[17] Mahmood M. S., Al Dabagh N. B. Blockchain technology and internet of things: review, challenge and security concern. International Journal of Electrical and Computer Engineering (IJECE). 2023. Vol. 13, no. 1. P. 718. URL: https://doi.org/10.11591/ijece.v13i1.pp718-735.
[18] Soria J., Moya J., Mohazab A. Optimal mining in proof-of-work blockchain protocols. Finance Research Letters. 2022, p. 103610. URL: https: //doi.org/ 10.1016/j.frl.2022.103610.
[19] Василишин С., Опірський І. Розробка безпеки систем електронного урядування на основі блокчейну. Ukrainian Information Security Research Journal. 2022. Т. 24, № 2. С. 58-70. URL: https://doi.org/10.18372/2410-7840.24.16931.
[20] Енергоспоживання Ethereum / ethereum.org. ethereum.org. URL: https: // ethereum.org / uk / energy-consumption/.
[21] Опірський І., Василишин С. Перспективи військового застосування технології блокчейну. Ukrainian Scientific Journal of Information Security. 2022. Т. 28, № 2. С. 57-66. URL: https://doi.org/10.18372/2225-5036.28.16950.
[22] What is block size? Bitstamp Learn Center / Learn Center. Learn Center. URL: https://www.bitstamp.net/learn/crypto-101/what-is-block-size/.
[23] Gas and fees / ethereum.org. URL: https: // ethereum. org/en/developers/docs/gas/.
[24] What is IPFS? / IPFS Docs. IPFS Documentation / IPFS Docs. URL: https://docs.ipfs.tech/concepts/what-is-ipfs/#defining-ipfs.
[25] What is Delegated Proof of Stake (DPoS)? / Analytics Steps. Analytics Steps. A leading source of Technical & Financial content. URL: https: // analyticssteps.com/blogs/what-delegated-proof-stake-dpos.

DEVELOPMENT OF THE CONCEPT OF THE METHOD OF USING BLOCKCHAIN TECHNOLOGY FOR BUILDING A MESSAGE EXCHANGE SYSTEM

In modern realities, fast information exchange is an important aspect of human life. That is why information, that circulates in message exchange systems, requires to be secured. There are several possible ways to implement this, but the fast development of technologies forces us to search for alternate ways. One of the possible ways may become blockchain technology, which is not widely used in such a context, but found its popularity in the sphere of cryptocurrency and decentralized finances for its user privacy-preserving possibilities. The main idea of blockchain consists of that this is the decentralized distributed network that allows storing of information in an immutable way and provides access to it for all users of the network alongside prohibitions of the existence of users with exceptional privileges, which allows considering the blockchain technology as the base of a quality system for message exchange system which will provide integrity and availability of information. This article examines the features of blockchain technology and decentralized applications, analyzes the weaknesses and strengths and opportunities they can offer to such a system, and proposes a concept of the method of using blockchain technology to build a messaging system. In addition, the shortcomings of such a system are analyzed and methods to overcome them are proposed.
Keywords: blockchain, privacy, messaging, DPoS, decentralization, information security.

Побережник Василь Олегович, аспірант кафедри захисту інформації Національного університету «Львівська політехніка».
Vasyl Poberezhnyk, Postgraduate Student of the Department of Information Protection of the National University "Lviv Polytechnic".
E-mail: vasyl.poberezhnyk@gmail.com.
Orcid ID: 0000-0002-7523-2557.

Опірський Іван Романович, д.т.н., проф., професор кафедри захисту інформації Національного університету «Львівська політехніка».
Ivan Opirskyy, Doctor of Technical Sciences, Professor, Professor of the Department of Information Protection of the National University "Lviv Polytechnic".
E-mail: iopirsky@gmail.com.
Orcid ID: 0000-0002-8461-8996.

DOI: 10.18372/2410-7840.25.17674
УДК 004.681.3

КІЛЬКІСНА ОЦІНКА КІБЕРЗАХИЩЕНОСТІ ІНФОРМАЦІЇ

Володимир Хорошко, Юлія Хохлачова, Наталія Вишневська, Олександр Чобаль, Петро Венгерський

Створення, впровадження та експлуатація комп'ютерних систем привело до виникнення нових проблем в сфері безпеки інформації. Кіберзахист інформаційних технологій повинен за своїми характеристиками бути відповідним масштабам загроз і ризиків. Відхилення від цього правила приведе до значних збитків. Для кожної комп'ютерної системи (КС) має бути свій оптимальний рівень кіберзахищеності, який необхідно

постійно підтримувати. Нажаль до цього часу не існує адекватної методики оцінки кількісного рівня кіберзахищеності. Основними проблемами, які необхідно вирішити для розробки математичних основ кількісного аналізу кіберзахищеності та визначення його рівня є: визначення функціональної залежності між методами атаки на КС і методами КЗ; розробка критерію оцінки рівня КЗ, виходячи з усієї сукупності її кількісних характеристик; визначення методики обґрунтування пріоритетних заходів, спрямованих на забезпечення заданого рівня кіберзахищенності інформації. Запропонована методика дасть можливість для використання нових методів обробки інформації з метою оцінки її кіберзахищеності, які раніше не застосовувались.

***Ключові слова**: кіберзахищеність, комп'ютерна система, кількісний аналіз, критерії оцінки рівня КЗ, рівень кібезахищеності.*

ВСТУП

Масове створення, впровадження та експлуатація комп'ютерних систем привело до виникнення нових проблем в сфері безпеки інформації. І це закономірно.

В сучасних умовах все більше розповсюджується аксіома, що кіберзахист інформаційних технологій повинен за своїми характеристиками бути відповідним масштабам загроз і ризиків. Відхилення від цього правила приведе до значних збитків. Для кожної комп'ютерної системи (КС) має бути свій оптимальний рівень кіберзахищеності, який необхідно постійно підтримувати. Немає сумнівів, що кіберзахист критично важливий для КС і баз даних. Він повинен відповідати міжнародним, державним, корпоративним стандартам, методичним документам та рекомендаціям. Однак немає відповіді на саме важливе питання – наскільки рішення, яке пропонується або реалізується, дійсно відповідає та задовольняє усім вимогам та рекомендаціям.

Метою кіберзахисту (КЗ) інформації є запобігання витоку або порушенню цілісності інформації (несанкціонованому її отримання). Це мета може бути досягнута побудовою системи кіберзахисту, що є організаційною сукупністю методів і засобів забезпечення захисту.

Кіберзахист здійснюється поетапно [1]:

-1 етап – визначення та аналіз загроз;

-2 етап – розроблення системи кіберзахисту;

-3 етап – реалізація кіберзахисту інформації;

-4 етап – контроль функціонування та керування системи КЗ (СКЗ) інформації.

На другому етапі визначається рівень захисту інформації системою кількісних та якісних показників, які забезпечують виконання вимог технічного завдання на ефективність кіберзахищеності. Крім того, на четвертому етапі слід постійно здійснювати контроль ефективності КЗ. Ці заходи забезпечують ліцензування СКЗ, а саме дають змогу оцінити якість та надійність заходів КЗ інформації.

На сьогодні у науковому світі активізувалася робота по оцінки рівня КЗ із застосуванням математичних методів [2-5]. Проте існуючи методи, доступні з відкритого друку, далекі від досконалості.

Таким чином до цього часу не існує адекватної методики оцінки кількісного рівня кіберзахищеності.

Основними проблемами, які необхідно вирішити для розробки математичних основ кількісного аналізу кіберзахищеності та визначення його рівня є:

-визначення функціональної залежності між методами атаки на КС і методами КЗ;

-розробка критерію оцінки рівня КЗ, виходячи з усієї сукупності її кількісних характеристик;

-визначення методики обґрунтування пріоритетних заходів, спрямованих на забезпечення заданого рівня кіберзахищенності інформації.

Мета досліджень – створення методики кількісного аналізу та визначення рівня кіберзахищеності інформації на об'єкті.

Запропонована методика дасть можливість для використання нових методів обробки інформації з метою оцінки її кіберзахищеності, які раніше не застосовувались.

ОСНОВНА ЧАСТИНА

На сьогодні кількісна оцінка якості та надійності кіберзахищеності інформації на об'єкті, яка б могла урахувати велику кількість варіантів впливу на нього невідома. Тому розроблені вирази, які пройшли апробацію, для кількісної оцінки кіберзахищеності інформації, що циркулює на технічному об'єкті (ТО) з урахуванням імовірності методів несанкціонованого доступу (МНД), імовірності

методів кіберзахисту інформації (МКЗІ), завад і дискретних сигналів.

Згідно до цього загальна схема для вирішення поставленої задачі наведена на рисунку 1.

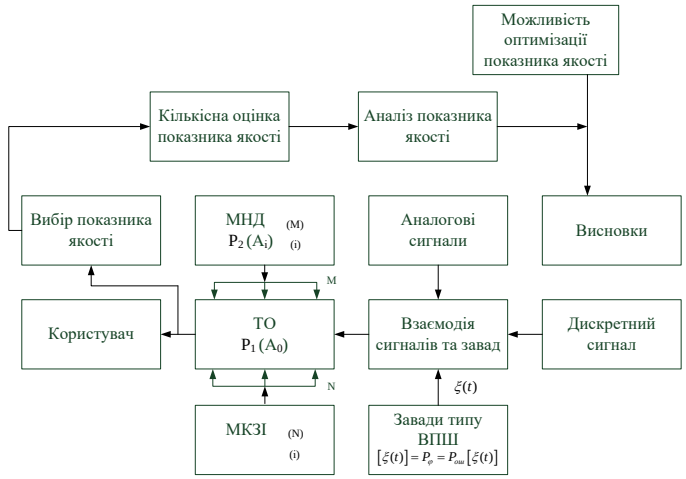

Рис. 1. Загальна схема вирішення поставленої задачі

При вирішенні задачі вводимо наступні обмеження та припущення:

- щодо вхідних умов:

-інформаційні сигнали – дискретні, які використовуються для передачі/прийому інформації;

-завади типу внутрішньоприйомний шум (ВПШ);

-алгоритм взаємодії інформаційних сигналів та завад – адитивний.

- щодо завад:

-методи несанкціонованого доступу до інформації у ТО $i=[0,m]$. При цьому: $P_1(A_0)$ – імовірність функціонування ТО, $P_1(A_0)=[1,0]$; $P_2(A_i)$ – апріорна імовірність доступу МНД до інформації у ТО, $0 \le P_2(A_i) \le 1$; $P_3(A_j)$ – апріорна імовірність МКЗІ у ТО $0 \le P_3(A_j) \le 1$; $P_4 = P_{пом}[\xi(t)]$ – імовірність помилки через $\xi(t)$, $[P_4[\xi(t)]]=1$; МКЗІ – методи кіберзахисту у ТО, $j=[0,N]$; ДП – джерело завад, з відомим законом розподілу $\xi_k(t)$ (математичні моделі завад, що діють у ТО, $i=[1,F]$.

В подальшому розгляді враховується завада $\xi_1(t)$, де $\xi_1(t)$ - ВПШ у ТО або інша завада з Гаусовим законом розподілу.

Випадкові події A_i – МНД та A_j – МКЗІ незалежні й несумісні.

Згідно вказаного, повну матрицю функціонування ТО, при наявності МКЗІ, МНД та $\xi_1(t)$ можна скласти, якщо враховувати, що $P_1[A_0]=[1,0]$, $P_2[A_i]=[1,0]$, $P_2[A_i]=[1,0]$, $P_3[A_j]=[1,0]$ та $P_4 = P_{пом}[\xi_1(t)]=[1]$.

У цьому випадку, $N=m^n=2^4=16$, де N - повна матриця ТО.

Тобто повна матриця станів функціонування ТО така як представлена в табл. 1.

Таблиця 1

Повна матриця станів функціонування ТО

$P_i\{i=1,4\}$ N	$P_1(A_0)$	$P_2(A_i)$ МНД	$P_3(A_j)$ МКЗІ	$P_4[\xi(t)]=$ $=P_{пом}[\xi(t)]$
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
10	1	0	1	0
11	1	0	1	1
12	1	1	0	0
13	1	1	0	1
14	1	1	1	0
15	1	1	1	1

Аналіз наявної матриці ТО перевірено за умови, що $P_1[A_0]=[1]$, $P_2[A_i]=[1,0]$, $P_2[A_i]=[1,0]$, $P_3[A_j]=[1,0]$ та $P_4 = P_{пом}[\xi_1(t)]=[1]$. З огляду на те що $P_1[A_0]=1$ та $P_4=1$, то повну матрицю ТО можна скоротити до вигляду табл.2.

З урахуванням подій A_i, A_j та значень табл. 2, імовірностей присутності завад типу ВПШ у ТО $P_{пом}[\xi(t)]=1$, матриця приймає вигляд табл.3.

Таблиця 2

Скорочена матриця станів функціонування ТО

$P_i\{i=1,4\}$ N	$P_1(A_0)$	$P_2(A_i)$ МНД	$P_3(A_j)$ МКЗІ	$P_4[\xi(t)]=$ $=P_{пом}[\xi(t)]$
1	1	1	1	1
2	1	1	0	1
3	1	0	1	1
4	1	0	0	1

Таблиця 3

Матриця станів функціонування ТО з урахуванням подій A_i, A_j

P_i N	$P_1(A_0)$	$P_2(A_i)$	$P_3(A_j)$	$P_4[\xi(t)]=$ $=P_{пом}[\xi(t)]$
11	1	1	0	1
14	1	0	1	1

Отже, розробка виразів кількісної оцінки кіберзахищеності інформації у користувача може бути отримана з урахуванням ситуації 11 та 14 (табл.3).

Обґрунтування вибору показника якості (кіберзахищеності інформації) ТО при його взаємодії з МКЗІ, МНД і завад типу ВПШ у користувача, за умов, що $P_1(A_0)=1$ та $P_4=P_{пом}[\xi(t)]=1$, означає що імовірність помилки на стороні користувача $P_4=P_{пом}[\xi(t)]=1$ завжди має місце.

Як показник кіберзахищеності інформації на стороні користувача можна розглядати:

-імовірність правильного прийому інформації користувачем (P);

-імовірність помилки при прийомі інформації користувачем (θ).

Таким чином, відповідно до теорії імовірності [6] та прийняття обмежень, як показника якості кіберзахищеності інформації на стороні об'єкта використаємо вираз:

$$P=1-\left\langle\left\{\left[\prod_{i=0}^{M}(1-P(A_i))\right]\left[\prod_{j=0}^{N}(1-P(A_j))\right]+P_{пом}[\xi(t)]\right\rangle, \quad (1)$$

$$\theta=I-P, \quad (2)$$

де $\prod_{i=0}^{M}(1-P(A_i))$ – добуток імовірностей пропуску з боку МКЗІ при впливі невідомих МНД. Це імовірність помилки з боку МКЗІ. $\prod_{j=0}^{N}(1-P(A_j))$ – добуток імовірностей доступу з боку МНД при недосконалості N та МКЗІ.

При цьому можливо:

-глушіння інформації;

-прослуховування з помилками через дію завади $\xi(t)$;

-містифікація інформації у ТО;

-порушення трафіка та ін.

Якщо проаналізувати співвідношення (1) та (2) з урахуванням припущень $P_2(A_i)=P_3(A_j)=0$; $P_1(A_0)=1$; $P_4[\xi(t)]=1$; $\theta=P_{пом}[\xi(t)]$, та якщо $P_2(A_i)=P_3(A_j)=\theta$; $P_1(A_0)=1$; $P[\xi(t)]=1$, $P=1-P_{пом}[\xi(t)]$ чи $P=1-\theta$, то можна зробити висновок, що кіберзахищеність інформації у користувача залежить від імовірності МКЗІ з імовірністю МНД завад типу ВПШ $[\xi(t)]$ з Гаусовим законом розподілу.

При цьому співвідношення (1) та (2) з позиції теорії імовірності правильні і можуть бути використані для кількісної оцінки кіберзахищеності інформації на стороні користувача з урахуванням імовірностей МКЗІ, імовірностей функціонування ТО та імовірностей помилки через заваду $[\xi(t)]$.

Окрім того, кількісна оцінка (математична) кіберзахищеності інформації на стороні користувача при наявності завад з Гаусовим законом розподілу миттєвих значень, враховуючи (1) та (2) можливо розглядати як завади типу ВПШ $[\xi(t)]$ миттєвих значень з параметрами a_{S1} та $\sigma_{З1}^2$ де: a_{S1} – математичне очікування завади типу ВПШ; $\sigma_{З1}^2$ – дисперсія завади типу ВПШ.

При цьому, якщо $[\xi(t)]$ – завада з $a_1\neq 0$ та $\sigma_1^2\neq 0$, то її миттєве значення описується як:

$$\omega(\xi_1)=\frac{1}{\sigma_{\xi_1}\sqrt{2\pi}}e^{\frac{\xi_1-a_1}{2\sigma_{\xi_1}}}, \quad (3)$$

або якщо заваду $[\xi(t)]$ розглядати в лінійному тракті $a_1 = 0$, тоді:

$$\omega(\xi_1) = \frac{1}{\sigma_{\xi_1}\sqrt{2\pi}} e^{\frac{\xi_1^2}{2\sigma_{\xi_1}}}. \qquad (4)$$

При кількісній оцінки кіберзахищеності інформації в ТО з урахуванням (3) та (4) необхідно врахувати початкові умови:

-розглядається цифрова система зв'язку (локальна обчислювальна мережа, мережа керування та інші), по яким передача інформації здійснюється за допомогою цифрових сигналів;

-цифрові сигнали передаються у стані кодових комбінацій, представлених у двійковій системі числення;

-елементарні цифрові сигнали у кодовій комбінації $S_1(t)$ та $S_2(t)$;

-перекручування та завмирання в каналі зв'язку відсутні;

-у каналі зв'язку де завада $[\xi(t)]$ типу ВПШ, миттєві значення якої описуються співвідношенням (3) або (4).

Функціонування в ТО здійснюється при передачі інформації кодовими комбінаціями, тобто при використанні кодових сигналів $S_1(t)$ та $S_2(t)$.

В подальшому вигляді за умов скорочення будемо використовувати наступне написання формул: $S_1(t) = S_1$ та $S_2(t) = S_2$. При цьому графік функціонування ТО буде мати такий вигляд, як на рис.2:

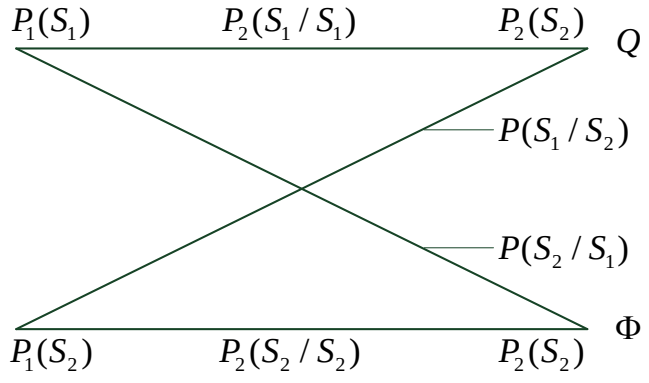

Рис. 2. графік функціонування ТО

де $P_1(S_1)$ – апріорна імовірність використання сигналу S_1 при передачі інформації користувачу; $P_1(S_2)$ – апріорна імовірність використання сигналу S_2 при передачі інформації користувачу; $P_2(S_1/S_1)$ – умовна імовірність правильного прийому сигналу S_1 користувачем, якщо був переданий сигнал S_1; $P_2(S_2/S_2)$ – умовна імовірність правильного прийому сигналу S_2 користувачем, якщо був переданий сигнал S_2; $P(S_1/S_2)$ – умовна імовірність помилки на стороні користувача, якщо був переданий сигнал S_1, а прийнятий – сигнал S_2 (Помилка); $P(S_2/S_1)$ – умовна імовірність помилки на стороні користувача, якщо був переданий сигнал S_2, а прийнятий – сигнал S_1 (Помилка); $\Phi[S_1, S_2]$ – повна імовірність правильного прийому інформації користувачем, при передачі сигналів S_1 та S_2; $Q[S_1, S_2]$ – повна імовірність помилкового прийому інформації користувачем, при передачі сигналів S_1 та S_2; $P_2(S_1)$ – повна імовірність прийому сигналу S_1 користувачем, за умови, що передавався сигнал S_1 і він через завади був прийнятий як сигнал S_1; $P_2(S_2)$ – повна імовірність прийому сигналу S_2 користувачем, за умови, що передавався сигнал S_2 і він через завади був прийнятий як сигнал S_2; A – рівень потенціалів при передачі сигналів S_1 та S_2; V – поріг «чутливості людини» чи поріг ухвалення рівня V технічною системою.

Далі розглянемо випадок, коли завада $[\xi_1(t)]$ є Гаусовою та центрованою, а сигнали S_1 та S_2 передаються з амплітудою $A_0 = [1, 0]$. У цьому випадку імовірність помилок і правильність прийому визначається при відсутності МНД характеристиками завад $[\xi_1(t)]$ і, зокрема СКО $[\xi_1(t)]$, V – порогом ухвалення рішення й амплітудою сигналів в кодовій комбінації A. При цьому треба врахувати,

що помилка типу $P(S_1/S_2)$ відбувається тоді коли $P\left[\xi_1(t) < V - A\right]$. Її значення визначається за формулою: $P(S_1/S_2) = \int_{-\infty}^{V-A} \omega(\xi_1) d\xi_1$. З обліком Гаусової завади при $a_1 = 0$: $P(S_1/S_2) = \int_{-\infty}^{V-A} \frac{1}{\sigma_{\xi_1}\sqrt{2\pi}} e^{\frac{-\xi^2}{\sigma_{\xi_1}^2}} d\xi$ та після заміни $x = \xi\sigma_{\xi_1}$, одержимо:

$$P(S_1/S_2) = \frac{1}{2\pi} \int_{-\infty}^{\frac{V-A}{\xi}} e^{\frac{-x^2}{dx}} = \Phi(\frac{V-A}{\sigma_{\xi_1}}), \qquad (5)$$

де $\Phi(\frac{V-A}{\sigma_{\xi_1}})$ – табульований інтеграл імовірностей.

Помилки типу $P(S_2/S_1)$ обчислюються за виразом:

$$P(S_2/S_1) = 1 - \Phi(\frac{M}{\sigma_{\xi_1}}) \qquad (6)$$

Значення інтегралу імовірності можна знайти в [7]. Розглянемо приклад використання співвідношень (5) та (6). Якщо припустити, що $A = 1|B|$; $V = 0,5A|B|$; $\sigma_{\xi_1} = 0,3|B|$, то відповідно до формули (5): $P(S_1/S_2) = 1 - \Phi(\frac{0,5-1}{0,3})$.

З огляду на те, що $\Phi(-\alpha) = 1 - \Phi(\alpha)$, то $P(S_1/S_2) = 1 - \Phi(1,66) = 1 - 0,95515 = 0,05$.

Це означає, що імовірність оцінки на стороні користувача при прийомі цифрової інформації дорівнює приблизно 0,05 [8, 9]. Якщо врахувати попередні припущення та (6), то $P(S_2/S_1) = 1 - \Phi(\frac{V}{\sigma_{\xi_1}})$, тоді маємо $P(S_2/S_1) = 1 - \Phi(\frac{0,5}{0,3}) = 1 - \Phi(1,66)$, $\Phi(1,66) = 0,95$, тоді $P(S_2/S_1) = 1 - 0,95 = 0,05$.

Згідно з цього можливо зробити висновок, якщо $P(S_1/S_2) = P(S_2/S_1)$, то канал зв'язку у мережі є симетричним. У цьому випадку $P(S_1/S_2) = P(S_2/S_1) = 0,5$.

ВИСНОВКИ

Згідно цього можна зробити наступні висновки: математичні співвідношення (1), (2), (3), (4), та (5) відповідність теорії імовірностей і їх можливо використовувати для кількісної оцінки кіберзахищеності в технічних каналах зв'язку на стороні користувача за умови загальної структури щодо вирішення задачі.

Можливо вирішення задачі структурної та параметричної оптимізації.

ЛІТЕРАТУРА

[1] ДСТУ 3396.0-96 Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення.

[2] Хорошко В.О. Методика кількісно-якісного аналізу та визначення рівня інформаційної безпеки / В.О. Хорошко, В.С. Чередниченко // Інформаційні технології та комп'ютерна інженерія №3(13), 2008. С. 49-57.

[3] Браіловський М.М. Аналіз кіберзахищеності інформаційних систем; Монографія / М.М. Браіловський, С.В. Зибін, А.А. Кобозєва та інші, К: ФОП Ямчинський О.В., 2021. 360 с.

[4] Козюра В.Д. Захист інформації в комп'ютерних системах / В.Д. Козюра, Ю.М. Ткач, М.Є. Шелест та інші, Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2020. 236 с.

[5] Пискун І.В. Кількісно-якісна оцінка та визначення рівня кібербезпеки інформаційних систем / І.В. Писарчук, Ю.М. Ткач, Ю.Є. Хохлачова та інші//Безпека інформації, Т.26, №3, 2020. С. 131-138.

[6] Сторський В.П. Математичний апарат інженера. Вид. 2-е. К: Техніка, 1985. 768 с.

[7] Зубарев В.П. Математичні методи оцінки та прогнозування технічних показників експлуатаційних властивостей радіоелектронних систем / В.В. Зубарев, О.П. Ковтуненко, Л.Г. Раснін, К.: НАУ, 2005. 184 с.

[8] Креденцер Б.П. Надійність систем з надлишковістю: методи, моделі оптимізації / Б.П. Креденцер, О.М. Буточков, А.І. Міночкін, Д.І. Могілевич, К.: Фенікс, 2013. 343 с.

[9] Атергауз С.М. та інші. Сравнение по вероятностным расчетам. М.: Сов.радіо, 1983. 326 с.

QUANTITATIVE ASSESSMENT OF CYBER PROTECTION OF INFORMATION

The creation, implementation and operation of computer systems has led to new problems in the field of information security. Cyber defense of information technology should be appropriate in its characteristics to the scale of threats

and risks. Deviation from this rule will lead to significant losses. Each computer system (CS) must have its own optimal level of cyber security, which must be constantly maintained. Unfortunately, there is still no adequate methodology for assessing the quantitative level of cyber security. The main problems that need to be solved to develop the mathematical foundations of quantitative analysis of cyber security and determine its level are: determining the functional relationship between the methods of attack on the CS and the methods of short circuit; development of a criterion for assessing the level of short-circuit, based on the totality of its quantitative characteristics; determining the methodology for substantiating priority measures aimed at ensuring a given level of cyber security of information. The proposed technique will enable the use of new methods of information processing in order to assess its cyber security, which were not previously used.

Keywords: cybersecurity, computer system, quantitative analysis, criteria for assessing the level of short-circuit, the level of cyber security.

Хорошко Володимир Олексійович, д.т.н., проф., професор кафедри безпеки інформаційних технологій Національного авіаційного університету.

Volodymyr Khoroshko, PhD., Professor, Professor, Department of Information Technology Security, National Aviation University.
E-mail: professor@ukr.net.
Orcid ID: 0000-0001-6213-7086.

Хохлачова Юлія Євгеніївна, к.т.н., доц., доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Yuliia Khokhlachova, Ph.D., Associate Professor, Department of Information Technology Security, National Aviation University.
E-mail: yuliiahohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

Вишневська Наталія Сергіївна, старший викладач кафедри безпеки інформаційних технологій Національного авіаційного університету.

Natalia Vishnevska, Senior Lecturer, Department of Information Technology Security, National Aviation University.
E-mail: viserj@ukr.net.
Orcid ID: 0000-0001-9036-6556.

Чобаль Олександр Ілліч, кандидат фізико-математичних наук, доцент кафедри твердотільної електроніки та інформаційної безпеки фізичного факультету УжНУ.

Oleksandr Chobal, Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Solid-State Electronics and Information Security of the Physical Faculty, UzhNU.
E-mail: oleksandr.chobal@uzhnu.edu.ua.
Orcid ID: 0000-0002-8042-8052.

Венгерський Петро Сергійович, д.т.н., проф., професор кафедри кібербезпеки Львівського національного університету імені Івана Франка.

Petro Venherskyi, Doctor of Technical Sciences, Prof., Professor of the Department of Cyber Security of Ivan Franko Lviv National University.
E-mail: petro.vengersky@gmail.com.
Orcid ID: 0000-0001-9808-7404.

DOI: 10.18372/2410-7840.25.17675
УДК 004.054

ДО ПИТАННЯ БЕЗПЕЧНОЇ БАГАТОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ У ВЕБ-ЗАСТОСУНКАХ

Валерій Дудикевич, Галина Микитин, Володимир Насилевський, Володимир Фігурняк

Розглянуто основні сегменти інфраструктури "розумного міста" із застосуванням автентифікації за вектором безпеки технологій Індустрії 4.0. Проаналізовано підходи до безпечної автентифікації, зокрема у ВЕБ-застосунках. Проведено порівняння способів автентифікації у ВЕБ-застосунках за вимогами та рівнем захищеності даних. Проаналізовано загрози автентифікації, механізми та технології захисту і, на цій основі, створено системну модель безпечної багатофакторної автентифікації у ВЕБ-застосунку на основі концепції "об'єкт – загроза – захист" за структурою "ВЕБ-сторінка – ВЕБ-сервер – база даних". Розроблено алгоритмічно-програмну реалізацію системи безпечної багатофакторної автентифікації у ВЕБ-застосунку на основі застосування криптографічної хеш-функції SHA-1 та симетричного алгоритму шифрування повідомлень AES засобами мови програмування JavaScript. Наведено практичну реалізацію покрокового алгоритму багатофакторної автентифікації у ВЕБ-застосунках за факторами – логін та пароль, відбиток пальця, смартфон.

Ключові слова: *багатофакторна автентифікація, безпека, ВЕБ-застосунок, системна модель, хеш-функція, алгоритм шифрування повідомлень.*