ЗАСТОСУВАННЯ ТЕОРІЇ ВИПАДКОВИХ ПРОЦЕСІВ У ДОСЛІДЖЕННІ КІБЕРБЕЗПЕКИ НА МОРСЬКОМУ ТРАНСПОРТІ

Кравцова Л.В., Камінська Н.Г.
Херсонська державна морська академія, Україна

Вступ. Одним з вимог, пов'язаних із загостренням кібернебезпеки, обумовленої тотальною діджиталізацією у всіх сферах людської діяльності, є забезпечення підготовки морських спеціалістів основам кібербезпеки на морському судні. Так, Міжнародна морська організація (ІМО) розробила та прийняла ряд документів з кібербезпеки, які зобов'язують адміністрацію забезпечити належний розгляд кіберризиків в системах управління безпекою. Як підкреслюється в ІМО [1], ефективне управління кіберризиками повинно впроваджувати культуру обізнаності про кіберризики на всіх рівнях, та забезпечити цілісний та гнучкий режим управління кіберризиками. Херсонська державна морська академія заслужено вважається флагманом морської освіти в Україні. Такому статусу передувала дуже кропітка та тривала робота керівництва, викладачів, співробітників академії, пов'язана зі становленням стратегії її формування, впровадженням компетентнісного підходу до підготовки фахівців морського профілю. Великою нагородою за це є визнання випускників академії на світовому ринку праці, їх конкурентоспроможність та затребуваність ведучими крюїнговими компаніями. Але такий рівень треба постійно підтверджувати, оновлюючи та осучаснюючи як матеріально-технічну базу, так і програми підготовки моряків.

Актуальність досліджень. Проблемам кібернебезпеки на морському транспорті, методам аналізу та прогнозування кіберзлочинів присвячено достатньо статей, авторами яких, як правило, є досвідчені моряки, які на практиці зіткнулись з проблемою захисту та збереження інформації. 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. Несанкціонований доступ кіберзлочинців призводить до нової області потенційних загроз, які виходять далеко за границі фізичного піратства. Це безумовно треба признати та прийняти відповідні дії для надання допомоги власникам суден та операторам з 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 [2], С. Семенов та багато інших. Аналіз їх робіт та статистичних даних з досліджуваної тематики не викликають сумнівів в її актуальності.

Основна частина. 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, проектування, перевозки вантажів, баласту, забезпечення безпеки, екологічного контролю та багато інших цілей, тому частка кіберризиків у загальному обсязі уразливостей, з якими стикається морська транспортна система, постійно підвищується. Це безумовно свідчить про необхідність підготовки фахівців морської галузі в цьому напрямку. Тому в перелік дисциплін програми підготовки майбутніх моряків включений курс «Кібербезпека на морських суднах», метою якого є всебічний аналіз джерел кібернебезпеки, цілей кібератак, методів прогнозування та захисту від можливих проявів небезпеки, а також підвищення безпеки моряків, оточуючого середовища, судна та вантажу. Кібербезпека – це не тільки запобігання доступу зловмисників до систем та інформації, який може привести 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 в морській галузі ми пропонуємо використовувати деякий математичний апарат, який дозволить на підставі досліджень та математичних розрахунків визначити ймовірність наступного втручання зловмисників та заздалегідь прийняти відповідні міри запобігання цім негативним факторам. Така спроба є абсолютно новою, тобто ми знаходимось на першому етапі великої творчої роботи, та сподіваємось на гарні результати.

Зупинимося на такому розповсюдженому та найбільш часто виникаючому явищі як неправомірне використання кіберпростору, тобто кіберзловживання, яке включає злочинну діяльність низького рівню, у тому числі вандалізм, порушення роботи систем, пошкодження веб-сайтів та несанкціонований доступ до системи. Таки дії можуть здійснюватися як не дуже досвідченими спеціалістами, так і інсайдерами, тобто співробітниками, які мають право доступу до конфіденціальної інформації даної організації, або незадовільними чомусь персоналом чи підрядниками; таки 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 законодавства таки дії вважаються кримінальною злочинністю.

Отже, припустимо, що фахівець, який відповідає за виявлення кібератак на судні, 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 веб-сайти. 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, моніторинг несправжніх або шкідливих 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. В свою чергу, він може встановити постійні інструменти або регістратор доступу до системи.

Настав час перейти до математичного, точніше, ймовірнісного опису розглянутого процесу. З точки зору 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. Структурування цієї інформації допоможе прогнозувати появу наступної кібератаки та за можливостю прийняти заходи до 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.

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 таки атаки і надалі, причому кожен раз вдосконалюючи методи атак та розгортаючи їх цілі.

Ретельний аналіз проблем кібербезпеки на морських суднах дозволив припустити, що результати спостережень підпорядковуються властивостям Марківських процесів. Це означає, що для визначення прогнозу стосовно поведінки процесу у майбутньому, достатньо інформації про сьогоднішній стан цього процесу, тобто дані про його поведінку в минулому ніяким чином не вплинуть на прогноз майбутнього. Таким чином, результати спостережень за кібернападами можна інтерпретувати як марковський процес з дискретним часом та дискретним простором станів.

Математично визначимо ланцюг Маркова так:

$$X = (X_n) = (X_0, X_1, X_2 \ldots.), \quad n \in N,$$

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:

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

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

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

$$P(X_0 = s_0, X_1 = s_1, X_2 = s_2, X_3 = s_3),$$

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

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

$$\left(q_{0,i}\right) = q_0(e_i) = P(X_0 = e_i)$$
$$p_{i,j} = p\left(e_i, e_j\right) = P(X_{n+1} = e_j | X_n = e_i)$$

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; подія B – зафіксований факт відкриття деяким членом команди відвідування підозрілих сайтів з борту судна з будь-якого пристрою; подія C – виявлення несправжніх або шкідливих сайтів, які змушують або заохочують персонал розкривати конфіденційну інформацію; подія D – виявлення невідповідності заданого об'єму інформації з об'ємом зайнятим на носії, що може свідчати 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 ймовірністю 0,3 було виявлено

електронного листа від невідомого відправника, з ймовірністю 0,5 зафіксований факт відвідування підозрілих сайтів, з ймовірністю 0,1 виявлено сайти-боти, та з ймовірністю 0,1 виявлено деякі невідповідності отриманих даних або інформації на носіях. Перехідна матриця надає інформацію про можливі події за вказаними напрямками контролю з боку CySO:

$$p = \begin{pmatrix} 0.3 & 0.2 & 0.3 & 0.2 \\ 0.4 & 0.3 & 0.0 & 0.3 \\ 0.1 & 0.5 & 0.4 & 0.0 \\ 0.2 & 0.1 & 0.3 & 0.4 \end{pmatrix}$$

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 правил дій з матричними формами, визначимо ймовірність кожного стану $E = \{A, B, C, D\}$ на наступний день:

$$q_1 = q_0 p = (0.3, 0.5, 0.1, 0.1) \begin{pmatrix} 0.3 & 0.2 & 0.3 & 0.2 \\ 0.4 & 0.3 & 0.0 & 0.3 \\ 0.1 & 0.5 & 0.4 & 0.0 \\ 0.2 & 0.1 & 0.3 & 0.4 \end{pmatrix} = (0.32, 0.27, 0.16, 0.25) ,$$

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

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

Отримані результати дозволяють з великою достовірністю прогнозувати випадки кібератак кожній позиції та заздалегідь попередити їх або мінімізувати їх наслідки.

На наступному етапі планується розширити коло джерел кібернебезпек, що дозволить як мінімум контролювати дії членів екіпажу, які невідповідально відносяться до такої важливої ділянки роботи на судні як кібербезпека.

ЛІТЕРАТУРА

1. Международная конвенция о подготовке и дипломировании моряков и несении вахты. (2011). Лондон.: ИМО. «Эшфорд Пресс».

2. Информационная безопасность судовождения : монография / Г. Б. Вильский ; Одес. нац. мор. акад. - Одесса ; Николаев : Швець В. Д., 2014. - 334 с.