УДК 656.61 **DOI: 10.31653/2306-5761.31.2021.99-107**

IMPLEMENTATION OF THE STRATEGY OF CYBERSECURITY IN SAFETY MANAGEMENT SYSTEMS OF THE SHIP

РЕАЛІЗАЦІЯ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ В СИСТЕМІ УПРАВЛІННЯ БЕЗПЕКОЮ СУДНА

Shumilova K.V., assistant, PhD student

Шумілова К. В., асистент, аспірант

National University «Odessa Maritime Academy», Ukraine

Національний університет «Одеська морська академія», Україна

ABSTRACT

Cyber security is becoming a top priority for world shipping. The paper investigates the latest cyber security reports, proving that navigation systems, port infrastructure, drilling rigs and on-board automated machinery can become extremely vulnerable to targeted cyber attacks. The analysis of today's marine information systems vulnerabilities brings into focus that ship crews with no knowledge on how to recognize and deal with cyber attacks are the "weakest link" in the cyber chain. Given the lack of proper procedure for responding to a cyber threat or cyber incident, the paper discusses the need to develop a cyber security strategy for the training of shore and ship personnel. The examination of the latest known information on security vulnerabilities demonstrates the possibility of conducting risk identification for each ship information system with the determination of the security level and through the rating scale of 0.0 to 10.0.

The paper determines the processes of cyber resilience analysis for developing a response plan on any vessel. Considering that professionals have no opportunity to reach the ship for urgent maintenance or modernization of essential systems and software, the paper suggests basic cyber security management procedures that enable to understand whether a device regularly connected to the "Crew" local network or the ship's network is detected, monitor the use of removable devices violating the safety rules, detect suspicious remote access to the ship's network or operational technologies network, and detect unusual communication connections between the "endpoints" of ship systems.

The conclusions define the need to develop a cyber defence strategy, which takes into account the ship's system vulnerabilities and is based on the comprehensive risk identification, cyber resilience analysis and development of a response plan, which will significantly reduce the risk of cyber attacks.

Keywords: safety of shipping, shipping risks, cyber-safety, cyber attacks, safety management system, information systems, information safety.

Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Увагою до даної теми послужило те, що з 1 січня 2021 року морські адміністрації ряду країн - членів комітету з безпеки на морі IMO (International Maritime Organization, Міжнародна морська організація) почнуть перевірки заходів в їх порти суден на предмет виконання рекомендацій IMO з кібербезпеки. Згідно з вимогами IMO (Резолюція MSC.428 (98) необхідно організувати облік сучасних кіберризиків в існуючих системах управління безпекою після 1 січня 2021 року [3,4].

Проблемою виникнення нових ризиків для морських систем безпеки є не тільки поширення мереж 5G. Окремі системи в мережі суднових OT/IT (операційні технології/інформаційні технології) є незахищеними і можуть бути сприйнятливими або

застарілими, в яких немає оновлень для системи безпеки, що збільшує вразливість щодо кібератак. Відсутність надійного захисту «кінцевих точок» (комп'ютери, сервери, ноутбуки, планшети, мобільні телефони та інші пристрої) інформаційних систем дозволила хакерам реалізувати відомі атаки, такі як «Petya», «Ruik», «WannaCry», «Bad Rabbit» [8, 10].

Далекоглядні судноплавні компанії стали включати в свою модель кіберзагроз такі проблеми вже зараз, розуміючи, що, коли хакери навчаться експлуатувати подібні вразливості, захищатися буде вже пізно. В умовах обмежень, пов’язаних з COVID-19 не може бути абсолютної безпеки, так як багато систем автоматизованих судноплавних процесів не можуть своєчасно оновлюватися і постійно знаходяться в зоні ризику кібератаки [5, 7]. Наслідком цього може стати те, що багато суден можуть піддаватися санкціям в іноземних портах за невиконання рекомендацій ІМО з кібербезпеки.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і виділення невирішених раніше частин загальної проблеми

На онлайн-форумі з кібербезпеки в липні 2020 року повідомлялося про кількість кібератак на системи операційних технологій в морській галузі, яке зросло на 900 відсотків [1]. У доповіді про кіберготовність компанії Acronis (Acronis Cyber Readiness Report), заснованої на опитуванні фахівців з 3400 транснаціональних компаній, повідомили, що через пандемію COVID-19 в дистанційному режимі працює 92% обстежених підприємств. Очевидно, що дії хакерів спрямовані на дистанційних працівників [6]. Атаки на відеоконференції додатків Zoom, Cisco Webex і Microsoft Teams за останні три місяці 2020 року пережили 39% компаній [7, 9]. Під час пандемії значно зросли атаки з використанням програм-вимагачів: про щоденні кібератаки повідомили 31% компаній, а 50% піддавалися їм як мінімум раз на тиждень [5,7, 10]. За оцінками Лондонського Ллойда, збиток від кібератак в морській галузі оцінюється в 200 млрд. доларів [8]. Всі ці дані наочно демонструють актуальність створення стратегії кіберзахисту в морському секторі.

Формулювання цілей статті (постановка завдання)

Метою статті є проведення аналізу можливих вразливостей і ризиків для морських інформаційних систем на основі даних звітів з кібербезпеки, показників провідних лабораторій з розробки та вивчення Інтернет технологій, а також складання реєстру вразливостей і визначення базових процедур для реалізації сучасної стратегії кібербезпеки на кожному судні. Необхідність вирішення проблеми кіберзахисту на судні пов'язана з відсутністю стратегії превентивної кібербезпеки, переліку ризиків і загроз з відповідним планом реагування.

Виклад матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів

Розглянемо результати звітів, отриманих в ході досліджень, перевірених аналітиками видання TechRadar Pro. Відповідно до отриманих даних, більш ніж 70% співробітників вважають, що кібербезпека є ключовою головною біллю керівників компаній, в яких вони працюють. Але, половина з них (45%) зізналася, що відчуває себе погано підготовленими до боротьби з кіберзагрозами [9].

Аналітики TechRadar Pro повідомляють про те, що співробітники підприємств не знають, що робити в разі кібератаки. Кожен четвертий учасник опитування (26%) заявив, що навчання з питань кібербезпеки в його компанії не відповідає стандартам. Ще майже третина респондентів (29%) зізналися, що поняття не мають, хто відповідає за вирішення питань кібербезпеки в їх організації. Зазначимо, що найдорожча кібератака NotPetya, що розповсюджувалася по всьому світу, на думку фахівців, спочатку була націлена на Україну – програма в безлічі українських організацій автоматично скачала апдейт, внаслідок чого було зашифровано всі комп'ютери на Windows. Від NotPetya дуже серйозний удар припав на

компанію Maersk: монітори комп'ютерів офісу компанії один за іншим ставали чорними і на них виводилося повідомлення з вимогою: «сплатіть 300 доларів в біткойн-еквіваленті і ми розшифруємо ваші дані» (рис.1) [8].

Рисунок 1. Зображення на екрані комп'ютера, зараженого вірусом NotPetya [8].

Кібератака WannaCry – вірус-шифрувальник проникав в віддалені комп'ютери через вразливість в Windows і шифрував весь вміст накопичувачів. При цьому хакери пропонували опцію: «заплати – відправимо код для розшифровки і повернення даних». У разі несплати викупу протягом семи днів з моменту зараження можливість розшифровки файлів втрачається назавжди (рис.2) [10].

Рисунок 2. Повідомлення про те, що всі файли пошифровані вірусом WannaCry [10].

Звернемо особливу увагу на базу даних загальновідомих вразливостей інформаційної безпеки – Common Vulnerabilities and Exposures (CVE), яка містить інформацію 2021 року [6]. Сформуємо таблицю по кожній вразливості, якій присвоюється ідентифікаційний номер виду CVE-рік-номер (наведено в табл.2) та ранжування за рівнем безпеки з діапазоном оцінок від 0,0 до 10,0 (табл. 1).

Таблиця 1. Діапазони базових оцінок за рейтингами вразливостей

Базовий діапазон оцінок				
Відсутній	Низький	Середній	Високий	Критичний
0,0	0,1-3,9	4,0-6,9	7,0-8,9	9,0-10,0

Таблиця 2. Уразливості (CVE) IT-систем за даними лабораторії NIST

Ідентифікація вразливостей	Рівень безпеки	Базові оцінки
CVE-2020-26294 – Vela – це інфраструктура конвеєрної автоматизації, побудована на технології контейнерів Linux. У компіляторі Vela до версії 0.6.1 є вразливість, яка дозволяє розкрити конфігурацію сервера. Це впливає на всіх користувачів Vela.	Середній	5.3
CVE-2020-36167 – проблема була виявлена на сервері в Veritas Backup Exec до версії 16.2, 20.6 до виправлення 298543 і 21.1 до виправлення 657517. При запуску завантажує бібліотеку OpenSSL з папки установки.	Високий	8.8
CVE-2021-21449 – SAP 3D Visual Enterprise Viewer, версія 9, дозволяє користувачеві відкривати оброблений файл IFF, отриманий з ненадійних джерел, що призводить до збою програми та стає тимчасово недоступним до тих пір, поки користувач не перезапустить додаток.	Високий	8.8
CVE-2021-21468 – інтерфейс бази даних BW не виконує необхідні перевірки авторизації для аутентифікованого користувача, що дозволяє хакеру практично зчитувати будь-яку таблицю бази даних.	Середній	6.5
CVE-2020-26773 – впровадження шкідливого коду в систему – дозволяє віддаленому аутентифікованому хакеру виконувати довільні команди SQL (шкідливий код) за допомогою параметра дати.	Високий	8.8
CVE-2021-21465 – інтерфейс бази даних BW дозволяє хакеру з низькими привілеями виконувати будь-які створені запити до бази даних, відкриваючи внутрішню базу даних. Хакер може включати свої власні команди SQL, які база даних буде виконувати без належної очистки.	Критичний	9.9
CVE-2021-21470 – надбудова SAP EPM для Microsoft Office, версія – 1010 і надбудова SAP EPM для SAP Analysis Office, версія 2.8, дозволяє перевіреному хакеру з правами користувача аналізувати шкідливі файли XML, що може привести до виникнення XXE-атаки на основі додатків.	Середній	4.4
CVE-2019-25002 – проблема в уразливих конфігураціях програмного забезпечення.	Критичний	9,8

За даними експертів з кібербезпеки в морському секторі найбільш уразливими до кібератак є системи наземного і космічного обладнання; системи глобального позиціонування, електронно-картографічні і навігаційно-інформаційні системи; системи реєстрації даних рейсу; системи вантажних операцій; системи управління двигунами, машинами і живленням; системи контролю доступу; публічні інтернет-мережі судна; адміністративні системи та мережі; системи зв'язку [2, 8, 10, 11].

Аналізуючи вищевказане можна зробити висновок, що чим більше даних буде зібрано, тим більш точні звіти і дії реагування на кіберзагрози буде виконувати система управління

безпекою судна. Тому визначимо необхідні процеси аналізу кіберстійкості суднової IT-системи (див. рис.3).

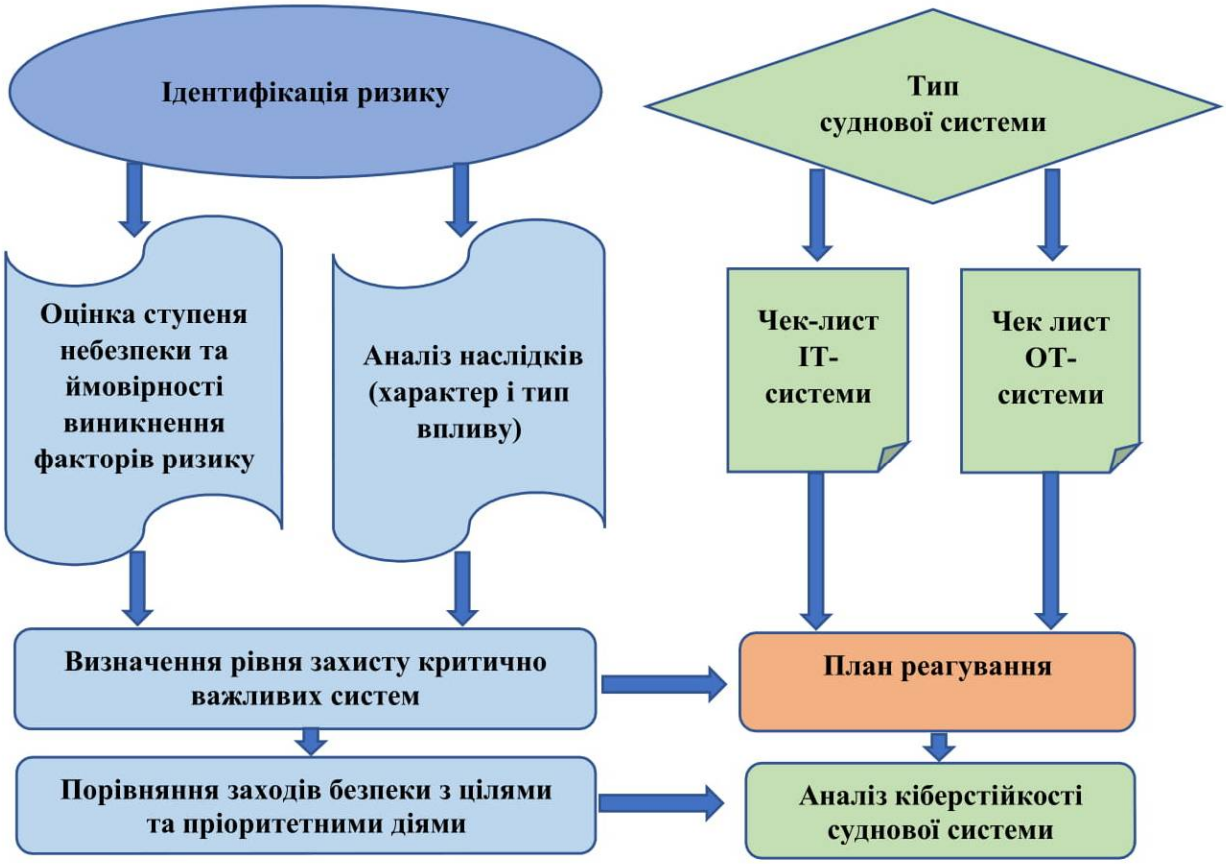

Рисунок 3. Процеси аналізу кіберстійкості суднової IT-системи

Ідентифікація ризику – це процес визначення елементів ризику, складання їх переліку та опису кожного з елементів ризику. Після визначення ризику, необхідно стежити за ним в журналі ризиків або реєстрі.

Оцінка ступеня небезпеки та ймовірності виникнення факторів ризику – забезпечує аналіз вхідних даних процесу загальної оцінки ризику, допомагає в прийнятті рішень щодо необхідності обробки ризику, а також допомагає вибрати відповідні стратегії і методи. Тут ви оціните ймовірність виникнення ризику, а також масштаб впливу на IT/OT-систему. Аналіз може бути якісним (використовуючи шкали, наприклад: «відсутній», «низький», «середній», «високий», «критичний») або кількісним (використовуючи числові терміни, наприклад: фінансовий вплив, процентна ймовірність).

Аналіз наслідків – визначення характеру і типу впливу, який може статися при виникненні конкретної події, ситуації або обставин.

Визначення рівня захисту критично важливих систем – визначення пріоритетів захисту і методів, що застосовуються для зниження конкретного ризику.

Порівняння заходів безпеки з цілями та пріоритетними діями – застосування методів обробки ризику, що забезпечують досягнення прийнятного рівня ризику; перевірка відповідності методів управління ризиком запланованим цілям і докази їх ефективності.

Чек-листи IT/OT-системи – можуть бути використані для ідентифікації небезпек і ризику або оцінки ефективності засобів управління на всіх стадіях життєвого циклу суднових систем, а також як частина інших методів оцінки ризику. Однак вони найбільш корисні для перевірки повноти розгляду досліджуваної проблеми при ідентифікації нових проблем.

План реагування – базується «на комплексній ідентифікації ризиків з визначенням основних етапів дій в надзвичайних ситуаціях і кризах, дозволяє організувати кризове управління на основі деталізації факторів ризику і визначенні його типів» [4, с. 45].

Аналіз кіберстійкості – виявлення прогалин у взаємодії систем і документуванні; моніторинг виконання планів реагування та аналіз наслідків.

Для забезпечення реалізації стратегії кібербезпеки визначимо основні процедури, які можуть бути використані для навчання суднового персоналу (табл.3).

Таблиця 3. Базові процедури управління кібербезпекою суднової IT-системи.

№ з/п	Категорії процедур. Пристрої	Необхідні дії
1.	**Відповідальні особи для забезпечення захисту інформації суднової IT-системи.** • Список відповідальних осіб.	• Своєчасно актуалізуйте список відповідальних осіб з врахуванням зміни екіпажу, хвороби, психічного стану та перерозподілу зобов'язань.
2.	**Список IT-технічних засобів судна.** • Експлуатаційна документація на кожну систему: AIS, ECDIS, VDR, TOS, EPIRB, GNSS, GPS та ін.	• Складіть і підтримуйте в актуальному стані список всіх IT-технічних засобів судна: ✓ адміністративні системи та мережі; ✓ системи зв'язку; ✓ системи ходового містка; ✓ системи обробки і управління вантажем; ✓ системи управління двигунами, машинами і живленням; ✓ системи контролю доступу; ✓ системи обслуговування і управління пасажирами; ✓ публічні інтернет-мережі судна, призначені для використання пасажирами.
3.	**Організаційно-розпорядчі документи.** • Правила, інструкції та процедури з кібербезпеки, в яких введено обмеження на несанкціоновані дії екіпажу, описано розмежування доступу, вказані вимоги до паролів.	• Ознайомлюйте екіпаж з обов'язковими документами під особистий підпис: ✓ вступний інструктаж на судні; ✓ первинний інструктаж на робочому місці; ✓ повторний інструктаж на робочому місці; ✓ позаплановий інструктаж на робочому місці; ✓ цільовий інструктаж.
4.	**Програмне забезпечення. Підключення.**	• Використовуйте на робочих IT-пристроях тільки встановлене програмне забезпечення (ПЗ). • Не відкривайте вкладення в листах з незнайомими розширеннями, від незнайомих адресатів. • Не ігноруйте попереджувальні повідомлення від програм. • Не підключайте непередбачені бездротові пристрої в мережу, навіть якщо це дуже зручно для вас. • Пам'ятайте, що бездротові з'єднання повинні бути відповідним чином захищені.
5.	**Мережеве обладнання.** • Журнали подій	• Перевірте, щоб були відсутні ресурси, доступні одночасно до мережі IT-системи судна і мережі

	мережевого обладнання. • Резервна копія конфігурації мережевого устаткування і еталонна копія вбудованого ПЗ.	операторів берегової компанії. • Для входу в інтерфейс управління мережевого обладнання використовуйте окремі облікові записи. • Зберігайте журнали подій мережевого обладнання не менше одного року. • Вимкніть невикористовувані порти і розташуйте мережеве обладнання в шафі, яка замикається. • Зберігайте резервну копію конфігурації мережевого устаткування і еталонну копію вбудованого ПЗ.
6.	**Управління доступом.** • Журнал для відслідковування процесу зміни користувачів.	• Для доступу в операційну систему, а також в привілейований конфігураційний режим повинні бути створені окремі облікові записи, недоступні операторам. • Нікому не повідомляйте дані про свої облікові записи (логін, пароль). • Привілеї доступу повинні бути призначені строго для виконання службових обов'язків і не більше того. • Використовуйте тільки свій обліковий запис, після закінчення роботи завершуйте сеанс свого облікового запису. Якщо зміна облікового запису не передбачена технологічним процесом, необхідно ведення журналу для відслідковування процесу зміни користувачів. • Пам'ятайте, що це допоможе при розслідуванні кіберінцидентів і убезпечить вас.
7.	**Фізичний доступ.**	• Обмежте доступ до всіх систем і блоків робочих IT-станцій (можливо-шляхом їх переміщення в залізні ящики з замками або приміщення з шафами і замками). Перевіряйте наявність замків. • Встановіть кілька недорогих IP-камер на найбільш критичних вузлах IT-систем.
8.	**Знімні носії.** • Журнал реєстрації носія з присвоєнням облікового номеру.	• Використовуйте тільки враховані носії інформації. Реєструйте носій в журналі, присвоюйте обліковий номер. • Використовуйте врахований носій тільки в робочих цілях і тільки на робочому комп'ютері. • Якщо є можливість, краще, щоб врахований носій був персонально вашим. • Зберігайте враховані носії в безпечному місці (наприклад, в шафі, яка замикається). • Не переміщуйте враховані носії за межі судна, не давайте для особистих цілей персоналу і самі в особистих цілях не використовуйте. • Перевіряйте враховані знімні носії перед використанням в IT-системі на віруси. • Не підключайте мобільні модеми до робочих IT-систем.
9.	**Мобільні пристрої.**	• Не підключайте мобільні пристрої, якщо це

		заборонено регламентом. • Не встановлюйте додатки для мобільних пристроїв з недовірених джерел. • Не здійснюйте маніпуляції, які заборонені або впливають на безпеку мобільного пристрою.
10.	**Паролі.**	• Перевіряйте наявність паролів на всіх пристроях, інтерфейсах, адміністративних і призначених для користувача облікових записах на комп'ютерах. • Ніколи не залишайте паролі за замовчуванням, застосовуйте складні і надійні паролі з наявністю спеціальних символів і різних регістрів. • Міняйте регулярно паролі. Якщо записали пароль на папірець, приберіть його в надійне місце.
11.	**Оновлення та резервне копіювання.**	• Регулярно і своєчасно оновлюйте системне і прикладне ПЗ. • Перед установкою оновлення обов'язково протестуйте його на сумісність з вже встановленим ПЗ. • Регулярно перевіряйте періодичне резервне копіювання інформації, конфігурацій ПЗ. • Ви повинні визнати, що ваше судно може стати мішенню для кіберзлочинців і зобов'язані забезпечити виконання основних заходів кібербезпеки, щоб ускладнити хакерам можливість здійснення кібератаки.
12.	**Моніторинг подій і оповіщення про інциденти.** • Журнали подій ОС, прикладних програм і обладнання. • Чек листи IT/OT-систем судна. • Форма донесення про подію. • Виписка з суднового і машинного журналу. • Письмові свідчення вахтового, членів екіпажу. • Звіт про вжиті заходи. • Телекси, електрона пошта і факсимільні повідомлення по суті події, а також копії всього листування, причетного до інциденту.	• Фіксуйте в журналі події, пов'язані зі спробами отримання доступу до управління компонентами суднової системи і засобами захисту, зі змінами конфігурацій компонентів IT-системи, зі змінами прав доступу, зі спробами несанкціонованого підключення до мережевої інфраструктури. • Збирайте і аналізуйте статистику роботи вузлів системи на предмет збоїв. Мета – виключити недобросовісних вендорів, які можуть підзаробляти на «підтримці і відновленні». • Своєчасно інформуйте берегові служби та компанію про інциденти.

Висновки і перспектива подальшої роботи по даному напрямку

Для розуміння реальної ситуації із забезпеченням безпеки суднових IT-систем необхідно створення стратегії кібербезпеки для навчання берегового і суднового персоналу [3]. Запропоновані базові процедури управління кібербезпекою суднової IT-системи дозволять визначити необхідні дії для реалізації такої стратегії. В перспективі актуальним

питанням може бути дослідження стану судноплавних процесів під впливом нових кібератак для організації обліку сучасних кіберризиків в існуючих системах управління безпекою судна, особливо після 1 січня 2021 року, згідно з вимогами Комітету з безпеки на морі IMO (Резолюція MSC.428 (98)).

ЛІТЕРАТУРА

1. Maritime cyber-attacks up by 900% in three years. Available at: https://thedigitalship.com/news/maritime-satellite-communications/item/6706-maritime-cyber-attacks-up-by-900-in-three-years?utm_source=dlvr.it&utm_medium=linkedin (viewed on 2021-02-05)
2. The Guidelines on Cyber Security Onboard Ships, version 3.0, BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, OCIMF, WSC and IUMI, 2018
3. IMO / Maritime cyber risk. Available at: www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx (viewed on 2020-12-31)
4. Shumilova K., Onishchenko O. ACTION PLANNING IN COMPREHENSIVE SHIPPING RISK IDENTIFICATION. The scientific heritage | International independent scientific journal. No 49 (2020). P.1. – P. 40-46. ISSN 9215 – 0365.
5. NATIONAL VULNERABILITY DATABASE / Information Technology Laboratory / NIST, 2021. Available at: https://nvd.nist.gov/ (viewed on 2021-01-03)
6. Acronis опубликовала доклад о киберготовности, 2020. Режим доступу: https://www.itweek.ru/security/news-company/detail.php?ID=214578 (переглянуто 2021-02-05)
7. Schroedinger's Pet(ya). 2017. Available at: https://securelist.com/schroedingers-petya/78870/ (viewed on 2020-11-20)
8. В большинстве компаний мира не верят в возможность успешного противостояния хакерам, 2020. Режим доступу: https://safe.cnews.ru/news/top/2020-09-22_v_bolshinstve_kompanij_mira (переглянуто 2021-01-15)
9. 10 самых впечатляющих кибератак в истории, 2020. Режим доступу: https://3dnews.ru/1009634/10-samih-vpechatlyayushchih-kiberatak-v-istorii (переглянуто 2020-12-19)
10. Уязвимости. Positive Technologies, 2021 [Електронний ресурс]. – Режим доступу: https://www.securitylab.ru/news/tags/ Positive+Technologies/ (переглянуто 2021-01-25)
11. Вильский Г.Б. Информационная безопасность судовождения: монография / Г. Б. Вильский. – Миколаїв: Видавництво ФОП Швець В. Д., 2014. – 336 с.