УДК 004.832.28
DOI https://doi.org/10.32782/tnv-tech.2024.3.3

АНАЛІЗ КІБЕРАТАК НА ІНФОРМАЦІЙНІ СИСТЕМИ МОРСЬКИХ ПОРТІВ ТА МЕТОДИ ПРОТИДІЇ ЇМ

Коновалов С. М. *– старший викладач кафедри технічної кібернетики й інформаційних технологій імені професора Р. В. Меркта Одеського національного морського університету*
ORCID ID: 0000-0002-2533-8660

Чумак О. А. *– старший викладач кафедри технічної кібернетики й інформаційних технологій імені професора Р. В. Меркта Одеського національного морського університету*
ORCID ID: 0009-0002-5802-9765

Тузова І. А. *– доцент кафедри технічної кібернетики й інформаційних технологій імені професора Р. В. Меркта Одеського національного морського університету*
ORCID ID: 0009-0002-4198-378X

Тузов О. В. *– старший викладач кафедри технічної кібернетики й інформаційних технологій імені професора Р. В. Меркта Одеського національного морського університету*
ORCID ID: 0009-0006-5443-4957

Панченко Т. Д. *– старший викладач кафедри технічної кібернетики й інформаційних технологій імені професора Р. В. Меркта Одеського національного морського університету*
ORCID ID: 0009-0007-4629-9537

Хотін С. Ю. *– кандидат технічних наук, доцент, доцент кафедри безпеки життєдіяльності, екології та хімії Одеського національного морського університету*
ORCID ID: 0000-0003-2424-9276

Розвиток інформаційних технологій в морських портах в останні декілька десятиліть спричинив також і розвиток різноманітних способів незаконному впливу на ці інформаційні технології за допомогою кібератак, кількість яких стає все більшою з кожним роком. Для протистояння цим загрозам потрібно дуже добре знати якомога більше про кібератаки. У даній статті проводиться аналіз кібератак, яких зазнавали морські порти в останні роки по всьому світу. Представлена статистика збільшення кількості кібератак за недавній короткий період у минулому (2017-2020 рр). Були розглянуті основні проблеми вразливості портів перед кібератаками. Також були приведені основні види кібератак: DDoS-атаки, атаки на системи SCADA, найбільш конкретно була звернена увага на шкідливе програмне забезпечення та віруси і на фішинг та соціальну інженерію, наведені приклади з їх описами та наслідками. Після цього були виведені основні наслідки від подібних кібератак, і на основі всіх цих даних, приведених вище, були виведені найбільш дієві засоби для протидії кібератакам на морські порти, особливу увагу було приділено компонентам, які становлять кібербезпеку морських портів, наведені описи та існуючі приклади. В кінці, на основі всіх проаналізованих та підпорядкованих даних стосовно

кібератак, була розроблена комплексна схема кібербезпеки морських портів, яка містить у собі дев'ять основних компонент, які представляють ключові аспекти кібербезпеки, що, у свою чергу, об'єднують у собі декілька засобів по протидії кібератакам. Все це представляє собою комплекс по загальному кіберзахисту морських портів, починаючи з фізичного захисту до комплаєнсу та управління ризиками. Виходячи з цього, можна зробити висновок, що майбутнє портової інфраструктури залежить від можливості адаптуватися до нових викликів кіберпростору. Тільки об'єднані зусилля та постійне вдосконалення заходів захисту зможуть гарантувати стійкість та безпеку морських портів в умовах цифрового світу, що швидко змінюється.

Ключові слова: *інформаційні технології, морські порти, кібератаки, програмне забезпечення, віруси, DDoS-атаки, фішинг, кібербезпека, наслідки, ризики, кіберзахист.*

Konovalov S. M., Chumak O. A., Tuzova I. A., Tuzov O. V., Panchenko T. D., Khotin S. Yu. Analysis of cyber attacks on information systems of seaports and methods of countering them

The development of information technologies in seaports in the last few decades has also led to the development of various ways to illegally influence these information technologies with the help of cyber attacks, the number of which is increasing every year. To counter these threats, you need to know as much as possible about cyber attacks. This article analyzes the cyber attacks experienced by seaports around the world in recent years. The statistics of the increase in the number of cyber attacks for a recent short period in the past (2017-2020) are presented. The main problems of port vulnerability to cyber attacks were considered. The main types of cyber attacks were also presented: DDoS attacks, attacks on SCADA systems, the most specific attention was paid to malicious software and viruses, and to phishing and social engineering, examples with their descriptions and consequences were given. After that, the main consequences of such cyber attacks were deduced, and based on all these data given above, the most effective means to counter cyber attacks on seaports were deduced, special attention was paid to the components that make up the cyber security of seaports, descriptions and existing examples were given. In the end, on the basis of all the analyzed and subordinated data regarding cyber attacks, a comprehensive scheme of cyber security of seaports was developed, which contains nine main components that represent key aspects of cyber security, which, in turn, combine several means of countering cyber attacks. All this represents a complex of general cyber protection of seaports, starting from physical protection to compliance and risk management. Based on this, we can conclude that the future of the port infrastructure depends on the ability to adapt to the new challenges of cyberspace. Only joint efforts and continuous improvement of security measures can guarantee the sustainability and security of seaports in the rapidly changing digital world.

Key words: *information technology, seaports, cyber attacks, software, viruses, DDoS attacks, phishing, cyber security, consequences, risks, cyber protection.*

Вступ. В останні десятиліття морські порти еволюціонували, ставши центрами високотехнологічної логістики та управління вантажопотоками. Інформаційні системи, що управляють процесами навігації, контролю вантажів та безпеки, стають невід'ємною частиною повсякденної роботи портів. Однак із зростанням цифровізації та інтеграції сучасних технологій в операційні процеси зростає і загроза кібератак [1, 2]. Ці атаки здатні порушити функціонування портів, викликати серйозні економічні та екологічні наслідки. В умовах, коли портові системи обробляють мільйони даних у реальному часі, захист від кіберзагроз стає критично важливим завданням для забезпечення стабільності та безпеки глобальної транспортної інфраструктури [3, 4, 5]. У цій статті ми розглянемо проблеми вразливості портів перед кібератаками, основні види кібератак, наслідки для морських портів, та на основі цих даних проаналізуємо головні заходи, які потрібно вживати для захисту від цих загроз.

Проблеми вразливості портів перед кібератаками. Останнім часом кількість кібератак на морській галузі сильно збільшилось. Кібератаки в системі морської галузі зросли на 900 % з 2017 по 2020 роки. Якщо у 2017 році було повідомлено про 50 атак, у 2018 році кількість атак зросла до 120, то у 2019 році було зареєстровано 310 атак, у 2020 році кількість атак вже перевищила 500 (рис. 1) [2, 4].

Рис. 1. Кібератаки на морські порти (2017-2020 рр.)

Розглянемо основні проблеми вразливості портів перед кібератаками [1]:

– складна і різнорідна інфраструктура – порти включають безліч різних систем і пристроїв: від судноплавних систем і кранів до IT-мереж і систем управління логістикою. Неправильна інтеграція або недостатній захист окремих компонентів можуть створити вразливості, які можуть використовувати хакери для проведення атак;

– недостатня обізнаність та навчання персоналу – співробітники портів можуть бути недостатньо обізнані про методи кібератак та засоби захисту від них, що призводить до того, що вони можуть стати жертвами фішингових атак або ненавмисно надати доступ зловмисникам;

– відсутність своєчасного оновлення та патчів – багато систем у портах працюють на застарілому програмному забезпеченні, яке не оновлюється вчасно. Непатчені уразливості можуть бути легко використані зловмисниками для проникнення в системи;

– неадекватне управління доступом – не всі порти мають суворі політики управління доступом та контролю привілеїв, це може призвести до несанкціонованого доступу до критичних систем та даних;

– відсутність сегментації мережі – у деяких портах відсутня сегментація мереж, що дозволяє зловмисникам поширювати атаки по всій мережі після початкового проникнення. Відсутність сегментації збільшує масштаби можливих пошкоджень і ускладнює локалізацію та усунення загроз;

– вразливості IoT (Internet of Things)-пристроїв – багато пристроїв в портах, такі як сенсори та камери, підключені до інтернету і можуть бути вразливі до атак. Недостатній захист пристроїв IoT може надати зловмисникам вхідну точку в мережі порту;

– недостатня увага до фізичної безпеки – фізична безпека часто розглядається окремо від кібербезпеки. Комбіновані атаки, що використовують як фізичні, так і кіберметоди, можуть бути більш успішними та руйнівними;

– відсутність постійного моніторингу та реагування на інциденти – брак ресурсів для постійного моніторингу мереж та систем порту. Це призводить до затримки у виявленні та реагуванні на кіберінциденти, що збільшує потенційні збитки.

Види кібератак. На підставі прецедентів різних кібератак [1, 4, 6] на інформаційні системи портової інфраструктури по всьому світу, можна виділити кілька основних видів кібератак, залежно від поширення та напряму шкідливої діяльності:

– шкідливе ПЗ (програмне забезпечення) та віруси – багато кібератак починаються із зараження систем шкідливим програмним забезпеченням. Шкідливі програми можуть впроваджуватись через електронну пошту, фішинг, заражені веб-сайти або навіть фізичні пристрої, такі як флешки. Після проникнення вірус може шпигувати, красти дані або виводити системи з ладу;

Приклади деяких подібних вірусів [4]:

− Stuxnet (2010) – міг би бути адаптований для атак на системи керування навігацією або обладнання портових терміналів, порушуючи їх роботу та викликаючи збої в управлінні;

− Emotet (2014) – може використовуватися для атаки на персонал порту, злому робочих станцій та розповсюдження шкідливого ПЗ по всій мережі порту, що призводить до витоку даних та порушення роботи систем;

− Triton (2017) – може бути використаний для атак на системи управління портами, що може призвести до порушення роботи обладнання та загрозливих екологічних наслідків;

− NotPetya (2017) – міг би атакувати інформаційні системи портів, зашифровуючи дані та паралізуючи їх роботу, що призводило б до зупинення всіх операцій та значних фінансових втрат.

Втрати від шкідливого ПЗ оцінюються як сума вартості простою та відновлення, а також вартості втрачених даних.

– DDoS-атаки (розподілені атаки на відмову в обслуговуванні) – DDoS-атаки спрямовані на перевантаження систем трафіком, що призводить до їх недоступності. У контексті морських портів такі атаки можуть паралізувати роботу систем управління та моніторингу, що створює серйозні перебої в логістиці, що спричиняє великі економічні втрати;

– атаки на системи SCADA – SCADA (Supervisory Control and Data Acquisition) використовуються для контролю та управління технологічними процесами в портах. Атаки на ці системи можуть призвести до відключення обладнання, аварій та інших небезпечних наслідків;

– фішинг та соціальна інженерія – хакери часто використовують методи соціальної інженерії, щоб обманним шляхом отримати доступ до конфіденційної інформації або систем [7]. У таблиці 1 представлені різні види фішингу, які застосовуються в атаках на порти, їх короткий опис та наслідки від роботи.

Таблиця 1

Методи фішингу

Метод фішингу	Опис	Наслідки
E-mail фішинг	Надсилання масових листів із шкідливими посиланнями або вкладеннями, які виглядають як легітимні повідомлення від відомих компаній чи осіб.	Втрата даних, зараження систем, крадіжка облікових даних.
Spear фішинг	Цілеспрямовані атаки на окремих співробітників чи групи, де листи чи повідомлення містять інформацію, що імітує легітимні запити колег чи партнерів.	Крадіжка облікових даних, доступ до конфіденційної інформації, витік даних.
Веб-фішинг	Створення підроблених веб-сайтів, що імітують легітимні сторінки, для збирання особистої інформації користувачів (логіни, паролі, банківські дані).	Крадіжка облікових даних, фінансові втрати, витік особистої інформації.

Продовження таблиці 1

SMS-фішинг (Smishing)	Надсилання фальшивих текстових повідомлень (SMS), що містять посилання на шкідливі веб-сайти або запити на надання особистої інформації.	Втрата даних, фінансові втрати, зараження мобільних пристроїв.
Вішинг (Vishing)	Використання телефонних дзвінків для отримання конфіденційної інформації, подання шахраїв як співробітників банків чи інших організацій.	Крадіжка особистих даних, фінансові втрати, соціальна інженерія.
Clone фішинг	Надсилання листів, які є копіями раніше надісланих легітимних листів, але із зміненими посиланнями або вкладеннями на шкідливі.	Зараження систем, крадіжка даних, поширення шкідливого ПЗ.
Фармінг (Pharming)	Перенаправлення користувачів на підроблені веб-сайти без їх відома шляхом зміни DNS-записів або використання зловмисного програмного забезпечення.	Крадіжка облікових даних, фінансові втрати, витік особистої інформації.

Наслідки кібератак. Наслідки від впливів кібератак можна умовно поділити на такі категорії:

– економічні втрати – порти є важливими елементами глобальних ланцюжків постачання. Збої у роботі можуть викликати значні економічні втрати для підприємств і країн. Простої, викликані кібератаками, можуть призвести до значних збитків через затримки у доставці вантажів та додаткові витрати на відновлення роботи;

– витік даних – конфіденційні дані, такі як інформація про вантажі, контракти та фінансові дані, можуть стати метою кібератак. Витік таких даних може завдати шкоди як окремим компаніям, так і національній безпеці;

– порушення безпеки – атаки на інформаційні системи портів можуть створити загрозу для безпеки, оскільки вони можуть вивести з ладу системи моніторингу та управління, що може призвести до аварій та екологічних катастроф.

Заходи захисту. З розвитком кібератак також розвивалися і заходи щодо захисту від них [1, 4], подібні заходи умовно об'єднаємо в наступні групи:

– посилення кібербезпеки – порти повинні активно інвестувати в кібербезпеку, впроваджуючи сучасні системи захисту та моніторингу. Важливо регулярно оновлювати програмне забезпечення та системи безпеки, щоб протистояти новим загрозам. У таблиці 2 представлені основні компоненти кібербезпеки портів та їх опис;

– навчання персоналу – навчання співробітників основам кібербезпеки та методам запобігання атакам є ключовим елементом захисту. Співробітники повинні бути поінформовані про можливі загрози та способи їх розпізнавання та запобігання;

– спільна робота – порти повинні активно співпрацювати з іншими організаціями, урядами та міжнародними структурами для обміну інформацією про кіберзагрози та спільної розробки ефективних заходів захисту;

– інцидент-менеджмент – розробка та впровадження плану дій у разі кібератаки є важливим кроком для мінімізації наслідків. План повинен включати заходи щодо швидкого відновлення роботи систем та мінімізації збитків.

Комплексна схема кібербезпеки морських портів. На основі аналізу кібератак на морські порти, було складено комплексну схему кібербезпеки морських портів (рис. 2).

Таблиця 2

Основні компоненти кібербезпеки портів

Компонент	Опис	Приклади
Антивіруси та антишпигунське ПЗ	Програмне забезпечення, призначене для виявлення, блокування та видалення шкідливих програм, шпигунських програм та вірусів.	Symantec Endpoint Protection, McAfee Endpoint Security.
Фаєрволы (Firewall)	Системи, які контролюють та фільтрують мережевий трафік, запобігаючи несанкціонованому доступу та атакам.	Cisco ASA, Fortinet FortiGate.
Системи виявлення та запобігання вторгненням (IDS/IPS)	Системи, які моніторять трафік мережі та системи на наявність підозрілих активностей, запобігаючи вторгненням та атакам.	Snort, Suricata, Palo Alto Networks.
Шифрування даних	Технології, які перетворюють дані на нечитабельний формат, доступний лише за наявності відповідного ключа.	AES (Advanced Encryption Standard), RSA.
Системи керування доступом (IAM)	Рішення, що забезпечують контроль над доступом користувачів до ресурсів та даних на основі їх ролей та прав.	Okta, Microsoft Active Directory, IBM Security Identity Governance.
Системи моніторингу та легування (SIEM)	Інструменти для збору, аналізу та візуалізації журналів подій та мережевого трафіку для виявлення та реагування на інциденти безпеки.	Splunk, LogRhythm, IBM QRadar.
Системи управління вразливістю (Vulnerability Management)	Інструменти для сканування та оцінки вразливостей у системах та програмах, а також управління патчами.	Nessus, Qualys, Rapid7.
Резервне копіювання та відновлення даних	Рішення для створення резервних копій даних та забезпечення їх відновлення у разі втрати чи пошкодження.	Veeam Backup & Replication, Acronis Backup.
Навчання та підвищення обізнаності персоналу	Програми навчання та тренінги, спрямовані на підвищення обізнаності співробітників про кіберзагрози та методи захисту.	KnowBe4, Cofense, SANS Security Awareness Training.
Плани реагування на інциденти (IRP)	Документовані процедури та плани дій для швидкого та ефективного реагування на кіберінциденти.	Визначення інцидентів, команди реагування, процедури сповіщення та відновлення.
Системи виявлення та запобігання DDoS-атак	Рішення, призначені для захисту мережевої інфраструктури від розподілених атак на відмову в обслуговуванні (DDoS).	Arbor Networks, F5 BIG-IP, Radware.
Багатофакторна автентифікація (MFA)	Технологія, що вимагає доступу до системи декількох форм ідентифікації (наприклад, пароль, біометрія, токен).	Google Authenticator, Microsoft Authenticator, Duo Security.

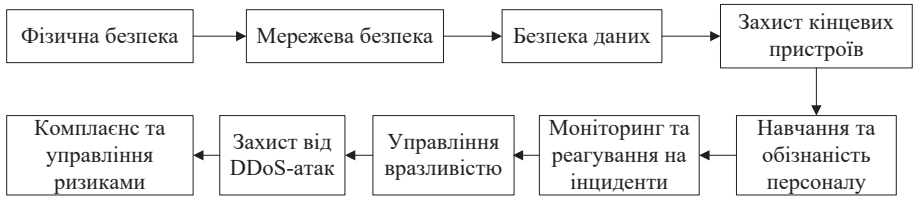

Рис. 2. Комплексна схема кібербезпеки морських портів

Ця схема охоплює ключові аспекти кібербезпеки морських портів та допомагає структурувати підхід до захисту інфраструктури від різних загроз. Розглянемо основні компоненти цієї схеми:

1. Фізична безпека:

– контроль доступу: використання систем контролю доступу (замки, карти, біометрія);

– відеоспостереження: камери та системи спостереження для моніторингу ключових об'єктів;

– охорона: патрулювання та фізичний захист критично важливих зон.

2. Мережева безпека:

– фаєрволи: запобігання несанкціонованому доступу;

– системи виявлення та запобігання вторгненням (IDS/IPS): моніторинг трафіку та виявлення підозрілих активностей;

– VPN: захищені канали зв'язку для віддаленого доступу.

3. Безпека даних:

– шифрування даних: захист даних у процесі передачі та зберігання;

– резервне копіювання та відновлення: регулярне створення резервних копій та плани відновлення даних;

– управління правами доступу (IAM): контроль та моніторинг доступу до даних та систем.

4. Захист кінцевих пристроїв:

– антивірусне ПЗ: захист від вірусів та шкідливого ПЗ;

– антиспам: фільтрація шкідливих та фішингових повідомлень;

– оновлення та патчі: регулярне оновлення програмного забезпечення для усунення вразливостей.

5. Навчання та обізнаність персоналу:

– регулярні тренінги: навчання співробітників основам кібербезпеки та діям у разі інцидентів;

– фішинг-тести: проведення регулярних тестів на виявлення фішингових атак.

6. Моніторинг та реагування на інциденти:

– системи управління подіями та інцидентами безпеки (SIEM): збір та аналіз логів для виявлення інцидентів;

– центри реагування на інциденти (SOC): команди фахівців, які готові оперативно реагувати на інциденти;

– плани реагування на інциденти: документовані процедури для швидкого та ефективного реагування.

7. Управління вразливістю:

– сканування уразливостей: регулярне сканування систем на наявність уразливостей;

– управління патчами: оперативне впровадження патчів та оновлень.

8. Захист від DDoS-атак:

– анти-DDoS системи: використання спеціалізованого ПЗ та обладнання для захисту від розподілених атак;

– моніторинг трафіку: аналіз мережевого трафіку для виявлення аномалій.

9. Комплаєнс та управління ризиками:

– відповідність стандартам: виконання вимог міжнародних та національних стандартів щодо кібербезпеки;

– управління ризиками: регулярна оцінка ризиків та розробка стратегій їх мінімізації.

Висновки. З розвитком технологій і збільшенням цифровізації морські порти стають дедалі вразливішими до кібератак, які стають все більш різноманітними і небезпечними. Економічні втрати, витік даних та порушення безпеки є основними негативними наслідками кібератак на порти. Ці інциденти можуть спричинити значні фінансові збитки, підірвати довіру до інфраструктури та завдати шкоди навколишньому середовищу. Приклади реальних атак підтверджують необхідність вжиття заходів щодо посилення кібербезпеки. Для ефективного захисту портів необхідно інвестувати в сучасні системи захисту, навчати персонал основ кібербезпеки, активно співпрацювати з іншими організаціями та розробляти плани реагування на інциденти. Комплексний підхід до кібербезпеки, що включає технічні, організаційні та освітні заходи, дозволить значно знизити ризики та забезпечити безперебійну роботу портів. Важливо пам'ятати, що кібербезпека – це безперервний процес, що потребує постійної уваги та покращення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Мельник О.М., Корякін К.С., Саф'ян О.С., Заяц С.В., Щенявський Г.С. Актуальні питання кібербезпеки морських портів. *Modern scientific researches.* 2022. № 18, part 1. С. 81-86. DOI: 10.30889/2523-4692.2021-18-01-019.

2. Zayats S.V. Ensuring maritime security and measures against cyber threats and cyber piracy at sea. *Science for modern man. Development of transport and transport systems.* Karlsruhe: ScientificWorld-NetAkhatAV. 2023. С. 63-89. DOI: 10.30890/2709-2313.2023-16-01-017. ISBN 978-3-949059-70-4.

3. Пядишев В.Г. Питання вдосконалення кібербезпеки морського транспорту: зарубіжний досвід. *Морська безпека та оборона*. 2023. № 1. С. 78-86.

4. Шумілова К.В. Навігаційні ризики в аспекті кібербезпеки транспортних суден і військових кораблів. *Scientific collection «Interconf»*. 2022. № 121. С. 391-408. DOI 10.51582/interconf.19-20.08.2022.037.

5. Cyber digest. Огляд подій в сфері кібербезпеки. 2023. 43 с.

6. Муравський А. Порти під кібератаками: Зростаюча загроза для морської галузі. *Центр транспортних стратегій.* 2024. URL: https://cfts.org.ua/articles/porti_pid_kiberatakami_zrostayucha_zagroza_dlya_morsko_galuzi_2021/140318 (дата звернення: 24.07.2024).

7. Фішинг: методи та приклади атак. *Gridinsoft*. 2023. URL: https://gridinsoft.ua/phishing (дата звернення: 24.07.2024).

REFERENCES:

1. Melnyk, O.M. & Koryakin, K.S. & Safian, O.S. & Zayats, S.V. & Shcheniavskyi, H.S. (2022). Aktualni pytannia kiberbezpeky morskykh portiv [Current issues of cyber security of seaports]. *Modern scientific researches*, *№ 18, part 1*, 81–86, DOI: 10.30889/2523-4692.2021-18-01-019 [in Ukrainian].

2. Zayats, S.V (2023). Ensuring maritime security and measures against cyber threats and cyber piracy at sea. *Science for modern man. Development of transport and transport systems*, Karlsruhe: ScientificWorld-NetAkhatAV, 63–89, DOI: 10.30890/2709-2313.2023-16-01-017, ISBN 978-3-949059-70-4 [in Ukrainian].

3. Piadyshev, V.H. (2023). Pytannia vdoskonalennia kiberbezpeky morskoho transportu: zarubizhnyi dosvid [The question of improving maritime transport cyber security: foreign experience]. *Morska bezpeka ta oborona. – Maritime security and defense, № 1,* 78–86 [in Ukrainian].

4. Shumilova, K.V. (2022). Navihatsiini ryzyky v aspekti kiberbezpeky transportnykh suden i viiskovykh korabliv [Navigational risks in the aspect of cyber security of transport vessels and warships]. *Scientific collection «Interconf», № 121,* 391–408, DOI 10.51582/interconf.19-20.08.2022.037 [in Ukrainian].

5. (2023). *Cyber digest. Ohliad podii v sferi kiberbezpeky – Cyber digest. Overview of events in the field of cyber security*, 43 [in Ukrainian].

6. Muravskyi, A. (2024) Porty pid kiberatakamy: Zrostaiucha zahroza dlia morskoi haluzi [Ports under cyber attacks: A growing threat to the maritime industry]. Tsentr transportnykh stratehii – Center for transport strategies. Retrieved from https://cfts.org.ua/articles/porti_pid_kiberatakami_zrostayucha_zagroza_dlya_morsko_galuzi_2021/140318 (date of access: 24.07.2024) [in Ukrainian].

7. (2023) Fishynh: metody ta pryklady atak [Phishing: methods and examples of attacks]. Gridinsoft. Retrieved from https://gridinsoft.ua/phishing (date of access: 24.07.2024) [in Ukrainian].