III. DNA CRYPTOSYSTEM USING REPLACEMENT

A one-time substitution system uses a group of plain text binary messages and a table group that defines a random mapping to encrypted text. The input chain has length n and is divided into unencrypted words of fixed length. The table displays all possible lines of unencrypted text with a fixed length in the corresponding lines of the encrypted text, so that there is a unique inverse mapping.

Encryption occurs by replacing each word of the plaintext of the DNA with the corresponding encrypted DNA word. The mapping is realized using a long DNA notebook consisting of a number of segments, each of which points to a single word with plain text for encoding word combinations. A word with plain text acts as a primer binding, which then lengthens. This leads to the formation of a text pair of plaintext and ciphertext.

An ideal one-time library will contain a huge number of notebooks, and each of them will provide a completely unique, random display of unprotected words in encrypted words.

A repeating block consists of: one word of the sequence C_i, from a set of words corresponding to the code or codebook and the prefix P_i. Note that P_i includes a unique subsequence that prevents the attacks of frequency analysis by comparing several instances of the same plaintext message with different encrypted words. In addition, this prefix may optionally be used to encode the position of a word in a message [6].

Each pair of sequences i uniquely connects a text word with a ciphertext word.

The sequence of stoppers prohibits the expansion of the growing DNA chain beyond the bounds of the pairwise encrypted word. Using this theme, a library of unique codebook chains is created. Each separate chain from this codebook library specifies a specific unique set of pair words.

A one-time notebook consists of a DNA chain of length n, containing

$$d = \frac{n}{L_1+L_2+L_3}$$

copies of a repeating pattern: an encrypted word of length L_2, a word of open text of length $L_1$and a length stop sequence L_3.

Note that the length of the word grows logarithmically along the entire length of the notebook. Definitely

$$L_1 = c_1 \log_2 n;\ L_2 = c_1 \log_2 n \text{ and } L_3 = c_3,$$

where c_1, c_2, c_3 are fixed integer constants and $c_1, c_2, c_3 > 1$. Each repeater specifies a single match pair, and no word from the codebook or text word will be used more than once in any notebook.

Therefore, given the encrypted word C_i, we are sure that it displays only one word with plaintext P and vice versa. The stopper sequence acts as a "punctuation" between repeating links, so that the DNA polymerase can not continue copying the matrix filament (notepad). Stopper sequences consist of a sequence of identical nucleotides that act to stop the copying of the chain by DNA polymerase, given the lack of complementary nucleotide triphosphate in the tube. For example, the TTTT sequence will act as a stopping point if the polymerization mixture lacks its complementary base [7].

The experimental feasibility depends on the following factors: the size of the lexicon, which is the number of pairs of words of plaintext-encrypted text, the size of each word, the number of disposable DNA, the notebooks that can be created in the synthesis cycle, and the length of each message that must be encrypted. If the lexicon used consisted of English words, its size would be in the range of 10,000 to 25,000 word pairs. If, for experimental reasons, a smaller lexicon is required, then the words used can be a smaller set, such as ASCII characters, which leads to the size of the dictionary 128.

IV. CONCLUSIONS

In the future, such systems will potentially save a huge amount of data on microscopic media. Imagine a "flash drive" of 100 mm3, capable of storing about 100,000 PBB of data. However, meanwhile, the biggest obstacle to the introduction of such technologies is time. Decoding and reading the DNA molecule takes many hours. Therefore, this kind of storage is hardly suitable for the content of frequently used data, but it can turn our notion of long-term storage in data centers.

REFERENCES

[1] DNA Data cryptography [Electronic resource] // URL: https://www.slideshare.net/mayukhmaitra/dna-cryptography.

[2] G. Baumslag, B.Fine, and X.Xu, Cryptosystems Using Linear Groups Appl. Alg. in Engineering, Communication and Computing 17, 2006.

[3] A.G. Myasnikov, V.Shpilrain and A. Ushakov, Group-Based Cryptography, CRM Barcelona, 415, 2007.

[4] K.Ko, J.Lee, J.H. Cheon, J.W. Han, J.Kang, C.Park, New Public-Key Cryptosystem Using Braid Groups , Advances in Cryptology - CRYPTO 2000 Santa Barbara CA , Lecture Notes in Computer Science, Springer 1880, 2000, 166-183.

[5] V.Shpilrain and A. Ushakov, The Conjugacy Search Problem in Public Key Cryptography; Unnecessary and Insufficient Applicable Algebra in Engineering, Communication and computing, 17, 2006 285-289.

[6] Cerm´ak, J. “Digital generators of chaos,” Phys. Lett. 525, 1996, 151–160.

[7] K.Ko, J.Lee, J.H. Cheon, J.W. Han, J.Kang, C.Park, New Public-Key Cryptosystem Using Braid Groups , Advances in Cryptology - CRYPTO 2000 Santa Barbara CA , Lecture Notes in Computer Science, Springer 1880, 2000, 166-183.

Дослідження Системи Управління Інформаційною Безпекою Судна на Мережі Петрі

Дмитро Бабійчук
кафедра комп'ютерних технологій та інформаційної безпеки
Національний університет кораблебудування імені адмірала Макарова
Миколаїв, Україна
cool.babiychyk2011@gmail.com

Марина Турти
кафедра комп'ютерних технологій та інформаційної безпеки
Національний університет кораблебудування імені адмірала Макарова
Миколаїв, Україна
turtym@meta.ua

Investigation of the information security management system of the vessel on Petri's network

Dmytro Babiichuk
Department of Computer Technologies and Information Security
Admiral Makarov National University of Shipbuilding
Mykolaiv, Ukraine
cool.babiychyk2011@gmail.com

Marina Turty
Department of Computer Technologies and Information Security
Admiral Makarov National University of Shipbuilding
Mykolaiv, Ukraine
turtym@meta.ua

***Анотація* — Проведено огляд принципів функціонування системи управління інформаційної безпеки (СУІБ). Визначено особливості об'єкта інформаційної діяльності, системи захисту інформації і СУІБ які доцільно враховувати в імітаційній моделі, проаналізовано математичні основи методів побудови імітаційних моделей СУІБ, створена інформаційна модель системи управління інформаційної безпеки судна та відповідна їй імітаційна модель.**

Abstract — An overview of the principles of the functioning of the information security management system (ISMS) was conducted. The peculiarities of the object of information activity, the information security system and the ISMS are determined, which should be taken into account in the simulation model, the mathematical bases of the methods of constructing simulation models of the ISMS are analyzed, the information model of the information security system of the ship and the simulation model

Ключові слова — інформаційна безпека, система управління інформаційною безпекою, імітаційна модель, мережі Петрі, суб'єкт, умови.

Keywords — information security, information security management system, simulation model, petri net, subject, conditions.

I. Вступ

Аналіз аварійності світового судноплавства показує, що майже 80% аварійних випадків пов'язані з «людським фактором», з помилками, порушеннями норм і правил з боку осіб суднового екіпажу. Тому відповідно до «Міжнародного кодексу з управління безпечною експлуатацією суден і запобіганням забрудненню» кожна судноплавна компанія повинна розробити і ввести в дію систему управління безпекою, до якої як складова входить система управління інформаційною безпекою.

Система управління інформаційною безпекою (СУІБ) (англ. Information security management system, ISMS) – частина загальної системи управління, яка грунтується на підході, що враховує ризики інформаційної безпеки як бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

СУІБ є дуже великим комплексом з ускладненою логікою, тому при розробці доцільно застосовувати проектні рішення, що перевірені на математичних моделях.

II. Аналіз літературних джерел та постановка проблеми

На даний час задачі імітаційного моделювання систем захисту інформації і СУІБ розглядаються багатьма вітчизняними і зарубіжними науковцями [1-5].

Формалізований опис СУІБ ускладнюється тим, що у зв'язку з різною специфікою робіт технологічної схеми на кожному етапі використовується власний метод специфікації, причому всі методи базуються на моделях, що становлять собою той або інший вид машини послідовностей [3].

Здебільшого наукові роботи в цій галузі присвячені розв'язку конкретної задачі (моделюванню конкретної системи) в різноманітних програмних середовищах і на основі різних математичних моделей. Однак, на даний час задача вибору оптимальної математичної моделі для вирішення задачі дослідження процесу функціонування конкретної СУІБ з врахуванням особливостей об'єкта інформаційної діяльності, система захисту інформації і СУІБ відсутні.

III. Мета і задачі дослідження

Метою даної роботи є розробка імітаційної моделі функціонування системи управління інформаційною безпекою, з врахуванням особливостей об'єкта інформаційної діяльності, системи захисту інформації і системи управління інформаційною безпекою на мережі Петрі.

Для досягнення поставленої мети необхідно розв’язати наступні задачі: проаналізувати методики дослідження систем на мережах Петрі, розробити інформаційну модель СУІБ судна і визначити особливості її використання.

IV. Аналіз методики дослідження систем на мережах Петрі

Формально мережею називають трійку <P, T, F>, де P - непорожня множина елементів, що називаються місцями (позиціями); T - це непорожня множина елементів, що називаються переходами; F⊆ PxT ∪ TxP - відношення інциндентності.

При цьому виконуються умови:

1. P∩T=0: жоден елемент не може бути переходом і позицією одночасно.

2. (F≠∅)∧(∀x∈P∪T, ∃y∈P∪T: xFy ∨ yFx): відсутні елементи. які не інциндентні хоча б одному елементу протилежного типу.

3. $\forall p_1 p_2 \in P$: $({}^0p_1={}^0p_2)\wedge(p_1{}^0=p_2{}^0)\Rightarrow (p_1=p_2)$, де ${}^0p=\{y \mid yFp\}$, $p^0=\{y \mid pFy\}$: відсутні різні позиції, у яких співпадали б множини вхідних та вихідних переходів відповідно. Функціонування системи на моделі у вигляді мережі Петрі веде до появи процесу, що являє собою реалізацію послідовно в часі ряду подій. Самі процеси є не детермінованими, тобто система в однакових умовах функціонує по-різному, породжуючи множину процесів. Якщо подія реалізується, то вона породжує дію (реалізація події може не відбутись або відбутись кілька разів). Множина процесів, що породжуються системою, характеризує динаміку поведінки системи.

Прості мережі Петрі відображають статику, оскільки ніяк не фіксується поточний стан процесу. Для реєстрації динаміки додають дві функції на множині елементів мережі: $F \to N \setminus \{0\}$ - функція кратності дуг, яка ставить кожній дузі у відповідність натуральне число відмінне від нуля (- множина натуральних чисел) та $\mu^0 : P \to N$ - функція початкової розмітки, що ставить у відповідність кожній позиції натуральне число, яке відповідає початковій кількості фішок в позиції.

Маркована мережа Петрі (S, μ) – це сукупність структури мережі Петрі $S = < P, T, I, O >$ і маркування $\mu^k = \{\mu_1^k, \mu_2^k, \ldots, \mu_n^k\}$ $\mu_i \in N$, $k = 0, 1, 2, \ldots$ - номер кроку процесу моделювання.

Якщо для деякої події всі вхідні позиції мають маркери у кількості не меншій за кількість дуг з позиції в перехід, то подія стає активною (дозволеною). Дозволений (активний) перехід в маркованій мережі Петрі – це перехід, для якого виконується умова

$$\forall (p_i \in P): \mu_i = \mu(p_i) \geq \#(p_i, I(t_j)) \cdot$$

Активних переходів може бути декілька, але в простій маркованій мережі спрацьовує тільки один перехід, що обумовлює наявність невизначеності в мережах Петрі, оскільки порядок спрацьовування активних переходів не є детермінованим. Коли активна подія спрацьовує, то вона прибирає по одному маркеру з кожної вхідної позиції і додає один маркер у кожну вихідну позицію.

Мережа Петрі може бути застосована для моделювання процесів в системі перед її реалізацією з метою перевірки правильності функціонування проекту або для аналізу існуючої системи з метою її оптимізації. При цьому можна використати або формальні методи аналізу, або імітаційні моделі з вбудованими генераторами випадкових величин для вибору з активних переходів переходу для запуску. Ситуаціям ставиться у відповідність співвідношення змінних компонентів моделі (розмітки позицій) з постійними компонентами (навантаження дуг). Моделюються тільки такі дії, результати яких відображаються відніманням або додаванням констант (навантаження дуг) до змінних моделі (розмітка позицій).

Для оцінки процесів функціонування систем на ординарних мережах Петрі і мережах із кратними дугами визначають наявність таких основних властивостей: досяжність певної розмітки при заданій початковій розмітці, що відповідає досяжності певного узагальненого стану системи, якому відповідає певна сукупність позицій,

і певної послідовності подій в системі; покриття мережі; відсутність чи наявність безвихідних станів (англ. deadlock): t -тупикових маркувань і тупикових маркувань мережі; потенційна живучість переходів; живучість переходів; живість мережі; обмеженість позицій; обмеженість мережі; безпечність позицій; безпечність мережі; консервативність мережі; строгу консервативність мережі; повторюваність спрацьовування переходів; стаціонарна повторюваність спрацьовування переходів; стійкість мережі; оборотність мережі; наявність станів прийому; адекватність мережі як моделі реальній досліджуваній системі; еквівалентність двох мереж; включення однієї мережі в іншу.

Більш широкі можливості аналізу систем надають інші типи мереж Петрі:

а) мережі Петрі із змінною кратністю дуг, які дозволяють моделювати ситуації типу «посадки пасажирів», коли рух відбувається із змінною кількістю пасажирів з доставкою їх за різними маршрутами;

б) кольорові мережі Петрі, в яких фішки мають різні кольори, а умови можливості спрацьовування і запуску переходів визначаються для кожного виду фішок незалежно;

в) мережі подій, які призначені для імітаційного моделювання систем з дискретними подіями;

г) Е-мережі, які використовуються для алгоритмічних описів виробничих систем, які можуть бути структурованими у вигляді мережі подій;

д) мережі Петрі із затримками в часі використовуються для аналізу систем, в яких діють обмеження на ресурси, що використовуються системою (об'єм оперативної пам'яті, потужність, швидкість обслуговування тощо). Таким обмеженням в цих моделях відповідає умова обмеженості розмітки на певних інтервалах виконання мережі. Функціонування таких мереж моделюється за наступними правилами: фішки в позиціях можуть бути доступними або недоступними; перехід є активним, якщо у всіх його вхідних позиціях є фішки, і ці фішки доступні; переходи спрацьовують миттєво; після запуску переходу фішки пересуваються як у звичайних мережах Петрі, але в новій позиції деякий визначений час залишаються недоступними.

V. Методологія дослідження

Основними проблемами створення СУІБ судна та автоматизації управління інформаційною безпекою судна є необхідність забезпечувати захист інформації такої складної системи як судно на всіх етапах «життя» судна: конструювання (планування, будівництво, випробування), експлуатація, утилізація (перебудова); залежність інформаційної безпеки судна від багатьох критеріїв; необхідність забезпечувати працездатність СУІБ судна на етапі експлуатації при відсутності професіоналів в галузі безпеки інформації. На інформаційну безпеку судна впливають фактори, які можна розбити на наступні групи: незадовільні властивості судна; несприятливі зовнішні умови; відмови суднових технічних засобів та обладнання; вплив вантажів, функціональних систем і пристроїв цільового призначення; помилки в діях екіпажу, пасажирів, персоналу.

Для мережі Петрі з пронумерованими позиціями $p_i, i=\overline{1,n}$ та переходами $t_j, j=\overline{1,m}$ складаємо дві матриці B та D розмірності $n\times m$, рядки в яких відповідають позиціям, а стовпці – переходам. Якщо для позиції p_i наявна вихідна дуга кратності k, що є вхідною дугою переходу t_j, то $b_{ij}=k$. Якщо для позиції p_i наявна вхідна дуга кратності k, що є вихідною дугою переходу t_j, то $d_{ij}=k$. В інших випадках елементи матриць B та D дорівнюють нулю. Матриці $B=\{b_{ij}\}, D=\{d_{ij}\}, i=\overline{1,n},\ j=\overline{1,m}$ відображають структуру мережі. Якщо мережа не має петель, то її структура може задаватися матрицею $C=D-B$. Початковий стан системи визначається початковим маркуванням $\mu^0=\{\mu_i^0\}$.

Для кожної позиції p_i задається індикатор - вектор $u^{p_i}=\{u_l^{p_i}\}, l=\overline{1,n}$, а для кожного переходу t_j задається індикатор - вектор $u^{t_j}=\{u_g^{t_j}\}, g=\overline{1,m}$. Всі елементи цих векторів дорівнюють нулю, окрім елемента, що відповідає *i*-ій позиції / *j*-ому переходу. Тоді добуток $u^{p_i}\times B=p_i^-$ є вектором кратностей вихідних дуг позиції p_i до кожного з m переходів (відсутність відповідної дуги виражається нулем), а добуток $u^{p_i}\times D=p_i^+$ є вектором кратностей вхідних дуг в позицію p_i від кожного з m переходів. Аналогічно добуток $B\times u^{t_j}=t_j^-$ є вектором кратностей вихідних дуг з переходу t_j до кожної з n позицій, а добуток $D\times u^{t_j}=t_j^+$ є вектором кратностей вхідних дуг переходу t_j від кожної з n позиції.

Умову активності переходу $t_j\in T$ представити у вигляді $\mu_i^k\ge t_{j_i}^-=B\times u^{t_j}$. Після спрацьовування переходу маркування зміниться на нове: $\mu_i^{k+1}=\mu_i^k-t_j^-+t_j^+=$ $=\mu_i^k-B\times u^{t_j}+D\times u^{t_j}=\mu_i^k+C\times u^{t_j}=\mu_i^k+C\times u^{t_j}$.

Таким чином, рівнянням стану мережі є система: $\mu^{k+1}=\mu_i^k+C\times u^{t_j}$, μ_i^0, $\mu^k\ge B\times u^{t_j}$. Рівняння стану мережі є повним формальним представленням динаміки мережі, але є рекурентним і не розв'язується алгебраїчно, оскільки містить нерівності.

Фундаментальне рівняння мережі Петрі $\mu^k=\mu^0+C\times\sum_{t\in\sigma}u^t=\mu^0+C\times\sigma$, де вектор $\sigma=\sum_{t\in\sigma}u^t$ є