УДК 001.891
Зайцева Т., Кравцова Л., Камінська Н.
Херсонська державна морська академія, Херсон, Україна
ORCID ID 0000-0001-6780-719X
ORCID ID 0000-0002-0152-635X
ORCID ID 0000-0002-9975-7403

МАРКОВСЬКІ ПРОЦЕСИ В ДОСЛІДЖЕННІ ЙМОВІРНОСТІ КІБЕРАТАК НА МОРСЬКОМУ СУДНІ

DOI 10.14308/ite000763

Судноплавство все більше покладається на цифрові рішення для виконання повсякденних завдань. Відбуваються постійні оновлення в галузі інформаційних технологій, доступності даних, швидкості обробки та передачі даних із розширеними можливостями для оптимізації роботи, економії витрат, підвищення безпеки та стійкості бізнесу. Поряд зі зростанням залежності від автоматизації, значно посилюється ризик зовнішнього втручання та порушення роботи ключових систем; хакери можуть втручатися в роботу корабля або навігаційних систем, відрізати всі зовнішні комунікації судна або отримувати конфіденційні дані.

Дослідження кібербезпеки об'єктів морського сектора є досить гострими на сьогодні і потребують постійної уваги та вдосконалення.

За даними експертів із кібербезпеки в морському секторі найбільш вразливими 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 та портова інфраструктура.

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

Ретельний аналіз джерел кібератак, які відбуваються найбільш часто, надає змогу припустити, що це випадковий процес, який підпорядковується законам, що в теорії ймовірностей (або, точніше, стохастичних процесів) називають марковськими процесами.

Предметом дослідження є побудова моделі на основі властивостей марковських процесів, яка дозволяє детальніше вивчити процес, виконати аналіз та прогнозування розвитку кіберінциденту для прийняття управлінського рішення щодо подальших конструктивних дій.

***Ключові слова**: кібербезпека, кіберінцидент, ланцюги Маркова, марковські процеси*

Постановка проблеми та її актуальність. Ворог прийшов на нашу землю. Він знищує наші міста, нашу культуру, наше надбання у всіх напрямках. Для нього немає нічого святого. Немає мети, немає мотивації, крім тотального знищення нашої держави, якщо тільки добре підзаробити навіть пограбуванням українського населення. Він використовує для цього будь-які засоби, зокрема кібератаки на інфраструктуру та на населення України.

Ворожі спеціалісти з інформаційних технологій перехоплюють розмови звичайних громадян, завдяки цьому відстежують важливу для них інформацію. Нам здається, що наша розмова з друзями чи родичами не несе ніякої корисної інформації для ворога або

злочинця. Але це не так. Навіть маленький натяк на щось, що може бути використано злочинцями, може спричинити дуже негативні наслідки. Це стосується не тільки особистого захисту. На жаль, на даний момент є приклади реального використання ворогом інформації із соціальних мереж. Так, бажання поділитися відзнятим вами відео може допомогти ворогові коригувати цілі обстрілу, розстановку техніки та військових. Уся ця інформація може бути передана за допомогою сучасних засобів зв'язку, а значить, безпосередньо пов'язана з кібернебезпекою в широкому сенсі цього слова.

Кібератаки з боку російських загарбників, спрямовані на знищення нашої країни, водночас наносять великої шкоди глобальним структурам, як, наприклад, це трапилося з польською залізницею, з метою завадити переміщенню вимушених переселенців з України. Злочинцям байдуже, що це лише жінки та діти, які втекли з рідного міста, втративши все, що мали. На цю проблему звернув увагу Євросоюз, який хоче посилити заходи кібер- та інформаційної безпеки у своїх установах. Про це заявив член ЄК з бюджету та адміністративних питань Йоганнес Хан, передає Інтерфакс-Україна. За його словами, у сучасному взаємопов'язаному середовищі якийсь єдиний інцидент у галузі кібербезпеки може завдати великої шкоди цілій організації. В ЄК вказують на те, що контекст пандемії COVID-19 та наростаючі геополітичні виклики підтвердили необхідність загального підходу в ЄС до кібер- та інформаційної безпеки. Тож Єврокомісія запропонувала відповідні єдині регламенти. Такої ж точки зору притримується і Міжнародна морська організація (ІМО), яка розробила та прийняла низку документів з кібербезпеки [1]. Ці документи зобов'язують адміністрацію забезпечити належний розгляд кіберризиків у системах управління безпекою.

Морська галузь потребує фахівців, які б могли на належному рівні контролювати ситуацію на всіх об'єктах, на які може бути спрямована кібератака ворога. Однією з вимог, пов'язаних із загостренням кібернебезпеки, зумовленої тотальною діджиталізацією у всіх сферах людської діяльності, є забезпечення підготовки морських спеціалістів основам кібербезпеки на морському судні. Як підкреслюють в ІМО, ефективне управління кіберризиками повинно впроваджувати культуру обізнаності про кіберінциденти на всіх рівнях і забезпечити цілісний та гнучкий режим управління кіберризиками [1].

Морську академію заслужено вважають флагманом морської освіти в Україні. Такому статусу передувала дуже кропітка та тривала робота керівництва, викладачів, співробітників академії, пов'язана зі становленням стратегії її формування, упровадженням компетентнісного підходу до підготовки фахівців морського профілю. Великою нагородою за це є визнання випускників академії на світовому ринку праці, їх конкурентоспроможність та затребуваність провідними крюїнговими компаніями. Але такий рівень треба постійно підтверджувати, оновлюючи та осучаснюючи як матеріально-технічну базу, так і програми підготовки моряків. Передусім це означає, що академія несе повну відповідальність за рівень знань, навичок та вмінь, які випускник отримав під час навчання, з урахуванням всіх новітніх тенденцій та вимог міжнародних крюїнгів.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми. Коротко зупинимося на фактах, які демонструють, як світ реагує на ці сьогоденні виклики. Комітет з безпеки на морі ІМО в червні 2017 року ухвалив Резолюцію MSC.428(98) – управління морськими кіберризиками в системах управління безпекою, як вже було зазначено вище [1].

На додаток до резолюції ІМО Національний інститут стандартів і технологій США (NIST) прийняв документ Cybersecurity Framework Version 1.1 (квітень 2018 р.) [2].

Міжнародна асоціація класифікаційних товариств (МАКО) випустила «Рекомендацію з кіберстійкості». Міжнародна палата судноплавства спільно з BIMCO (Балтійська та міжнародна морська рада) у 2019 році підготували Cyber Security Workbook

for On Board Ship Use (Навчальний посібник з кібербезпеки для використання на борту судна) [3].

З 1 січня 2021 р. морські адміністрації низки країн розпочали перевірки суден, що входять до їх портів, на предмет виконання рекомендацій щодо кібербезпеки. Резолюція IMO MSC.428(98) закликає адміністрації забезпечити облік кіберризиків у системах управління безпекою суден. На виконання резолюції, Регістру доручено з 01 січня 2021 року при продовженні чи отриманні нового Свідоцтва про відповідність здійснювати спостереження за виконанням зазначеної резолюції в компаніях [4].

Однак поки далеко не всі судновласники та оператори суден знають, що робити, і найголовніше, не розуміють, як це робити, тому досі немає чітких вказівок, як діяти в конкретних умовах. Є тільки загальні методики та технології боротьби з кібератаками, які повинні бути адаптовані до сучасних вимог.

Проблемам кібербезпеки на морському транспорті, методам аналізу та прогнозування кіберзлочинів присвячено достатньо статей, авторами яких, як правило, є досвідчені моряки, які на практиці зіткнулися з проблемою захисту та збереження інформації. Так, у роботі «Підвищення кібербезпеки транспорту в умовах деструктивного впливу на інформаційно-комунікаційні системи» автор Лахно В.А. [5] акцентував на тому, що для підвищення інформаційної безпеки транспортних систем необхідно проводити дослідження, які спрямовані на подальший розвиток методів та моделей розпізнавання кіберзагроз інформаційно-комунікаційному середовищу транспорту (ІКСТ) та прийняття рішень при нечітко заданій вхідній інформації. Автор також пропонує методи інтелектуального розпізнавання загроз на широкому класі задач кількісного і якісного розпізнавання кібернападів. Як зазначив капітан Еміль Мукчін у виданні «Морський репортер та інженерні новини» 28 серпня 2018 року [6], виконавча влада США заявила, що кіберзагроза є однієї з найсерйозніших проблем в галузі економіки та національної безпеки. Несанкціонований доступ кіберзлочинців призводить до нової області потенційних загроз, які виходять далеко за межі фізичного піратства. Це, безумовно, треба визнати та прийняти відповідні дії для надання допомоги власникам суден та операторам із обслуговування інформаційних суднових систем, що включає також розуміння методів аналізу та прогнозування кібератак. Багато уваги кібербезпеці на морському транспорті приділяли у своїх роботах Г. Вільський [7], С. Семенов [8] та багато інших. Аналіз їх робіт та статистичних даних із досліджуваної тематики не викликають сумнівів в її актуальності.

Виклад основного матеріалу. Кібербезпека на сьогодні є одним із пріоритетів у системі національної безпеки України та всього світу. Оператори суден та портових об’єктів використовують комп’ютери і кіберзалежні технології для навігації, зв’язку, проєктування, перевозки вантажів, баласту, забезпечення безпеки, екологічного контролю та багато інших цілей, тому частка кіберризиків у загальному обсязі вразливостей, з якими стикається морська транспортна система, постійно підвищується. Це, безумовно, свідчить про необхідність підготовки фахівців морської галузі в цьому напрямі. Тому в перелік дисциплін програми підготовки майбутніх моряків включено курс «Кібербезпека суднових комп’ютерних систем та мережах», метою якого є всебічний аналіз джерел загроз, цілей кібератак, методів прогнозування та захисту від можливих проявів небезпеки, а також підвищення безпеки моряків, навколишнього середовища, судна та вантажу. Проблемами кібербезпеки, зокрема на морському транспорті, займаються спеціалізовані компанії, оскільки ігнорування або недооцінювання цих проблем може призвести до втрати довіри потенційних клієнтів, фінансових втрат, а також таких наслідків, як фізичне пошкодження системи забезпечення роботи судна, втрата конфіденційної інформації, зокрема і комерційних або власних даних, та взагалі злочинної діяльності, встановлення програм-вимагачів та багато іншого.

Кібербезпека – це не тільки запобігання доступу зловмисників до систем та інформації, який може призвести до втрати контролю або конфіденційності. Це також

забезпечення захисту суднових систем від будь-яких втручань, підтримка належної роботи всіх модулів судна та берегових служб.

З метою кращої систематизації випадків кібератак у морській галузі ми пропонуємо використовувати деякий математичний апарат, який дозволить на підставі досліджень та математичних розрахунків визначити ймовірність наступного втручання зловмисників та заздалегідь вжити відповідні заходи запобігання цим негативним факторам. Така спроба є абсолютно новою, тобто ми знаходимось на першому етапі великої творчої роботи та сподіваємось на позитивні результати.

Спочатку треба визначити, який із модулів системи, що можуть бути атаковані зловмисниками, ми будемо досліджувати. Тому проведемо структуризацію кібернебезпеки за ступенем її наслідків, цілей кібератак, їх джерел. Важливим елементом у цьому процесі є людський фактор, оскільки більшість інцидентів ініціюється саме діями суднового персоналу. Але треба підкреслити, що налаштуванням систем управління судном, його інтернет-мереж, відстежуванням кібератак будь-якого напряму займаються спеціальні служби, висококваліфіковані спеціалісти, які мають доступ до всіх систем та відповідний дозвіл на дії, спрямовані на запобігання кібератакам або ліквідацію їх наслідків. Задачею вказаного курсу «Кібербезпека суднових комп'ютерних систем та мережах» є навчання майбутнього моряка елементарним правилам поведінки, пов'язаним із використанням інтернет-мереж на судні, роботою суднових комунікаційних систем, уразливих до зовнішніх кібератак, а також використання інтерфейсів систем керування вантажем, мостових систем, систем управління рухом судна.

Міжнародна морська організація до уразливих суднових систем відносить [1]**:**

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

Тобто, очевидним є факт великої уразливості судна перед спланованою атакою.

Перш за все, перерахуємо найбільш розповсюджені кібервразливості, які можна визначити як на борту вже наявних, так і деяких нових суден:

- застарілі та неоновлені операційні системи;
- застаріле або зовсім відсутнє антивірусне програмне забезпечення та захист від шкідливих програм;
- неефективне управління мережею та використання облікових записів та паролів адміністраторів за замовчуванням;
- суднові комп'ютерні мережі, які не мають засобів захисту границь та сегментації мереж;
- небезпека з боку критично важливого обладнання або системи, що підключені до берегових систем;
- відсутність або неповнота контролю доступу для третіх осіб, включаючи підрядників та постачальників послуг.

Але глобальна небезпека визначається векторами кібератак через морське середовище або саме у цьому середовищі.

Підкреслюємо, що вказана проблема належить до сфери діяльності фахівців морської транспортної системи (МТС), але керівництво кожного морського судна та його екіпаж повинні мати чітке уявлення про всі джерела та канали кіберзагроз.

До цієї сфери відносять:

- роботу з кораблями, яку забезпечують оперативні мережі управління суднами, вантажем, системи навігації та зв'язку, інші специфічні функції;

- забезпечення роботи зовнішніх та внутрішніх мереж, таких як сайти компаній, портали для клієнтів та партнерів, системи бронювання та інші комерційні операції;
- управління персоналом, графіками робіт та технічного обслуговування, правова підтримка та багато іншого;
- велике коло портових операцій, таких як управління суднами, що заходять в порт або виходять з порту; контроль роботи служб митниці, імміграційної, логістичної та інвентаризаційної служби;
- управління потоком суден у портах, каналах, системи визначення місця знаходження судна, навігації, часу та багато інших функцій, що забезпечують ефективний рух суден, вантажів, пасажирів.

Кожен із перерахованих пунктів є потенційно небезпечним із погляду ймовірності кібератак. Наприклад, якщо судно, що перевозить небезпечний вантаж, такий як нафта, скраплений газ, підпадає під контроль кіберзлочинців, наслідки можуть бути непоправні. Це означає, якщо керівництво судна або хтось із членів екіпажу помітить деякі невідповідності у роботі суднової системи або оточуючого трансферу суден, треба негайно інформувати про інцидент керівництво.

Нагадаємо, що кібербезпеку можна визначити як деяку суперпозицію концепцій безпеки, політики, принципів керівництва, управління ризиками, дії, навчання, технології, практики, тобто все те, що можна використовувати для захисту кіберсередовища існування системи з урахуванням зацікавленості організації та збереження її активів. Добре спланований та реалізований кіберзахист захищає не тільки власні системи організації, а і всі системи, з якими дані цієї організації вступають у контакт.

Мотивацію кібератаки на суднову систему можна схематично представити так (рис.1).

Рис.1. Мотивація кібератаки на суднову систему

Зупинимося на такому розповсюдженому явищі, що найбільш часто виникає, як неправомірне використання кіберпростору, тобто кіберзловживання, яке включає злочинну діяльність низького рівня, зокрема вандалізм, порушення роботи систем, пошкодження

вебсайтів та несанкціонований доступ до системи. Такі дії можуть здійснюватися як не дуже досвідченими спеціалістами, так і інсайдерами, тобто співробітниками, які мають право доступу до конфіденційної інформації даної організації, або незадовільним персоналом чи підрядниками; такі дослідники отримують доступ до системи без санкції керівника системи. Хоча й не завжди такі дії можуть нести будь-який злий намір, це може бути відсутність необхідних правових знань або звичайна цікавість, але згідно із законодавством такі дії вважаються кримінальною злочинністю.

Треба зазначити, що кібератаки, як правило, проводяться поетапно. Підготовка кібератаки потребує деякого часу, який визначається метою зловмисника, надійністю технічних засобів контролю кіберризиків, ступенем оновленості програмного забезпечення систем судна. Досвідчений, підготовлений фахівець, який не є професійним системним програмістом, тим не менш здатний виявити злочинні спроби, відстежити найбільш уразливі ключові позиції, та на підставі аналізу отриманої інформації, зробити висновки про деяку злочинну зацікавленість до судна та його систем забезпечення. Це дозволить заздалегідь передбачити більш серйозні кібератаки та зберегти час і витрати на оновлення роботи системи.

Отже, припустимо, що фахівець, який відповідає за виявлення кібератак, відстежує декілька позицій, на підставі аналізу яких можна стверджувати про спроби виконання кібератак на судно. По-перше, він може виявити наявність електронного листа від невідомого відправника. Такий лист може містити шкідливі файли або посилання на шкідливі вебсайти.

По-друге, досвідчений фахівець ніколи не буде використовувати судновий або власний комп'ютер для спілкування у соціальних мережах, технічних форумах тощо, але члени команди можуть нехтувати забороною та відкривати підозрілі сайти, тому обов'язково треба відстежити, які сайти відкривалися на борту судна з будь-якого пристрою.

По-третє, фахівець періодично проводить моніторинг фішингових сайтів, які змушують або заохочують персонал розкривати конфіденційну інформацію.

Далі – контроль зовнішніх носіїв, які можуть бути використані для оновлення програмного забезпечення бортової системи, а також обов'язкова перевірка фактичних даних, що поступають на судно або передаються з судна на берег.

Якщо зловмисник тим чи іншим способом отримує доступ до системи, він буде намагатися поетапно використати всю систему. Це призведе до спроби завантажити скрипти, експлойти, сканування мережі. Він може встановити постійні інструменти або реєстратор доступу до системи.

Перейдемо до математичного, точніше, ймовірнісного опису розглянутого процесу.

З погляду теорії випадкових процесів, кібератака (у будь-якій формі) є неперервною випадковою величиною, адже може відбуватися у будь-який момент. Але контроль з боку CySO (Cyber security officer, або офіцер кібербезпеки) здійснюється періодично за встановленим графіком, тобто дискретно, що свідчить про дискретність результатів спостереження. Звісно, за певний період накопичується статистична інформація про всі випадки кібератак, які вдалося виявити та відстежити. Аналіз цієї інформації допоможе прогнозувати появу наступної кібератаки та, за можливості, вжити заходи для її запобігання.

Ретельний аналіз джерел кібератак, які відбуваються найбільш часто, надає змогу припустити, що це випадковий процес, який підпорядковується законам, що в теорії ймовірностей (або, точніше, стохастичних процесів) називають марковськими процесами. За визначенням, марковський процес – це випадковий процес, для якого «майбутнє» залежить лише від «сьогодні» та не залежить від «вчора», тобто, випадковий процес називається марковським процесом (або процесом без післядії), якщо для кожного моменту часу **t** ймовірність будь-якого стану системи в майбутньому залежить тільки від її стану в теперішньому і не залежить від того, як система прийшла до цього стану.

Так звані ланцюги (цепі) Маркова – це міцні та широко відомі інструменти стохастичного моделювання, які можуть бути корисні експертам-аналітикам.

Отже, випадковою величиною *X* вважають величину, що визначається як результат випадкового явища. У нашому випадку результатом події може бути виявлення втручання у систему, втрата даних (повна або часткова), відмова системи або її елементів. Узагалі простір можливих результатів випадкової величини може бути дискретним або неперервним, у залежності від цього її поведінка відповідає тим чи тим законам розподілу, наприклад, нормальному (неперервна випадкова величина) або пуасоновському (дискретна випадкова величина).

Випадковий процес, який інакше називають стохастичним, визначають як набір випадкових величин, які можна представити у вигляді індексованого одномірного масиву *T*, елементами якого є моменти часу прояву події. Якщо цей масив є множиною натуральних чисел, тоді маємо випадковий процес із дискретним часом, інакше це буде випадковим процесом із неперервним часом.

Випадкові величини можуть бути залежними одна від одної в різні моменти часу або ні. Так, кібератаки можуть здійснювати абсолютно різні злочинці, як поодинці, так і організованими висококваліфікованими групами. Але не виключається і така ситуація, що дехто провів кібератаку, але не був виявлений та покараний за цей злочин, тому ця особа буде здійснювати такі атаки і надалі, причому кожен раз удосконалюючи методи атак та розгортаючи їх цілі.

У теорії випадкових процесів досліджені та мають широке застосування різні види моделей: гаусові, пуасонівські, авторегресія, ланцюги Маркова та багато інших. Вибір моделі обов'язково відповідає сутності досліджуваного явища, глибокого аналізу його характерних рис, статистичного аналізу числових результатів. Побудована модель дозволяє детальніше вивчити процес, виконати аналіз та прогнозування розвитку події і вчасно прийняти управлінське рішення щодо подальших конструктивних дій.

Ретельний аналіз проблем кібербезпеки на морських суднах дозволив припустити, що результати спостережень підпорядковуються властивостям марковських процесів. Це означає, що для визначення прогнозу стосовно поведінки процесу в майбутньому, достатньо інформації про сьогоднішній стан цього процесу, тобто дані про його поведінку в минулому ніяким чином не вплинуть на прогноз майбутнього. Можна також зазначити, що для визначення прогнозу та розуміння тенденції не треба мати ніякої інформації про минуле. Інакше це називається властивістю «відсутності пам'яті».

Отже, однорідні ланцюги Маркова з дискретним часом, або просто ланцюги Маркова**,** – це марковський процес з дискретним часом та дискретним простором станів. Інакше, ланцюг Маркова – це дискретна послідовність станів, кожен з яких отримуємо з дискретного простору станів, яке може бути скінченим або нескінченим, та задовольняє відповідним властивостям.

Математично визначимо ланцюг Маркова так:

$$X = \left(X_n\right) = \left(X_0, X_1, X_2 \ldots\right), \quad n \in N, \tag{1}$$

де в кожен момент часу процес приймає значення з дискретної множини *E,* такий, що $X_n \in E,\ \forall n \in N$.

Тоді послідовність станів можна визначити таким співвідношенням:

$$P\left(X_n = s_n, X_{n-1} = s_{n-1}, \ldots\right) = P(X_{n+1} = s_{n+1} | X_n = s_n) \tag{2}$$

Тобто такий математичний опис відображує основну суть процесу Маркова: розподіл імовірностей наступного стану системи залежить тільки від її поточного стану, але не залежить від минулого стану.

Звісно, на даному етапі досліджень вважаємо, що процес, який розглядається, є простий однорідний ланцюг Маркова з дискретним часом. У процесі майбутніх

досліджень будемо додавати додаткові характеристики системи, які більш повно її описують, та тим самим розширювати ймовірнісний опис моделі.

Отже, можна характеризувати динаміку ймовірності ланцюга Маркова. Для цього визначаємо тільки два аспекти: вихідний розподіл ймовірностей, тобто розподіл імовірностей у момент часу *n=0*, а саме, $P\left(X_0 = s\right) = q_0(\mathrm{s}), \quad \forall s \in E$, та матрицю перехідних ймовірностей, яка надає інформацію про можливі наступні стани, яку можна визначити як

$$P\left(X_{n+1} = s_{n+1} | X_n = s_n\right) = p\left(s_n, s_{n+1}\right) \quad \forall\left(s_{n+1}, s_n\right) \in E \times E \tag{3}$$

Такий опис дозволяє визначити повну динаміку всього процесу, який, по суті, є циклічним.

У нашому випадку ми будемо досліджувати чотири позиції можливих кібератак на систему, які можуть бути виявлені при моніторингу системи. Згідно з моделлю треба визначити ймовірність того, що система приймає такий стан: s_0, s_1, s_2, s_3. Тоді формальний опис стану буде мати вигляд:

$$P(X_0 = s_0,\ X_1 = s_1,\ X_2 = s_2,\ X_3 = s_3), \tag{4}$$

тобто результатом буде ймовірність виникнення кібернебезпеки системи на основі аналізу її попереднього стану.

З курсу теорії ймовірностей відомо, що формула повної ймовірності отримання стану s_0, s_1, s_2, s_3. враховує послідовно ймовірність виникнення наступного стану за умови того, що попередній стан був здійснений. Але припущення того, що процес можна визначити як ланцюг Маркова, значно спрощує математичні викладки, не порушуючи основні тенденції розвитку подій. Тоді ймовірнісна динаміка процесу має вигляд:

$$P\left(X_0 = s_0, X_1 = s_1, X_2 = s_2, X_3 = s_3\right) = P\left(X_0 = s_0\right)P\left(X_0 = s_0\right) \bullet \tag{5}$$

$$P\left(X_1 = s_1\right)P\left(X_2 = s_2\right) = q\left(s_0\right)p\left(s_0, s_1\right)p\left(s_1, s_2\right)p(s_2, s_3) \tag{6}$$

Таким чином можна отримати повну ймовірнісну динаміку процесу тільки на основі вихідного розподілу ймовірностей q_0 і матриці перехідної ймовірності p, тобто розподіл імовірності в момент часу $n+1$ відносно розподілу ймовірностей в момент часу n:

$$q_{n+1}\left(s_{n+1}\right) = P\left(X_{n+1} = s_{n+1}\right) = \sum P(X_n = s)P\left(X_n = s\right) = \sum q_n(s)p(s, s_{n+1}), \quad s \in E \tag{7}$$

Ланцюги Маркова підпорядковуються всім правилам дій із матричними формами. Якщо множину можливих кінцевих станів системи n представити як вектор-строку $E = \left\{e_1, e_2, ..., e_N\right\}$, тоді перехідні ймовірності можна представити матрицею $n \times n$, так що

$$\left(q_{0,i}\right) = q_0\left(e_i\right) = P(X_0 = e_i) \tag{8}$$

$$p_{i,j} = p\left(e_i, e_j\right) = P(X_{n+1} = e_j | X_n = e_i) \tag{9}$$

Інакше казати, при такому описі процесу для отримання взаємозв'язків між теперішнім та наступним станом системи можна користуватися звичайними матричними формами та відповідно звичайними діями над матрицями, наприклад, у нашому випадку має місце правило

$$q_{n+1} = q_n p, \quad q_{n+2} = q_{n+1}p = \left(q_n p\right)p = q_n p^2, \quad \ldots \quad q_{n+m} = q_n p^m \tag{10}$$

Очевидно, таке представлення, яке до того ж доволі просто довести математично, значно спрощує процес прогнозу ситуації, тобто кібератаки на суднову систему на підставі ймовірнісного аналізу даних на теперішній час. Це означає, що додаток вектору розподілу ймовірностей кібератак на систему обслуговування судна на деякому етапі часу на матрицю перехідних ймовірностей у якості результату надає розподіл ймовірних кібервтручань на наступному етапі часу.

Для наочності також можна користуватися формою зв'язку у вигляді нормованого орієнтованого графу, де кожен вузол визначає стан, а перехід між станами характеризує ймовірність настання події.

Отже, за нашим експериментом, на вахту заступив CySO, тобто офіцер кібербезпеки. Обмежимося наступними подіями *A, B, C, D*, де подія *A* – виявлення наявності електронного листа від невідомого відправника, та є велика підозра, що лист може містити шкідливі файли або посилання на шкідливі вебсайти; подія *B* – зафіксований факт відкриття відвідування деяким членом команди підозрілих сайтів із борту судна з будь-якого пристрою; подія *C* – виявлення несправжніх або шкідливих сайтів, які змушують або заохочують персонал розкривати конфіденційну інформацію; подія *D* – ситуація, коли ретельний контроль зовнішніх носіїв, які можуть бути використані для оновлення програмного забезпечення бортової системи, виявив невідповідність заданого об'єму інформації з об'ємом, зайнятим на носії, що може свідчити про приховані шкідливі файли.

Тоді простір станів можна представити вектором – рядком $E = \{A, B, C, D\}$. Припустимо, що поточна інформація про події, тобто вектор розподілу ймовірностей, має вигляд (на підставі попереднього аналізу): $q_0 = (0.3, 0.5, 0.1, 0.1)$, тобто з імовірністю 0.3 було виявлено електронного листа від невідомого відправника, з імовірністю 0.5 зафіксований факт відвідування підозрілих сайтів, з імовірністю 0.1 виявлено сайти-боти, та з імовірністю 0.1 виявлено деякі невідповідності отриманих даних або інформації на носіях.

Перехідна матриця надає інформацію про можливі події за вказаними напрямами контролю з боку CySO:

$$p = (0.3\ 0.2\ 0.3\ \ 0.2\ 0.4\ 0.3\ 0.0\ \ 0.3\ 0.1\ 0.5\ 0.4\ \ 0.0\ 0.2\ \ \ 0.1\ \ \ 0.3\ \ 0.4) \quad (11)$$

Нагадаємо, що кожен рядок матриці – це можливі ймовірності подій за дослідженими станами, сума значень за кожним рядком дорівнює одиниці, тобто ймовірності достовірної події. Тоді згідно з правилами дій із матричними формами, визначимо ймовірність кожного стану $E = \{A, B, C, D\}$ на наступний день:

$$q_1 = q_0 p = (0.3, 0.5, 0.1, 0.1)(0.3\ 0.2\ 0.3\ \ 0.2\ 0.4\ 0.3\ 0.0\ \ 0.3\ 0.1\ 0.5\ 0.4\ \ 0.0\ 0.2\ \ 0.1\ \ 0.3\ \ 0.4) = (0.32, 0.27, 0.16, 0.25), \quad (12)$$

тобто з імовірністю 0.32 можна очікувати виявлення наявності електронного листа від невідомого відправника, з імовірністю 0.27 можливо зафіксувати факт відкриття деяким членом команди відвідування підозрілих сайтів із борту судна з будь-якого пристрою, з імовірністю 0.16 виявити спроби заохочування персоналу розкривати конфіденційну інформацію з боку кіберзлочинців та з імовірністю 0.25 виявлення невпізнаної інформації на носіях.

Звернемо увагу на те, що сума значень рядку результату дорівнює 1, тобто дійсно ймовірнісні закони підпорядковуються законам матричної алгебри. Отриманий результат дозволяє прогнозувати випадки кібератак на наступний момент часу, заздалегідь провести відповідну роботу, розставивши пріоритети згідно з імовірностями появи різних видів загроз, та попередити можливі втручання з боку зловмисників.

Більш наочно матрицю переходу представимо графічно, що надає можливість візуально оцінювати кібернебезпеку (рис. 2).

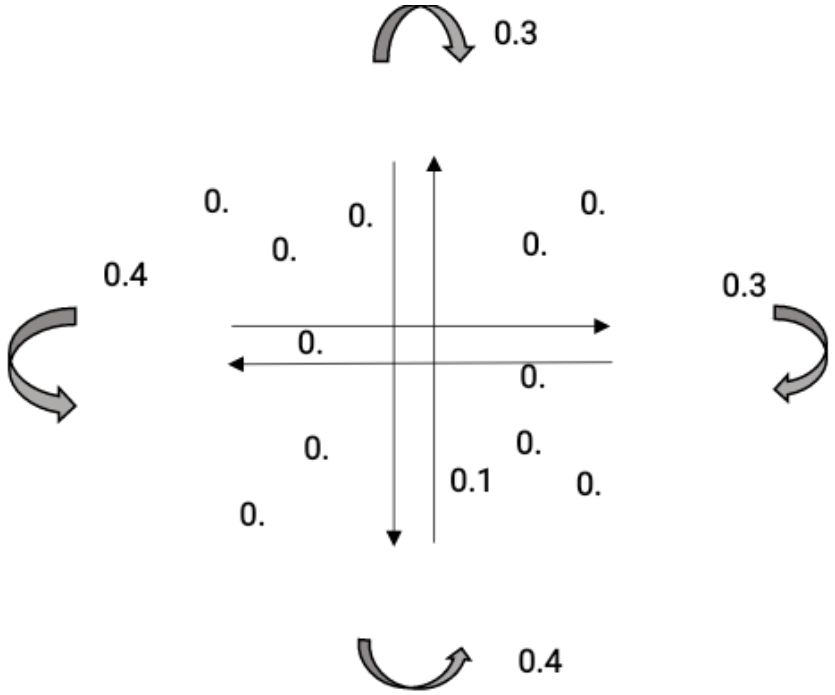


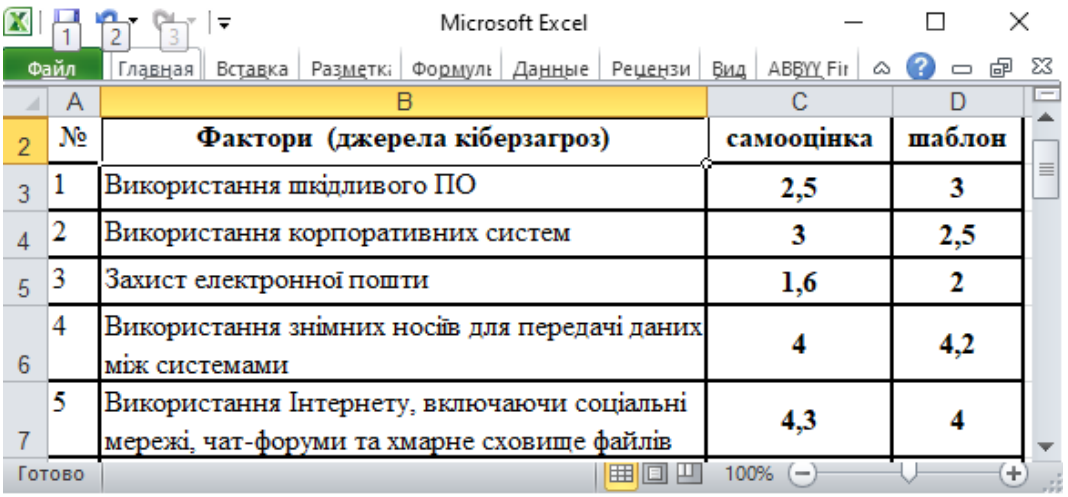
Рис.2. Графічне представлення матриці переходу

Використовуючи властивості ланцюгів Маркова, можна виявити цікаві та корисні результати дослідження процесу. Так, легко довести, що в нашому прикладі ланцюг аперіодичний, не розкладається та всі його стани позитивно зворотні. Це дозволяє розрахувати період повернення у поточний стан, тобто для будь-якого початкового стану процес отримує стаціонарний розподіл.

Результати дослідження. Розуміючи важливість забезпечення кібербезпеки морської галузі, провідні викладачі кафедри інноваційних технологій та технічних засобів судноводіння пропонували магістрам судноводіння теми кваліфікаційних робіт, пов'язані саме з забезпеченням кібербезпеки на морському транспорті. Магістри, особливо заочної форми навчання, професійні моряки, що вже мають достатній стаж роботи на морських суднах, свідомо обрали наукові теми, які на сьогодні є актуальними для тих, хто претендує на керівну посаду в цій галузі.

Але для виконавців дослідження участь чинних моряків-судноводіїв також є важливим фактором, оскільки це надає можливість аналізувати стан кіберзахищеності інформаційних систем судна безпосередньо на підставі досвіду судноводіїв, детально зрозуміти найбільш вразливі з погляду нанесення кібератак об'єкти на судні та якнайкраще підготувати здобувачів вищої освіти до роботи в офіцерському складі судна.

Треба обов'язково відзначити, що за планом підготовки дипломної роботи магістрант, знаходячись у рейсі, тобто на судні, повинен провести експеримент, результати якого або підтверджують наукову гіпотезу, або спростовують її. У даній роботі гіпотеза полягає в тому, що можна математично прогнозувати настання події, пов'язаної з кібератакою на суднову систему. Зокрема, декількома магістрантами, з дозволу керівного складу суден, було проведено анкетування членів екіпажу з питань їх усвідомленості можливих кібератак та методів протистояння таким явищам (рис. 3).



	A	B	C	D
2	№	**Фактори (джерела кіберзагроз)**	**самооцінка**	**шаблон**
3	1	Використання шкідливого ПО	**2,5**	**3**
4	2	Використання корпоративних систем	**3**	**2,5**
5	3	Захист електронної пошти	**1,6**	**2**
6	4	Використання знімних носіїв для передачі даних між системами	**4**	**4,2**
7	5	Використання Інтернету, включаючи соціальні мережі, чат-форуми та хмарне сховище файлів	**4,3**	**4**

Рис. 3. Фрагмент анкети з перевірки схильності членів екіпажу до зовнішніх кібератак

Результати анкетувань, виконаних на різних суднах з різними екіпажами, дозволяють систематизувати основні помилки у використанні інноваційних технологій із позиції їх кібербезпеки, та коригувати вплив людського фактору з боку екіпажу на підвищення кіберзагрози під час рейсу.

Висновки. Для розуміння реальної ситуації із забезпеченням безпеки суднових IT-систем необхідно створення стратегії кібербезпеки для навчання берегового і суднового персоналу. Запропоновані базові процедури управління безпекою суднової IT-системи дозволять визначити необхідні дії для реалізації такої стратегії. У перспективі актуальним питанням може бути дослідження стану судноплавних процесів під впливом нових кібератак для організації обліку сучасних кіберризиків у наявних системах управління безпекою судна.

Щоб протистояти кіберінцидентам компанії впроваджують такі елементи, як:

- визначення ролі та відповідальності ключового персоналу та керівництва як на березі, так і на борту суден;
- визначення системи, активів, даних та можливості, які в разі порушення можуть становити загрозу для роботи та безпеки судна;
- впровадження технічних, процедурних заходів для захисту від кіберінцидентів та забезпечення безперервності роботи судна;
- впровадження планів боротьби з кіберзагрозами (Cyber Security Plan) на основі прогнозування розвитку атак;
- проведення заходів з підготовки персоналу та швидкого реагування на кібератаки.

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

На наступному етапі заплановано розширити коло джерел кіберінцидентів, що дозволить як мінімум контролювати дії членів екіпажу, які невідповідально ставляться до такої важливої ділянки роботи на судні, як кібербезпека, та провести повне аналітичне дослідження можливості створення безпечного простору на борту судна.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Резолюція MSC.428(98) «Управління морськими кіберризиками в системах управління безпекою». (2018). URL: http://rise.odessa.ua/texts/MSC428_98.php3

2. Gary, C. Kessler & Steven. D. Shepard. (2020). *Maritime Cybersecurity: A Guide for Leaders and Managers*. USA: LVHW.
3. The Guidelines on Cyber Security Onboard Ships. (2022). V. 4. URL: https://shop.witherbys.com/cyber-security-workbook-for-on-board-ship-use-4th-edition-2023/.
4. A Primer on IMO Cyber Risk Management Guidelines. URL: https://www.american-club.com/files/files/A_Primer_on_IMO_Cyber_Risk_Management_Guidelines.pdf.
5. Lahno, V. (2014). Ensuring of information processes' reliability and security in critical application data processing systems. *MEST Journal*, 2(1). 71–79. doi: 10.12709/mest.02.02.01.07.
6. Мукчін, Еміль. (2015). Борьба с угрозами морской кибербезопасности. *Морський репортер та інженерні новини.* URL: http://magazines.marinelink.com/Magazines/MaritimeReporter.
7. Вільський, Г. Б. (2012). Информационные риски судовождения. *Наук. Вісник ХДМА*, 1(4). 17–26.
8. Семенов, С. (2018). Кибербезопасность на флоте. *Служба морской безопасности*, 1. 24–36.
9. Voloshinov, S., Kravtsova, L. & Zaytseva, T. (2021). Development of a methodology for a systematic approach to cyber security problems on board a ship. Maritime security of the Baltic-Black sea region: challenges and threats. Riga: Izdevnieciba «Baltija Publishing». 19–23.
10. Cyber Security for Ships. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf.
11. Hugh Boyes & Roy Isbell. *Cyber Security for Ships: Code of Practice*. (2017). London: Queen's Printer and Controller of Her Majesty's Stationery Office.
12. Сайт дистанційного навчання ХДМА. URL: http://www.mdl.kma.ks.ua/.

REFERENCES

1. Resolution MSC.428(98) "Maritime Cyber Risk Management in Security Management Systems". (2018). Retrieved from http://rise.odessa.ua/texts/MSC428_98.php3.
2. Gary, C. Kessler & Steven, D. Shepard. (2020). *Maritime Cybersecurity: A Guide for Leaders and Managers.* USA: LVHW.
3. The Guidelines on Cyber Security Onboard Ships. (2022). V. 4. Retrieved from https://shop.witherbys.com/cyber-security-workbook-for-on-board-ship-use-4th-edition-2023/.
4. A Primer on IMO Cyber Risk Management Guidelines. Retrieved from https://www.american-club.com/files/files/A_Primer_on_IMO_Cyber_Risk_Management_Guidelines.pdf.
5. Lahno, V. (2014). Ensuring of information processes' reliability and security in critical application data processing systems. *MEST Journal*, 2(1). 71–79. doi: 10.12709/mest.02.02.01.07.
6. Mukchin, Emil. (2015). *Combating threats to maritime cyber security. Marine Reporter and Engineering News*. Retrieved from http://magazines.marinelink.com/Magazines/MaritimeReporter.
7. Vilskyi, G.B. (2012). Information risks of driving. *Science Bulletin of the KhDMA*, 1(4). 17–26.
8. Semenov, S. (2018). Cyber security in the fleet. *Maritime Safety Service*, 1. 24–36.
9. Voloshinov, S., Kravtsova, L. & Zaytseva, T. (2021). Development of a methodology for a systematic approach to cyber security problems on board a ship. Maritime security of the Baltic-Black sea region: challenges and threats. Riga: Izdevnieciba «Baltija Publishing». 19-23.
10. Cyber Security for Ships. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf.

11. Hugh, Boyes & Roy, Isbell. *Cyber Security for Ships: Code of Practice.* (2017). London: Queen's Printer and Controller of Her Majesty's Stationery Office.
12. The KSMA's Distance Learning Site. Retrieved from http://www.mdl.kma.ks.ua/.

Lyudmyla Kravtsova, Tetyana Zaytseva, Natalia Kaminskaya
Kherson State Maritime Academy, Kherson, Ukraine

MARKOV PROCESSES IN RESEARCHING THE PROBABILITY OF CYBER ATTACKS ON MARINE VESSELS

Shipping is increasingly relying on digital solutions for everyday tasks. There are constant updates in the field of information technology, data availability, speed of processing and transfer of data with advanced possibilities to optimize work, save costs, increase security and sustainability of business. Along with the growing dependence on automation, the risk of external interference and disruption of key systems significantly increases; hackers can interfere with the operation of the ship or navigation systems, cut off all external communications of the ship or obtain confidential data.

Research on cyber security of maritime sector facilities is quite acute today and requires constant attention and improvement.

According to cyber security experts in the maritime sector, ground and space equipment systems are most vulnerable to cyberattacks; global positioning systems, electronic cartographic and navigational information systems; flight data registration systems; cargo operations systems; engine, machine and power management systems; access control systems; ship's public internet networks; administrative systems and networks; communication systems and port infrastructure.

Analyzing the above, it can be concluded that the more data is collected, the more accurate reports and response actions to cyber threats will be performed by the ship's security management system.

A careful analysis of the sources of cyberattacks, which occur most often, allows us to assume that this is a random process that obeys the laws that are called Markov processes in the theory of probabilities (or, more precisely, stochastic processes).

The subject of the study is the construction of a model based on the properties of Markov processes, which allows for a more detailed study of the process, analysis and forecasting of the development of a cyberincident in order to make a management decision regarding further constructive actions.

Key words: cyber security, cyber incident, Markov chains, Markov processes

Стаття надійшла до редакції 13.12.2022
The article was received 13 December 2022