ДОСЛІДЖЕННЯ ЙМОВІРНОСТІ КІБЕР*ІНЦИДЕНТУ* В УМОВАХ РЕЙСУ

Кравцова Людмила Володимирівна
канд. техн. наук, доцент, доцент кафедри інноваційних технологій та технічних засобів судноводіння
Херсонська державна морська академія, Україна

Зайцева Тетяна Василівна
канд. пед. наук, доцент, доцент кафедри інноваційних технологій та технічних засобів судноводіння
Херсонська державна морська академія, Україна

Камінська Наталія Геннадіївна
викладач кафедри інноваційних технологій та технічних засобів судноводіння
Херсонська державна морська академія, Україна

Кібербезпека на сьогодні є одним із пріоритетів у системі національної безпеки України та 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 вразливостей, 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 суднових комп'ютерних систем та мереж», метою якого є всебічний аналіз джерел загроз, цілей кібератак, методів прогнозування та захисту від можливих проявів небезпеки, а також підвищення безпеки моряків, оточуючого середовища, судна та вантажу.

З метою кращої систематизації випадків кібератак в морській галузі ми пропонуємо використовувати математичний апарат, який дозволить на підставі досліджень та 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. Такі дії можуть здійснюватися як не дуже досвідченими спеціалістами, так і інсайдерами, тобто співробітниками, які мають право доступу до конфіденціальної інформації, 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 законодавства 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, ступеню оновленості програмного забезпечення систем судна [1]. 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.

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». 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.

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. Взагалі простір можливих результатів випадкової величини може бути дискретним або неперервним, в залежності від цього її поведінка відповідає тим чи іншим законам розподілу, наприклад, нормальному (неперервна випадкова величина) або пуасоновському (дискретна випадкова величина). Випадковий процес (стохастичний), визначають як набір випадкових величин, які можна представити у вигляді індексованого одномірного масиву T, елементами якого є моменти часу прояви події. Якщо цей масив є множиною натуральних чисел, тоді маємо випадковий процес з дискретним часом, інакше це буде випадковим процесом з неперервним часом.

Вибір моделі обов'язково відповідає сутності досліджуваного явища, глибокому аналізу його характерних рис, статистичному аналізу числових результатів. Побудована модель дозволяє детальніше вивчити процес, виконати аналіз та прогнозування розвитку події, та вчасно прийняти управлінське рішення щодо подальших конструктивних дій.

Математично визначимо ланцюг Маркова так:

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

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:

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

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.

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

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

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 такий стан: s_0, s_1, s_2, s_3. Тоді формальний опис стану буде мати наступний вигляд:

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

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:

$$P(X_0 = s_0, X_1 = s_1, X_2 = s_2, X_3 = s_3) = P(X_0 = s_0)P \quad (5)$$

$$P(X_2 = s_2|X_1 = s_1)P(X_3 = s_3|X_2 = s_2) = q(s_0)p(s_0, s_1)p(s_1, s_2)p(s_2, s_3) \quad (6)$$

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

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

Ланцюги Маркова підпорядковуються всім правилам дій з матричними формами. Якщо множину можливих кінцевих станів системи n представити як вектор-строку, тоді перехідні ймовірності можна представити матрицею:

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

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

При такому опису 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:

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

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 розуміння реальної ситуації із забезпеченням безпеки суднових ІТ-систем необхідно створення стратегії кібербезпеки для навчання берегового і суднового персоналу. Запропоновані базові процедури управління безпекою суднової ІТ-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.

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

Список використаних джерел:

1. Резолюція MSC.428(98) «Управління морськими кіберризиками в системах управління безпекою». (2018). Режим доступу: https://rise.odessa.ua/texts/MSC428_98.php3.
2. The Guidelines on Cyber Security Onboard Ships. (2022). V. 4. Режим доступу: https://shop.witherbys.com/cyber-security-workbook-for-on-board-ship-use-4th-edition-2023/.