



**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ МОРСЬКИЙ УНІВЕРСИТЕТ**

Кафедра «Кібербезпека та захист інформації»

КОНСПЕКТ ЛЕКЦІЙ
освітнього компонента (навчальної дисципліни)
**СУЧАСНІ КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ЇХ
ОСОБЛИВОСТІ**

назва освітнього компонента (навчальної дисципліни)

обов'язковий компонент циклу професійної підготовки

Рівень вищої освіти	<u>другий (магістерський)</u> перший (бакалаврський), другий (магістерський), третій (освітньо-науковий)
Форма здобуття освіти	<u>очна (денна)</u> очна (денна), заочна, дистанційна
Мова викладання	<u>Українська</u>

2025/2026 навчальний рік

Конспект лекцій освітнього компонента (навчальної дисципліни) «**Сучасні КСЗІ та їх особливості**» для здобувачів очної (денної) форми здобуття освіти другого (магістерського) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації галузі знань F Інформаційні технології / Укл.: Зоріло В.В. – Одеса, 2025. – 56 с.

Розробник: Зоріло Вікторія Вікторівна, доцент кафедри «Кібербезпека та захист інформації»

Схвалено на засіданні кафедри «Кібербезпека та захист інформації»
Протокол від №2 від 06.10.2025.

Схвалено на засіданні НМК ННІ ІТІП
Протокол від №2 від 14.10.2025

Зміст

Тема 1. Вступ до дисципліни. Поняття, мета та завдання сучасних КСЗІ	5
Тема 2. Загрози, вразливості та моделі порушників в інформаційних системах.....	8
Тема 3. Архітектура сучасних КСЗІ	17
Тема 4. Міжнародні стандарти та кращі практики побудови КСЗІ	22
Тема 5. Системи управління інформаційною безпекою (СУІБ).....	26
Тема 6. Криптографічні методи захисту інформації у КСЗІ.....	28
Тема 7. Технічні засоби та методи захисту інформації	30
Тема 8. Аудит та моніторинг ефективності КСЗІ	37
Тема 9. Захист критичної інфраструктури та бізнес-процесів.....	40
Тема 10. Управління інцидентами та прийняття рішень у сфері кібербезпеки	51
Список використаних джерел	56

Тема 1. Вступ до дисципліни. Поняття, мета та завдання сучасних КСЗІ

Комплексна система захисту інформації (КСЗІ) – сукупність організаційних, інженерно-технічних, програмно-апаратних і криптографічних заходів і засобів, що забезпечують захист інформації в інформаційно-телекомунікаційній системі (ІТС) відповідно до вимог законодавства. ІТС – це інформаційна, телекомунікаційна або інтегрована (що поєднує перші дві) система. Сучасна КСЗІ – ризик-орієнтована система, що охоплює весь життєвий цикл інформації: створення, обробку, зберігання, передавання та знищення.

Мета КСЗІ – забезпечити конфіденційність, цілісність і доступність інформації та спостережність дій користувачів, запобігаючи несанкціонованому доступу (НСД), витоку, модифікації, блокуванню чи знищенню інформації.

Основні завдання: реалізація політики безпеки і розподіл відповідальності; керування доступом, ідентифікація та автентифікація; захист від шкідливого ПЗ і мережових атак; криптографічний захист; резервне копіювання і відновлення; моніторинг, реагування на інциденти, контроль і аудит.

1.1. Еволюція засобів та систем захисту інформації

До 1960-х рр. захист зводився до фізичної охорони носіїв, режиму секретності та ручних і механічних шифрів. У 1960–1980-ті рр. з'явилися паролі й розмежування доступу в ЕОМ, критерії TCSEC (1983) і криптографія з відкритим ключем. У 1990-ті рр. поширилися антивіруси, захист від побічних електромагнітних випромінювань і наведень (ПЕМВН), загальні критерії Common Criteria; в Україні сформувалася система технічного захисту інформації (ТЗІ). У 2000-ні рр. стандартом стали міжмережеві екрани, VPN, PKI і системи управління ІБ (ISO/IEC 27001), в Україні – НД ТЗІ 3.7-003-2005. У 2010–2020-ті рр. відповіддю на хмари, мобільні пристрої, IoT, цільові атаки й програми-вимагачі стали SIEM і центри безпеки (SOC), EDR/XDR, архітектура нульової довіри (Zero Trust) і штучний інтелект. Захист переходить від «охорони периметра» до безперервного управління ризиками; в Україні Закон № 4336-IX (2025) замінює обов'язкову КСЗІ профілями безпеки.

1.2. Комплексний підхід: організаційні, технічні, правові та програмні аспекти

Комплексність означає узгоджене застосування всіх видів захисту на всіх етапах життєвого циклу і для всіх елементів системи, адже рівень захищеності визначається найслабшою ланкою. Аспекти захисту: **правовий** – закони, стандарти, відповідальність за порушення; **організаційний** – охорона, пропускний режим, регламентація доступу, добір і навчання персоналу; **інженерний** – обмежувальні конструкції, контроль доступу, відеоспостереження, охоронно-пожежна сигналізація; **технічний (ТЗІ)** – протидія витоку інформації технічними каналами та її блокуванню; **програмний і програмно-апаратний** – антивіруси, міжмережеві екрани, комплекси засобів захисту від НСД (КЗЗ); **криптографічний (КЗІ)** – захист від розголошення та модифікації шляхом математичних перетворень.

1.3. Види КСЗІ та їх застосування

За класом автоматизованої системи (НД ТЗІ 2.5-005-99) розрізняють: клас «1» – одномашинний однокористувацький комплекс; клас «2» – локалізований багатомашинний багатокористувацький комплекс; клас «3» – розподілений комплекс, що передає інформацію каналами зв'язку.

За видом інформації: КСЗІ для державної таємниці, для службової та іншої конфіденційної інформації, для відкритої інформації (захищають її цілісність і доступність, наприклад вебсторінок).

За складом: КСЗІ з комплексом засобів захисту від НСД (обов'язковий для державних інформаційних ресурсів) і КСЗІ з додатковим комплексом ТЗІ від витоку технічними каналами (для державної таємниці). За Законом № 4336-IX державні системи поступово переходять від атестованих КСЗІ до авторизованих систем, що реалізують базові, галузеві та цільові профілі безпеки.

Позначення та скорочення:

ТЗІ - технічний захист інформації

ТЗ - технічне завдання

СЗІ - служба захисту інформації

ПЕМВН - побічні електромагнітні випромінювання та наведення

ОТЗ - основні технічні засоби

НСД - несанкціонований доступ

НДР - науково-дослідна робота

НД ТЗІ - нормативний документ системи технічного захисту інформації

НД - нормативний документ

КСЗІ - комплексна система захисту інформації

КС - комп'ютерна система

КЗЗ - комплекс засобів захисту від несанкціонованого доступу

ІТС - інформаційно-телекомунікаційна система

ЕСПД - єдина система програмної документації

ЕСКД – єдина система конструкторської документації

ДТЗ - допоміжні технічні засоби

ДСТУ - державний стандарт України

ГОСТ - регіональний (міждержавний) стандарт

АС - автоматизована система

Комплексна система захисту інформації (КСЗІ) – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС.

Під інформаційно-телекомунікаційною системою будемо розуміти будь-яку систему, яка відповідає одному з трьох наведених вище видів автоматизованих систем (ІС, ТС або інтегрованої системи).

Інтегрована система – сукупність двох або кількох взаємопов'язаних інформаційних та (або) телекомунікаційних систем, в якій функціонування однієї (кількох) з них залежить від результатів функціонування іншої (інших) таким чином, що цю сукупність у процесі взаємодії можна розглядати як єдину систему.

Телекомунікаційна система (ТС) – організаційно-технічна система, що реалізує технологію інформаційного обміну за допомогою технічних і програмних засобів шляхом передавання та приймання інформації у вигляді сигналів, знаків, звуків, зображень чи іншим чином.

Інформаційна система (ІС) – організаційно-технічна система, що реалізує технологію обробки інформації за допомогою засобів обчислювальної техніки та програмного забезпечення.

Засоби і системи захисту інформації – основний метод боротьби із несанкціонованим доступом до інформації можливими каналами витоку інформації.

Еволюція засобів та систем захисту інформації.

У сучасних умовах цифровізації КСЗІ має важливе значення для захисту державних і корпоративних інформаційних ресурсів забезпечення безперервності функціонування інформаційних систем, дотримання вимог законодавства та підвищення рівня довіри користувачів і партнерів.

Основними завданнями сучасної КСЗІ є формування та реалізація політики інформаційної безпеки, визначення ролей і відповідальності персоналу, організація контролю доступу користувачів до інформаційних ресурсів, забезпечення ідентифікації та автентифікації користувачів, захист інформації від шкідливого програмного забезпечення і мережних атак, застосування криптографічних засобів захисту інформації під час її зберігання та передавання, організація резервного копіювання і відновлення даних, постійний моніторинг подій безпеки, своєчасне виявлення, реагування та розслідування інцидентів інформаційної безпеки, а також проведення контролю і аудиту відповідності встановленим вимогам.

Метою створення і функціонування КСЗІ є забезпечення належного рівня інформаційної безпеки, що полягає у збереженні конфіденційності цілісності та доступності інформації, а також у запобіганні несанкціонованому доступу, витоку, модифікації, блокуванню або знищенню інформаційних ресурсів.

Сучасна КСЗІ розглядається як інтегрована ризик орієнтована система, що охоплює весь життєвий цикл інформації від її створення та обробки до зберігання передавання і знищення, поєднує технічні та організаційні заходи адаптується до змін загроз та функціонує з урахуванням національних і міжнародних стандартів інформаційної безпеки.

КСЗІ або комплексна система захисту інформації – це сукупність організаційних, інженерно технічних, програмно апаратних та криптографічних заходів засобів і процедур спрямованих на забезпечення захисту інформації в інформаційно телекомунікаційних системах відповідно до вимог законодавства та нормативних документів.

Контрольні запитання до теми 1

1. Дайте визначення КСЗІ.
2. Які види систем охоплює поняття ІТС?
3. Яка мета КСЗІ?
4. Назвіть основні завдання КСЗІ.
5. Що означає ризик-орієнтований характер сучасної КСЗІ?
6. Назвіть основні етапи еволюції засобів захисту інформації.
7. У чому полягають комплексний підхід і принцип «найслабшої ланки»?
8. Назвіть аспекти (види) захисту інформації та наведіть приклади засобів.
9. Як класифікують автоматизовані системи за НД ТЗІ 2.5-005-99?
10. Що змінює Закон № 4336-IX у підході до побудови систем захисту?

Тема 2. Загрози, вразливості та моделі порушників в інформаційних системах

Загроза – потенційна подія чи дія, що може порушити властивості інформації або системи; **вразливість** – недолік системи, який можна використати для реалізації загрози; **ризик** – поєднання ймовірності реалізації загрози та розміру збитків; **джерело загрози** – її генератор або носій (люди, технічні засоби, програми, алгоритми, зовнішнє середовище).

2.1. Класифікація загроз

Загрози класифікують за **походженням** – випадкові (відмови, збої, помилки, побічні впливи, стихійні лиха) і навмисні (зловмисні дії людей); за **передумовами** – об'єктивні (кількісна чи якісна недостатність елементів системи) і суб'єктивні (іноземні розвідки, промислове шпигунство, кримінал, недобросовісний персонал); за **властивістю, що порушується**, – загрози конфіденційності, цілісності, доступності, спостережності та керованості; за **способом реалізації** – підключення до ліній зв'язку, маскування під легального користувача, закладні пристрої, шкідливі програми.

Модель загроз розробляє служба захисту інформації (СЗІ) на підставі акта обстеження та моделі порушника. Вона описує загрози і способи атак так, щоб можна було оцінити збитки та ймовірність кожної з них.

Модель порушника – опис можливих дій порушника, його знань, кваліфікації, часу й місця дії. **Внутрішні** порушники – допоміжний персонал, основний персонал (найнебезпечніший) і співробітники служби безпеки; **зовнішні** – відвідувачі, клієнти, конкуренти, іноземні служби, особи поза контрольованою зоною. Мотиви порушень – безвідповідальність, самоствердження, корисливість. Порушників класифікують за рівнем знань, за можливостями (від агентурних методів до активного впливу із закладками), за часом і місцем дії. Настанови Міжнародної морської організації (ІМО) виділяють такі категорії суб'єктів кіберзагроз: активісти, кримінальні угруповання, опортуністи, держави та підтримувані ними організації, терористи.

2.2. Методи аналізу ризиків та оцінки рівня захищеності

Управління ризиками (ISO/IEC 27005, ISO 31000) складається з етапів: встановлення контексту і критеріїв, ідентифікація ризиків (активи, загрози, вразливості), аналіз, оцінювання, обробка, моніторинг. Критерії оцінки враховують цінність активів, міру збитку та допустимий рівень ризику. Методи аналізу бувають **якісні** (шкала «низький – середній – високий», матриця «ймовірність × наслідки»), **кількісні** ($R = P \times U$; очікувані річні втрати $ALE = ARO \times SLE$, де ARO – річна частота інцидентів, SLE – збиток від одного інциденту) і змішані. Ризик можна зменшити, уникнути, передати (страхування, аутсорсинг) або прийняти; ризик, що лишається після обробки, називають **залишковим**. Захищеність оцінюють перевіркою відповідності вимогам, скануванням вразливостей (шкала CVSS 0–10) і тестуванням на проникнення.

2.3. Приклади реальних атак та їх наслідків

У грудні 2015 р. атака BlackEnergy на три обленерго України залишила без світла близько 225 тис. споживачів, а у 2016 р. Industroyer знеструмив київську підстанцію «Північна». 27.06.2017 NotPetya, поширений через оновлення M.E.Doc, паралізував тисячі організацій, зокрема 17 із 76 терміналів Maersk (збитки – близько 300 млн дол. США). У 2017 р. в Чорному морі GPS-спуфінг «перемістив» десятки суден на сушу біля Новоросійська, а з 2019 р. масові GNSS-аномалії фіксують на Близькому Сході. Атак зазнали також порти Барселони й Сан-Дієго, компанії MSC і Anglo-Eastern. Атака на ланцюг постачання SolarWinds (2020) уразила близько 18 тис. клієнтів, а атака на «Київстар» (12.12.2023) залишила без зв'язку мільйони абонентів. Висновки: потрібні ізольовані резервні копії, сегментація мереж і плани безперервності.

Зростання ступеня захищеності може досягатись як підсиленням певних послуг, тобто включенням до профілю більш високого рівня послуги, так і включенням до профілю нових послуг. Кожна послуга є набором функцій, які дозволяють протистояти певній множині загроз. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз.

Рівні послуг мають ієрархію за повнотою захисту, хоча й не є точними підмножинами один одного. Рівні починаються з першого й зростають до певного значення, унікального для кожного виду послуг. До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від:

Визначаються загальна структура та склад КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації, обмеження щодо середовищ функціонування ІТС та використання її ресурсів для реалізації завдань захисту, припустимі витрати на створення КСЗІ, умови створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів), загальні вимоги до застосування в ІТС (окремих її підсистемах, компонентах) організаційних, технічних, криптографічних та інших заходів захисту інформації, що ввійдуть до складу КСЗІ. Для ІТС формується перелік необхідних функціональних послуг захисту (далі - ФПЗ) від НСД та вимог до рівнів реалізації кожної з них, визначається рівень гарантій реалізації послуг. Визначені вимоги складають профіль захищеності інформації в ІТС або її компоненті. ФПЗ є ієрархічними в тому розумінні, що їх реалізація забезпечує зростаючу захищеність від загроз відповідного типу (конфіденційності - К, цілісності - Ц і доступності - Д).

На підставі визначених завдань і функцій ІТС, результатів аналізу її середовищ функціонування, моделей загроз і порушників та результатів аналізу ризиків визначаються компоненти ІТС (наприклад, ЛОМ, спеціалізований АРМ, Інтернетвузол тощо), для яких необхідно або доцільно розробляти свої власні політики безпеки, відмінні від загальної політики безпеки в ІТС.

Якщо залишковий ризик перевищує гранично допустимий, вносять відповідні зміни до складу заходів і засобів захисту, після чого всі процедури виконують повторно до одержання прийняттого результату.

На етапі проектування КСЗІ, після формування пропозицій щодо складу заходів і засобів захисту, здійснюється оцінка залишкового ризику для кожної пропозиції (наприклад, за критерієм «ефективність/вартість»), вибирається найбільш оптимальна серед них і первинна оцінка уточнюється.

Після цього необхідно здійснити первинне (попереднє) оцінювання допустимих витрат на блокування загроз, виходячи з вибраного варіанту побудови КСЗІ і виділених на це коштів:

- досягнення максимального рівня захищеності інформації за необхідних витрат і **мінімального** рівня обмежень на технологію її обробки в ІТС;
- досягнення необхідного рівня захищеності інформації за допустимих витрат і **заданого** рівня обмежень на технологію її обробки в ІТС;
- досягнення необхідного рівня захищеності інформації за мінімальних витрат і **допустимого** рівня обмежень на технологію її обробки в ІТС;

Загальна структура та склад КСЗІ. Вибір варіанту побудови КСЗІ Після завершення аналізу всіх можливих ризиків необхідно здійснити вибір варіанту побудови КСЗІ в залежності від ступеня обмеження доступу до інформації, яка обробляється в ІТС, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних, фінансових та інших ресурсів, які є у розпорядженні власника ІТС.

Вибір варіанту побудови КСЗІ.

включати вимоги для майбутньої додаткової обробки, наприклад, ризик може бути прийнятий, якщо є згода на дії щодо його зниження до прийняттого рівня у рамках певного періоду часу.

визначатися як кількісне співвідношення оціненої вигоди до оціненого ризику для бізнесу;

включати багато порогових значень з бажаним рівнем ризику, але за умови, що при певних обставинах керівництво прийматиме ризики, що знаходяться вище вказаного рівня;

При розробці критеріїв прийняття ризику слід враховувати, що вони можуть:

соціальних і гуманітарних чинників.

фінансів;

технологій;
операцій;
нормативно-правових і договірних аспектів;
критеріїв якості бізнес-процесів;
Критерії прийняття ризику повинні встановлюватися з урахуванням:
порушення нормативно-правових вимог або договірних зобов'язань.
збиток для репутації;
порушення планів і кінцевих термінів;
втрата цінності бізнесу та фінансової цінності;
погіршення бізнес-операцій;
порушення властивості інформації (втрата конфіденційності, цілісності або доступності);

цінність інформаційного активу, на який виявлений вплив;

Крім того, критерії оцінки ризиків можуть використовуватися для визначення пріоритетів для обробки ризиків. Критерії впливу повинні розроблятися, виходячи з міри збитку, враховуючи наступне:

важливість доступності, конфіденційності та цілісності інформації.

нормативно-правові вимоги та договірні зобов'язання;

критичність інформаційних активів;

стратегічна цінність обробки інформації;

Критерії оцінки ризику повинні розроблятися, враховуючи наступне:

Визначення критеріїв. На цьому етапі використовуються дані обстеження всіх середовищ ІТС з метою визначення того, які інформаційні та технічні ресурси зі складу ІТС і з якою детальністю повинні розглядатися в процесі керування ризиком. Крім того, необхідно розробити критерії оцінки ризиків, впливу на активи та прийняття ризиків.

Визначення критеріїв оцінки ризиків.

6-го класу – канали, які у процесі обробки інформації з доступом зловмисника до елементів ІТС і зі зміною останніх. Сюди може бути віднесено незаконне підключення до апаратури та ліній зв'язку, а також зняття інформації на шинах живлення різних елементів ІТС.

Серед цих каналів: підміна і розкрадання носіїв інформації й апаратури, включення до програм блоків типу троянський кінь, комп'ютерний черв'як тощо.

5-го класу – канали, які проявляються безвідносно до обробки інформації з доступом зловмисника до елементів ІТС і зі зміною програмних або апаратних засобів.

Сюди може бути віднесено запам'ятовування і копіювання інформації в процесі обробки, використання програмних пасток тощо.

4-го класу – канали, які у процесі обробки інформації з доступом зловмисника до елементів ІТС, але без зміни останніх.

До них відносяться всілякі види копіювання носіїв інформації і документів, а також розкрадання виробничих відходів.

3-го класу – канали, які проявляються безвідносно до обробки інформації з доступом зловмисника до елементів ІТС, але без зміни останніх.

Сюди можуть бути віднесені електромагнітні випромінювання різних пристроїв ІТС, апаратури та ліній зв'язку, паразитні наведення в ланцюгах живлення, телефонних мережах, системах теплопостачання, вентиляції тощо.

2-го класу – канали, які у процесі обробки інформації без доступу зловмисника до елементів ІТС.

Сюди може бути віднесено підслуховування розмов, а також провокування на розмови осіб, що мають відношення до ІТС, і використання зловмисником візуальних, оптичних та акустичних засобів.

1-го класу – канали, які проявляються безвідносно до обробки інформації і без доступу зловмисника до елементів системи.

Наведемо орієнтовну характеристику каналів несанкціонованого отримання інформації виділених нами класів.

існуючі тільки в робочому стані ІТС (наприклад, побічні електромагнітні випромінювання та наведення).

потенційно існуючі незалежно від стану ІТС (наприклад, викрадати носії інформації можна незалежно від того, в робочому стані знаходяться засоби АС чи ні);

За другим критерієм (залежність появи КВІ від стану ІТС) КВІ можуть бути розділені на:

У свою чергу, такі канали можуть не залишити слідів в ІТС (наприклад, візуальний перегляд зображень на екранах моніторів або документів на паперових носіях), а можуть і залишити ті чи інші сліди (наприклад, розкрадання документів або машинних носіїв інформації).

вимагають доступу в приміщення ІТС.

не вимагають доступу, тобто дозволяють отримувати необхідну інформацію дистанційно (наприклад, шляхом візуального спостереження через вікна приміщень ІТС),

За першим критерієм (необхідність доступу до елементів ІТС для реалізації того чи іншого КВІ) КВІ можуть бути розділені на такі, що:

Всі можливі канали витоку інформації (КВІ) можна класифікувати за двома критеріями: необхідністю доступу до елементів ІТС для реалізації того чи іншого КВІ і залежністю появи КВІ від стану ІТС.

Джерело загрози – це безпосередній їх генератор або носій. Таким джерелом можуть бути люди, технічні засоби, моделі (алгоритми), а також – програми, технологічні схеми обробки, зовнішнє середовище. Спробуємо тепер, спираючись на наведену системну класифікацію загроз безпеки інформації, визначити повну множину загроз, потенційно можливих у сучасних автоматизованих системах. При цьому ми повинні врахувати не лише всі відомі (ті, що раніше проявлялися) загрози, але й такі загрози, які раніше не виявлялися, але потенційно можуть виникнути при застосуванні нових концепцій архітектурної побудови АС і технологічних схем обробки інформації.

Джерела загроз інформації в ІТС. Характеристика каналів витоку інформації.

Опис моделі загроз (у частині, що стосується переліку можливих способів реалізації загроз та їх класифікації), має бути викладений настільки детально, щоб дозволяти (на етапі аналізу ризиків, пов'язаних з реалізацією загроз для інформації в ІТС) однозначне визначення як збитків, що завдаються у випадку успішної реалізації загрози, так і ймовірності реалізації загрози (здійснення атаки) в певний спосіб.

застосування закладних пристроїв чи програм, вкорінення комп'ютерних вірусів.

подолання заходів захисту з метою використання інформації або нав'язування хибної інформації,

маскування під зареєстрованого користувача,

шляхом підключення до апаратури та ліній зв'язку,

можливі способи здійснення (механізм реалізації) загроз:

зовнішнє середовище.

технологія функціонування ІТС;

моделі, алгоритми, програми ІТС;

технічні засоби ІТС;

персонал ІТС;

джерела виникнення (які суб'єкти ІТС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу):

загрози спостережності та керованості ІТС – відмова в ідентифікації, автентифікації та реєстрації небезпечних дій;

загрози доступності – порушення можливості використання ІТС або оброблюваної інформації (відмова в обслуговуванні користувача);

загрози цілісності – несанкціонована модифікація (спотворення, фальсифікація, викривлення) інформації;

загрози конфіденційності – несанкціоноване ознайомлення з інформацією;
на порушення яких властивостей інформації або ІТС вона спрямована:

Для кожної з загроз необхідно визначити:

Перелік суттєвих загроз має бути максимально повним і деталізованим.
інші.

впровадження та використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);

неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо;

одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача;

читання залишкової інформації з оперативної пам'яті ЕОТ, зовнішніх накопичувачів;

несанкціоноване копіювання носіїв інформації;

крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);

використання (шантаж, підкуп тощо) з корисливою метою персоналу ІТС;

впровадження та використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;

порушення режимів функціонування ІТС (обладнання і ПЗ);

порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІТС (електроживлення, заземлення, охоронної сигналізації, кондиціонування тощо.);

порушення фізичної цілісності ІТС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи ІТС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути:

наслідки некомпетентного застосування засобів захисту тощо.

неправомірне впровадження та використання заборонених політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення тощо);

будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

невиконання вимог до організаційних заходів захисту чинних в ІТС розпорядчих документів;

неумисне зараження ПЗ комп'ютерними вірусами;

неправомірна зміна режимів роботи ІТС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

ненавмисне пошкодження носіїв інформації;

дії, що призводять до відмови ІТС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм тощо);

Випадковими загрозами суб'єктивної природи (дії, які здійснюються персоналом або користувачами по неухважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

навмисні дії (спроби) потенційних порушників.

помилки персоналу (користувачів) ІТС під час експлуатації;

наслідки помилок під час проектування та розробки компонентів ІТС (технічних засобів, технології обробки інформації, ПЗ, засобів захисту, структур даних тощо);

збої та відмови у роботі технічних або програмних засобів (ПЗ) ІТС;
зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);

Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно ІТС і повинні враховуватись у моделі загроз, наприклад:

Загрози для інформації, що обробляється в ІТС, залежать від характеристик ОС, апаратного складу, програмних засобів, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні.

перелік можливих способів реалізації загроз певного типу (способів атак) відносно різних інформаційних об'єктів ІТС у різному стані класифікований, наприклад, за такими ознаками, як компонент обчислювальної системи ІТС або програмний засіб, уразливості яких експлуатуються порушником, причини виникнення відповідної уразливості тощо.

перелік можливих типів загроз, класифікований за результатом впливу на інформацію, тобто на порушення яких її властивостей вони спрямовані (конфіденційності, цілісності або доступності інформації);

Модель загроз має містити абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз для інформації, яка потребує захисту. Модель загроз повинна визначити:

На підставі Акту обстеження та Моделі порушника політики безпеки СЗІ розробляє «Модель загроз для інформації в ІТС», яка затверджується керівником організації-власника (розпорядника) ІТС, та вноситься, за необхідності, до відповідних розділів Плану захисту та Технічного завдання на створення КСЗІ.

якісна недостатність – недосконалість конструкції (організації) елементів системи, в силу цього можуть з'являтися можливості випадкового або навмисного негативного впливу на оброблювану або збережену інформацію.

кількісна недостатність – фізична нестача одного або декількох елементів системи, що викликає порушення технологічного процесу обробки даних і / або перевантаження наявних елементів;

Перераховані різновиди передумов інтерпретуються таким чином:

Передумови появи загроз можуть бути об'єктивними (кількісна або якісна недостатність елементів системи) і суб'єктивними. До останніх відносяться діяльність розвідувальних органів іноземних держав, промислове шпигунство, діяльність кримінальних елементів, дії недобросовісного персоналу ІТС.

Навмисне походження загроз обумовлюється зловмисними діями людей.

побічний вплив – негативний вплив на систему в цілому або окремі її елементи, чиниться будь-якими явищами, що відбуваються всередині системи або у зовнішньому середовищі.

помилка – неправильне (разове або систематичне) виконання елементом однієї або декількох функцій, що відбувається внаслідок специфічного (постійного або тимчасового) його стану;

збій – тимчасове порушення працездатності якого-небудь елемента системи, наслідком чого може бути неправильне виконання ним у цей момент своєї функції;

відмова – порушення працездатності якого-небудь елемента системи, що призводить до неможливості виконання нею основних своїх функцій;

Випадкове походження обумовлюється спонтанними і не залежними від волі людей обставинами, що виникають в ІТС в процесі її функціонування. Найбільш відомими подіями цього плану є відмови, збої, помилки, стихійні лиха та побічні впливи. Сутність перерахованих подій (окрім стихійних лих) визначається таким чином:

Походження загроз може бути випадковим і навмисним.

Після проведення обстеження середовищ ІТС необхідно визначити всі можливі потенційні загрози для ІТС.

Модель загроз для інформації в ІТС

Слід зауважити, що всі злочини, зокрема і комп'ютерні, здійснюються людиною. Користувачі ІТС, з одного боку, є її складовою частиною, а з іншого – основною причиною і руховою силою порушень і злочинів. Отже, питання безпеки захищених ІТС фактично є питанням людських відносин та людської поведінки.

За результатами формування моделі порушника обов'язково повинні бути визначені: імовірність реалізації загрози, своєчасність виявлення та відомості про порушення.

Припускається, що в своєму рівні порушник – це фахівець вищої кваліфікації, який має повну інформацію про ІТС і засоби захисту. Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.

НСД може бути наслідком помилок користувачів, адміністраторів, а також хибної прийнятої технології обробки інформації тощо.

порушник, плануючи спробу НСД, приховує свої несанкціоновані дії від інших співробітників;

робота з підбору кадрів і спеціальні заходи утруднюють можливість створення коаліцій порушників, тобто злочинного угруповання (змови) і цілеспрямованих дій по подоланню системи захисту двох і більше порушників;

Враховуються також такі обмеження та припущення про характер дій можливих порушників:

- з доступом у зону управління засобами забезпечення безпеки.

- з доступом у зону даних (баз даних, архівів тощо);

- з робочих місць кінцевих користувачів (операторів);

- усередині приміщень, але без доступу до технічних засобів;

- з контрольованої території без доступу до будівель та споруджень;

- без доступу на контрольовану територію організації;

- За місцем дії:

 - як у процесі функціонування, так і в період неактивності системи.

 - у період неактивності системи (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування та ремонтів і т.д.);

 - у процесі функціонування (під час роботи компонентів системи);

- За часом дії:

 - застосовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передавання даних, впровадження програмних закладок та використання спеціальних інструментальних та технологічних програм).

 - використовує тільки штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, які можуть бути тайком пронесені крізь пости охорони;

 - застосовує пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи);

 - застосовує чисто агентурні методи отримання відомостей;

 - знає структуру, функції і механізм дії засобів захисту, їх сильні і слабкі сторони. За рівнем можливостей (методам та засобам, що використовуються):

 - має високий рівень знань в області програмування й обчислювальної техніки, проектування й експлуатації автоматизованих інформаційних систем;

 - має високий рівень знань і досвід роботи з технічними засобами системи і їх обслуговуванням;

 - знає функціональні особливості ІТС, основні закономірності формування в ній масивів даних і потоків запитів до них, уміє користуватися штатними засобами;

Порушення безпеки ІТС може бути викликано корисливим інтересом користувача ІТС. У цьому випадку він буде цілеспрямовано намагатися подолати систему захисту для

несанкціонованого доступу до інформації в ІТС. Усіх порушників можна класифікувати за рівнем знань про ІТС:

Деякі користувачі вважають одержання доступу до системних наборів даних значним успіхом, затіваючи свого роду гру заради самоствердження або у власних очах, або в очах колег.

Можна виділити також 3 основних мотиви порушень: безвідповідальність, самоствердження та з корисною метою. При порушеннях, викликаних безвідповідальністю, користувач цілеспрямовано або випадково виробляє руйнуючі дії, які не пов'язані проте зі злим умислом. У більшості випадків це наслідок некомпетентності або недбалості.

співробітників служби безпеки, які часто формально не допущені до життєво важливого центру ІТС, але реально мають достатньо широкі можливості для збору необхідної інформації і скоєння акції.

основний персонал, що допущений до життєво важливого центру (найбільш небезпечний тип порушників);

допоміжний персонал об'єкту, що допущений на об'єкт, але не допущений до життєво важливого центру ІТС;

Потенціальних внутрішніх порушників можна розділити на:

будь-які особи за межами контрольованої зони.

особи, які випадково або навмисно порушили пропускний режим (без мети порушити безпеку);

представники конкуруючих організацій (іноземних служб) або особи, що діють за їх завданням;

представники організацій, взаємодіючих з питань забезпечення систем життєдіяльності організації (енерго-, водо-, теплопостачання тощо);

відвідувачі (запрошені з якого-небудь приводу);

клієнти (представники організацій, громадяни);

Сторонні особи, що можуть бути порушниками:

поодиноких порушників, що не мають допуску на об'єкт і намагаються діяти потайки й обережно, так як вони усвідомлюють, що сили реагування мають перед ним переваги.

добре озброєну та технічно оснащену групу, що діє зовні швидко і напролом;

Порушники спочатку поділяються на дві основні групи: зовнішні та внутрішні. Зовнішніх порушників можна розділити на:

нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);

отримання необхідної інформації у потрібному обсязі та асортименті;

Метою порушника можуть бути:

припущення про характер його дій.

припущення про кваліфікацію порушника;

категорії персоналу, користувачів ІТС та сторонніх осіб, із числа яких може бути порушник;

можливі цілі порушника та їх градація за ступенями небезпечності для ІТС та інформації, що потребує захисту;

Модель порушника – це абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апіорні знання, час та місце дії тощо. Як порушник розглядається особа, яка може одержати несанкціонований доступ (НСД) до роботи з включеними до складу ІТС засобами. Модель порушника повинна визначати:

На підставі Акту обстеження та визначення загроз для ІТС СЗІ розробляє «Модель порушника безпеки інформації в ІТС», яка затверджується керівником організації-власника (розпорядника) ІТС, та вноситься, за необхідності, до відповідних розділів Плану захисту.

Модель порушника безпеки інформації в ІТС

Контрольні запитання до теми 2

1. Дайте визначення понять «загроза», «вразливість», «ризик».
2. Чим відрізняються випадкові та навмисні загрози?
3. Наведіть класифікацію загроз за властивостями інформації.
4. Що містить модель загроз і хто її розробляє?
5. Чим відрізняються внутрішні та зовнішні порушники?
6. Які мотиви порушень виділяють?
7. Назвіть етапи управління ризиками за ISO/IEC 27005.
8. Поясніть формулу $ALE = ARO \times SLE$.
9. Які існують способи обробки ризику? Що таке залишковий ризик?
10. Наведіть приклади реальних атак і висновки з них.

Тема 3. Архітектура сучасних КСЗІ

3.1. Принципи побудови КСЗІ

Принципи побудови КСЗІ: **системність, комплексність, безперервність** захисту на всіх етапах життєвого циклу, **розумна достатність** (витрати не перевищують можливих збитків), **гнучкість, відкритість механізмів** (стійкість не залежить від секретності алгоритмів), **простота використання, ешелонованість** (defense in depth), **мінімальні привілеї, розподіл обов'язків і нульова довіра** (Zero Trust – «ніколи не довіряй, завжди перевіряй»).

Захист реалізують циклом із чотирьох етапів: **виявлення → зупинення → нейтралізація → попередження**. **Виявлення** – сигналізація, відеоспостереження, пасивні бар'єри; **зупинення** – блокування НСД міжмережевими екранами, антивірусами та КЗЗ з документуванням дій порушника; **нейтралізація** – розслідування та відновлення з резервних копій за планом аварійного відновлення; **попередження** – аналіз загроз, оновлення політики, навчання персоналу. Варіант побудови КСЗІ обирають за результатами аналізу ризиків: необхідний рівень захищеності за мінімальних чи допустимих витрат або максимальний рівень за необхідних витрат. Для кожного варіанта оцінюють залишковий ризик за критерієм «ефективність/вартість». Результат – профіль захищеності, тобто перелік функціональних послуг безпеки та їх рівнів.

3.2. Рівні захисту: мережевий, системний, прикладний

Архітектура КСЗІ багаторівнева й спирається на фізичний захист. **Мережевий рівень**: сегментація (VLAN, демілітаризовані зони), міжмережіві екрани нового покоління (NGFW), системи виявлення та запобігання вторгненням (IDS/IPS), VPN, захист від DDoS-атак, контроль підключень (NAC). **Системний рівень** (ОС, сервери, робочі станції): автентифікація, розмежування доступу (дискреційне, мандатне, рольове), безпечне конфігурування, оновлення, EDR, журналювання, резервне копіювання. **Прикладний рівень**: безпечна розробка (OWASP Top 10), захист вебзастосунків (WAF), розмежування доступу в застосунках і базах даних, шифрування даних, запобігання витоку (DLP).

3.3. Інтеграція засобів кіберзахисту в корпоративних і державних системах

Ядром інтеграції в організації є система управління подіями безпеки (SIEM) і центр операцій з безпеки (SOC), куди надходять журнали з мережевого обладнання, серверів, EDR і застосунків. Їх доповнюють єдине керування ідентифікацією (IAM, SSO, багатофакторна автентифікація), автоматизація реагування (SOAR) та обмін індикаторами компрометації. На державному рівні діє національна система кібербезпеки (Закон № 2163-VIII): Держспецзв'язку, СБУ, кіберполіція, Міноборони, розвідка, НБУ за координації РНБО. Закон № 4336-IX створює національну систему реагування на кіберінциденти (CERT-UA, галузеві та регіональні команди), систему обміну інформацією про кіберзагрози та посади фахівців із кібербезпеки в держорганах. У морській галузі дані ECDIS і системи моніторингу механізмів MMC надходять до системи управління безпекою судна (SMS) і класифікаційного товариства (DNV) під кібермоніторингом.

Критерії гарантій включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації. В цих Критеріях вводиться сім рівнів гарантій (Г-1, ..., Г-7), які є ієрархічними. Ієрархія рівнів гарантій відбиває поступово наростаючу міру певності в тому, що реалізовані в комп'ютерній системі послуги дозволяють протистояти певним загрозам, що механізми, які їх реалізують, в свою чергу коректно реалізовані і можуть забезпечити очікуваний споживачем рівень захищеності інформації під час експлуатації комп'ютерної системи.

Спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості. Якщо існують вимоги щодо контролю за діями користувачів або легальністю доступу і за спроможністю комплексу засобів захисту виконувати свої функції, то відповідні послуги треба шукати у розділі “Критерії спостереженості”. В цьому розділі описані такі послуги: реєстрація,

ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, автентифікація при обміні, автентифікація відправника (невідмова від авторства), автентифікація одержувача (невідмова від одержання). Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в комп'ютерній системі, цей документ містить критерії гарантій, що дозволяють оцінити коректність реалізації послуг.

Доступність. Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності. Якщо існують вимоги щодо захисту від відмови в доступі або захисту від збоїв, то відповідні послуги треба шукати в розділі “Критерії доступності”. В цьому розділі описані такі послуги: використання ресурсів, стійкість до відмов, горяча заміна, відновлення після збоїв.

Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. Якщо існують вимоги щодо обмеження можливості модифікації інформації, то відповідні послуги треба шукати в розділі “Критерії цілісності”. В цьому розділі описані такі послуги: довірча цілісність, адміністративна цілісність, відкат і цілісність при обміні.

Конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Якщо існують вимоги щодо обмеження можливості ознайомлення з інформацією, то відповідні послуги треба шукати в розділі “Критерії конфіденційності”. В цьому розділі описані такі послуги: довірча конфіденційність, адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні (експорту/імпорту).

Рівні починаються з першого (1) і зростають до значення n , де n – унікальне для кожного виду послуг. Функціональні критерії розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів.

В контексті Критеріїв комп'ютерна система розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного.

вимоги до гарантій.

вимоги до функцій захисту (послуг безпеки);

Нормовані специфікації ФПЗ, структуровані за видами загроз для інформації і за способами здійснення цих загроз, наведені в НД ТЗІ 2.5-001-99 . В процесі оцінки спроможності комп'ютерної системи забезпечувати захист оброблюваної інформації від несанкціонованого доступу розглядаються вимоги двох видів:

Функціональні послуги захисту. Функціональна послуга захисту (ФПЗ) являє собою взаємопов'язаний набір виконуваних у середовищі експлуатації АТС елементарних функцій, що дозволяє протистояти певній множині загроз для інформації. У найпростішому випадку ФПЗ є одна елементарна функція, спрямована на протидію визначеній одній загрозі. З позицій ТЗІ АТС разом із реалізованою на ній системою захисту розглядається як набір ФПЗ.

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами експлуатації ІТС. Створення комплексів технічного захисту інформації від витoku технічними каналами здійснюється, якщо в ІТС обробляється інформація, що становить державну таємницю, або коли необхідність цього визначено власником інформації.

спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскуванню під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або

нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів тощо;

витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;

Зростання ступеня захищеності може досягатись як підсиленням певних послуг, тобто включенням до профілю більш високого рівня послуги, так і включенням до профілю нових послуг. Кожна послуга є набором функцій, які дозволяють протистояти певній множині загроз. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, хоча й не є точними підмножинами один одного. Рівні починаються з першого й зростають до певного значення, унікального для кожного виду послуг. До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від:

Визначаються загальна структура та склад КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації, обмеження щодо середовищ функціонування ІТС та використання її ресурсів для реалізації завдань захисту, припустимі витрати на створення КСЗІ, умови створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів), загальні вимоги до застосування в ІТС (окремих її підсистемах, компонентах) організаційних, технічних, криптографічних та інших заходів захисту інформації, що увійдуть до складу КСЗІ. Для ІТС формується перелік необхідних функціональних послуг захисту (далі - ФПЗ) від НСД та вимог до рівнів реалізації кожної з них, визначається рівень гарантій реалізації послуг. Визначені вимоги складають профіль захищеності інформації в ІТС або її компоненті. ФПЗ є ієрархічними в тому розумінні, що їх реалізація забезпечує зростаючу захищеність від загроз відповідного типу (конфіденційності - К, цілісності - Ц і доступності - Д).

На підставі визначених завдань і функцій ІТС, результатів аналізу її середовищ функціонування, моделей загроз і порушників та результатів аналізу ризиків визначаються компоненти ІТС (наприклад, ЛОМ, спеціалізований АРМ, Інтернетвузол тощо), для яких необхідно або доцільно розробляти свої власні політики безпеки, відмінні від загальної політики безпеки в ІТС.

Якщо залишковий ризик перевищує гранично допустимий, вносять відповідні зміни до складу заходів і засобів захисту, після чого всі процедури виконують повторно до одержання прийняттого результату.

На етапі проектування КСЗІ, після формування пропозицій щодо складу заходів і засобів захисту, здійснюється оцінка залишкового ризику для кожної пропозиції (наприклад, за критерієм «ефективність/вартість»), вибирається найбільш оптимальна серед них і первинна оцінка уточнюється.

Після цього необхідно здійснити первинне (попереднє) оцінювання допустимих витрат на блокування загроз, виходячи з вибраного варіанту побудови КСЗІ і виділених на це коштів.

досягнення максимального рівня захищеності інформації за необхідних витрат і мінімального рівня обмежень на технологію її обробки в ІТС.

досягнення необхідного рівня захищеності інформації за допустимих витрат і заданого рівня обмежень на технологію її обробки в ІТС;

досягнення необхідного рівня захищеності інформації за мінімальних витрат і допустимого рівня обмежень на технологію її обробки в ІТС;

Можливі такі варіанти:

Загальна структура та склад КСЗІ. Вибір варіанту побудови КСЗІ Після завершення аналізу всіх можливих ризиків необхідно здійснити вибір варіанту побудови КСЗІ в залежності від ступеня обмеження доступу до інформації, яка обробляється в ІТС, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних, фінансових та інших ресурсів, які є у розпорядженні власника ІТС.

На технічному рівні – це застосування пасивних засобів захисту: штор на вікнах, систем екранування, заземлення та зашумлення, а також оновлення та впровадження нових систем і засобів ТЗІ.

На організаційному рівні – це проведення аналізу відомих загроз, пошук нових запобіжних заходів, оновлення політики безпеки, навчання та тренування персоналу.

Етап попередження

інформаційних ресурсів – їх відновлення за допомогою резервних і архівних копій, які зберігаються на зовнішніх носіях.

операційної системи та програмних засобів – їх відновлення за допомогою інсталяційних файлів (дисків);

технологічних процесів – їх відновлення за допомогою плану аварійного відновлення та проведення ремонтних заходів;

На апаратно-програмному рівні – це подолання наслідків реалізації загроз у разі порушень:

На організаційно-правовому рівні – це дисциплінарне або адміністративне (кримінальне) розслідування правопорушення (злочину) та притягнення винних до відповідальності.

Етап нейтралізації

сприяння притягненню винних до відповідальності (кримінальної, адміністративної, цивільно-правової, дисциплінарної).

взаємодії (у разі необхідності) з державними правоохоронними органами щодо виявлення та розкриття правопорушення (в тому числі за готування до злочину і за замах на злочин);

збереження слідів правопорушення;

наступного дослідження їх;

Зазначимо, що ці заходи можуть бути спрямовані на документування методів НСД до АС для:

Для цього в АС встановлюються міжмережеві екрани, файерволи (брандмауери), антивірусні програмні засоби та спеціальні комплекси засобів захисту інформації від НСД.

Ці заходи забезпечують апаратно-програмне блокування спроб несанкціонованого доступу (НСД) порушника (хакера) до інформації в АС або ураження системи вірусами за допомогою спеціальних апаратних комплексів та програмних засобів захисту інформації.

Етап зупинення

комплексні засоби захисту (органічне поєднання всіх груп).

пасивні засоби захисту: закриття вікон та встановлення на них ґрат, закриття та опечатування дверей, системних блоків, роз'ємів технічних засобів АС тощо;

активні засоби захисту: охоронна сигналізація та відеоспостереження;

На організаційному рівні – це використання заходів розвідки та дезінформації. На інженерно-технічному рівні – це впровадження засобів ТЗІ, які поділяються на:

Етап виявлення

Виявлення ► Зупинення ► Нейтралізація ► Попередження

Стосовно автоматизованих (комп'ютерних) систем (АС) ці принципи та етапи дають можливість також визначити 4 етапи та види захисту від загроз для електронних інформаційних ресурсів АС, які циклічно повторюються з метою постійного оновлення та підвищення ефективності заходів і засобів захисту.

4) попередження загроз, тобто аналіз відомих загроз та впровадження відповідних запобіжних заходів.

3) забезпечення нейтралізації та ліквідації загроз, а також подолання наслідків загроз, які не вдалося блокувати;

2) організація протидії загрозам та їх блокування, тобто зупинення та локалізації загроз під час їх реалізації;

1) організація зовнішніх рубежів безпеки з метою своєчасного виявлення загроз;

Загальний аналіз проблем організування захисту від будь-яких загроз дає можливість визначити 4 головні принципи та етапи заходів:

Комплексна система захисту інформації (КСЗІ) – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС.

Контрольні запитання до теми 3

1. Назвіть основні принципи побудови КСЗІ.
2. У чому полягає принцип розумної достатності?
3. Що означають ешелонований захист і нульова довіра?
4. Охарактеризуйте етапи виявлення, зупинення, нейтралізації та попередження.
5. Які варіанти побудови КСЗІ існують?
6. Що таке профіль захищеності?
7. Які засоби захисту застосовують на мережевому рівні?
8. Які механізми діють на системному та прикладному рівнях?
9. Яку роль відіграють SIEM, SOC і SOAR?
10. Хто входить до національної системи кібербезпеки України?

Тема 4. Міжнародні стандарти та кращі практики побудови КСЗІ

4.1. ISO/IEC 27000, NIST Cybersecurity Framework, COBIT

Серія ISO/IEC 27000 – стандарти систем управління інформаційною безпекою (СУІБ): 27001 (вимоги для сертифікації), 27002 (заходи), 27005 (ризики), 27007 (аудит), 27017 (хмари), 27035 (інциденти). ISO/IEC 27001:2022 містить вимоги розділів 4–10 (контекст, лідерство, планування, підтримка, функціонування, оцінювання, поліпшення) і додаток А з 93 заходами в чотирьох темах: організаційні (37), людські (8), фізичні (14), технологічні (34). **NIST Cybersecurity Framework 2.0** (2024) – добровільна рамкова модель із шістьма функціями: Govern (врядування, додана у версії 2.0), Identify, Protect, Detect, Respond, Recover. Організація визначає поточний і цільовий профілі та рівень зрілості (Tiers 1–4); модель NIST рекомендують і настанови ІМО. **COBIT 2019** (ISACA) – рамкова модель врядування та управління ІТ, яка пов'язує безпеку з цілями бізнесу. Вона містить 40 цілей у п'яти доменах (EDM, APO, BAI, DSS, MEA), а зрілість процесів оцінюють за рівнями 0–5.

4.2. Європейські підходи (ENISA, GDPR)

ENISA – Агентство ЄС з кібербезпеки (засноване 2004 р.). Cybersecurity Act (Регламент 2019/881) надав йому постійний мандат і запровадив європейську сертифікацію кібербезпеки продуктів і послуг. **Директива NIS2** (2022/2555) охоплює суттєві та важливі суб'єкти (енергетика, транспорт, зокрема водний, банки, охорона здоров'я), робить керівництво відповідальним за кіберризики і встановлює строки звітування про інциденти: 24 год (раннє попередження), 72 год (повідомлення), 1 місяць (фінальний звіт). Штрафи – до 10 млн євро або 2 % світового обороту. **GDPR** (Регламент 2016/679, застосовується з 25.05.2018) встановлює принципи обробки персональних даних (законність, обмеження мети, мінімізація, точність, обмеження зберігання, цілісність і конфіденційність, підзвітність) і вимоги privacy by design, оцінки впливу (DPIA) та повідомлення про порушення протягом 72 год. Штрафи – до 20 млн євро або 4 % світового обороту. Для України ці акти є орієнтиром гармонізації законодавства.

4.3. Українська нормативно-правова база

Основу становлять закони України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах» (№ 80/94-ВР), «Про державну таємницю», «Про захист персональних даних», «Про основні засади забезпечення кібербезпеки України» (№ 2163-VIII від 05.10.2017), «Про електронну ідентифікацію та електронні довірчі послуги», «Про критичну інфраструктуру» (2021). Серед підзаконних актів – Правила забезпечення захисту інформації (постанова КМУ № 373 від 29.03.2006) і Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури (постанова КМУ № 518 від 19.06.2019). Технічні вимоги визначають ДСТУ 3396 та НД ТЗІ: 2.5-004-99 (критерії оцінки захищеності), 2.5-005-99 (класи АС), 3.7-003-2005 (порядок створення КСЗІ), 1.6-005-2013 (категорювання).

Закон № 4336-IX від 27.03.2025 (чинний з 20.04.2025, окремі норми – з 19.10.2025) скасовує обов'язковість КСЗІ і запроваджує управління ризиками на основі базових (затверджує Держспецзв'язку), галузевих і цільових профілів безпеки. Власники систем самі оцінюють ризики й обирають заходи, системи авторизують за декларативним принципом, а державний контроль має три рівні: самооцінювання, оцінювальні заходи (аудит), контрольні заходи. Для КСЗІ, створення яких уже розпочато, передбачено перехідний період, а їх напрацювання можна використати під час авторизації.

У міжнародних нормативних актах об'єктами кіберзахисту розглядаються інформаційні технологічні системи у їх взаємозв'язку та взаємодії. Натомість вітчизняні підходи зосереджені переважно на захисті інформації, що обробляється в автоматизованих системах управління, особливо тих, які використовуються на критично важливих або потенційно небезпечних об'єктах. Галузева специфіка, зокрема особливості морського транспорту, при цьому практично не враховується.

На відміну від цього, міжнародна практика зосереджується на забезпеченні безпеки безпосередньо суден і портових об'єктів як цілісних систем. Вітчизняний підхід базується на визначенні значущості об'єктів критичної інфраструктури, що підлягають захисту, унаслідок

чого менш значущі об'єкти фактично залишаються поза межами правового регулювання. У міжнародних же документах вимоги щодо кібербезпеки поширюються на всі судна та портові засоби без винятку. Крім того, положення українського законодавства не містять детальних практичних рекомендацій, що ускладнює їх застосування на рівні конкретного судна або портової інфраструктури та потребує додаткової адаптації.

Передусім Закон орієнтований на захист об'єктів критичної інформаційної інфраструктури, до яких належать комунікаційні системи незалежно від форми власності, що забезпечують обробку національних інформаційних ресурсів або використовуються в діяльності органів державної влади, місцевого самоврядування, правоохоронних структур і військових формувань. До сфери його регулювання також віднесено системи, що забезпечують суспільні потреби, зокрема у галузях електронного урядування, електронних послуг, електронної комерції та документообігу. При цьому об'єктами захисту виступають насамперед інформаційні системи та мережі, а не фізичні об'єкти, на яких вони функціонують.

До спеціалізованого законодавства у сфері протидії кіберзагрозам належить Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 №45 [10]. Водночас, попри визначення ним правових та організаційних засад захисту національних інтересів у кіберпросторі, а також ключових напрямів державної політики у сфері кібербезпеки та механізмів координації відповідної діяльності, цей нормативний акт має загальний характер і поширюється на всі галузі економіки. Він не враховує специфічних особливостей транспортної сфери загалом і морського транспорту зокрема.

Разом із тим діяльність Міністерства інфраструктури України у сфері нормативно-правового забезпечення інформаційної безпеки морського транспорту не відповідає сучасним викликам. Основна увага зосереджується переважно на технічних аспектах регламентування та захисту інформації, тоді як комплексний розвиток системи морської кібербезпеки відбувається недостатньо ефективно.

Водночас розроблена Національним інститутом стандартів і технологій США рамкова модель підвищення кібербезпеки критичної інфраструктури була рекомендована до застосування відповідними циркулярами ІМО. Більшість ключових нормативних і методичних документів у цій сфері створено саме у США та інших провідних морських державах, тому українська морська галузь значною мірою орієнтується на їхні підходи та рекомендації.

Якщо в ІТС обробляються інші види інформації, то вимоги цього нормативного документа суб'єкти системи ТЗІ можуть використовувати як рекомендації. Порядок створення КСЗІ в ІТС є єдиним незалежно від того, створюється КСЗІ в ІТС, яка проектується, чи в діючій ІТС, якщо виникла необхідність забезпечення захисту інформації або модернізації вже створеної КСЗІ.

Встановлений цим НД ТЗІ порядок є обов'язковим для всіх суб'єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, в ІТС яких обробляється інформація, яка належить до державних інформаційних ресурсів, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством.

НД ТЗІ призначений для суб'єктів інформаційних відносин (власників або розпорядників ІТС, користувачів), діяльність яких пов'язана з обробкою інформації, що підлягає захисту, розробників комплексних систем захисту інформації в ІТС, для постачальників компонентів ІТС, а також для фізичних та юридичних осіб, які здійснюють оцінку захищеності оброблюваної інформації на відповідність вимогам ТЗІ.

НД ТЗІ не встановлює нових норм, а систематизує в одному документі вимоги, норми і правила, які безпосередньо або непрямо витікають з положень діючих нормативних документів.

Основний керівний документ – це НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення КСЗІ в ІТС» Він визначає порядок прийняття рішень щодо складу комплексної системи захисту інформації в залежності від умов функціонування ІТС і видів оброблюваної

інформації, визначення обсягу і змісту робіт, етапності робіт, основних завдань та порядку виконання робіт кожного етапу. Побудований у вигляді керівництва, яке містить перелік робіт і посилання на діючі нормативні документи, у відповідності до яких ці роботи необхідно виконувати. Якщо якийсь з етапів чи видів робіт не нормовано, наводиться короткий зміст робіт та якими результатами вони повинні закінчуватись. Дія цього НД ТЗІ поширюється тільки на ІТС, в яких здійснюється обробка інформації автоматизованим способом. Відповідно, для таких ІТС чинні всі нормативно-правові акти та нормативні документи щодо створення ІТС та щодо захисту інформації в АС.

НД ТЗІ 2.7-010-2009. Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу, затверджений наказом Адміністрації Держспецзв'язку від 24.07.2009 № 172.

Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу, затверджений наказом Адміністрації Держспецзв'язку від 24.07.2009 № 172 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.

Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах, затверджений наказом Адміністрації Держспецзв'язку від 25.03.2011 № 65 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806. НД ТЗІ 2.7-009-2009.

Порядок формування реєстру організаторів державної експертизи у сфері ТЗІ та реєстру експертів з питань ТЗІ, затверджений наказом Адміністрації Держспецзв'язку від 16.04.2008 № 64 НД ТЗІ 2.6-001-2011.

Державна експертиза КСЗІ Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 16.05.2007 № 93 та зареєстроване в Міністерстві юстиції України 16.07.2007 за № 820/14087.

НД ТЗІ 3.3-001-2007. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації, затверджений наказом Адміністрації Держспецзв'язку від 12.12.2007 № 232.

НД ТЗІ 3.1-001-2007. Створення комплексу технічного захисту інформації. Передпроектні роботи, затверджений наказом Адміністрації Держспецзв'язку від 12.12.2007 № 232.

НД ТЗІ 2.1-002-2007. Випробування комплексу технічного захисту інформації. Основні положення, затверджений наказом Адміністрації Держспецзв'язку від 12.12.2007 № 232.

НД ТЗІ 1.1-005-2007. Створення комплексу технічного захисту інформації. Основні положення, затверджений наказом Адміністрації Держспецзв'язку від 12.12.2007 № 232.

Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок, затверджені наказом Державної служби України з питань технічного захисту інформації від 09.06.95 № 25.

Створення комплексів ТЗІ на об'єктах інформаційної діяльності ТР ЕОТ - 95.

НД ТЗІ 2.5-010-2003. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 02.04.2003 № 33 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.

НД ТЗІ 2.5-008-2002. Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2, затверджений наказом ДСТСЗІ СБ України від 13.12.2002 № 84 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.

НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.99 № 22.

Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.99 № 22.

НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.99 № 22.
НД ТЗІ 2.5-004-99.

Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.99 № 22.

Захист інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 1.1-002-99.

Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБ України від 28.04.99 № 22 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.

Типове положення про службу захисту інформації в автоматизованій системі, затверджений наказом ДСТСЗІ СБ України від 04.12.2000 № 53. НД ТЗІ 3.7-001-99.

НД ТЗІ 1.6-005-2013. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці, затверджений наказом Адміністрації Держспецзв'язку від 15.04.2013 № 215 НД ТЗІ 1.4-001-2000.

Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі, затверджений наказом ДСТСЗІ СБ України від 08.11.2005 № 125 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.

Створення КСЗІ в автоматизованій системі НД ТЗІ 3.7-003-2005.

Нормативні документи системи технічного захисту інформації

ДСТУ 3396.2-97. Технічний захист інформації. Терміни та визначення.

ДСТУ 3396.1-96. Технічний захист інформації. Порядок проведення робіт.

ДСТУ 3396.0-96. Технічний захист інформації. Основні положення.

ДСТУ 2853-94. Програмні засоби ЕОМ. Підготовка і проведення випробувань.

ДСТУ 2851-94. Програмні засоби ЕОМ. Документування результатів випробувань.

ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення.

Державні стандарти України

Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.2006 № 373 з останніми змінами згідно ПКМУ № 938 від 07.09.2011.

Основні нормативно-правові акти України Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

Нормативні документи системи технічного захисту інформації. Їх роль та призначення.

Контрольні запитання до теми 4

1. Які стандарти входять до серії ISO/IEC 27000?
2. Як згруповано заходи додатка А ISO/IEC 27001:2022?
3. Назвіть шість функцій NIST CSF 2.0.
4. Що таке профілі та рівні зрілості в NIST CSF?
5. Яке призначення COBIT 2019 і які його домени?
6. Яке призначення ENISA і що запровадив Cybersecurity Act?
7. Які строки повідомлення про інциденти встановлює NIS2?
8. Назвіть принципи обробки персональних даних за GDPR.
9. Які закони становлять основу захисту інформації в Україні?
10. Що змінив Закон № 4336-IX від 27.03.2025?

Тема 5. Системи управління інформаційною безпекою (СУІБ)

СУІБ – частина системи управління організацією, яка на основі оцінки ризиків забезпечує створення, впровадження, моніторинг і постійне поліпшення інформаційної безпеки (ISO/IEC 27001). КСЗІ захищає конкретну систему, тоді як СУІБ охоплює процеси, ролі та документи всієї організації.

5.1. Стратегії і політики інформаційної безпеки

Стратегія ІБ визначає довгострокові цілі захисту, узгоджені з бізнес-стратегією, допустимим рівнем ризику та законодавством; на державному рівні діє Стратегія кібербезпеки України (2021). **Політика безпеки** – сукупність правил, обмежень та інструкцій, що регламентують порядок обробки інформації. Її документи утворюють ієрархію: загальна політика ІБ, затверджена керівником; тематичні політики (доступ і паролі, антивірусний захист, резервне копіювання, мобільні пристрої, хмари); інструкції для окремих ролей. За НД ТЗІ 3.7-003-2005 політику розробляють разом із вибором варіанту КСЗІ, планом захисту і календарним планом робіт; переглядають її щонайменше раз на рік.

5.2. Життєвий цикл СУІБ

Життєвий цикл СУІБ будується за циклом **PDCA**: Plan – область дії, політика, оцінка ризиків, план обробки ризиків, Положення про застосовність (SoA); Do – впровадження заходів і навчання; Check – моніторинг, внутрішній аудит, аналіз керівництвом; Act – коригувальні дії та поліпшення. Національний аналог – етапи створення КСЗІ за НД ТЗІ 3.7-003-2005: 1) формування вимог (СЗІ, категоріювання, обстеження, моделі порушника і загроз, аналіз ризиків); 2) політика безпеки і план захисту; 3) технічне завдання, погоджене з Держспецзв'язку; 4) проєктування; 5) введення в дію (випробування, дослідна експлуатація, державна експертиза, атестат відповідності); 6) супровід.

5.3. Впровадження та супровід у реальних організаціях

Роботи організовує **служба захисту інформації** (НД ТЗІ 1.4-001-2000) або керівник з ІБ (CISO). **Категоріювання** обов'язкове для об'єктів інформаційної діяльності, де обробляють інформацію з обмеженим доступом (НД ТЗІ 1.6-005-2013). За ТПКО-95 є чотири категорії: I – «особливої важливості», II – «цілком таємно», III – «таємно» та інша передбачена законом таємниця, IV – інформація, що не становить державної таємниці. Категоріювання буває первинним, черговим (не рідше раз на 5 років) і позачерговим; результати фіксують в акті, чинному 5 років. **Обстеження середовищ функціонування** (обчислювального, інформаційного, користувацького, фізичного) описує склад системи, канали зв'язку, наявні засоби захисту; його результати – акт обстеження, формуляр ІТС і перелік інформації, що підлягає захисту. Впровадження СУІБ потребує підтримки керівництва, інвентаризації активів, оцінки ризиків, навчання персоналу та внутрішніх аудитів. Сертифікат ISO/IEC 27001 видають на 3 роки з щорічними наглядовими аудитами.

помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

невиконання вимог до організаційних заходів захисту чинних в ІТС розпорядчих документів;

неумисне зараження ПЗ комп'ютерними вірусами;

неправомірною зміною режимів роботи ІТС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

ненавмисне пошкодження носіїв інформації;

дії, що призводять до відмови ІТС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм тощо);

Випадковими загрозами суб'єктивної природи (дії, які здійснюються персоналом або користувачами по неухважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

навмисні дії (спроби) потенційних порушників.
помилки персоналу (користувачів) ІТС під час експлуатації;
наслідки помилок під час проектування та розробки компонентів ІТС (технічних засобів, технології обробки інформації, ПЗ, засобів захисту, структур даних тощо);
збої та відмови у роботі технічних або програмних засобів (ПЗ) ІТС;
зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);

Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно ІТС і повинні враховуватись у моделі загроз, наприклад:

Загрози для інформації, що обробляється в ІТС, залежать від характеристик ОС, апаратного складу, програмних засобів, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні.

перелік можливих способів реалізації загроз певного типу (способів атак) відносно різних інформаційних об'єктів ІТС у різному стані класифікований, наприклад, за такими ознаками, як компонент обчислювальної системи ІТС або програмний засіб, уразливості яких експлуатуються порушником, причини виникнення відповідної уразливості тощо.

2.4. Складання календарного плану робіт із захисту інформації

2.3. Складання плану захисту

2.2. Складання політики безпеки

2.1. Вибір варіанту КСЗІ

2. Розробка політики безпеки інформації в ІТС.

Контрольні запитання до теми 5

1. Дайте визначення СУІБ. Чим вона відрізняється від КСЗІ?

2. Що визначає стратегія ІБ?

3. Що таке політика безпеки і яка ієрархія її документів?

4. Опишіть етапи циклу PDCA.

5. Що таке Положення про застосовність (SoA)?

6. Назвіть етапи створення КСЗІ за НД ТЗІ 3.7-003-2005.

7. Що підтверджує атестат відповідності КСЗІ?

8. Яку роль відіграє служба захисту інформації?

9. Які категорії об'єктів встановлює ТПКО-95?

10. Яка мета обстеження середовищ функціонування ІТС?

Тема 6. Криптографічні методи захисту інформації у КЗІ

6.1. Сучасні криптографічні алгоритми та протоколи

Криптографія забезпечує конфіденційність, цілісність, автентичність і неспростовність; за принципом Керкгоффса стійкість шифру має залежати лише від секретності ключа. **Симетричні шифри** (один спільний ключ): AES (128/192/256 біт), ChaCha20, національний ДСТУ 7624:2014 «Калина»; DES і RC4 застаріли. **Асиметричні алгоритми** (відкритий і особистий ключі): RSA (від 2048–3072 біт), криптографія на еліптичних кривих (ECDH, ECDSA), національний стандарт цифрового підпису ДСТУ 4145-2002. **Геш-функції**: SHA-2, SHA-3, ДСТУ 7564:2014 «Купина» (MD5 і SHA-1 не рекомендовані). **Протоколи**: TLS 1.3 (вебтрафік), IPsec (VPN), SSH (віддалене адміністрування), S/MIME (пошта). Через загрозу квантових комп'ютерів NIST у 2024 р. затвердив постквантові стандарти FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) і FIPS 205 (SLH-DSA), тому системи мають бути криптогнучкими, тобто дозволяти заміну алгоритмів.

6.2. Електронний підпис, PKI, керування ключами

Електронний підпис (ЕП) створюють особистим ключем від геш-значення документа, а перевіряють відкритим ключем із сертифіката. Закон «Про електронну ідентифікацію та електронні довірчі послуги», гармонізований з європейським регламентом eIDAS, визначає види підписів: електронний, удосконалений і **кваліфікований (КЕП)**, що прирівнюється до власноручного. **Інфраструктура відкритих ключів (PKI)** – політики, процедури та засоби для видачі, зберігання й відкликання сертифікатів X.509. В Україні функції центрального засвідчувального органу виконує Мінцифри, а сертифікати видають кваліфіковані надавачі електронних довірчих послуг (КНЕДП). Довіра будується ланцюжком «кореневий сертифікат → надавач → користувач», а статус сертифіката перевіряють за списками відкликаних сертифікатів (CRL) чи протоколом OCSP. **Керування ключами** охоплює генерацію, розповсюдження, захищене зберігання (токени, HSM, хмарний «Дія.Підпис»), заміну, відкликання та знищення.

6.3. Прикладне застосування в державних і бізнес-системах

Державні системи: «Дія» (хмарний КЕП «Дія.Підпис»), система взаємодії реєстрів «Трембіта», Prozorro, «Електронний суд», електронна звітність до ДПС. Для державних ресурсів використовують засоби КЗІ з позитивним висновком Держспецзв'язку. Бізнес-системи: HTTPS, VPN, «клієнт-банк», шифрування дисків, документообіг із КЕП. У морській галузі стандарт S-63 Міжнародної гідрографічної організації визначає захист офіційних електронних навігаційних карт, а для обміну даними з портами й митницею застосовують EDI/EDIFACT, електронні коносаменти та ЕП.

Перші кроки до регламентації інформаційного обміну на морі були зроблені ще у 1979 році, коли було ухвалено резолюцію щодо розвитку систем передавання повідомлень про лихо і безпеку. Надалі ці підходи були розвинені у документах, що визначають принципи функціонування судових систем повідомлень, а також у правилах електронного документообігу, зокрема електронних коносаментів. Важливу роль відіграли також типові закони ЮНСІТРАЛ щодо електронної торгівлі та електронних підписів, які стали основою для формування як міжнародних, так і національних нормативних систем.

У сучасних умовах паперовий документообіг дедалі частіше виявляється неефективним, тому у сфері морських перевезень активно впроваджуються системи електронного обміну даними, такі як EDI та EDIFACT, що відповідають положенням Конвенції з полегшення міжнародного морського судноплавства.

Усі суб'єкти інформаційної взаємодії оперують, зокрема, конфіденційними даними, компрометація яких може призвести до серйозних наслідків: збоїв у роботі бортових систем, відхилення судна від заданого курсу, фінансових втрат унаслідок витоку комерційної чи персональної інформації, а також отримання неточних або несвоєчасних відомостей про технічний стан обладнання і механізмів. Найбільш уразливими об'єктами атак є інформаційні ресурси навігаційних систем і систем морського зв'язку. Для їх захисту застосовуються криптографічні методи, системи автентифікації, електронний цифровий підпис та інші

інструменти. Зокрема, Міжнародна гідрографічна організація запровадила стандарт S63, який регламентує захист офіційних електронних навігаційних карт.

виконання вимог з кібербезпеки в інформаційних мережах.

організаційно-технічні заходи, спрямовані на забезпечення збереження інформації з обмеженим доступом;

захист від несанкціонованих дій через канал зв'язку від осіб, що не допущені до засобів шифрування, але що переслідують цілі компрометації таємної інформації і дезорганізації роботи абонентських пунктів;

забезпечення захисту програмних продуктів та засобів обчислювальної техніки від внесення в них програмних вірусів та закладок;

забезпечення захисту технічних засобів та приміщень, в яких ведеться обробка конфіденційної інформації, від витоку через побічні канали і від можливо вбудованих в них електронних пристроїв знімання інформації;

виявлення порушень цілісності об'єктів даних;

підтвердження справжності об'єктів даних та користувачів (аутентифікація сторін, що встановлюють зв'язок);

захист інформації в каналах зв'язку та базах даних криптографічними методами;

Завдання забезпечення безпеки інформації:

Безпека інформації забезпечується шляхом організації допуску до неї, захисту її від перехвату, спотворення чи введення помилкової інформації. З цією метою застосовуються фізичні, технічні, апаратні, програмно-апаратні та програмні засоби захисту. Останні посідають центральне місце в системі забезпечення безпеки інформації в інформаційних системах та телекомунікаційних мережах.

Безпека інформації в інформаційній системі чи телекомунікаційній мережі забезпечується здатністю цієї системи зберігати таємність інформації при її введенні, виведенні, передаванні, обробці та зберіганні, а також протистояти її руйнуванню, крадіжкам чи спотворенню.

4. Організаційний – попередження доступу на об'єкт інформаційної діяльності сторонніх осіб за допомогою організаційних заходів (охорона, пропускний режим, регламентація доступу тощо).

- попередження несанкціонованого розголошення.

- попередження несанкціонованої модифікації;

3. Криптографічний (КЗІ) – попереджує доступ до інформації за допомогою математичних перетворень:

Контрольні запитання до теми 6

1. Сформулюйте принцип Керкгоффа.
2. Чим відрізняються симетричні та асиметричні алгоритми?
3. Назвіть національні криптографічні стандарти України.
4. Яке призначення геш-функцій?
5. Для чого використовують TLS, IPsec і SSH?
6. Що таке постквантова криптографія?
7. Як створюють і перевіряють електронний підпис?
8. Чим кваліфікований електронний підпис відрізняється від інших видів?
9. Що таке PKI і як перевіряють статус сертифіката?
10. Назвіть етапи життєвого циклу криптографічних ключів.

Тема 7. Технічні засоби та методи захисту інформації

7.1. Засоби захисту від несанкціонованого доступу

Оснoву захисту від НСД становить **комплекс засобів захисту (КЗЗ)**: ідентифікація та автентифікація (паролі, токени, смарт-картки, біометрія, багатофакторна автентифікація), розмежування доступу, реєстрація подій, контроль цілісності. Його доповнюють міжмережеві екрани, IDS/IPS, антивіруси та EDR, DLP і засоби фізичного захисту. НД ТЗІ 2.5-004-99 розглядає систему як набір **функціональних послуг безпеки**, кожна з яких має кілька рівнів. Послуги конфіденційності – довірча й адміністративна конфіденційність, повторне використання об'єктів, аналіз прихованих каналів; цілісності – довірча й адміністративна цілісність, відкат; доступності – використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв; спостережності – реєстрація, ідентифікація й автентифікація, достовірний канал, розподіл обов'язків, самотестування. Коректність реалізації послуг оцінюють за сімома рівнями гарантій (Г-1...Г-7).

7.2. Канали витоку інформації та методи їх нейтралізації

Канали витоку інформації (КВІ) поділяють на групи: **акустичні й віброакустичні** (стіни, вентиляція, направлені мікрофони, лазерне знімання з вікон); **електромагнітні** (ПЕМВН моніторів, наведення на лінії зв'язку, мережі живлення, заземлення, труби опалення); **візуально-оптичні** (відеозакладки, спостереження за моніторами й документами); **матеріально-речові** (крадіжка носіїв, відходи, погано стерті носії); **програмно-апаратні** (закладки, віруси, несанкціоноване копіювання); **через персонал**. За потребою доступу до системи та залежністю від її стану виділяють шість класів КВІ – від підслуховування без доступу до підключення до апаратури під час обробки.

Методи нейтралізації. Організаційні: контрольована зона, режимні заходи, спецперевірки обладнання та спецобстеження приміщень. Пасивні технічні: екранування, заземлення, фільтри мереж живлення, звуко- і віброізоляція, захисні плівки на вікнах, обладнання в захищеному виконанні (TEMPEST). Активні технічні: просторове, лінійне та віброакустичне зашумлення, пошук закладок нелінійними локаторами. Носії, які більше не потрібні, гарантовано знищують.

7.3. Комплексні рішення технічного захисту

Комплекс ТЗІ на об'єкті створюють за НД ТЗІ 1.1-005-2007: передпроектні роботи (НД ТЗІ 3.1-001-2007), розроблення і впровадження заходів (3.3-001-2007), випробування (2.1-002-2007), експертиза та періодичний контроль. **Інтегровані системи безпеки об'єкта** поєднують контроль доступу, відеоаналітику й охоронно-пожежну сигналізацію з єдиним пунктом керування. У мережах використовують UTM/NGFW (міжмережевий екран, IPS, антивірус, VPN і вебфільтр в одному пристрої), платформи XDR і SASE/ZTNA для захищеного віддаленого доступу.

Для організації робіт зі створення КСЗІ в ІТС створюється Служба захисту інформації в ІТС. Вона створюється після прийняття рішення про необхідність створення КСЗІ.

Створення комплексу засобів захисту від несанкціонованого доступу (далі – КЗЗ) здійснюється в усіх ІТС, де обробляється інформація, яка належить до державних інформаційних ресурсів, належить до державної чи іншої таємниці або до окремих видів інформації, необхідність захисту якої визначено законодавством, а також в ІТС, де така необхідність визначена власником інформації. Рішення щодо необхідності вжиття заходів захисту від спеціальних впливів на інформацію приймається власником інформації в кожному випадку окремо. Роботи зі створення КСЗІ виконуються організацією-власником (розпорядником) ІТС з дотриманням вимог нормативно-правових актів щодо провадження діяльності у сфері захисту інформації.

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами експлуатації ІТС. Створення комплексів технічного захисту інформації від витоку технічними каналами здійснюється, якщо в ІТС обробляється інформація, що становить державну таємницю, або коли необхідність цього визначено власником інформації.

До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від: витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустoeлектричні та інші канали; несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскуванню під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів тощо; спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами експлуатації ІТС. Створення комплексів технічного захисту інформації від витоку технічними каналами здійснюється, якщо в ІТС обробляється інформація, що становить державну таємницю, або коли необхідність цього визначено власником інформації.

спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскуванню під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів тощо;

витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустoeлектричні та інші канали;

стратегічна цінність обробки інформації;

Критерії оцінки ризику повинні розроблятися, враховуючи наступне:

Визначення критеріїв. На цьому етапі використовуються дані обстеження всіх середовищ ІТС з метою визначення того, які інформаційні та технічні ресурси зі складу ІТС і з якою детальністю повинні розглядатися в процесі керування ризиком. Крім того, необхідно розробити критерії оцінки ризиків, впливу на активи та прийняття ризиків.

Визначення критеріїв оцінки ризиків.

6-го класу – канали, які у процесі обробки інформації з доступом зловмисника до елементів ІТС і зі зміною останніх. Сюди може бути віднесено незаконне підключення до апаратури та ліній зв'язку, а також зняття інформації на шинах живлення різних елементів ІТС.

Серед цих каналів: підміна і розкрадання носіїв інформації й апаратури, включення до програм блоків типу троянський кінь, комп'ютерний черв'як тощо.

5-го класу – канали, які проявляються безвідносно до обробки інформації з доступом зловмисника до елементів ІТС і зі зміною програмних або апаратних засобів.

Сюди може бути віднесено запам'ятовування і копіювання інформації в процесі обробки, використання програмних пасток тощо.

4-го класу – канали, які у процесі обробки інформації з доступом зловмисника до елементів ІТС, але без зміни останніх.

До них відносяться всілякі види копіювання носіїв інформації і документів, а також розкрадання виробничих відходів.

3-го класу – канали, які проявляються безвідносно до обробки інформації з доступом зловмисника до елементів ІТС, але без зміни останніх.

Сюди можуть бути віднесені електромагнітні випромінювання різних пристроїв ІТС, апаратури та ліній зв'язку, паразитні наведення в ланцюгах живлення, телефонних мережах, системах теплопостачання, вентиляції тощо.

2-го класу – канали, які у процесі обробки інформації без доступу зловмисника до елементів ІТС.

Сюди може бути віднесено підслуховування розмов, а також провокування на розмови осіб, що мають відношення до ІТС, і використання зловмисником візуальних, оптичних та акустичних засобів.

1-го класу – канали, які проявляються безвідносно до обробки інформації і без доступу зловмисника до елементів системи.

Наведемо орієнтовну характеристику каналів несанкціонованого отримання інформації виділених нами класів.

існуючі тільки в робочому стані ІТС (наприклад, побічні електромагнітні випромінювання та наведення).

потенційно існуючі незалежно від стану ІТС (наприклад, викрадати носії інформації можна незалежно від того, в робочому стані знаходяться засоби АС чи ні);

За другим критерієм (залежність появи КВІ від стану ІТС) КВІ можуть бути розділені на:

У свою чергу, такі канали можуть не залишити слідів в ІТС (наприклад, візуальний перегляд зображень на екранах моніторів або документів на паперових носіях), а можуть і залишити ті чи інші сліди (наприклад, розкрадання документів або машинних носіїв інформації).

вимагають доступу в приміщення ІТС.

не вимагають доступу, тобто дозволяють отримувати необхідну інформацію дистанційно (наприклад, шляхом візуального спостереження через вікна приміщень ІТС),

За першим критерієм (необхідність доступу до елементів ІТС для реалізації того чи іншого КВІ) КВІ можуть бути розділені на такі, що:

Всі можливі канали витоку інформації (КВІ) можна класифікувати за двома критеріями: необхідністю доступу до елементів ІТС для реалізації того чи іншого КВІ і залежністю появи КВІ від стану ІТС.

Джерело загрози – це безпосередній їх генератор або носій. Таким джерелом можуть бути люди, технічні засоби, моделі (алгоритми), а також – програми, технологічні схеми обробки, зовнішнє середовище. Спробуємо тепер, спираючись на наведену системну класифікацію загроз безпеки інформації, визначити повну множину загроз, потенційно можливих у сучасних автоматизованих системах. При цьому ми повинні врахувати не лише всі відомі (ті, що раніше проявлялися) загрози, але й такі загрози, які раніше не виявлялися, але потенційно можуть виникнути при застосуванні нових концепцій архітектурної побудови АС і технологічних схем обробки інформації.

Джерела загроз інформації в ІТС. Характеристика каналів витоку інформації.

Опис моделі загроз (у частині, що стосується переліку можливих способів реалізації загроз та їх класифікації), має бути викладений настільки детально, щоб дозволяти (на етапі аналізу ризиків, пов'язаних з реалізацією загроз для інформації в ІТС) однозначне визначення як збитків, що завдаються у випадку успішної реалізації загрози, так і ймовірності реалізації загрози (здійснення атаки) в певний спосіб.

застосування закладних пристроїв чи програм, вкорінення комп'ютерних вірусів.

подолання заходів захисту з метою використання інформації або нав'язування хибної інформації,

маскування під зареєстрованого користувача,

шляхом підключення до апаратури та ліній зв'язку,

можливі способи здійснення (механізм реалізації) загроз:

зовнішнє середовище.

технологія функціонування ІТС;

моделі, алгоритми, програми ІТС;

технічні засоби ІТС;

персонал ІТС;

джерела виникнення (які суб'єкти ІТС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу):

загрози спостережності та керованості ІТС – відмова в ідентифікації, автентифікації та реєстрації небезпечних дій;

загрози доступності – порушення можливості використання ІТС або оброблюваної інформації (відмова в обслуговуванні користувача);

загрози цілісності – несанкціонована модифікація (спотворення, фальсифікація, викривлення) інформації;

загрози конфіденційності – несанкціоноване ознайомлення з інформацією;

на порушення яких властивостей інформації або ІТС вона спрямована:

Для кожної з загроз необхідно визначити:

Перелік суттєвих загроз має бути максимально повним і деталізованим.

інші.

впровадження та використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж);

неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо;

одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача;

читання залишкової інформації з оперативної пам'яті ЕОТ, зовнішніх накопичувачів;

несанкціоноване копіювання носіїв інформації;

крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);

використання (шантаж, підкуп тощо) з корисливою метою персоналу ІТС;

впровадження та використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;

порушення режимів функціонування ІТС (обладнання і ПЗ);

порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІТС (електроживлення, заземлення, охоронної сигналізації, кондиціонування тощо.);

порушення фізичної цілісності ІТС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи ІТС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути:

наслідки некомпетентного застосування засобів захисту тощо.

неправомірне впровадження та використання заборонених політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення тощо);

будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

невиконання вимог до організаційних заходів захисту чинних в ІТС розпорядчих документів;

неумисне зараження ПЗ комп'ютерними вірусами;

неправомірною зміною режимів роботи ІТС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

ненавмисне пошкодження носіїв інформації;

дії, що призводять до відмови ІТС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм тощо);

Випадковими загрозами суб'єктивної природи (дії, які здійснюються персоналом або користувачами по неувважності, недбалості, незнанню тощо, але без навмисного наміру) можуть бути:

навмисні дії (спроби) потенційних порушників.
помилки персоналу (користувачів) ІТС під час експлуатації;
наслідки помилок під час проектування та розробки компонентів ІТС (технічних засобів, технології обробки інформації, ПЗ, засобів захисту, структур даних тощо);
збої та відмови у роботі технічних або програмних засобів (ПЗ) ІТС;
зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, пожежа або інші випадкові події);

Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно ІТС і повинні враховуватись у моделі загроз, наприклад:

Загрози для інформації, що обробляється в ІТС, залежать від характеристик ОС, апаратного складу, програмних засобів, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні.

перелік можливих способів реалізації загроз певного типу (способів атак) відносно різних інформаційних об'єктів ІТС у різному стані класифікований, наприклад, за такими ознаками, як компонент обчислювальної системи ІТС або програмний засіб, уразливості яких експлуатуються порушником, причини виникнення відповідної уразливості тощо.

перелік можливих типів загроз, класифікований за результатом впливу на інформацію, тобто на порушення яких її властивостей вони спрямовані (конфіденційності, цілісності або доступності інформації);

Модель загроз має містити абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз для інформації, яка потребує захисту. Модель загроз повинна визначити:

На підставі Акту обстеження та Моделі порушника політики безпеки СЗІ розробляє «Модель загроз для інформації в ІТС», яка затверджується керівником організації-власника (розпорядника) ІТС, та вноситься, за необхідності, до відповідних розділів Плану захисту та Технічного завдання на створення КСЗІ.

якісна недостатність – недосконалість конструкції (організації) елементів системи, в силу цього можуть з'являтися можливості випадкового або навмисного негативного впливу на оброблювану або збережену інформацію.

кількісна недостатність – фізична нестача одного або декількох елементів системи, що викликає порушення технологічного процесу обробки даних і / або перевантаження наявних елементів;

Перераховані різновиди передумов інтерпретуються таким чином:

Передумови появи загроз можуть бути об'єктивними (кількісна або якісна недостатність елементів системи) і суб'єктивними. До останніх відносяться діяльність розвідувальних органів іноземних держав, промислове шпигунство, діяльність кримінальних елементів, дії недобросовісного персоналу ІТС.

Навмисне походження загроз обумовлюється зловмисними діями людей.

побічний вплив – негативний вплив на систему в цілому або окремі її елементи, чиниться будь-якими явищами, що відбуваються всередині системи або у зовнішньому середовищі.

помилка – неправильне (разове або систематичне) виконання елементом однієї або декількох функцій, що відбувається внаслідок специфічного (постійного або тимчасового) його стану;

збій – тимчасове порушення працездатності якого-небудь елемента системи, наслідком чого може бути неправильне виконання ним у цей момент своєї функції;

відмова – порушення працездатності якого-небудь елемента системи, що призводить до неможливості виконання нею основних своїх функцій;

Випадкове походження обумовлюється спонтанними і не залежними від волі людей обставинами, що виникають в ІТС в процесі її функціонування. Найбільш відомими подіями

цього плану є відмови, збої, помилки, стихійні лиха та побічні впливи. Сутність перерахованих подій (окрім стихійних лих) визначається таким чином:

Походження загроз може бути випадковим і навмисним.

Після проведення обстеження середовищ ІТС необхідно визначити всі можливі потенційні загрози для ІТС.

Модель загроз для інформації в ІТС

виконання вимог з кібербезпеки в інформаційних мережах.

організаційно-технічні заходи, спрямовані на забезпечення збереження інформації з обмеженим доступом;

захист від несанкціонованих дій через канал зв'язку від осіб, що не допущені до засобів шифрування, але що переслідують цілі компрометації таємної інформації і дезорганізації роботи абонентських пунктів;

забезпечення захисту програмних продуктів та засобів обчислювальної техніки від внесення в них програмних вірусів та закладок;

забезпечення захисту технічних засобів та приміщень, в яких ведеться обробка конфіденційної інформації, від витоку через побічні канали і від можливо вбудованих в них електронних пристроїв знімання інформації;

виявлення порушень цілісності об'єктів даних;

підтвердження справжності об'єктів даних та користувачів (аутентифікація сторін, що встановлюють зв'язок);

захист інформації в каналах зв'язку та базах даних криптографічними методами;

Завдання забезпечення безпеки інформації:

Безпека інформації забезпечується шляхом організації допуску до неї, захисту її від перехвату, спотворення чи введення помилкової інформації. З цією метою застосовуються фізичні, технічні, апаратні, програмно-апаратні та програмні засоби захисту. Останні посідають центральне місце в системі забезпечення безпеки інформації в інформаційних системах та телекомунікаційних мережах.

Безпека інформації в інформаційній системі чи телекомунікаційній мережі забезпечується здатністю цієї системи зберігати таємність інформації при її введенні, виведенні, передаванні, обробці та зберіганні, а також протистояти її руйнуванню, крадіжкам чи спотворенню.

4. Організаційний – попередження доступу на об'єкт інформаційної діяльності сторонніх осіб за допомогою організаційних заходів (охорона, пропускний режим, регламентація доступу тощо).

- попередження несанкціонованого розголошення.

- попередження несанкціонованої модифікації;

3. Криптографічний (КЗІ) – попереджує доступ до інформації за допомогою математичних перетворень:

2. Інженерний – попереджує руйнування носія внаслідок навмисних дій або природного впливу інженерно-технічними засобами (обмежуючі конструкції, відеоспостереження, охоронно-пожежна сигналізація тощо).

- попередження блокування;

- попередження витоку інформації технічними каналами;

Технічний (ТЗІ) – забезпечує обмеження доступу до носія інформації апаратно-технічними засобами (антивіруси, фаєрволи, маршрутизатори, смарт-карти тощо):

Контрольні запитання до теми 7

1. Які функції реалізує КЗЗ від НСД?

2. Що таке багатофакторна автентифікація?

3. Назвіть групи функціональних послуг безпеки за НД ТЗІ 2.5-004-99.

4. Що таке рівні гарантій?

5. Назвіть основні групи каналів витоку інформації.

6. За якими критеріями класифікують КВІ?

7. Які пасивні методи нейтралізації КВІ ви знаєте?
8. Які активні методи нейтралізації КВІ ви знаєте?
9. Які етапи передбачає створення комплексу ТЗІ?
10. Що таке UTM/NGFW і XDR?

Тема 8. Аудит та моніторинг ефективності КСЗІ

8.1. Методи аудиту інформаційних систем

Аудит ІБ – систематичний, незалежний і задокументований процес отримання доказів та їх оцінювання на відповідність критеріям (ISO 19011, ISO/IEC 27007). Аудит буває внутрішнім і зовнішнім, аудитом відповідності (НД ТЗІ, ISO/IEC 27001, GDPR) або технічним. Методи: аналіз документів, інтерв'ю, перевірка налаштувань, сканування вразливостей, тестування на проникнення («чорна», «сіра», «біла скринька»), перевірка стійкості до соціальної інженерії. Аудит проходить етапи планування, збирання доказів, аналізу, складання звіту та контролю коригувальних дій. За Законом № 4336-IX державну експертизу КСЗІ замінюють самооцінювання, аудит і контрольні заходи. У морській галузі кіберризиків з 2021 р. перевіряють під час аудитів за кодексом ISM.

8.2. Інструменти моніторингу (SIEM, SOC)

SIEM збирає журнали подій, нормалізує й корелює їх (у тому числі методами поведінкової аналітики UEBA), генерує сповіщення та зберігає дані для розслідувань; приклади – Splunk, IBM QRadar, Microsoft Sentinel, Wazuh. **SOC** – підрозділ цілодобового моніторингу та реагування, власний або аутсорсинговий (MSSP). Аналітики L1 сортують сповіщення, L2 розслідують інциденти, L3 проактивно шукають загрози. SOC використовує SIEM, SOAR (автоматизація реагування), EDR/XDR і розвідку загроз, а техніки атак описує за матрицею MITRE ATT&CK.

8.3. Метрики оцінки безпеки та звітність

Метрики безпеки мають бути вимірюваними й пов'язаними з цілями (ISO/IEC 27004). **Операційні метрики:** середній час виявлення (MTTD) і реагування (MTTR), кількість інцидентів за критичністю, частка систем з актуальними оновленнями, час усунення критичних вразливостей, показники відновлення RPO/RTO, частка персоналу, що пройшов навчання. **Стратегічні:** індикатори ризику (KRI), рівень зрілості. **Звітність** буває оперативною (звіти SOC), управлінською (тренди та ризику), стратегічною для керівництва і регуляторною (повідомлення CERT-UA; за NIS2 – 24/72 год, за GDPR – 72 год).

Зростання ризиків кібератак через взаємодію «судно–порт» обумовлює необхідність проведення комплексного аудиту систем кіберзахисту судноплавних компаній і портової інфраструктури, а також розроблення адаптованих до галузевих умов заходів безпеки.

Ігнорування рекомендацій у сфері кібербезпеки може негативно вплинути на конкурентоспроможність національного флоту та портів у міжнародному середовищі.

Ефективне вирішення проблем кібербезпеки на морському транспорті значною мірою залежить від підготовки кваліфікованих фахівців із кіберзахисту, зокрема безпосередньо на борту суден.

Необхідно чітко визначити сутність і класифікацію загроз інформаційній безпеці у сфері мореплавства, що дозволить удосконалити механізми державного регулювання та протидії таким загрозам.

Висновки.

Стрімкий розвиток інтелектуальних інформаційних технологій зумовлює необхідність оперативного впровадження сучасних заходів кібербезпеки. Зволікання у цьому процесі значно підвищує вразливість судноплавних компаній до кіберзагроз. Саме тому системний аналіз ризиків і своєчасне усунення недоліків у системах захисту є ключовими умовами забезпечення безпеки.

Запровадження систем штучного інтелекту потребує проведення комплексного аудиту діяльності судноплавних компаній. Такий аудит має охоплювати аналіз ризиків інформаційної безпеки, оцінку рівня захищеності інформаційних ресурсів, виявлення вразливих місць, перевірку відповідності стандартам і розроблення рекомендацій щодо підвищення ефективності кіберзахисту.

Резолюція MSC.428(98) зробила кібербезпеку обов'язковим елементом управління безпекою судна, що вимагає системного підходу до захисту всіх цифрових і навігаційних систем на борту.

дії за чек-листами при інцидентах
дотримання процедур доступу
перевірка достовірності навігаційних даних
необхідність навчання з кібербезпеки
Практичні наслідки для екіпажу:
Відновлення

Відновлення систем і даних після інциденту

Реагування

Інструкції для екіпажу при кібератаках

Виявлення

Моніторинг аномалій (наприклад GNSS spoofing)

Захист

Контроль доступу, антивірус, сегментація мереж

Ідентифікація.

Визначення критичних систем (ECDIS, AIS, GPS тощо)

Основні принципи управління кіберризиками (ІМО)

Перевіряється в рамках ISM-аудитів

До 1 січня 2021 року (або до першого аудиту після цієї дати)

На технічному рівні – це застосування пасивних засобів захисту: штор на вікнах, систем екранування, заземлення та зашумлення, а також оновлення та впровадження нових систем і засобів ТЗІ.

На організаційному рівні – це проведення аналізу відомих загроз, пошук нових запобіжних заходів, оновлення політики безпеки, навчання та тренування персоналу.

Етап попередження

інформаційних ресурсів – їх відновлення за допомогою резервних і архівних копій, які зберігаються на зовнішніх носіях.

операційної системи та програмних засобів – їх відновлення за допомогою інсталяційних файлів (дисків);

технологічних процесів – їх відновлення за допомогою плану аварійного відновлення та проведення ремонтних заходів;

На апаратно-програмному рівні – це подолання наслідків реалізації загроз у разі порушень:

На організаційно-правовому рівні – це дисциплінарне або адміністративне (кримінальне) розслідування правопорушення (злочину) та притягнення винних до відповідальності.

Етап нейтралізації

сприяння притягненню винних до відповідальності (кримінальної, адміністративної, цивільно-правової, дисциплінарної).

взаємодії (у разі необхідності) з державними правоохоронними органами щодо виявлення та розкриття правопорушення (в тому числі за готування до злочину і за замах на злочин);

збереження слідів правопорушення;

наступного дослідження їх;

Зазначимо, що ці заходи можуть бути спрямовані на документування методів НСД до АС для:

Для цього в АС встановлюються міжмережеві екрани, файерволи (брандмауери), антивірусні програмні засоби та спеціальні комплекси засобів захисту інформації від НСД.

Ці заходи забезпечують апаратно-програмне блокування спроб несанкціонованого доступу (НСД) порушника (хакера) до інформації в АС або ураження системи вірусами за допомогою спеціальних апаратних комплексів та програмних засобів захисту інформації.

Етап зупинення

комплексні засоби захисту (органічне поєднання всіх груп).

пасивні засоби захисту: закриття вікон та встановлення на них ґрат, закриття та опечатування дверей, системних блоків, роз'ємів технічних засобів АС тощо;

активні засоби захисту: охоронна сигналізація та відеоспостереження;

На організаційному рівні – це використання заходів розвідки та дезінформації. На інженерно-технічному рівні – це впровадження засобів ТЗІ, які поділяються на:

Етап виявлення

Контрольні запитання до теми 8

1. Дайте визначення аудиту ІБ.
2. Які види аудиту розрізняють?
3. Назвіть методи аудиту інформаційних систем.
4. Чим відрізняються моделі тестування на проникнення?
5. Що замінює державну експертизу КСЗІ за Законом № 4336-ІХ?
6. Які функції виконує SIEM?
7. Що таке SOC і які рівні аналітиків у ньому працюють?
8. Для чого використовують SOAR і MITRE ATT&CK?
9. Що означають метрики MTTD і MTTR?
10. Які види звітності з ІБ існують?

Тема 9. Захист критичної інфраструктури та бізнес-процесів

9.1. Особливості КСЗІ для об'єктів критичної інфраструктури

Закон «Про критичну інфраструктуру» (2021) встановлює чотири категорії критичності об'єктів і визначає сектори: енергетика, транспорт, зв'язок, фінанси, водопостачання, охорона здоров'я; вимоги до кіберзахисту встановлює постанова КМУ № 518. Особливості захисту критичної інфраструктури (КІ): доступність і безпека технологічного процесу важливіші за конфіденційність; АСУ ТП і SCADA використовують протоколи без вбудованого захисту (Modbus, DNP3); обладнання служить 15–30 років і рідко оновлюється; атаки мають фізичні наслідки. Застосовують стандарт IEC 62443 (зони, канали, рівні безпеки SL 1–4), сегментацію та односпрямовані шлюзи.

Морський сектор. Найуразливіші – навігаційні системи (GNSS, AIS, ECDIS) і супутниковий зв'язок. Резолюція IMO MSC.428(98) (2017) вимагає врахувати кіберризик в системах управління безпекою судна (SMS) за кодексом ISM з 01.01.2021; настанови MSC-FAL.1/Circ.3 визначають функції ідентифікації, захисту, виявлення, реагування та відновлення. З 2018 р. OCIMF включає оцінку кібербезпеки в контракти, а DNV сертифікує кібербезпеку суден. Проблеми України – відсутність галузевого регулювання, єдиної термінології та фахівців на борту. Ігнорування вимог IMO загрожує санкціями в закордонних портах, втратою контрактів і зростанням страхових тарифів.

9.2. Хмарні середовища, мобільні технології та IoT

Хмари працюють за моделлю спільної відповідальності: провайдер захищає інфраструктуру, клієнт – дані, облікові записи та налаштування. Основні ризики – помилки конфігурації, витік ключів, компрометація облікових записів. Заходи захисту: багатофакторна автентифікація, шифрування з керуванням ключами, контроль конфігурацій (CSPM), журналювання, резервування; стандарти ISO/IEC 27017/27018; в Україні – Закон «Про хмарні послуги» (2022). **Мобільні пристрої** захищають системами MDM, шифруванням, віддаленим стиранням, оновленнями та контейнеризацією корпоративних даних. **IoT-пристрої** часто мають заводські паролі й не оновлюються: ботнет Mirai (2016), зібраний із таких пристроїв, провів масштабну DDoS-атаку. Морські приклади IoT – система MMC (передає параметри двигунів на берег для прогнозного обслуговування), система управління портом MPMS і безпілотні надводні апарати (USV).

9.3. Кейс-стаді: приклади впровадження захисту

Maersk після NotPetya (2017) приблизно за 10 днів перевстановила близько 4 тис. серверів і 45 тис. ПК. Відновити Active Directory вдалося завдяки контролеру домену в Гані, випадково відключеному від мережі; звідси висновок про потребу в офлайн-копіях і сегментації. **Виявлення спуфінгу на судні.** Ознаки AIS-спуфінгу: ціль є на AIS, але відсутня на радарі; нереалістична швидкість і «стрибки» координат; дублювання ідентифікатора MMSI; розбіжність із даними служби руху суден (VTS). Ознаки GPS-спуфінгу: розбіжність із радаром і компасом, однакові координати в багатьох суден. Захист – інтеграція AIS, радара та ECDIS, кілька джерел позиціонування, навчання екіпажу; ключовий принцип – **ніколи не довіряти одному джерелу даних**. **Міграція державних реєстрів України в хмару (2022)** зберегла дані в умовах обстрілів.

Зростання ризиків кібератак через взаємодію «судно–порт» обумовлює необхідність проведення комплексного аудиту систем кіберзахисту судноплавних компаній і портової інфраструктури, а також розроблення адаптованих до галузевих умов заходів безпеки.

Ігнорування рекомендацій у сфері кібербезпеки може негативно вплинути на конкурентоспроможність національного флоту та портів у міжнародному середовищі.

Ефективне вирішення проблем кібербезпеки на морському транспорті значною мірою залежить від підготовки кваліфікованих фахівців із кіберзахисту, зокрема безпосередньо на борту суден.

Необхідно чітко визначити сутність і класифікацію загроз інформаційній безпеці у сфері мореплавства, що дозволить удосконалити механізми державного регулювання та протидії таким загрозам.

Висновки.

Стрімкий розвиток інтелектуальних інформаційних технологій зумовлює необхідність оперативного впровадження сучасних заходів кібербезпеки. Зволікання у цьому процесі значно підвищує вразливість судноплавних компаній до кіберзагроз. Саме тому системний аналіз ризиків і своєчасне усунення недоліків у системах захисту є ключовими умовами забезпечення безпеки.

Запровадження систем штучного інтелекту потребує проведення комплексного аудиту діяльності судноплавних компаній. Такий аудит має охоплювати аналіз ризиків інформаційної безпеки, оцінку рівня захищеності інформаційних ресурсів, виявлення вразливих місць, перевірку відповідності стандартам і розроблення рекомендацій щодо підвищення ефективності кіберзахисту.

Подальший розвиток цифрових технологій у морській галузі пов'язаний із впровадженням систем штучного інтелекту (AI), які здатні аналізувати середовище та приймати рішення з певним рівнем автономності. Однак їх використання супроводжується новими ризиками. Для забезпечення довіри до таких систем необхідно дотримання низки вимог, серед яких: обґрунтованість алгоритмів і даних, чітке визначення цілей функціонування, здатність до перевірки результатів, надійність і стійкість до кібератак, взаємодія з іншими системами та прозорість для користувачів.

SMS - MMC: фідбек, інциденти, протоколи безпеки

MMC - DNV GL: звіти для аудиту та сертифікації

MMC - SMS: планування безпеки, технічний контроль

ECDIS - MMC: стан навігації, оновлення карт

↘ Кібермоніторинг ↗

Система MMC забезпечує прозорість процесів технічного обслуговування, надає можливість контролю виконання робіт, відстеження термінів і планування подальших дій. Вона також інтегрується з іншими інформаційними ресурсами, включаючи дані автоматичної ідентифікаційної системи (AIS) та метеорологічну інформацію, що розширює можливості управління флотом.

MMC – це як “розумний датчик + хмарна платформа”, який дозволяє інженерам на березі і на борту бачити стан обладнання та планувати ремонт до того, як станеться поломка.

Дозволяє проводити прогнозне обслуговування (Predictive Maintenance) замість простого планового

Передає ці дані у порталні сервіси судновласника або виробника обладнання

Збирає дані в реальному часі (температура, тиск, вібрації, оберти)

Призначена для відстеження стану двигунів, генераторів, насосів та інших механічних систем судна.

MMC (Machinery Maintenance Connect) – це система віддаленого моніторингу та управління технічним обслуговуванням суднового обладнання.

Завдяки впровадженню систем типу MMC (Machinery Maintenance Connect) процес технічного обслуговування суден зазнав суттєвих змін. Дані про стан обладнання в режимі реального часу передаються зацікавленим сторонам, що дає змогу застосовувати аналітичні алгоритми та здійснювати дистанційне управління технічним обслуговуванням як окремих суден, так і цілих флотів. Узагальнення інформації дозволяє отримувати повну картину технічного стану флоту, планувати ремонтні роботи, оптимізувати експлуатаційні процеси та підвищувати їхню ефективність.

оцінка ризиків і кібербезпеки

аудит і сертифікація систем управління

класифікація суден і плавзасобів

Основні функції:

Працює в морській, енергетичній, нафтовій та інших галузях

Це міжнародна сертифікаційна та класифікаційна компанія

DNV GL – Det Norske Veritas Germanischer Lloyd.

У цьому контексті важливу роль відіграють рішення, запропоновані міжнародними класифікаційними товариствами, зокрема DNV GL, які впроваджують дистанційний моніторинг, оцінювання ризиків і консалтинг.

Це «мозок порту», який координує рух суден, роботу причалів і логістику вантажів, щоб все було безпечно і ефективно.

інтеграції з AIS, VTS та іншими навігаційними системами

обліку і планування ресурсів порту

контролю за вантажними операціями

керування судноплавним рухом у порту

MPMS – це комплекс програмно-технічних та процедурних рішень для:

Реалізація превентивних заходів є значно ефективнішою, ніж реагування на вже здійснені атаки або їхні наслідки. При цьому сучасні виклики стосуються не лише навігаційних чи комунікаційних систем, а й систем технічного обслуговування, зокрема MPMS - Maritime Port Management System (Система управління морським портом).

Наявні системи управління безпекою здатні частково протидіяти лише внутрішнім загрозам, зокрема діям персоналу. Водночас вони не забезпечують належного рівня захисту від більш складних і організованих форм кібератак. Тому сучасний підхід передбачає формування комплексної системи кіберзахисту. У міжнародній практиці оцінка кібербезпеки та план її забезпечення оформлюються як окремі документи, причому план кібербезпеки судна розглядається як складова плану його охорони. Крім того, відповідальні за безпеку посадові особи мають включати до своїх функцій і питання кіберзахисту.

– терористичні структури.

– організації, що діють за підтримки держав;

– держави;

– випадкові (опортуністичні) зловмисники;

– кримінальні угруповання;

– активісти (у тому числі незадоволені працівники);

Слід зазначити, що морська кібербезпека не обмежується формальним внесенням окремих положень до системи управління безпекою судна. Відповідно до рекомендацій ІМО, викладених у «Керівництві з кібербезпеки на борту суден», визначено основні категорії суб'єктів кіберзагроз, серед яких:

У випадку реалізації кібератак на судові системи через взаємодію «судно-порт» можуть виникати значні фінансові претензії, які нерідко суттєво перевищують витрати на впровадження заходів кіберзахисту.

Варто зазначити, що рекомендації з кібербезпеки, які вже кілька років застосовуються у морській практиці, мають ширший зміст, ніж просто реагування на кіберзагрози. Вони формують комплексний підхід до аналізу та запобігання інцидентам на стику «судно-порт». Їх ігнорування або формальне виконання може мати серйозні наслідки не лише для окремих компаній чи портів, а й для галузі в цілому. Зокрема, порти можуть бути визнані небезпечними з точки зору кібербезпеки, що вплине на їх інвестиційну привабливість, вартість перевезень і навіть може стати підставою для міжнародних обмежень. Відповідно, суднам, що працюють із такими портами, доведеться впроваджувати підвищені заходи кіберзахисту.

Проте значна частина українських судовласників і операторів не має достатнього розуміння механізмів реалізації цих вимог. Недотримання таких рекомендацій може призвести до негативних наслідків, зокрема застосування санкцій у закордонних портах, відмови у укладенні комерційних контрактів, а також зниження конкурентоспроможності українського флоту через підвищення страхових тарифів.

Резолюція MSC.428(98) зробила кібербезпеку обов'язковим елементом управління безпекою судна, що вимагає системного підходу до захисту всіх цифрових і навігаційних систем на борту.

дії за чек-листами при інцидентах

дотримання процедур доступу

- перевірка достовірності навігаційних даних
- необхідність навчання з кібербезпеки
- Практичні наслідки для екіпажу:
- Відновлення
- Відновлення систем і даних після інциденту
- Реагування
- Інструкції для екіпажу при кібератаках
- Виявлення
- Моніторинг аномалій (наприклад GNSS spoofing)
- Захист
- Контроль доступу, антивірус, сегментація мереж
- Ідентифікація.
- Визначення критичних систем (ECDIS, AIS, GPS тощо)
- Основні принципи управління кіберризиками (ІМО)
- Перевіряється в рамках ISM-аудитів
- До 1 січня 2021 року (або до першого аудиту після цієї дати)
- Термін впровадження
- оновлення програмного забезпечення
- процедур доступу до систем
- людського фактору
- Обов'язкове врахування:
- впровадження заходів захисту
- оцінку ризиків
- ідентифікацію загроз і вразливостей
- Необхідно забезпечити:
- Вимоги поширюються як на судна, так і на берегові структури
- Управління кіберризиками має бути інтегроване у всі процеси компанії
- Кіберризики визнаються частиною загальної системи безпеки судна (SMS)
- Основні положення
- International Maritime Organization MSC.428(98) (Maritime Cyber Risk Management in Safety Management Systems, 2017) встановлює вимоги щодо інтеграції кіберризиків у систему управління безпекою суден відповідно до International Safety Management Code.
- Резолюція ІМО MSC.428(98): ключові положення
- Починаючи з 1 січня 2021 року, морські адміністрації окремих держав здійснюють перевірки суден щодо дотримання рекомендацій ІМО MSC.428(98), які регламентують управління кіберризиками у системах безпеки.
- Окремою проблемою для України є відсутність єдиного та узгодженого термінологічного апарату у сфері морської кібербезпеки. Нерідко спостерігається невідповідність між англійськими термінами та їх українськими аналогами або ж використання близьких за змістом, але не тотожних понять. Це призводить до неоднозначного трактування положень у нормативних і технічних документах, що ускладнює їх практичне застосування та знижує ефективність впровадження заходів кіберзахисту.
- Кіберзлочинність активно розвивається. Зловмисники постійно вдосконалюють програмно-технічні засоби для втручання в інформаційні процеси на борту суден, що спричиняє зростання рівня загроз у сфері торговельного мореплавства. Оскільки такі загрози часто мають транснаціональний характер, це потребує формування ефективних міжнародних механізмів протидії, які поєднували б правові, організаційні та технічні інструменти.
- AIS і GNSS входять до кіберризик-менеджменту судна і розглядаються як вразливі компоненти інформаційної інфраструктури.
- Тому в сучасних вимогах International Maritime Organization:
- Хоч AIS і GPS – не системи захисту, але вони є джерелами критичних даних. Їх компрометація – це ризик для безпеки судна.

Ніколи не довіряти одному джерелу даних
Ключовий принцип
моніторинг аномалій
навчання екіпажу (critical thinking)
використання кількох джерел позиціонування
інтеграція AIS + радар + ECDIS (Electronic Chart Display and Information System,
Електронна картографічна навігаційно-інформаційна система)

Практичні заходи:

Як захищаються на судні
курс за компасом і курс за GPS відрізняються.

4. Перевірка курсу

«ідеальна» точність (підозріло точна)

аномальна потужність сигналу

3. Аналіз супутникових сигналів

однакові координати у багатьох суден

різкі зміни координат

2. Контроль стабільності сигналу

візуальні орієнтири

інерціальна навігація

радар

1. Порівняння з альтернативними системами

Основні підходи виявлення:

На Близькому Сході з 2019 року, а особливо у 2022–2025 роках, фіксуються масові GNSS-аномалії – збої супутникової навігації (GPS, Galileo), які проявляються у вигляді глушіння сигналу (jamming) або підміни координат (spoofing), через що судна, літаки та дрони можуть отримувати некоректні дані про своє місцезнаходження (наприклад, AIS показує судно на суші); ці явища напряду пов'язані з військовими конфліктами в регіоні, і хоча офіційної відповідальності ніхто не визнає, експерти найчастіше пов'язують їх із діями Ізраїлю, а також Ірану та пов'язаних сил, які використовують засоби радіоелектронної боротьби для протидії ракетам, дронам і навігації противника, що в результаті впливає і на цивільне судноплавство та авіацію.

Район Близького Сходу – масові GNSS-аномалії.

У червні 2017 року у акваторії Чорного моря було зафіксовано один із перших масштабних випадків GNSS-спуфінгу, коли десятки суден одночасно почали передавати хибні координати і на навігаційних системах «перемістилися» в одну точку – в районі порту Новоросійськ, фактично опинившись «у порту» на суші, хоча в реальності залишалися у відкритому морі; цей інцидент вважається прикладом навмисного втручання в супутникову навігацію (spoofing), і хоча офіційно відповідальність не була визнана, більшість експертів пов'язують його з діяльністю росії, яка могла використовувати засоби радіоелектронної боротьби для тестування або захисту стратегічних об'єктів, що водночас продемонструвало вразливість цивільних навігаційних систем.

Чорне море (2017) – десятки суден «перемістилися» в один порт

Відомі випадки:

Судно «думає», що знаходиться в іншому місці. Підвищується ризик посадки на міліну або зіткнення. Виникає збій маршрутів і навігації.

впливає на всі системи, що залежать від GNSS (AIS, ECDIS, автопілот)

змушує судно визначати неправильні координати

GPS spoofing – це передача фальшивого GPS-сигналу, який:

Доступ DNV GL для аудиту та сертифікації безпілотних операцій.

MMC → SMS для планування процедур безпеки.

Дані USV → MMC для аналізу та контролю.

Взаємодія з іншими системами:

Потребує захисту від кіберзагроз (наприклад, перехоплення управління чи GPS-джамінг).

USV може бути інтегрований у MMC та ECDIS, передавати дані про навігацію та стан обладнання.

У контексті кібербезпеки та технічного контролю судна:

Військові та оборонні завдання.

Використання у наукових дослідженнях, картографуванні, гідрології.

Моніторинг та патрулювання водних шляхів.

Призначення:

Тип: Судно без екіпажу, яке керується дистанційно або автономно.

Основні характеристики USV:

USV означає Unmanned Surface Vehicle – безпілотний надводний апарат.

Джаммер – це пристрій або система, яка зумисне створює перешкоди для радіосигналів, щоб порушити або заблокувати зв'язок, навігацію або інші радіотехнічні системи.

GPS spoofing (підміна координат)

берегові станції VTS (VTS - Vessel Traffic Service (Служба управління рухом суден).

VTS – це система, яка працює з берега і: контролює рух суден у портах і прибережних зонах, забезпечує безпеку навігації, допомагає уникати зіткнень. Це як «диспетчерська для кораблів», схожа на авіадиспетчерів, тільки для морського транспорту)

супутниковий AIS

4. Дані з інших джерел

невідповідність типу судна

дублювання ідентифікаторів

3. Аналіз MMSI (Maritime Mobile Service Identity (Ідентифікатор морської рухомої служби). MMSI – це унікальний 9-значний номер, який присвоюється: суднам, береговим радіостанціям, іншим морським об'єктам зв'язку. Він використовується в системах зв'язку та ідентифікації, зокрема: AIS (автоматична ідентифікаційна система). DSC (цифровий вибіркового виклик). Це як “номер телефону” або “ID” судна).

«стрибки» координат

нереалістична швидкість або маневри

2. Перевірка логіки руху

AIS показує ціль, а радар – ні. Така ситуація повинна викликати підозру.

1. Порівняння з радаром

Основні методи виявлення

приховування реального маршруту

маскування незаконної діяльності (контрабанда, рибальство)

«фантомні» судна біля портів

Реальні сценарії:

Для виконання відбувається використання спеціальних передавачів VHF, програмна генерація AIS-пакетів, ін'єкція даних у бортові системи.

підмінити ідентифікацію (MMSI, назву)

змінити позицію реального судна

створити «примарні судна»

AIS spoofing – це передача фальшивих AIS-повідомлень, щоб:

AIS spoofing (підміна даних AIS)

Кіберзагрози для навігаційних систем судна – це вже не теорія, а реальні інциденти, які фіксуються у світі. Найбільш відомі – AIS spoofing і GPS spoofing. Обидві атаки впливають на ситуаційну обізнаність екіпажу й можуть створити ризик аварій.

Безпека мореплавства значною мірою забезпечується використанням сучасних інформаційних і навігаційних технологій. Зокрема, відповідно до вимог Конвенції SOLAS-74, судна певної тоннажності та всі пасажирські судна мають бути оснащені автоматичною

ідентифікаційною системою (AIS), функціональні та технічні характеристики якої визначені міжнародними стандартами та рекомендаціями.

Перші кроки до регламентації інформаційного обміну на морі були зроблені ще у 1979 році, коли було ухвалено резолюцію щодо розвитку систем передавання повідомлень про лихо і безпеку. Надалі ці підходи були розвинені у документах, що визначають принципи функціонування суднових систем повідомлень, а також у правилах електронного документообігу, зокрема електронних коносаментів. Важливу роль відіграли також типові закони ЮНСІТРАЛ щодо електронної торгівлі та електронних підписів, які стали основою для формування як міжнародних, так і національних нормативних систем.

У сучасних умовах паперовий документообіг дедалі частіше виявляється неефективним, тому у сфері морських перевезень активно впроваджуються системи електронного обміну даними, такі як EDI та EDIFACT, що відповідають положенням Конвенції з полегшення міжнародного морського судноплавства.

Усі суб'єкти інформаційної взаємодії оперують, зокрема, конфіденційними даними, компрометація яких може призвести до серйозних наслідків: збоїв у роботі бортових систем, відхилення судна від заданого курсу, фінансових втрат унаслідок витоку комерційної чи персональної інформації, а також отримання неточних або несвоєчасних відомостей про технічний стан обладнання і механізмів. Найбільш уразливими об'єктами атак є інформаційні ресурси навігаційних систем і систем морського зв'язку. Для їх захисту застосовуються криптографічні методи, системи автентифікації, електронний цифровий підпис та інші інструменти. Зокрема, Міжнародна гідрографічна організація запровадила стандарт S63, який регламентує захист офіційних електронних навігаційних карт.

Широке коло учасників інформаційного обміну у морській галузі зумовлює виникнення значної кількості загроз для суднових інформаційних ресурсів. Серед них – несанкціонований доступ до каналів супутникового зв'язку між судном і береговими центрами управління, спотворення навігаційних GPS-даних, а також втручання у системи оперативного керування судном.

Сучасні процеси цифровізації та автоматизації охоплюють усі сфери діяльності, включаючи торговельне мореплавство. Зокрема, активно впроваджується електронний документообіг, який широко застосовується у міжнародній морській практиці. Галузь характеризується постійним інформаційним обміном між різними учасниками: вантажовідправниками та вантажоодержувачами з адміністрацією судна щодо комерційної експлуатації; судновласниками або фрахтувальниками – з питань безпеки судноплавства; адміністрацією судна – з портовими та митними органами щодо оформлення вантажів і судна в портах; а також між членами екіпажу та їхніми родинами. Така інтенсивна інформаційна взаємодія додатково підвищує вимоги до забезпечення належного рівня кібербезпеки у морській галузі.

У міжнародних нормативних актах об'єктами кіберзахисту розглядаються інформаційні технологічні системи у їх взаємозв'язку та взаємодії. Натомість вітчизняні підходи зосереджені переважно на захисті інформації, що обробляється в автоматизованих системах управління, особливо тих, які використовуються на критично важливих або потенційно небезпечних об'єктах. Галузева специфіка, зокрема особливості морського транспорту, при цьому практично не враховується.

На відміну від цього, міжнародна практика зосереджується на забезпеченні безпеки безпосередньо суден і портових об'єктів як цілісних систем. Вітчизняний підхід базується на визначенні значущості об'єктів критичної інфраструктури, що підлягають захисту, унаслідок чого менш значущі об'єкти фактично залишаються поза межами правового регулювання. У міжнародних же документах вимоги щодо кібербезпеки поширюються на всі судна та портові засоби без винятку. Крім того, положення українського законодавства не містять детальних практичних рекомендацій, що ускладнює їх застосування на рівні конкретного судна або портової інфраструктури та потребує додаткової адаптації.

Передусім Закон орієнтований на захист об'єктів критичної інформаційної інфраструктури, до яких належать комунікаційні системи незалежно від форми власності, що забезпечують обробку національних інформаційних ресурсів або використовуються в діяльності органів державної влади, місцевого самоврядування, правоохоронних структур і військових формувань. До сфери його регулювання також віднесено системи, що забезпечують суспільні потреби, зокрема у галузях електронного урядування, електронних послуг, електронної комерції та документообігу. При цьому об'єктами захисту виступають насамперед інформаційні системи та мережі, а не фізичні об'єкти, на яких вони функціонують.

До спеціалізованого законодавства у сфері протидії кіберзагрозам належить Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 №45 [10]. Водночас, попри визначення ним правових та організаційних засад захисту національних інтересів у кіберпросторі, а також ключових напрямів державної політики у сфері кібербезпеки та механізмів координації відповідної діяльності, цей нормативний акт має загальний характер і поширюється на всі галузі економіки. Він не враховує специфічних особливостей транспортної сфери загалом і морського транспорту зокрема.

Разом із тим діяльність Міністерства інфраструктури України у сфері нормативно-правового забезпечення інформаційної безпеки морського транспорту не відповідає сучасним викликам. Основна увага зосереджується переважно на технічних аспектах регламентування та захисту інформації, тоді як комплексний розвиток системи морської кібербезпеки відбувається недостатньо ефективно.

Водночас розроблена Національним інститутом стандартів і технологій США рамкова модель підвищення кібербезпеки критичної інфраструктури була рекомендована до застосування відповідними циркулярами ІМО. Більшість ключових нормативних і методичних документів у цій сфері створено саме у США та інших провідних морських державах, тому українська морська галузь значною мірою орієнтується на їхні підходи та рекомендації.

В Україні питання морської інформаційної безпеки перебуває на початковому етапі розвитку. Наукові публікації з цієї тематики є поодинокими, рівень обізнаності залишається низьким, а системні заходи з боку держави як адміністрації прапора фактично не реалізуються. Спеціалізоване нормативно-правове регулювання у сфері морської кібербезпеки практично відсутнє, і ці питання недостатньо відображені навіть у стратегічних документах.

У сучасних умовах кібернапади дедалі частіше стають складовою комплексних злочинних дій. Зловмисники прагнуть отримати контроль над командними, керуваними та експлуатаційними системами суден. У разі успішного втручання судно може перетворитися на потенційно небезпечний об'єкт, що створює загрозу для портової інфраструктури та інших елементів морської логістики.

Засоби масової інформації регулярно повідомляють про успішні кібернапади на об'єкти морської транспортної інфраструктури в різних країнах світу. Зокрема, у 2017 році вірус NotPetya вразив 17 із 76 вантажних терміналів компанії Maersk; у 2018 році зафіксовано атаки на порти Барселони та Сан-Дієго; у 2020 році відбулися кібератаки на термінал Шахід Раджаї в Ірані, логістичну групу Toll Group в Австралії, контейнерного перевізника Mediterranean Shipping Company, а також на інформаційні системи компанії Anglo-Eastern. За оцінками фахівців Лондонського Ллойда, загальні втрати морської галузі від кіберінцидентів сягають близько 200 млрд доларів США. Водночас лише незначна частина компаній має напрацьовані плани забезпечення безперервності діяльності у випадку кібератак.

Попри це, проблема кібербезпеки у морській галузі залишається вкрай актуальною. Однією з ключових причин є дефіцит кваліфікованих фахівців із кіберзахисту безпосередньо на борту суден. Це обумовлює необхідність подальших наукових досліджень і розроблення ефективних підходів до забезпечення належного рівня захисту об'єктів морського транспорту від кіберзагроз.

У сучасних умовах кожен моряк активно використовує мобільний зв'язок, інтернет та інші цифрові технології. Проте разом із перевагами цифровізації зростає і кількість

кіберзагроз. У зв'язку з цим у 2015 році було внесено відповідні зміни до Закону України «Про основи національної безпеки України».

Водночас важливу роль відіграють і галузеві об'єднання. Так, починаючи з 2018 року, у межах діяльності Міжнародного морського форуму нафтових компаній (OCIMF) оцінювання кібербезпеки стало обов'язковим елементом комерційних контрактів. Крім того, класифікаційне товариство DNV GL із 2017 року впровадило процедури сертифікації кібербезпеки суден, а з 2018 року – спеціальні класифікаційні позначення, що відображають рівень кіберзахисту.

У більшості країн імплементація рекомендацій ІМО у сфері морської кібербезпеки здійснюється шляхом їх адаптації та доповнення національними нормативно-правовими актами і практичними рекомендаціями.

Зокрема, у червні 2017 року Комітет з безпеки на морі ухвалив резолюцію MSC.428(98), що стосується управління кіберризиками в системах управління безпекою суден [9]. У зв'язку з активним впровадженням автоматизованих систем на морському транспорті та зростанням пов'язаних із цим ризиків, ІМО наголошує на необхідності інтеграції заходів кібербезпеки у всі аспекти функціонування галузі. Починаючи з 1 січня 2021 року, адміністраціям держав рекомендовано забезпечити врахування кіберризиків у системах управління безпекою суден.

Комітети з безпеки на морі та захисту морського середовища мають у своїй структурі дев'ять підкомітетів, які готують проекти документів для розгляду на засіданнях відповідних комітетів. Остаточне затвердження таких документів зазвичай відбувається на сесіях Асамблеї. Водночас ІМО може скликати дипломатичні конференції для ухвалення стратегічно важливих рішень у сферах безпеки судноплавства, охорони довкілля та міжнародно-правового регулювання морської діяльності.

Комітет з полегшення формальностей судноплавства (FAL).

Комітет з технічного співробітництва (KTC);

Юридичний комітет (LEG – ЮРКОМ);

Комітет із захисту морського середовища (MEPC – КЗМС);

Комітет з безпеки на морі (MSC – КБМ);

Станом на сьогодні до складу Міжнародної морської організації (ІМО) входять 174 держави-члени, а також три асоційовані учасники – Фарерські острови, Гонконг і Макао. Найвищим керівним органом ІМО є Асамблея держав-членів. Організаційна структура ІМО включає секретаріат на чолі з Генеральним секретарем і п'ять основних комітетів:

Характерною рисою зазначених документів є їх комплексний і масштабний характер: вони охоплюють загальні принципи організації кібербезпеки на рівні портів, портових систем і суден як для всіх держав-членів ІМО, так і для окремих розвинених морських країн. Водночас такі рекомендації не завжди можуть бути безпосередньо застосовані в умовах держав із менш розвиненою морською економікою, зокрема України.

<https://www.wcdn.imo.org/localresources/en/OurWork/Facilitation/FAL%20related%20nonmandatory%20documents/MSC-FAL.1-Circ.3-Rev.3.pdf>

Зокрема, у 2020 році в США було створено некомерційний центр кібербезпеки портів, а також подано до Сенату законодавчу ініціативу щодо посилення кіберзахисту морської галузі. Ще раніше, у 2015 році, Міністерство внутрішньої безпеки США оприлюднило посібник із впровадження систем кібербезпеки у транспортному секторі. У Великій Британії за підтримки Міністерства транспорту та Міністерства оборони у 2016 році було підготовлено документ, присвячений кібербезпеці портів і портових систем, а у 2017 році – зведення правил кіберзахисту для суден. Крім того, провідні світові судноплавні компанії розробили рекомендації, які у 2017 році були підтримані Міжнародною морською організацією у вигляді «Керівництва з кібербезпеки на борту суден». Текст керівництва за цим посиланням

Аналіз сучасних наукових досліджень і публікацій свідчить, що проблематика кібербезпеки у морській галузі активно висвітлюється в зарубіжних спеціалізованих інформаційних ресурсах. Значна частина матеріалів присвячена розробленню міжнародних і національних рекомендацій у сфері кіберзахисту в провідних морських державах, зокрема у

США, Великій Британії, країнах Європейського Союзу, а також у Данії, Норвегії, Сінгапурі та інших.

Таким чином, досягнення високого рівня інформаційної безпеки у сфері морського транспорту в умовах впровадження «Керівництва з кібербезпеки на борту суден» є актуальним науково-практичним завданням, спрямованим на підвищення захищеності об'єктів критичної інфраструктури держави.

Існуючі системи захисту інформації недостатньо оперативно враховують появу нових загроз, що призводить до затримок у проведенні досліджень, розробленні ефективних заходів протидії та мінімізації їх наслідків.

Відсутня належна формалізація завдань щодо визначення оптимального складу та методів захисту інформації, здатних адекватно реагувати на сучасні виклики.

Не в повному обсязі враховано вплив засобів і механізмів захисту інформації на технічні та експлуатаційні характеристики інформаційних систем морського і річкового транспорту.

Не сформовано цілісної методології оцінювання ефективності функціонування комплексних систем захисту інформації (КСЗІ), що зумовлено недостатнім дослідженням поведінки та стратегій кіберзловмисників.

Недостатньо ґрунтовно опрацьовані методи та засоби забезпечення збереження інформації і резервування критично важливих даних галузі.

Відсутні уніфіковані підходи до формування захищеного інформаційно-комунікаційного середовища галузі, яке було б адаптоване до роботи в складних експлуатаційних умовах.

З метою протидії кіберзлочинності доцільно визначити ключові проблемні аспекти, пов'язані із захистом інформаційно-комунікаційного середовища морської галузі України.

Водночас активне впровадження сучасних інформаційних технологій, особливо в мобільному, розподіленому та бездротовому середовищах, істотно підвищує ймовірність виникнення специфічних загроз інформаційній безпеці. Це підтверджується стрімким зростанням кількості виявлених уразливостей у інформаційних системах морської галузі та, як наслідок, збільшенням кількості інцидентів, пов'язаних із захистом інформації на судах, у портах, компаніях і організаціях.

Підвищення значущості інформаційно-комунікаційної складової зумовлене тим, що вона забезпечує ефективну взаємодію морського та річкового транспорту з іншими секторами економіки. Зокрема, це проявляється у зменшенні затримок під час перевезення вантажів, обробки суден, контейнерів, залізничних вагонів та інших вантажних одиниць завдяки впровадженню електронних накладних, систем типу «клієнт-банк», електронного бізнесу, технологій GSM-R, VSAT, а також налагодженню взаємодії з клієнтами і партнерами.

У кожній економічно розвиненій державі транспортна галузь належить до ключових складових господарського комплексу. Активний прогрес інформаційних технологій протягом останніх десятиліть висунув сферу зв'язку, або, у сучасному розумінні, інформаційно-комунікаційну компоненту, на провідні позиції в транспортній системі в цілому і в морській галузі зокрема.

Огляд сучасних тенденцій і викликів у кібербезпеці морських інформаційних систем.

Роль КСЗІ у забезпеченні безпеки судноплавства, портових систем та морської логістики.

Значення захисту інформації в морському секторі та критичних об'єктах.

Роль КСЗІ у морському секторі.

Контрольні запитання до теми 9

1. Які сектори та категорії критичності визначає Закон «Про критичну інфраструктуру»?
2. Чим захист АСУ ТП відрізняється від захисту офісних систем?
3. Яке призначення стандарту ІЕС 62443?
4. Які інформаційні системи судна найуразливіші?

5. Що вимагає резолюція ІМО MSC.428(98)?
6. Поясніть модель спільної відповідальності в хмарах.
7. Як захищають корпоративні мобільні пристрої?
8. Які ризики пов'язані з IoT?
9. За якими ознаками виявляють AIS- і GPS-спуфінг?
10. Які уроки впливають із кейсу Maersk?

Тема 10. Управління інцидентами та прийняття рішень у сфері кібербезпеки

10.1. Алгоритми реагування на кіберінциденти

Кіберінцидент – подія, що порушує або загрожує порушити конфіденційність, цілісність чи доступність інформації. За NIST SP 800-61 Rev. 2 реагування складається з фаз: підготовка; виявлення та аналіз; локалізація, усунення й відновлення; післяінцидентний аналіз. Редакція Rev. 3 (2025) вбудовує реагування в шість функцій NIST CSF 2.0. Практичний алгоритм: фіксація події → визначення критичності → ескалація → локалізація (ізоляція вузлів, блокування облікових записів) → збереження доказів → усунення причини → відновлення з резервних копій → повідомлення CERT-UA, кіберполіції та регуляторів → аналіз уроків. Для типових інцидентів (вимагачі, фішинг, DDoS) складають сценарії реагування (playbooks). На суднах екіпаж діє за чек-листами ІМО.

10.2. Використання сучасних методів прогнозування та оптимізації

Прогнозування загроз спирається на аналіз часових рядів, байєсові мережі та марковські моделі атак, графи атак, машинне навчання (виявлення аномалій), розвідку загроз та оцінку ймовірності експлуатації вразливостей (EPSS). **Оптимізація** розв'язує задачу вибору засобів захисту за обмеженого бюджету: максимізувати $\sum \Delta R_i x_i$ за умови $\sum C_i x_i \leq B$, де $x_i \in \{0; 1\}$ (задача про рюкзак). Окупність інвестицій оцінюють показником $ROSI = (ALE_{до} - ALE_{після} - C) / C$; застосовують також теорію ігор і генетичні алгоритми.

10.3. Прийняття рішень в умовах невизначеності

Якщо ймовірності станів середовища відомі (умови ризику), застосовують **критерій Байєса** – мінімум очікуваних втрат. Якщо ймовірності невідомі (умови невизначеності), використовують **критерій Вальда** (мінімізація максимальних втрат), **Севіджа** (мінімізація максимального «жалю» – відхилення від найкращого рішення для кожного стану), **Гурвіца** (компроміс песимізму й оптимізму з коефіцієнтом α) та **Лапласа** (стани рівноймовірні). **Приклад:** втрати (тис. грн) для варіантів захисту A1 (мінімальний), A2 (базовий), A3 (посилений) за станів S1–S3 (низька, середня, масована активність зловмисників).

Варіант	S1	S2	S3	Вальд (max)	Лаплас (середнє)	Севідж (max «жалю»)
A1	10	60	200	200	90	120
A2	30	45	90	90	55	20
A3	70	75	80	80	75	60

За Вальдом обирають A3, за Лапласом, Севіджем і Гурвіцем ($\alpha = 0,5$: A1 – 105, A2 – 60, A3 – 75) – A2. Отже, вибір залежить від ставлення до ризику; для критичної інфраструктури доцільний обережний критерій Вальда. Застосовують також метод Дельфі, нечітку логіку й цикл OODA («спостереження – орієнтація – рішення – дія»).

Реалізація превентивних заходів є значно ефективнішою, ніж реагування на вже здійснені атаки або їхні наслідки. При цьому сучасні виклики стосуються не лише навігаційних чи комунікаційних систем, а й систем технічного обслуговування, зокрема MPMS - Maritime Port Management System (Система управління морським портом).

Наявні системи управління безпекою здатні частково протидіяти лише внутрішнім загрозам, зокрема діям персоналу. Водночас вони не забезпечують належного рівня захисту від більш складних і організованих форм кібератак. Тому сучасний підхід передбачає формування комплексної системи кіберзахисту. У міжнародній практиці оцінка кібербезпеки та план її забезпечення оформлюються як окремі документи, причому план кібербезпеки судна розглядається як складова плану його охорони. Крім того, відповідальні за безпеку посадові особи мають включати до своїх функцій і питання кіберзахисту.

- терористичні структури.
- організації, що діють за підтримки держав;
- держави;
- випадкові (опортуністичні) зловмисники;
- кримінальні угруповання;

– активісти (у тому числі незадоволені працівники);

Слід зазначити, що морська кібербезпека не обмежується формальним внесенням окремих положень до системи управління безпекою судна. Відповідно до рекомендацій ІМО, викладених у «Керівництві з кібербезпеки на борту суден», визначено основні категорії суб'єктів кіберзагроз, серед яких:

У випадку реалізації кібератак на суднові системи через взаємодію «судно-порт» можуть виникати значні фінансові претензії, які нерідко суттєво перевищують витрати на впровадження заходів кіберзахисту.

Варто зазначити, що рекомендації з кібербезпеки, які вже кілька років застосовуються у морській практиці, мають ширший зміст, ніж просто реагування на кіберзагрози. Вони формують комплексний підхід до аналізу та запобігання інцидентам на стику «судно-порт». Їх ігнорування або формальне виконання може мати серйозні наслідки не лише для окремих компаній чи портів, а й для галузі в цілому. Зокрема, порти можуть бути визнані небезпечними з точки зору кібербезпеки, що вплине на їх інвестиційну привабливість, вартість перевезень і навіть може стати підставою для міжнародних обмежень. Відповідно, суднам, що працюють із такими портами, доведеться впроваджувати підвищені заходи кіберзахисту.

Проте значна частина українських судновласників і операторів не має достатнього розуміння механізмів реалізації цих вимог. Недотримання таких рекомендацій може призвести до негативних наслідків, зокрема застосування санкцій у закордонних портах, відмови у укладенні комерційних контрактів, а також зниження конкурентоспроможності українського флоту через підвищення страхових тарифів.

Резолюція MSC.428(98) зробила кібербезпеку обов'язковим елементом управління безпекою судна, що вимагає системного підходу до захисту всіх цифрових і навігаційних систем на борту.

дії за чек-листами при інцидентах
дотримання процедур доступу
перевірка достовірності навігаційних даних
необхідність навчання з кібербезпеки
Практичні наслідки для екіпажу:
Відновлення

Відновлення систем і даних після інциденту

Реагування

Інструкції для екіпажу при кібератаках

Виявлення

Моніторинг аномалій (наприклад GNSS spoofing)

Захист

Контроль доступу, антивірус, сегментація мереж

Ідентифікація.

Визначення критичних систем (ECDIS, AIS, GPS тощо)

Основні принципи управління кіберризиками (ІМО)

У червні 2017 року у акваторії Чорного моря було зафіксовано один із перших масштабних випадків GNSS-спуфінгу, коли десятки суден одночасно почали передавати хибні координати і на навігаційних системах «перемістилися» в одну точку – в районі порту Новоросійськ, фактично опинившись «у порту» на суші, хоча в реальності залишалися у відкритому морі; цей інцидент вважається прикладом навмисного втручання в супутникову навігацію (spoofing), і хоча офіційно відповідальність не була визнана, більшість експертів пов'язують його з діяльністю росії, яка могла використовувати засоби радіоелектронної боротьби для тестування або захисту стратегічних об'єктів, що водночас продемонструвало вразливість цивільних навігаційних систем.

Кіберзагрози для навігаційних систем судна – це вже не теорія, а реальні інциденти, які фіксуються у світі. Найбільш відомі – AIS spoofing і GPS spoofing. Обидві атаки впливають на ситуаційну обізнаність екіпажу й можуть створити ризик аварій.

Безпека мореплавства значною мірою забезпечується використанням сучасних інформаційних і навігаційних технологій. Зокрема, відповідно до вимог Конвенції SOLAS-74, судна певної тоннажності та всі пасажирські судна мають бути оснащені автоматичною ідентифікаційною системою (AIS), функціональні та технічні характеристики якої визначені міжнародними стандартами та рекомендаціями.

Перші кроки до регламентації інформаційного обміну на морі були зроблені ще у 1979 році, коли було ухвалено резолюцію щодо розвитку систем передавання повідомлень про лихо і безпеку. Надалі ці підходи були розвинені у документах, що визначають принципи функціонування судових систем повідомлень, а також у правилах електронного документообігу, зокрема електронних коносаментів. Важливу роль відіграли також типові закони ЮНСІТРАЛ щодо електронної торгівлі та електронних підписів, які стали основою для формування як міжнародних, так і національних нормативних систем.

У сучасних умовах паперовий документообіг дедалі частіше виявляється неефективним, тому у сфері морських перевезень активно впроваджуються системи електронного обміну даними, такі як EDI та EDIFACT, що відповідають положенням Конвенції з полегшення міжнародного морського судноплавства.

Усі суб'єкти інформаційної взаємодії оперують, зокрема, конфіденційними даними, компрометація яких може призвести до серйозних наслідків: збоїв у роботі бортових систем, відхилення судна від заданого курсу, фінансових втрат унаслідок витоку комерційної чи персональної інформації, а також отримання неточних або несвоєчасних відомостей про технічний стан обладнання і механізмів. Найбільш уразливими об'єктами атак є інформаційні ресурси навігаційних систем і систем морського зв'язку. Для їх захисту застосовуються криптографічні методи, системи автентифікації, електронний цифровий підпис та інші інструменти. Зокрема, Міжнародна гідрографічна організація запровадила стандарт S63, який регламентує захист офіційних електронних навігаційних карт.

Широке коло учасників інформаційного обміну у морській галузі зумовлює виникнення значної кількості загроз для судових інформаційних ресурсів. Серед них – несанкціонований доступ до каналів супутникового зв'язку між судном і береговими центрами управління, спотворення навігаційних GPS-даних, а також втручання у системи оперативного керування судном.

Сучасні процеси цифровізації та автоматизації охоплюють усі сфери діяльності, включаючи торговельне мореплавство. Зокрема, активно впроваджується електронний документообіг, який широко застосовується у міжнародній морській практиці. Галузь характеризується постійним інформаційним обміном між різними учасниками: вантажовідправниками та вантажоодержувачами з адміністрацією судна щодо комерційної експлуатації; судовласниками або фрахтувальниками – з питань безпеки судноплавства; адміністрацією судна – з портовими та митними органами щодо оформлення вантажів і судна в портах; а також між членами екіпажу та їхніми родинами. Така інтенсивна інформаційна взаємодія додатково підвищує вимоги до забезпечення належного рівня кібербезпеки у морській галузі.

У міжнародних нормативних актах об'єктами кіберзахисту розглядаються інформаційні технологічні системи у їх взаємозв'язку та взаємодії. Натомість вітчизняні підходи зосереджені переважно на захисті інформації, що обробляється в автоматизованих системах управління, особливо тих, які використовуються на критично важливих або потенційно небезпечних об'єктах. Галузева специфіка, зокрема особливості морського транспорту, при цьому практично не враховується.

На відміну від цього, міжнародна практика зосереджується на забезпеченні безпеки безпосередньо суден і портових об'єктів як цілісних систем. Вітчизняний підхід базується на визначенні значущості об'єктів критичної інфраструктури, що підлягають захисту, унаслідок чого менш значущі об'єкти фактично залишаються поза межами правового регулювання. У міжнародних же документах вимоги щодо кібербезпеки поширюються на всі судна та портові засоби без винятку. Крім того, положення українського законодавства не містять детальних

практичних рекомендацій, що ускладнює їх застосування на рівні конкретного судна або портової інфраструктури та потребує додаткової адаптації.

Передусім Закон орієнтований на захист об'єктів критичної інформаційної інфраструктури, до яких належать комунікаційні системи незалежно від форми власності, що забезпечують обробку національних інформаційних ресурсів або використовуються в діяльності органів державної влади, місцевого самоврядування, правоохоронних структур і військових формувань. До сфери його регулювання також віднесено системи, що забезпечують суспільні потреби, зокрема у галузях електронного урядування, електронних послуг, електронної комерції та документообігу. При цьому об'єктами захисту виступають насамперед інформаційні системи та мережі, а не фізичні об'єкти, на яких вони функціонують.

До спеціалізованого законодавства у сфері протидії кіберзагрозам належить Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 №45 [10]. Водночас, попри визначення ним правових та організаційних засад захисту національних інтересів у кіберпросторі, а також ключових напрямів державної політики у сфері кібербезпеки та механізмів координації відповідної діяльності, цей нормативний акт має загальний характер і поширюється на всі галузі економіки. Він не враховує специфічних особливостей транспортної сфери загалом і морського транспорту зокрема.

Разом із тим діяльність Міністерства інфраструктури України у сфері нормативно-правового забезпечення інформаційної безпеки морського транспорту не відповідає сучасним викликам. Основна увага зосереджується переважно на технічних аспектах регламентування та захисту інформації, тоді як комплексний розвиток системи морської кібербезпеки відбувається недостатньо ефективно.

Водночас розроблена Національним інститутом стандартів і технологій США рамкова модель підвищення кібербезпеки критичної інфраструктури була рекомендована до застосування відповідними циркулярами ІМО. Більшість ключових нормативних і методичних документів у цій сфері створено саме у США та інших провідних морських державах, тому українська морська галузь значною мірою орієнтується на їхні підходи та рекомендації.

В Україні питання морської інформаційної безпеки перебуває на початковому етапі розвитку. Наукові публікації з цієї тематики є поодинокими, рівень обізнаності залишається низьким, а системні заходи з боку держави як адміністрації прапора фактично не реалізуються. Спеціалізоване нормативно-правове регулювання у сфері морської кібербезпеки практично відсутнє, і ці питання недостатньо відображені навіть у стратегічних документах.

У сучасних умовах кібернапади дедалі частіше стають складовою комплексних злочинних дій. Зловмисники прагнуть отримати контроль над командними, керуючими та експлуатаційними системами суден. У разі успішного втручання судно може перетворитися на потенційно небезпечний об'єкт, що створює загрозу для портової інфраструктури та інших елементів морської логістики.

Засоби масової інформації регулярно повідомляють про успішні кібернапади на об'єкти морської транспортної інфраструктури в різних країнах світу. Зокрема, у 2017 році вірус NotPetya вразив 17 із 76 вантажних терміналів компанії Maersk; у 2018 році зафіксовано атаки на порти Барселони та Сан-Дієго; у 2020 році відбулися кібератаки на термінал Шахід Раджаї в Ірані, логістичну групу Toll Group в Австралії, контейнерного перевізника Mediterranean Shipping Company, а також на інформаційні системи компанії Anglo-Eastern. За оцінками фахівців Лондонського Ллойда, загальні втрати морської галузі від кіберінцидентів сягають близько 200 млрд доларів США. Водночас лише незначна частина компаній має напрацьовані плани забезпечення безперервності діяльності у випадку кібератак.

Якщо залишковий ризик перевищує гранично допустимий, вносять відповідні зміни до складу заходів і засобів захисту, після чого всі процедури виконують повторно до одержання прийняттого результату.

На етапі проектування КСЗІ, після формування пропозицій щодо складу заходів і засобів захисту, здійснюється оцінка залишкового ризику для кожної пропозиції (наприклад,

за критерієм «ефективність/вартість»), вибирається найбільш оптимальна серед них і первинна оцінка уточнюється.

Контрольні запитання до теми 10

1. Що таке кіберінцидент?
2. Назвіть фази реагування на інциденти за NIST SP 800-61.
3. Опишіть практичний алгоритм реагування на інцидент.
4. Що таке playbook?
5. Які методи використовують для прогнозування загроз?
6. Сформулюйте задачу оптимального вибору засобів захисту.
7. Як розраховують показник ROSI?
8. Чим умови ризику відрізняються від умов невизначеності?
9. Сформулюйте критерії Вальда, Севіджа, Гурвіца й Лапласа.
10. Чому різні критерії дають різні рішення?

Список використаних джерел

1. 2. НД ТЗІ 3.7-003-2005; НД ТЗІ 2.5-004-99; НД ТЗІ 2.5-005-99; НД ТЗІ 1.6-005-2013.
3. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX.
4. ISO/IEC 27001:2022. Information security management systems – Requirements.
5. NIST Cybersecurity Framework 2.0 (2024); NIST SP 800-61 Rev. 3 (2025).
6. Directive (EU) 2022/2555 (NIS2); Regulation (EU) 2016/679 (GDPR).
7. ISACA. COBIT 2019 Framework.
8. IMO. Resolution MSC.428(98); MSC-FAL.1/Circ.3. Guidelines on Maritime Cyber Risk Management.