), а також просто перебувати на плаву.

Нанотехнології – це галузь науки та техніки, яка займається розробкою, виготовленням та застосуванням матеріалів, пристроїв і систем, функціонування яких визначається їхньою наноструктурою (розміром від 1 до 100 нанометрів).

Піратство — це будь-який неправомірний акт насилля, затримання або будь-який грабіж, що здійснюється з приватною метою екіпажем або пасажирами будь-якого приватного судна проти будь-якого судна, особи або майна на борту судна.

Подія загрози – це ситуація або подія, спричинена загрозою, що має потенціал несприятливого впливу.

Політичний екстремізм — це схильність до крайніх поглядів та дій у політиці, що часто виявляється в агресивних та деструктивних способах досягнення політичних цілей. Він характеризується крайніми, іноді насильницькими методами, та може включати загрози чи насилля щодо тих, хто не поділяє екстремістські ідеї.

Прогнозне моделювання – моделювання, що ґрунтується на результатах, які на момент прийняття рішення ще невідомі або знаходяться в недосліджуваному діапазоні значень аргументів.

Ризики морської безпеки – широкий спектр потенційних загроз та небезпек, що можуть впливати на морську діяльність, включаючи, але не обмежуючись, безпеку суден, особового складу, портів та морського транспорту.

Рівень впливу загрозливої події – це величина шкоди, яку можна очікувати в результаті наслідків неавторизованого розкриття, модифікації, знищення або втрати інформації чи втрати доступності інформаційної системи.

Середовище безпеки – поняття, що служить для обмеження (визначення) сфер безпеки суднових систем.

Спостереження – процес активного, систематичного та цілеспрямованого сприйняття об'єктів та явищ, що дає змогу отримати знання про їх властивості та взаємозв'язки.

Суб'єкт загрози – це фізична чи юридична особа, яка реалізує загрозу кібербезпеці, є відповідальною за інцидент, і може бути внутрішньою або зовнішньою щодо організації.

Судно – плавзасіб, призначений для транспортних, промислових, військових, наукових, спортивних та інших цілей.

Тероризм (лат. terror — жах) — у широкому сенсі використання або загроза застосування насильства для досягнення політичної, релігійної або ідеологічної мети.

Тероризм танкерів (або терористичні дії, що спрямовані на танкери) — використання або загроза насильства щодо танкерів (суден, що перевозять нафту та інші нафтопродукти) для досягнення політичних, релігійних або ідеологічних цілей.

Технологія блокчейн —це, по суті, децентралізована та розподілена система реєстру, яка дозволяє записувати та перевіряти транзакції прозоро та безпечно.

Тріада КЦД (конфіденційність, цілісність, доступність) – це парадигма, призначена для регулювання правил інформаційної безпеки

Цілісність даних – це внутрішня єдність, пов'язаність усіх частин чого-небудь, єдине ціле. Це може стосуватися як фізичних об'єктів (наприклад, незламність мосту), так і більш абстрактних понять, таких як особистість, мораль або інформація.

ШІ (штучний інтелект) – галузь інформатики, що розробляє системи, здатні виконувати завдання, які зазвичай потребують людського інтелекту.

ШПЗ (шкідливе програмне забезпечення) – зловмисне програмне забезпечення, призначене для отримання доступу до комп'ютера, сервера чи мережі або заподіяння їм шкоди без відома жертви.

ACSD (Advanced Container Security Device) – пристрій розширеного контролю безпеки контейнерів. Удосконалений пристрій безпеки контейнерів. Використовується для контролю фізичного стану вантажних контейнерів, виявлення втручань та потенційної ідентифікації присутності людини всередині контейнера. Це допомагає запобігти крадіжкам, контрабанді та іншим ризикам безпеки.

AIS (англ. Automatic Identification System) – автоматична ідентифікаційна система, яка служить для ідентифікації суден, їх габаритів, курсу та інших даних з використанням ультра коротких радіохвиль, призначена для роботи на коротких відстанях (на відміну від LRIT, що на довгих).

APT (Advanced Persistent Threat) – просунута стійка загроза – такі атаки є широко визнаним найскладнішим найпотужнішим класом загроз безпеці.

ARPA (Automatic Radar Plotting Aid) - це автоматична система, яка використовується на судах для обробки інформації з радара, щоб допомогти штурману уникати зіткнень та покращити навігацію.

ATT (ADMIRALTY TotalTide) –«адміралтійський загальний приплив» – система, що надає командам капітанських містків швидкі та точні прогнози висоти припливів та припливних течій для понад 7000 портів та 3000 припливних течій

Cerberus360 – Антитерористична система виявлення водолазів.

CLIA (Cruise Lines International Association) - Міжнародна асоціація круїзних ліній.

CMI (франц. Comité Maritime International) – Міжнародний морський комітет.

CSI (the Container Security Initiative) – Ініціатива з безпеки контейнерів (CSI), започаткована у 2002 р. з метою посилення безпеки контейнерних вантажів, що перевозяться до США.

DGPS (Differential Global Positioning System) – диференціальна система глобального позиціонування, підвищує точність GPS-позиціонування, використовуючи корекції від фіксованих опорних станцій, що покращує точність визначення місцезнаходження судна.

ECDIS (Electronic Chart Display and Information System) - електронна система відображення карт та інформації.

ECDIS (Electronic Chart Display and Information System) – електронно-картографічна навігаційно-інформаційна система – комп'ютерна система, що відображає електронні карти та іншу навігаційну інформацію, що забезпечує безпеку судноводіння.

ECS (Electronic Cards System Navigation System) – Електронна картографічна навігаційна система (ЕКНС), що використовує електронні карти для надання навігаційних даних і відображення їх на екрані, наприклад, на судні.

GMDSS (англ. Global Maritime Distress and Safety System) – глобальна морська система зв'язку у разі лиха та небезпеки.

GNSS (англ. Global navigation satellite systems) - глобальні навігаційні супутникові системи – використовують супутники для надання послуг глобального позиціонування. системи управління вантажами.

GPS (англ. Global Positioning System) – глобальна система позиціонування, що відіграє вирішальну роль у морській навігації, надаючи точні та надійні дані про місцезнаходження, швидкість та напрямок руху.

GRDU (англ. gamma radiation detection unit) – блок детектування нейтронного випромінювання у складі системи для сканування контейнера під час його переміщення.

ICSO (англ. the International Container Standardization Organization) – не є офіційно визнаною організацією, відповідає за розробку та публікацію міжнародних стандартів, зокрема стандартів для вантажних контейнерів.

ILO (англ. International Labor Organization) – Міжнародна організація праці.

IMB (англ. International Maritime Bureau) – Міжнародне морське бюро – це, по суті, Міжнародна морська організація (IMO).

IMO (англ. International Maritime Organization) – Міжнародна морська організація, міжурядова організація, спеціалізована установа ООН. Діяльність IMO спрямована на скасування дискримінаційних дій, що стосуються міжнародного торговельного судноплавства, а також прийняття норм (стандартів) із забезпечення безпеки на морі і запобігання забруднення з суден довкілля, в першу чергу, морського.

IoT (англ. internet of things) – Інтернет речей, мережа фізичних об'єктів ("речей"), що з'єднані через інтернет та можуть обмінюватися даними і взаємодіяти один з одним та з оточуючим середовищем.

ISO (англ. International Organization for Standardization) – Міжнародна організація зі стандартизації. Стандарти, створені нею, забезпечують основу для управління різними аспектами судноплавства та логістики, включаючи якість, безпеку, екологічні показники тощо.

ISPS (англ. International Ship and Port Facility Security Code) – Міжнародний кодекс з охорони суден і портових засобів (з 12.12.2002) – багатостороння угода.

LRIT (англ. Long-range Identification and Tracking) – система далекої ідентифікації та відстеження автоматично передає необхідну інформацію кожні 6 годин, призначена для роботи на великих відстанях (на відміну від AIS, що на коротких).

NRDU (англ. Neutron Radiation Detection Unit) – блок детектування нейтронного випромінювання у складі системи для сканування контейнера під час його переміщення.

RADAR (англ. Radio Detection And Ranging) – радіовиявлення та встановлення дальності – важливі навігаційні інструменти, що використовують радіохвилі для виявлення та відстеження інших суден, суші та потенційних небезпек.

ROV (англ. Remotely Operated Vehicle) – «дистанційно керований транспортний засіб» – система дистанційного керування морськими транспортними засобами

Safety (англ.) – запобігання нещасним випадкам.

Secure-Ship - несмертоносна електрифікуюча огорожа судна,

Security (англ.) – захист від зовнішньої загрози.

SID (англ. Seafarer's Identity Document) – посвідчення особи моряка, містить також біометричні дані, служить формою посвідчення особи моряків, подібно паспорту, і визнається на міжнародному рівні.

SOLAS (англ. International Convention for the Safety of Life at Sea) – Міжнародна конвенція з охорони людського життя на морі (з 1974 р.), суть якої полягає у її документах, що послідовно виходили і є, мабуть, найважливішою з усіх міжнародних угод з безпеки торгових суден.

SOS (англ. Send Only Scanned) – принцип, за яким контейнер слід перевантажувати та відправляти, лише якщо його було відскановано.

SPO-20 – безпечна система огляду людей для виявлення небезпеки.

SUA (англ. Convention for the Suppression of Unlawful Acts against the Safety

of Maritime Navigation) – Конвенція про боротьбу із незаконними актами проти безпеки морського судноплавства – багатосторонній договір.

SUA-88 – Міжнародна конференція 1988 р. щодо боротьби з незаконними актами, спрямованими проти безпеки морського судноплавства.

TWIC (англ. Transportation Worker Identification Credential) – посвідчення особи працівника транспорту – життєво важливий інструмент безпеки. Це посвідчення дозволяє особам отримувати доступ до безпечних зон морських об'єктів та суден без потреби в супроводі. Схему започатковано урядом США.

UNCLOS (англ. United Nations Convention on the Law of the Sea) — юридично обов'язкова для держав-учасниць міжнародна угода, що встановлює правові рамки для морської та приморської діяльності у світі, зокрема щодо використання природних ресурсів та запобігання забрудненню довкілля, а також збереження миру.

VDR (англ. Voyage data recorder) – «система навігаційного містка» – система реєстрації даних рейсу, що розроблена для всіх суден, які зобов'язані дотримуватися вимог Міжнародної конвенції SOLAS IMO.

VTMS (англ. Vessel Traffic Management System) – система управління рухом суден, використовується для управління та моніторингу руху суден у портах, гаванях та прибережних районах, підвищуючи безпеку та ефективність.

VTS (англ. Vessel Traffic Service) - служба руху суден – це система, призначена для підвищення безпеки та ефективності руху суден у певному районі, зазвичай у портах, гаванях або на жвавих водних шляхах.

WTTC (англ. World Travel & Tourism Council) – Всесвітня рада з подорожей і туризму.

Zephyr — це надлегкий літальний апарат із вуглецевого волокна, здатний літати на сонячній енергії, яка генерується масивами аморфного кремнію, встановленими на крилах літака.