Лекція1. Закон України «Про основні засади забезпечення кібербезпеки». Міжнародні норми кібербезпеки на морському транспорті. Джерела кібернебезпеки. Сучасні загрози інформаційній безпеці.

Морський сектор є життєво важливою частиною світової економіки, незалежно від того, чи перевозить він вантажі, пасажирів або транспортні засоби. Судна стають все більш складними і залежними від широкого використання цифрових і комунікаційних технологій на всіх етапах їх експлуатації.

Наслідки нехтування безпекою:

Погана безпека може привести до значної втрати довіри клієнтів і / або галузі, репутаційний збиток, потенційно серйозні фінансові втрати або штрафи і судові розгляди, зачіпаючи залучені компанії.

(A) фізичне пошкодження системи, суднового персоналу або вантажу - в гіршому випадку це може привести до небезпеки для життя і / або загибелі корабля;

(B) збої, викликані тим, що судно більше не функціонує або ходить не за призначенням;

(C) втрата конфіденційної інформації, включаючи комерційні або особисті дані;

(D) дозвіл злочинної діяльності, включаючи викрадення, піратство, шахрайство, крадіжку вантажу, установку програм-вимагачів.

Основні положення

- Комітет з безпеки на морі ІМО в червні 2017 року прийняв Резолюцію MSC.428 (98) - управління морськими кіберризиками в системах управління безпекою. Резолюція закликає адміністрації забезпечити належний облік кіберризиків в існуючих системах управління безпекою.
- З 1 січня 2021 р. морські адміністрації ряду країн почали перевірки суден які заходять в їх порти на предмет виконання рекомендацій ІМО з кібербезпеки. Як було відзначено, резолюція ІМО MSC.428 (98) закликає адміністрації забезпечити облік кіберризиків в системах управління безпекою суден.
- Невиконання міжнародних норм може служити приводом для санкцій як щодо судновласницької компанії - члена ІМО, так і відповідних портів.

Закон України «Про основні засади забезпечення кібербезпеки» (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403).

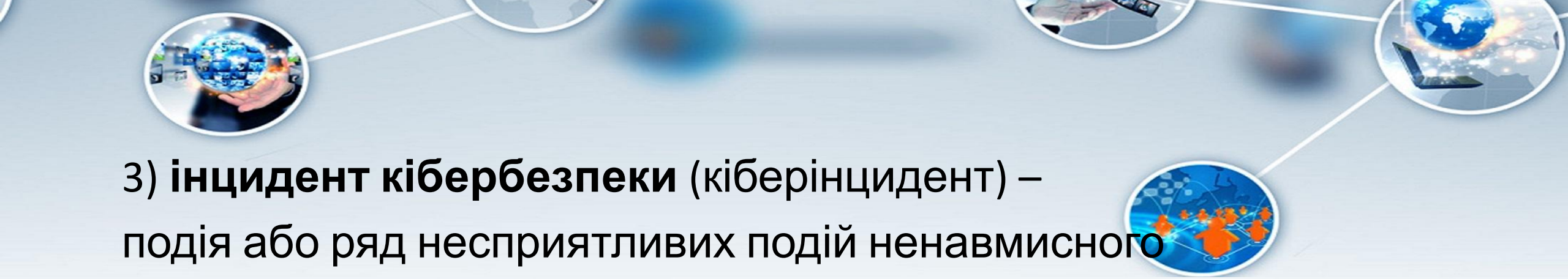
Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

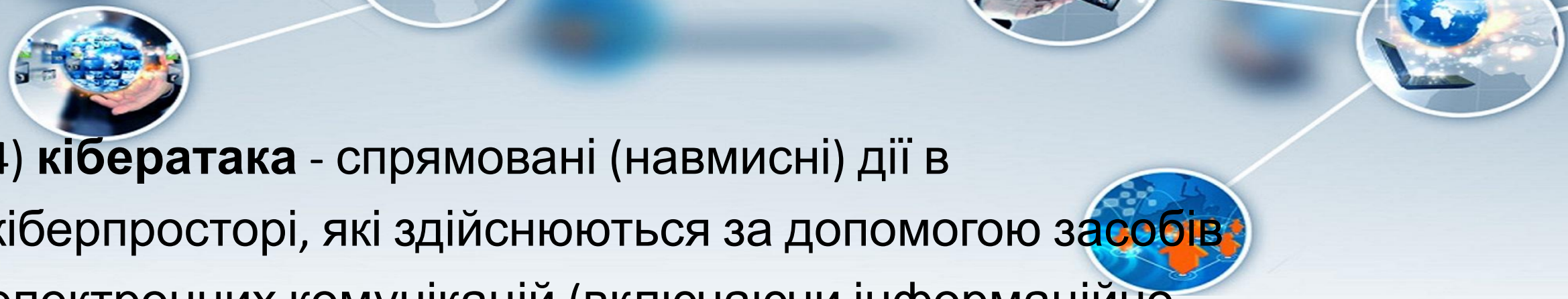
1) **індикатори кіберзагроз** - показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;

2) **інформація про інцидент кібербезпеки** - відомості про обставини кіберінциденту, зокрема про те, які об’єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;



3) **інцидент кібербезпеки** (кіберінцидент) –

подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактору) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;



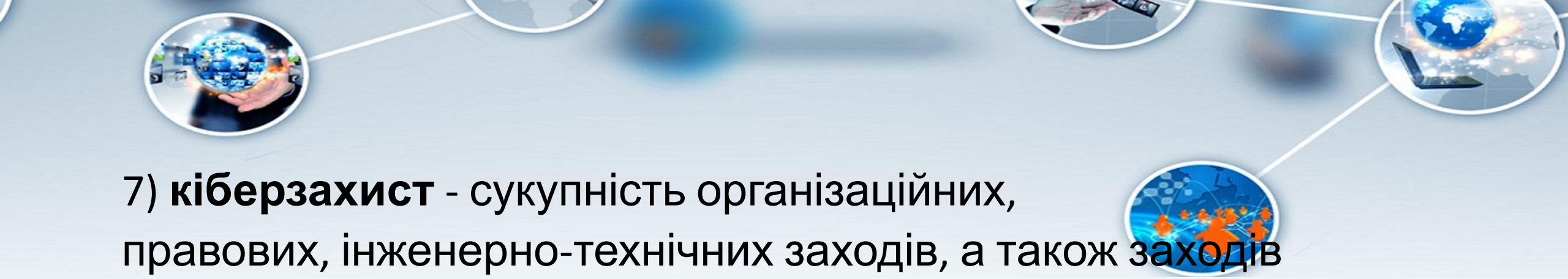
4) **кібератака** - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту;





5) **кібербезпека** - захищеність життєво важливих інтересів людини, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

6) **кіберзагроза** - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів;



7) **кіберзахист** - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

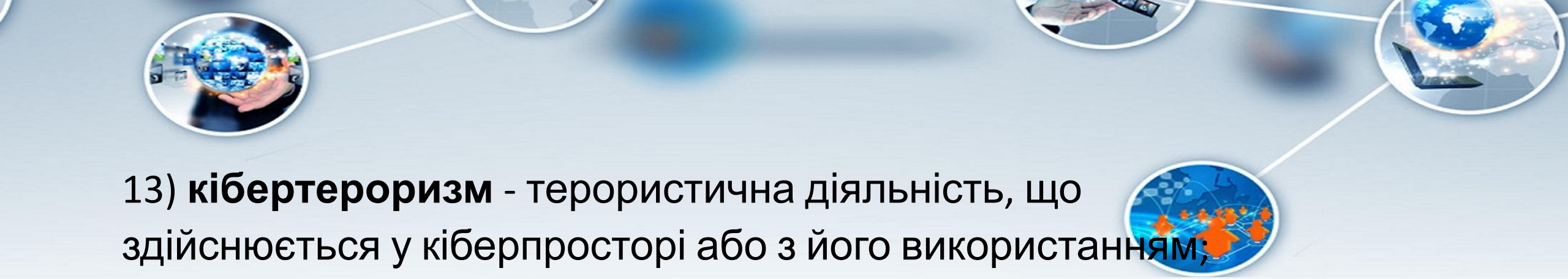
8) **кіберзлочин** (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

9) **кіберзлочинність** - сукупність кіберзлочинів;

10) **кібероборона** - сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;

11) **кіберпростір** - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;

12) **кіберрозвідка** - діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його



13) **кібертероризм** - терористична діяльність, що здійснюється у кіберпросторі або з його використанням;

14) **кібершпигунство** - шпигунство, що здійснюється у кіберпросторі або з його використанням;

15) **критична інформаційна інфраструктура** - сукупність об’єктів критичної інформаційної інфраструктури;

16) **критично важливі об’єкти інфраструктури** - підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов’язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров’я людей;

17) **національна телекомунікаційна мережа** – сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв’язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам;

18) **національні електронні інформаційні ресурси** - систематизовані електронні інформаційні ресурси,

які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів;

19) **об’єкт критичної інформаційної інфраструктури** - комунікаційна або технологічна система об’єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об’єкта критичної інфраструктури;

20) **система управління технологічними процесами** - автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних;

21) **системи електронних комунікацій** –

системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою дротових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв’язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв’язку, комп’ютери, інша комп’ ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних.

Терміни "національна безпека", "національні інтереси", "загрози національній безпеці" вживаються в цьому Законі у значенні, визначеному Законом України "Про основи національної безпеки України".

{Статтю 1 доповнено частиною третьою згідно із Законом № 1591-IX від 30.06.2021 - вводиться в дію з 01.08.2022}

Питання для самоконтролю

Визначте основні терміни Статті 1 Закону України «Про основні засади забезпечення кібербезпеки»:

1) індикатори кіберзагроз
2) інцидент кібербезпеки
3) кібератака
4) кібербезпека
5) кіберзагроза
6) кіберзахист
7) кіберзлочин
8) кібероборона
9) кіберпростір
10) кіберрозвідка
11) кібертероризм
12) кібершпигунство

Міжнародні норми кібербезпеки на морському транспорті

Міжнародна морська організація до уразливих суднових систем відносить:

- системи ходового містка;
- системи обробки і управління вантажем;
- системи управління двигунами, машинами і живленням;
- системи контролю доступу;
- системи обслуговування і управління пасажирами;
- публічні інтернет-мережі судна, призначені для використання пасажирами;
- адміністративні системи та мережі;
- системи зв'язку.

Кібербезпека - це не тільки запобігання доступу хакерів до систем та інформації, який потенційно призводить до втрати конфіденційності та / або контролю. Вона також стосується підтримання цілісності та доступності інформації і систем, забезпечення безперервності бізнесу і постійної корисності цифрових активів і систем. Судновласникам і операторам необхідно розуміти важливість кібербезпеки і підвищувати поінформованість про це зацікавлені сторони, включаючи їх судновий персонал.

Поняття і визначення

Глосарій максимально відповідає тому, який міститься в Міжнародній конвенції з охорони людського життя на морі 1974 р. (СОЛАС) з поправками.

Актив.
Предмет, річ або об'єкт, який має потенційну або фактичну цінність для організації.

Інформація про активи. Вона може включати інформацію щодо моделі, документи, зображення, програмне забезпечення, просторову інформацію або інформацію, пов'язану з діяльністю.

Компанія

Власник судна або будь-яка інша організація або особа, яка взяла на себе відповідальність за експлуатацію судна від власника судна, або ті, хто, приймаючи на себе таку відповідальність, погодився взяти на себе обов'язки, покладені Міжнародним кодексом управління безпекою (ISM). [Міжнародний кодекс охорони суден і портових засобів (ОСПЗ), розділ 1.8, стор.10].

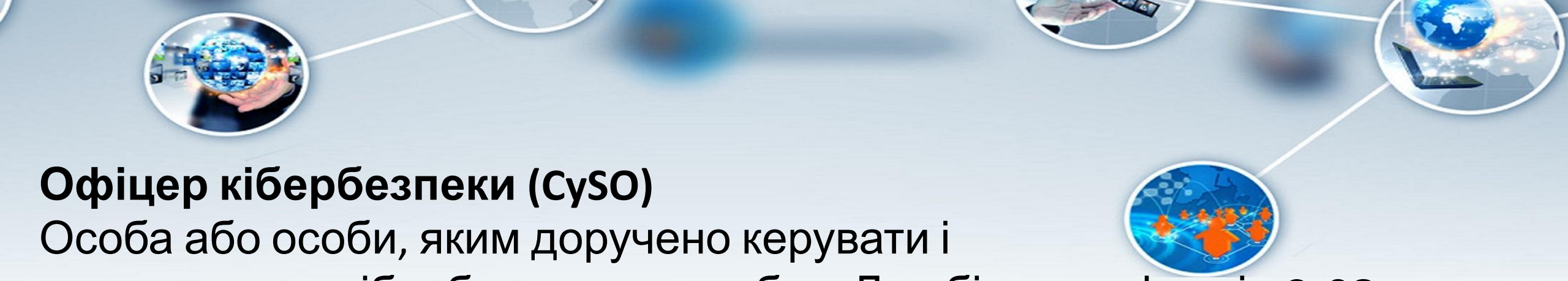
Офіцер безпеки компанії (CSO)

Особа, призначена Компанією для забезпечення об'єктивності оцінки безпеки судна (SSA), підтвердження того що план охорони судна (SSP) розроблений, поданий на затвердження, і згодом впроваджується і підтримується, а також для зв'язку з охороною портових офіцерів (PFSOs) і офіцерів служби безпеки судна (SSO). [Кодекс ОСПЗ, розділ 1.8, стор.10]

Кібератака (Cyberattack) - будь-який вид втручання в IT- і OT-системи, комп'ютерні мережі та / або персональні комп'ютери зі спробою зламати, знищити або отримати доступ до баз даних компанії, судновим системам і даними

Кіберфізична система (CPS)

Система, розроблена як об'єкт або набір об'єктів, з певною метою або для досягнення поставлених цілей. CPS повинна включати обчислювальний аспект (кібер) і фізичний аспект спільної роботи над виконанням завдання або функції. Кібер-аспект має контролюючий вплив на фізичні частини системи, наприклад, автоматизовані системи управління судном для підтримування заданого курсу



Офіцер кібербезпеки (CySO)

Особа або особи, яким доручено керувати і координувати кібербезпекою корабля. Для більших флотів CySO, ймовірно, буде підкорятися начальнику служби інформаційної безпеки компанії. Офіцер (CISO) або CSO, для невеликих флотів підпорядковується керівнику компанії безпеки.

Позиція з високим ризиком

Посада, яка має доступ до деталей SSA, SSP, CSP і / або інформації, що відноситься до чутливих активів, посаду, яка виконує адміністративні функції IT, OT або системи зв'язку


Інцидент безпеки

Будь-яка підозріла дія або обставина, що загрожує безпеці судна або портового засобу, або будь-якого інтерфейсу судно / порт або інтерфейсу судно-судно. [Кодекс ОСПЗ, розділ 1.8, стор. 12]

Рівень безпеки

Кваліфікація ступеня (ймовірності і впливу) ризику, пов'язаного з інцидентом безпеки, стосується це розпочатої спроби або вже атаки що сталася. [Кодекс ОСПЗ, розділ 1.8, стор. 12]

Інформація, важлива для безпеки

Розкриття інформації може поставити під загрозу безпеку судна, в тому числі: експлуатаційні дані судна, інформація, що міститься в будь-яких пов'язаних з персоналом файлах, або конфіденційна інформація, яка може поставити під загрозу будь-яку особу, систему або організації

Конфіденційна інформація

Інформація, втрата, неправильне використання або зміна якої, або несанкціонований доступ до якої можуть:

(a) негативно вплинути на приватне життя, благополуччя або безпеку людини або окремих осіб;

(в) порушувати інтелектуальну власність або комерційну таємницю організації;

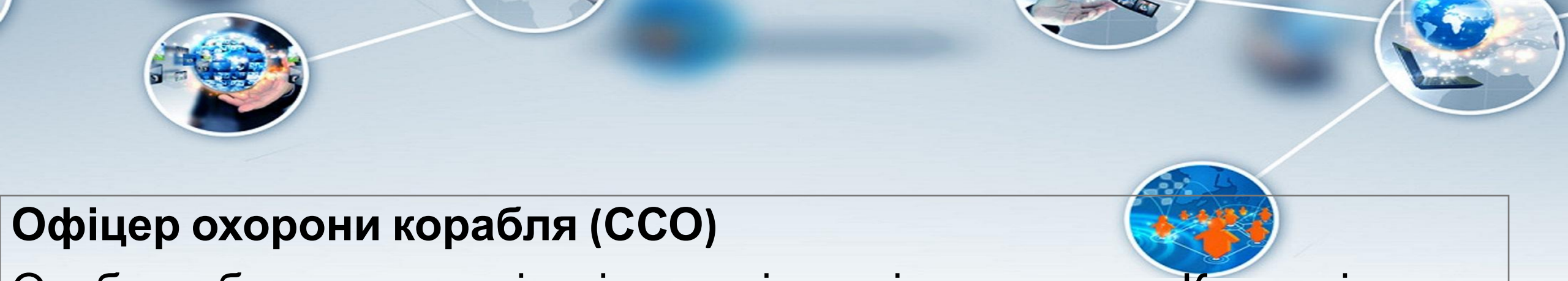
(c) заподіяти комерційний або економічних збитків організації або країні; або (d) ставити під загрозу безпеку, внутрішні і зовнішні справи нації, в залежності від рівня чутливості і характеру інформації.

Суднова система оповіщення про безпеку (SSAS)

Засоби, за допомогою яких судно може передати попередження про порушення безпеки компетентному органу на берег, вказуючи на те, що безпека судна знаходиться під загрозою або була порушена. [Кодекс ОСПЗ, розділ 1.8, стор. 12]

Оцінка безпеки судна (SSA)

Оцінка ризиків, що проводиться співробітником служби безпеки компанії або для нього в якості підготовки плану охорони судна, або перевірки, або поправка схваленого плану безпеки судна. [Кодекс ОСПЗ, розділ 1.8, стор. 12]



Офіцер охорони корабля (CSO)

Особа на борту судна, підзвітна капітанові, призначена Компанією як відповідальна за безпеку судна, включаючи реалізацію і підтримку плану безпеки судна, і зв'язок з офіцером служби безпеки компанії, і офіцери служби безпеки портового засобу. [Кодекс ОСПЗ, розділ 1.8, стор. 12]

План охорони судна (SSP)

План, розроблений для забезпечення застосування на борту судна заходів, спрямованих на захист людей які знаходяться на борту, вантаж, вантажні транспортні одиниці, суднові запаси або судно від ризику порушення безпеки. [Кодекс ОСПЗ, розділ 1.8, стор. 12]

Acronyms Абревіатури

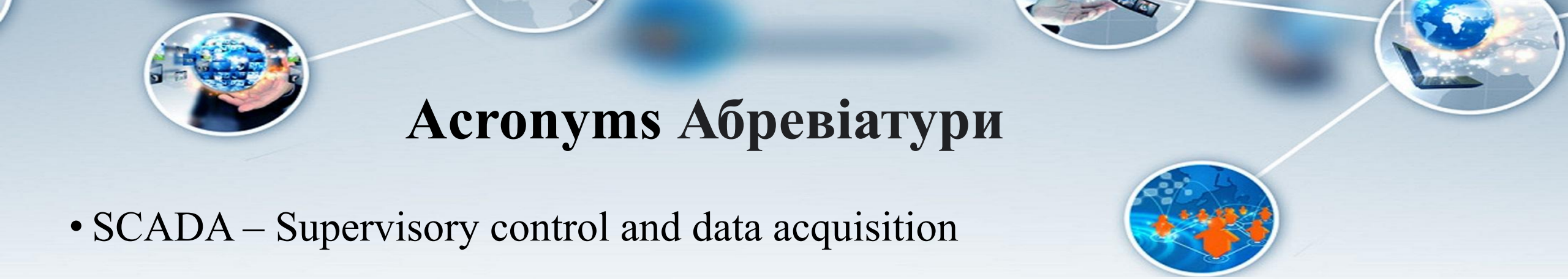
- CCTV – Closed circuit television **Система охоронного телебачення**
- CiSP – Cyber Information Sharing Partnership (UK) **Партнерство по обміну кібер-інформацією**
- CoP – Code of Practice **Кодекс практики**
- CPS – Cyber-physical system **Кібер-фізична система**
- CSA – Cyber security assessment **Оцінка кібербезпеки**
- CSO – Company security officer **Співробітник служби безпеки**
- CSP – Cyber security plan **план кібербезпеки**
- CySO – Cyber security officer **Офіцер кібербезпеки**

Acronyms Абревіатури

- DDoS – Distributed denial of service **розподілена відмова в обслуговуванні**
- DfT – Department for Transport **Департамент транспорту**
- Dstl – Defence Science & Technology Laboratory (UK) **Лабораторія оборонної науки і технології**
- EDi – Electronic data interchange **Електронний обмін даними**
- FSC – Fleet security committee **Комитет з безпеки флоту**
- GNSS – Global navigation satellite system **Глобальна навігаційна супутникова система**
- GPS – Global positioning system **Глобальная система позиционирования**


Acronyms Абревіатури

- ILO – International Labour Organization **Міжнародна організація праці**
- IMO – International Maritime Organization **Міжнародна морська організація**
- ITU – International Telecommunications Union **Міжнародна спілка телекомунікацій**
- ISPS – International ship and port facility security **Міжнародна охорона суден та портових споруд**
- MODU – Mobile offshore drilling units **Мобільні морськи бурові установки**
- NCSC – National Cyber Security Centre (NCSC) **Національний центр кібербезпеки (NCSC)**
- OT – Operational technology **Операційні технології**



Acronyms Абревіатури

- SCADA – Supervisory control and data acquisition

диспетчерський контроль та збір даних

- SOC – Security operations centre **Центр безпеки операцій**
- SOLAS – International Convention on the Safety of Life at Sea **Міжнародна конвенція з охорони людського життя на морі**
- SSAS – Ship security alert system **Суднова система сповіщення про безпеку**
- SSA – Ship security assessment **Оцінка безпеки судна**
- SSO – Ship security officer **Офіцер охорони корабля**
- SSP – Ship security plan **План охорони судна**

Інформаційна безпека

Інформаційна безпека - це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації.

Інформаційна безпека — це комплекс заходів для захисту даних та інформаційної системи від випадкових або навмисних пошкоджень та несанкціонованого доступу.

Принципи інформаційної безпеки

Інформаційна безпека

- Цілісність
- Конфіденційність
- Доступність
- Достовірність

- Конфіденційність
  - лише уповноважені користувачі можуть ознайомитись з інформацією
- Цілісність
  - лише уповноважені користувачі можуть модифікувати інформацію
- Доступність
  - уповноважені користувачі можуть отримати доступ до інформації, не очікуючи довше за заданий (малий) час





Джерела кібернебезпеки

Виявлення загрози

Кіберризик залежить від компанії, судна, операції і / або торгівлі. При оцінці ризику компанії повинні враховувати будь-які конкретні аспекти своєї діяльності, які можуть підвищити їх уразливість перед кіберінцидентами.


Наступні приклади дають певне уявлення про створювачів загрозу та потенційні наслідки для компаній і суден, якими вони управляють

Активісти (в тому числі незадоволені співробітники): репутаційний збиток; порушення роботи; - знищення даних, публікація конфіденційних даних, увага ЗМІ, відмова в доступі до цільової послузі або системі;

Злочинці: фінансова вигода.

Комерційне шпигунство: промислове шпигунство, продаж вкрадених даних, викуп вкрадених даних, працездатність системи викупу, організація незаконного перевезення вантажів, збір розвідданих для більш складних злочинів, точне місцезнаходження вантажу, плани транспортування і обробки суден і т. д.

Крім того, існує ймовірність того, що **персонал компанії на борту і на березі** може поставити під загрозу кіберсистеми і


Виявлення уразливості

Рекомендується, щоб судноплавна компанія спочатку провела оцінку ризиків, з якими можна реально зіткнутися. Після цього повинна бути проведена оцінка систем і бортових процедур, щоб скласти карту їх стійкості для боротьби з поточним рівнем загрози. Цьому можуть сприяти внутрішні експерти або сторонні експерти, знайомі з морською галуззю і її ключовими процесами. Результатом повинна стати стратегія, зосереджена на ключових ризиках.

Сучасні загрози інформаційній безпеці

Бортові системи можуть включати:

- системи управління вантажами;
- мостові системи (системи капітанського містка);
- системи управління рухом і механізмами, а також системи управління потужністю;
- системи контролю доступу;
- системи обслуговування пасажирів і управління;


Сучасні загрози інформаційній безпеці

- мережі загального користування, для обслуговування пасажирів;
- адміністративні системи і системи соціального забезпечення екіпажу. Ці системи слід розглядати як неконтрольовані, і їх не слід підключати до будь-якої бортової системи, критичною для безпеки;
- комунікаційні системи - доступність підключення до Інтернету через супутник і / або іншу бездротовий зв'язок може підвищити вразливість суден.



Відносно виробників і третіх сторін, включаючи підрядників і постачальників послуг, слід враховувати наступне:

1. **Поінформованість виробника і постачальника послуг з управління кіберризиками і процедурами.**

Ці компанії повинні мати оновлену політику компанії з управління кіберризиками, яка включає процедури навчання та управління доступними бортовими системами IT і OT.

2. Поширені уразливості:

- застарілі і ти що не підтримуються операційні системи;

- застаріле обладнання мостових систем, систем управління рухом судна та інших систем, та, головне, **визначенням міри відповідальності кожного члена екіпажу за его дії,** які можуть привести до тяжких наслідків кібератак.


Питання для самоконтролю

1. Назвіть суднові системи, які **Міжнародна морська організація відносить до уразливих.**
2. Назвіть найбільш розповсюджені **джерела кібернебезпеки.**
3. Яким чином проводиться **виявлення уразливості?**
4. Які елементи можуть включати **бортові системи?**

Працюємо в парах

Що таке особиста інформаційна безпека та інформаційна безпека держави? (обговоріть у парах)

Обговорюємо

- Що таке інформаційна безпека?
  - Що є об’єктом інформаційної безпеки? суб’єктом інформаційної безпеки?
- Які основні складові має інформаційна безпека?