blog.zeppelin.solutions/the-hitchhikers-guide-to-smartcontracts-in-ethereum-848f08001f05.

[14] Asia, O. (2018, January 29). Tracing back stolen cryptocurrency (XEM) from Japan's Coincheck. Режим доступу: https://www.forbes.com/sites/outofasia/2018/01/29/tracing-back-stolen-cryptocurrency-xem-from-japans-coincheck/.

[15] Ateniese, G., Faonio, A., Magri, B., & de Medeiros, B. (2014). Certified bitcoins. In I. Boureanu, P. Owesarski, & S. Vaudenay (Eds.), Applied cryptography and network security (Vol. 8479, pp. 80-96). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-07536-5_6.

SECURITY DEVELOPMENT OF ELECTRONIC GOVERNMENT SYSTEMS BASED ON BLOCKCHAIN

In the realities of protecting information in cyberspace, there are many means and approaches to the security of the government, business, and private sectors, one of which is likely to be systems built on the basis of blockchain. Every year, the amount of information that passes through the World Wide Web and the number of users grows exponentially, together with these factors, the number of technologies that ensure the security and privacy of user data in the network grows. At the current rate, technologies can age faster than they have time to occupy their niche in the market, and therefore their support ceases to be relevant, which allows attackers to break through protection or find new vulnerabilities in already existing systems. Blockchain is one of the technologies that are not so often used in government and business systems as a technology around which you can build your network protection. Very often, this is due to the fact that such institutions need individual approaches to solve their problems and needs. The development of their system on the basis of blockchain requires a lot of financial investment and specialists, which are not so many on the market at the moment. However, in the future, when the blockchain becomes more accessible not only for operating cryptocurrencies and for their use in internal systems, it will be able to offer a new standard in the protection of information systems and become one of the most powerful on the market due to its strong protection system. This article proposes a security system built using this technology for government, private, and business sectors.

Keywords: blockchain, information protection, privacy, communication nodes, data transfer.

Василишин Святослав Ігорович аспірант кафедри захисту інформації Національного університету «Львівська політехніка».

Vasylyshyn Sviatoslav, Postgraduate Student of the Department of Information Protection of the National University "Lviv Polytechnic".
Email: swat2244@gmail.com.
Orcid ID: 0000-0003-1944-2979.

Опірський Іван Романович, д.т.н., проф., професор кафедри захисту інформації Національного університету «Львівська політехніка».

Opirskyy Ivan, Doctor of Technical Sciences, Professor, Professor of the Department of Information Protection of the National University "Lviv Polytechnic"
E-mail: ivan.r.opirskyi@lpnu.ua.
Orcid ID: 0000-0002-8461-8996.

DOI: 10.18372/2410-7840.24.16932
УДК 004.681

МОДЕЛІ ОЦІНЮВАННЯ ЗАЛИШКОВОГО РИЗИКУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Володимир Хорошко, Юлія Хохлачова, Володимир Погорелов, Ахмад Аясрах

Для забезпечення базових характеристик безпеки ресурсів інформаційних систем за рахунок унеможливлення доступу неавторизованих користувачів до інформації та розкриття її змісту необхідно застосовувати засоби (апаратурні чи програмні) адміністрування доступу, управління фізичним доступом, захисту від витоків інформації технічними каналами, засоби криптографічного перетворення (для шифрування та дешифрування закритої інформації, а також засоби генерації та розповсюдження ключів), засоби охоронної сигналізації та організаційного обмеження доступом тощо. В роботі розроблено моделі процесу взаємодії засобів реалізації кібератак з засобами кіберзахисту для забезпечення базових характеристик безпеки ресурсів інформаційних систем в яких, за рахунок величини залишкового ризику та варіювання режимами функціонування або несанкціонованого

використання засобів зберігання носіїв інформації і порушення таким чином її цілісності, доступності та конфіденційності, дозволяє забезпечити кількісно-якісне оцінювання стану кіберзахищеності. Також представлена модель процесу взаємодії засобів захисту, в якій за рахунок використання моделі процесу взаємодії засобів реалізації кібератак з засобами кберзахисту і декомпозиції базових характеристик безпеки ресурсів інформаційних систем та урахування відповідних показників базових характеристик безпеки в процесі кіберзахисту ресурсів інформаційних систем дозволяє підвищити точність динамічного оцінювання залежності ефективності від інтенсивності впливів кібератак. Запропоні моделі кіберзахисту дають можливість блокувати кібератаки в інформаційних системах ще до того, як вони почали діяти на систему. Таким чином кіберзахист може більш ефективно використовувати свої ресурси, що не потребує реагування на кожне попередження, оскільки можуть бути і хибні попередження. Розглянуті моделі дозволяють, запропонувати вирази для оцінки залишкового ризику при захисті ресурсів базових характеристик безпеки у вигляді ймовірностей їх порушення та сформувати умови переходу захищеного ресурсу в режим штучної відмови.

Ключові слова: *кіберзахищеність, інформаційні системи, кібератаки, захищеність ресурсів, забезпечення кіберзахищеності.*

ВСТУП

Існуючі засоби забезпечення окремих функціональних властивостей захищеності, зокрема в частині контролю, контролю та поновленню цілісності, цифрового підпису інформаційних ресурсів вузлів різних рівнів та в засобах телекомунікаційної мережі не завжди можуть забезпечити потрібну ефективність реалізації деяких з функціональних властивостей захищених ресурсів.

Однією з причин такого стану є недосконалість відомих методів оцінки та забезпечення таких функціональних властивостей. Тому основною задачею є розроблення методики оцінки впливу способів організації обміну на характеристики захищеності інформації в ІС.

ОСНОВНА ЧАСТИНА

Порушення конфіденційності є можливим шляхом ознайомлення (читання з розумінням змісту) з інформаційними об'єктами в разі подолання порушником засобів та механізмів обмеження доступу (організаційного, фізичного, адміністрування, засобів охоронної сигналізації тощо), засобів захисту телекомунікаційної мережі та використання витоків інформації технічними каналами.

Тобто, конфіденційність ресурсів можна забезпечувати шляхом:

1) унеможливлення будь-якого несанкціонованого доступу до інформаційних ресурсів ІС;

2) представлення інформації при її циркулюванні в ІС у вигляді, який унеможливлює розкриття її змісту.

Для побудови системи забезпечення конфіденційності з такими можливостями та оцінки її характеристик (у вигляді залишкового ризику – ймовірності подолання неавторизованим користувачем засобів захисту) в роботі пропонується модель взаємодії засобів реалізації атак з засобами протидії цим кіберзагрозам – засобами забезпечення конфіденційності інформації, яка представлена на рис. 1. При цьому подію, пов'язану з порушенням конфіденційності слід розглядати як складну та таку, що складається з подій:

- несанкціонованого отримання користувачем інформації тим чи іншим чином з метою ознайомлення з нею чи будь-якого подальшого використання;
- розкриття змісту інформації з обмеженим доступом (ІзОД) після отримання її тим чи іншим шляхом.

Останнє слід трактувати як можливість подолання порушником відповідних засобів криптозахисту. При цьому будемо враховувати, що подолання неавторизованим користувачем системи захисту для різних інформаційних об'єктів ІС залежить від того, звідкіля (в межах чи поза межами контролюємої зони, безпосередньо чи дистанційно) здійснюється атака і в якому стані (оброблення, зберігання чи передавання) знаходиться даний ресурс.Як витікає з моделі, несанкціоноване отримання користувачем інформації тим чи іншим чином при безпосередньому впливі є можливим при умові подолання неавторизованим користувачем системи захисту, до складу якої входять засоби:

1. Організаційного обмеження доступу (кон-

троль доступу та управління доступом до приміщень організаційними засобами, наприклад реалізацією перепускного режиму до будівель чи окремих приміщень та таке інше).

2. Такі дії слід очікувати, скоріше за все, від «терплячих неавторизованих сторін» – авторизованих користувачів, які мають атрибути легального доступу до певних приміщень ІС (наприклад, перепустки чи їх еквіваленти), або від «рішучих неавторизованих сторін», які вимушено використовують підроблені атрибути легального доступу до приміщень ІС.

3. Охоронної сигналізації (тобто шляхом «обходу» засобів організаційного обмеження доступом. Такі дії слід очікувати, скоріше за все, від «рішучих неавторизованих сторін», які мають на меті будь-що порушити ту чи іншу властивість захищеної інформації.

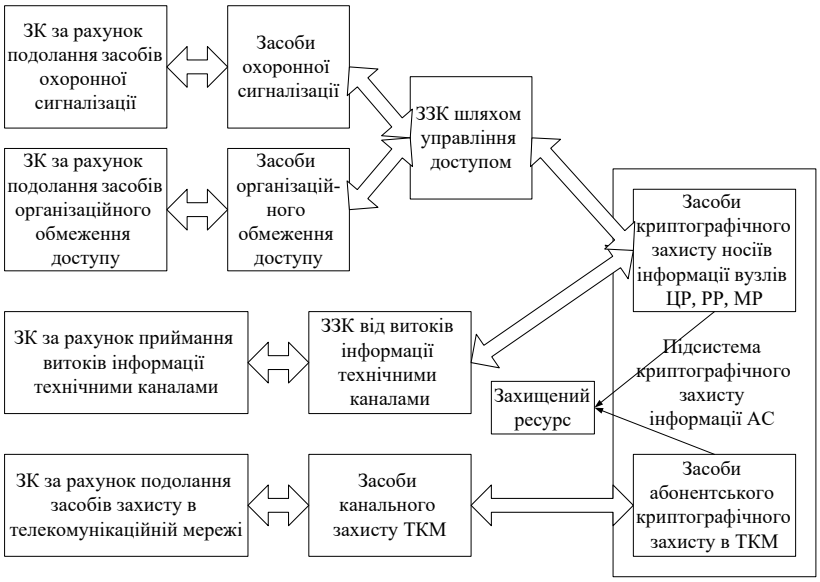

Рис. 1. Модель процесу взаємодії засобів реалізації атак із засобами забезпечення конфіденційності в інформаційних системах

3. Управління доступу, включаючи засоби управління фізичним доступом (дозвіл чи блокування доступу до приміщень, терміналів, системних блоків, клавіатури та інших фізичних засобів) та адміністрування доступу (адміністрування суб'єктів, об'єктів, побудови і реалізації моделі захищеної системи, розмежування доступу тощо).

Такі дії слід очікувати, скоріше за все, від «терплячих неавторизованих сторін», які порушують політику безпеки даної послуги навмисно, але без рішучих дій, маскуючись, шляхом підбору атрибутів доступу інших користувачів з метою прихованого подолання засобів управління (адміністрування) доступом до інформації, або від «випадкових порушників» –авторизованих користувачів, які порушують конфіденційність не навмисно, а помилково – шляхом випадкового подолання засобів управління (адміністрування) доступом до об'єкту захисту, виконання непередбачених дій відносно цього інформаційного об'єкту тощо.

Тоді ймовірність несанкціонованого отримання користувачем інформації при безпосередньому впливі P_1 можна визначити з виразу:

$$P_1 = P_{\text{уд}}\left[1 - \left(1 - P_{оод}\right)\left(1 - P_{ос}\right)\right], \qquad (1)$$

де:

$P_{\text{уд}}$ – ймовірність подолання засобів управління доступом;

$P_{оод}$ – ймовірність подолання засобів організаційного обмеження доступу;

$P_{ос}$ – ймовірність подолання засобів охоронної сигналізації.

В свою чергу, ймовірність $P_{\text{уд}}$ подолання засобів управління доступом є також ймовірністю складної події, яка полягає в подоланні порушником як засобів управління фізичним доступом, так і засобів адміністрування доступом з використанням механізмів базового та прикладного програмного забезпечення. Якщо позначити ці ймовірності через $P_{\text{уфд}}$ і $P_{\text{ад}}$ відповідно, то:

$$P_{\text{уд}}=P_{\text{уфд}} \times P_{\text{ад}}. \quad (2)$$

Тоді зрозуміло,

$$P_1 = P_{\text{уфд}} \times P_{\text{ад}}\left[1-\left(1-P_{\text{оод}}\right)\left(1-P_{oc}\right)\right]. \quad (3)$$

Окрім того, несанкціоноване отримання користувачем інформації є можливим і через засоби віддаленого доступу до інформаційних об'єктів (перша з можливостей дистанційного впливу), використовуючи витоки інформації технічними каналами при умові подолання неавторизованим користувачем відповідних засобів захисту. Нехай ймовірність подолання засобів захисту від витоків інформації технічними каналами дорівнює $P_{\text{зві}}$.

Після отримання ІзОД тим чи іншим шляхом порушнику необхідно здійснити розкриття її змісту.

Подія, яка полягає в тому, що порушник може розкрити ІзОД (при умові подолання системи захисту даного інформаційного об'єкту) є також складною і складається з події: першої – порушник знає мову, якою інформація представляється, другої – порушник знає і може застосувати програмні засоби або апаратуру для криптографічного перетворення (для дешифрування закритої інформації) та третьої – має необхідні ключі (ключові набори) для такого перетворення з ймовірностями цих подій $P_{\text{зм}}$, $P_{\text{зкп}}$, $P_{\text{кн}}$ відповідно.

При цьому $P_{\text{кзі}}$ – ймовірність подолання неавторизованим користувачем засобів криптозахисту (можливість розкрити зміст ІзОД) інформації можна визначити з виразу:

$$P_{\text{кзі}} = P_{\text{зм}} \times P_{\text{зкп}} \times P_{\text{кн}}. \quad (4)$$

Тоді вираз для розрахунку ймовірності P_2 порушення конфіденційності інформації з подоланням розглянутих засобів захисту можна записати у вигляді

$$P_2 = P_{\text{кзі}}[1-(1-P_1)(1-P_{\text{зві}})]. \quad (5)$$

Друга з можливостей дистанційного порушення конфіденційності інформації може бути реалізованою порушниками з шляхом подолання засобів захисту інформацій в телекомунікаційних мережах. Позначимо ймовірність такої події P_3. З урахуванням того, що такий захист може здійснюватися засобами канального (з ймовірністю $P_{\text{ккрз}}$) чи абонентського криптографічного захисту інформації (з ймовірністю $P_{\text{акрз}}$) телекомунікаційної мережі

$$P_3 = P_{\text{ккрз}} \times P_{\text{акрз}}. \quad (6)$$

Тоді ймовірність порушення конфіденційності $q_1 = 1 - p_{\text{в1}}$, де $p_{\text{в1}}$ – як і в [20], – ймовірність виявлення і усунення загроз конфіденційності, можна знайти з виразу

$$q_1 = 1-(1-P_2)(1-P_3) = \\ = 1-\left\{1-P_{\text{кзі}}[1-(1-P_1)(1-P_{\text{зві}})]\left[1-\right.\right. \\ \left.\left.-P_{\text{ккрз}} \times P_{\text{акрз}}\right]\right\}. \quad (7)$$

Запропонована модель дозволяє:

1. Використати вираз (7) для розрахунку значення залишкового ризику у вигляді ймовірності порушення конфіденційності при визначення оптимальних чи допустимих параметрів системи кіберзахисту інформації.

Цей же вираз, навпаки, можна використати для визначення параметрів засобів забезпечення конфіденційності ресурсів ІС при заданому значенні значення залишкового ризику q_1.

2. Зробити, висновок про те, що для забезпечення конфіденційності за рахунок унеможливлення доступу неавторизованих користувачів до інформації та розкриття її змісту необхідно застосовувати засоби (апаратурні чи програмні) адміністрування доступу, управління фізичним доступом, захисту від витоків інформації технічними каналами, засоби криптографічного перетворення (для шифрування та дешифрування закритої інформації, а також засоби генерації та розповсюдження ключів), засоби охоронної сигналізації та організаційного обмеження доступом.

Методика включає наступні етапи:

1. Оцінка можливих способів організації та реалізації ефективного захисту інформаційного обміну в телекомунікаційних мережах сучасних ієрархічних ІС з погляду забезпечення цілісності, швидкості обміну та часу доставляння повідомлень (як однієї з кількісних характеристик доступності) та вироблення рекомендацій щодо способів організації обміну, які б забезпечували удосконалення та підвищення рівня захищеності інформаційних об'єктів (інформаційних повідомлень) під час обміну.

2. Оцінка та розроблення можливих варіантів підвищення цілісності та доступності інформації в ІС.

3. Оцінка можливої шкоди із-за неефективної організації обміну в ІС.

Останнє пов'язане з тим, що як показано в розділі 1, власника ІС турбує не лише можливість забезпечення засобами кіберзахищеності інформації (КЗІ) тієї чи іншої властивості захищеності, а і

ефективність цих засобів, тобто якою "ціною" забезпечується досягнення цієї функціональної властивості, то певна увага в даному розділі приділена оцінці відповідності витрат на захист інформації в ІС тому виграшу, який при цьому досягається, тобто оцінці оптимальності захищеності ІС з погляду можливих економічних втрат.

Етап оцінки можливих способів організації та реалізації ефективного захисту інформаційного обміну в телекомунікаційних мережах сучасних ієрархічних ІС з погляду забезпечення цілісності, швидкості обміну та часу доставляння повідомлень (як однієї з кількісних характеристик доступності) та вироблення рекомендацій щодо способів організації обміну, які б забезпечували удосконалення та підвищення рівня захищеності інформаційних об'єктів (інформаційних повідомлень) під час обміну передбачає:

1. Оцінку цілісності інформаційних об'єктів в ІС при реалізації того чи іншого способу організації обміну. Для оцінки цілісності запропоновано використання такої характеристики як правильність передачі даних (ймовірність правильної доставки повідомлення чи отримання на приймальному боці невикривленої інформації).

2. Оцінку доступності ІС, яка здійснюється через такі її характеристики як відносна та абсолютна швидкості обміну інформації в ІС та час затримки в доставлянні повідомлень при реалізації того чи іншого способу організації обміну.

3. Оцінку можливої шкоди із-за неефективної організації обміну.

З метою отримання рекомендацій щодо практичного вибору ефективних методів та способів організації обміну оцінку характеристик цілісності та доступності по першій та другій методиках здійснено одночасно із порівняльною оцінкою найбільш поширених способів організації обміну в ІС. У випадку відсутності однозначності висновків щодо переваг того чи іншого способу організації обміну запропоновано використання комплексної характеристики ефективності забезпечення в ІС цілісності та доступності у вигляді ефективної швидкості обміну.

Нагадаємо, що сукупність загроз тій чи іншій функціональній властивості захищеної системи чи її елементам можна розглядати як їх потік, який, в свою чергу, складається з потоків штучних та природних впливів. При цьому потік штучних впливів породжується користувачами – ненавмисними чи навмисними діями авторизованих користувачів, тобто таких користувачів, що мають дозвіл на використання певного ресурсу ІС, та неавторизованих користувачів (неавторизована сторонаів, що мають за мету завдати якоїсь шкоди ІС, інформації чи її власникам). Останні впливи кіберзагроз породжуються спробами, які, при умові подолання ними системи управління доступом, мають назву спроб несанкціонованого доступу до відповідних ресурсів ІС (зрозуміло, при наявності у складі ІС засобів КЗІ).

Потік природних впливів в ІС виникає внаслідок: наявності впливів зовнішніх електромагнітних полів (завад) на елементи підсистеми та на середовище передачі інформації; недостатньої надійності елементів, з яких складається телекомунікаційна мережа; порушення умов та режимів їх експлуатації; недостатньої спроможності первинних технічних засобів запобігти дії таких впливів та інших причин.

При цьому слід очікувати [2, 4, 7], що в загальну інтенсивність потоку загроз для телекомунікаційних мереж, які складаються з сукупності вузлів комутації та каналів зв'язку і побудовані на загальних принципах, найбільший внесок дає потік природних впливів. Тобто природні впливи кіберзагроз на елементи ІС є найбільш імовірними. Це пов'язано, по-перше, із їх значною інтенсивністю в ІС (принаймні в її каналах передачі даних), а, по-друге, із підкресленим уже фактом зниження інтенсивності штучних впливів за рахунок їх проріджения засобами управління доступом.

По відношенню до інформації ІС слід говорити про те, що первинним наслідком впливів усіх загроз є те чи інше її викривлення – порушення правильності чи цілісності інформації, яке, в свою чергу, може призвести до порушення інших функціональних властивостей інформаційного об'єкта, насамперед, його доступності. Топологія ІС при цьому, принаймні для проблеми, що розглядається, принципового значення не має [1, 2].

Найчастіше під правильністю [3, 5, 6, 8] розуміють стійкість інформації щодо викривлень поодинокого символу чи групи символів в наслідок природних впливів, а під цілісністю – видалення чи модифікацію певної кількості символів чи усього повідомлення в наслідок штучних впливів. Звернемо увагу на те, що ці визначення не завжди

відрізняються сутністю, а дуже часто – лише сферою (галуззю) застосування.

Тому, з погляду проблематики забезпечення захищеності інформаційних ресурсів, їх доречно звести до поняття цілісності цих ресурсів, хоча при цьому, безумовно, слід враховувати джерело походження загроз цій цілісності, оскільки штучні, навмисні викривлення інформаційних об'єктів можуть приховуватися, маскуватися.

Окрім того, в даній роботі запропоновано застосувати такі поняття цілісності, які є близькими до понять протоколів розподілу функцій у відповідності з концепцією взаємного зв'язку відкритих систем (ISO) та до розподілу способів забезпечення конфіденційності в ІС (чи то канальне, чи то абонентське шифрування). При цьому можна розподілити (в розрізі напрямків даних досліджень) взагалі єдину задачу забезпечення властивостей захищеності ресурсів ІС на:

1. Задачу забезпечення властивостей захищеності ресурсів в каналах (канальні цілісність та доступність) – задачу забезпечення правильності та мінімального часу затримки інформації, яка передається в каналах зв'язку по певному маршруту телекомунікаційної мережі [5] між вихідним та вхідним каналоутворюючим обладнанням відповідних елементів ІС у відповідності з протоколами 1-4 рівнів (фізичний, канальний, мережний та транспортний).

2. Ця задача вирішується шляхом подолання наслідків природних чи інших впливів на елементи канального та мережного обладнання.

3. Задачу забезпечення властивостей захищеності ресурсів ІС в цілому (абонентські цілісність та доступність) – задачу забезпечення цілісності та доступності інформації, яка передається від одного елемента ІС (абонента –абонентської ЕОМ) до іншого [5] у відповідності з протоколами 5-7 рівнів (сеансовий, представницький та прикладний), шляхом подолання наслідків усіх штучних впливів та тих природних впливів на елементи ІС канального обладнання, які не усунені засобами забезпечення цілісності в елементах канального обладнання.

Модель взаємодії засобів в процесі КЗІ в телекомунікаційних системах можна уявити так, як це представлено на рис. 2.

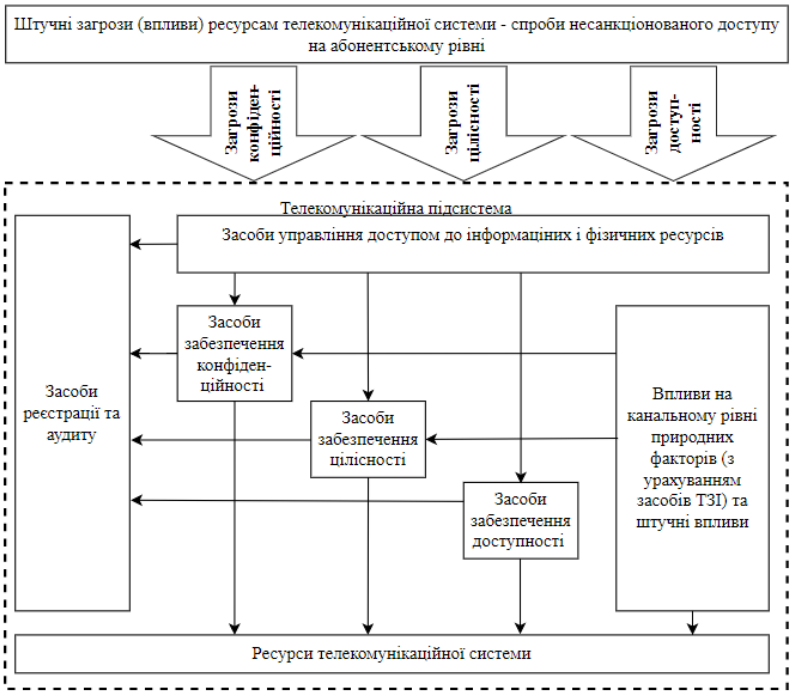

Рис. 2. Модель взаємодії засобів в процесі кіберзахисту інформації

З цієї моделі витікає, що штучні впливи кіберзагроз, які генеруються на абонентському рівні з боку передавача

з інтенсивністю $\lambda_{\text{ша}}$ дають наслідки лише при умові подолання ними системи управління доступом до інформаційних та фізичних ресурсів, тобто тільки в разі їх невиявлення засобами управління доступом.

Тоді інтенсивність таких штучних загроз, які впливають на засоби забезпечення відповідної функціональної послуги ІС, зменшується (за рахунок проріджування, фільтрації штучних впливів засобами управління доступом) до $\lambda_{\text{ша}}, P_{\text{уд}}$, де $P_{\text{уд}}$ – ймовірність подолання засобів управління доступом.

Природні ж впливи кіберзагроз не відповідають вимогам та умовам формування справжніх повідомлень і тому частка ресурсу ІС витрачається на їх виявлення і усунення (зменшення доступності ІС). На цілісність ресурсів ІС вони впливають тільки в разі неспроможності виявити та усунути їх засобами канального забезпечення цілісності. Тобто, інтенсивність природних загроз λ, які впливають на засоби забезпечення цілісності ресурсів ІС, також зменшується (за рахунок проріджування, фільтрації природних загроз канальними засобами) до $\lambda P_{\text{ккц}}$ де $P_{\text{ккц}}$ – ймовірність подолання засобів канального захисту інформації в телекомунікаційної мережі. Тоді результуюча інтенсивність загроз доступності ресурсів ІС $\lambda_{\text{рд}}$ може бути розрахованою як

$$\lambda_{\text{рд}} = \lambda_{\text{ша}} P_{\text{уд}} + \lambda_{\text{шк}} + \lambda\,, \qquad (7)$$

а результуюча інтенсивність загроз цілісності ресурсів ССП може бути розрахованою як

$$\lambda_{\text{рц}} = \lambda_{\text{ша}} P_{\text{уд}} + \lambda_{\text{шк}} + \lambda P_{\text{ккц}}. \qquad (8)$$

Зрозуміло, що з цією ж інтенсивністю з (8) кіберзагрози впливають і на засоби захисту абонентського рівня. Тоді, з урахуванням застосування відповідних засобів захисту – засобів забезпечення цілісності ресурсів ІС (на абонентському рівні в ІС вузлів центрального, регіонального чи місцевого рівнів ІС), імовірність подолання яких – $P_{\text{акц}}$ результуюча інтенсивність $\lambda_{\text{н}}$ загроз, не усунутих системою ТЗІ, може бути розрахованою як:

$$\lambda_{\text{н}} = \lambda_{\text{рц}} P_{\text{акц}} = \left(\lambda_{\text{ша}} P_{\text{уд}} + \lambda_{\text{шк}} + \lambda P_{\text{ккц}}\right) P_{\text{акц}}. \quad (9)$$

Звернемо увагу на те, що найбільший вплив на ресурси ІС, як витікає з (9), слід очікувати від штучних впливів на канальному рівні, оскільки вони не зменшуються (не проріджуються) ніякими засобами, окрім засобів забезпечення цілісності ресурсів ІС на абонентському рівні, та особливу необхідність при цьому зменшення ймовірності подолання засобів абонентського контролю цілісності інформації $P_{\text{акц}}$, або збільшення ймовірності виявлення та усунення впливу засобами абонентського контролю цілісності інформації $\left(1 - P_{\text{акц}}\right)$.

Виходячи з визначень функціональних властивостей захищеності ресурсів ІС та моделі загроз, подію, пов'язану з порушенням цілісності інформаційних ресурсів слід розглядати як складну та таку, що складається з подій:

- виведення з ладу, зміни режимів функціонування або несанкціонованого використання засобів зберігання носіїв інформації і порушення таким чином її цілісності;
- несанкціонованої модифікації (зміни, підміни, знищення та т.п.) ІзОД в середовищах її оброблення, зберігання чи передавання з метою унеможливлення подальшого її використання чи нанесення іншої шкоди власнику даного ресурсу.

На рис. 3 представлена модель взаємодії атак з засобами протидії цим кібератакам – засобами забезпечення цілісності (на цьому рис. ЗЦ – кіберзагроза цілісності).

При цьому, як і для моделі взаємодії засобів реалізації загроз конфіденційності інформації та засобів протидії цим кіберзагрозам, подолання неавторизованим користувачем системи захисту $P_{\text{іcз}}$ можливе, якщо:

1. Подолано засоби охоронної сигналізації або засоби організаційного обмеження доступу та (і) засоби управління доступом, включаючи засоби управління фізичним доступом (дозвіл чи блокування доступу до приміщень, терміналів, системних блоків, клавіатури та інших фізичних засобів) та адміністрування доступу (адміністрування суб'єктів, об'єктів, побудови і реалізації моделі захищеної системи, розмежування доступу тощо). P_1 яка уже визначена раніше.

2. Подолано засоби контролю цілісності інформації відповідного вузла і засоби захисту від спеціального впливу на інформацію по технічним каналам. Ймовірність такої події $P_{\text{кц}}$.

3. В телекомунікаційній мережі подолано засоби канального та абонентського захисту цілісності інформації, яка передається (приймається) в вузлах центрального, регіонального чи місцевого рівнів ІС. Ймовірність такої події P_4 можна визначити з виразу

$$P_4 = P_{\text{акц}} \times P_{\text{ккц}}, \qquad (10)$$

де:

$P_{\text{акц}}$ – ймовірність подолання засобів абонентського контролю цілісності інформації в ТКМ вузлів центрального, регіонального чи місцевого рівнів ІС;

$P_{\text{ккц}}$ – ймовірність подолання засобів канального контролю цілісності інформації в телекомунікаційної мережі.

Тоді ймовірність порушення цілісності інформаційних ресурсів $q_2 = 1 - p_{\text{в2}}$, де $p_{\text{в2}}$ – ймовірність виявлення і усунення загроз цілісності, можна знайти з виразу

$$q_2 = 1-(1-P_1)(1-P_{кц})(1-P_4) = 1-\left\{1-P_{уд}\left[1-(1-P_{ood})(1-P_{ос})\right]\right\}\times \left[1-P_{кц}\right]\left[1-P_{акц}P_{ккц}\right]. \quad (11)$$

Розглянута модель дозволяє:

1. Використати вираз (11) для розрахунку значення залишкового ризику у вигляді ймовірності порушення цілісності при визначення оптимальних чи допустимих параметрів системи кіберзахисту інформації. Цей же вираз, навпаки, можна використати для визначення параметрів засобів забезпечення цілісності інформаційних ресурсів ІС при заданому значенні значення залишкового ризику q_2.

2. Зробити висновок про те, що для забезпечення цілісності за рахунок унеможливлення доступу до інформації та модифікації неавторизованим користувачем змісту інформаційного об'єкту необхідно застосовувати засоби (апаратурні чи програмні) для адміністрування доступу, для контролю цілісності, для управління фізичним доступом, засоби охоронної сигналізації та організаційного обмеження доступом.

3. З останнього витікає необхідність, на відміну від моделі взаємодії засобів реалізації загроз та засобів забезпечення конфіденційності, застосування для забезпечення цілісності інформаційних об'єктів замість засобів криптографічного захисту – засобів контролю цілісності з відповідними механізмами та замість засобів захисту від витоків – засобів захисту від спеціального впливу.

4. Для унеможливлення порушення цілісності за рахунок отримання неавторизованим користувачем доступу до інформації з обмеженим доступом (ІзОД) слід застосовувати такі ж засоби захисту (апаратурні чи програмні), як і для забезпечення конфіденційності.

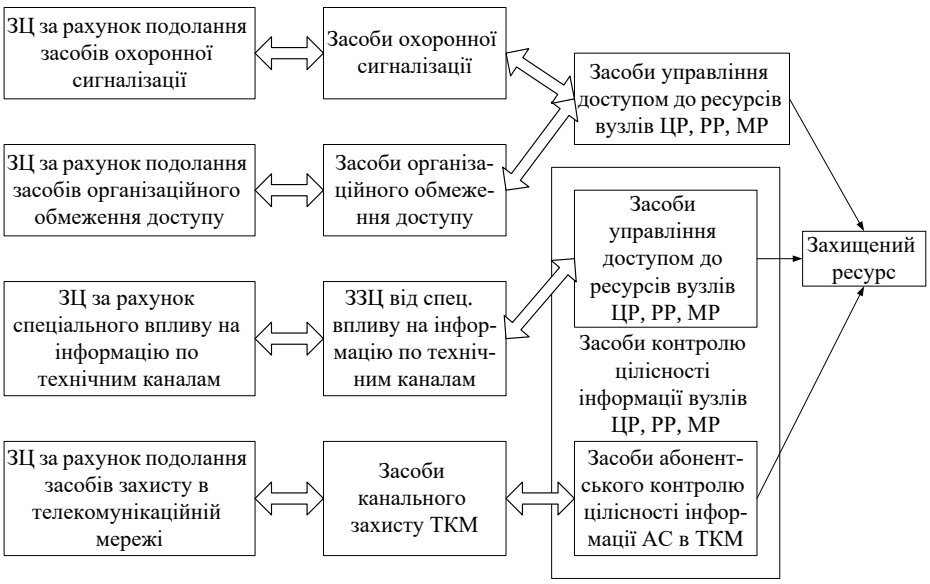

Рис.3. Модель процесу взаємодії засобів реалізації атак із засобами забезпечення цілісності в інформаційних системах

5. Для унеможливлення порушення цілісності за рахунок модифікації ІзОД необхідно забезпечити чітке дотримання політики безпеки в частині правил розмежування доступу та надання тих чи інших привілеїв користувачам (наприклад, обмеження прав доступу типу «видалити» – delete, «вставити» –

insert? «все» – all та т.п.), забезпечити відкат процесів в разі порушення цілісності, а також забезпечити контроль цілісності інформаційних об'єктів та унеможливлення їх використання в разі порушення цілісності. Виходячи з визначень функціональних властивостей захищеності ресурсів ІС та моделі загроз подію, пов'язану з порушенням доступності слід розглядати як складну та таку, що складається з подій:

- несанкціонованого використання інформаційного ресурсу шляхом захоплення (неконтрольованого використання, утримання, занадто тривалого використання) ресурсів і створенню таким чином перешкод авторизованим користувачам в використання цих ресурсів;
- переводу ресурсу в режим штучної відмови (тривалої неможливості використання ресурсу за призначенням). Це можливе, по-перше, шляхом неконтрольованої суттєвої (за обсягом) модифікації (зміни, підміни, знищення та т.п.) неавторизованим користувачем ІзОД з метою унеможливлення подальшого її використання чи нанесення іншої шкоди власнику даного ресурсу і потребує відновлення, поновлення цілісності ресурсу шляхом, наприклад, використання його резервної копії. По-друге – шляхом генерації потоку заважаючих запитів несправжніх запитів на обслуговування, несправжніх пакетів вхідної інформації, спроб підбору паролів та т.п.; – завад процесу обслуговування справжніх запитів) з такою інтенсивністю, коли їх період (середня тривалість проміжку часу між двома сусідніми запитами) не перевищує тривалості обслуговування кожного з таких запитів, тобто такого потоку, коли захищений ресурс призначається для обслуговування лише заважаючих запитів;
- вплив природних чи штучних збоїв (короткочасних впливів) шляхом неконтрольованої несуттєвої (за обсягом, але не за змістом) модифікації (зміни, підміни, знищення та т.п.) неавторизованим користувачем ІзОД з метою унеможливлення подальшого її використання чи нанесення іншої шкоди власнику даного ресурсу, що потребує того чи іншого відновлення цілісності ресурсу після збоїв; фізичного впливу па ресурс з метою виведення його з ладу чи зміни режимів його функціонування.

На рис. 4 представлена модель взаємодії засобів реалізації атак з засобами протидії цим кібератакам – засобами забезпечення доступності (на цьому рисунку ЗД – кіберзагрози доступності).

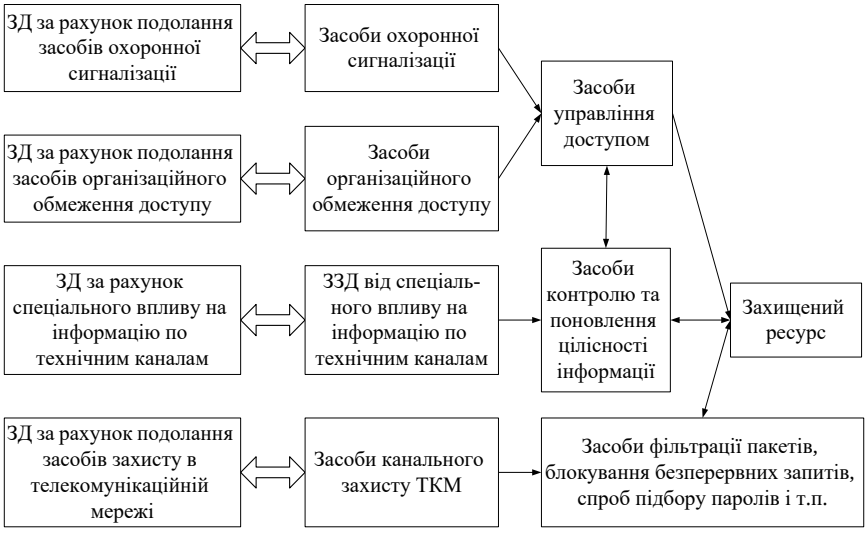

Рис. 4. Модель взаємодії засобів реалізації атак із засобами забезпечення доступності в інформаційних системах

При цьому, як і для моделі взаємодії засобів реалізації загроз цілісності інформації та засобів протидії цим кіберзагрозам, подолання неавторизованим користувачем системи захисту $P_{\text{псз}}$ можливе, якщо:

1. Подолано засоби охоронної сигналізації або засоби організаційного обмеження доступу та (і) засоби управління доступом, включаючи засоби управління фізичним доступом (дозвіл чи блокування доступу до приміщень терміналів, системних блоків, клавіатури та інших фізичних засобів) та адміністрування доступу (адміністрування суб'єктів, об'єктів,

побудови і реалізації моделі захищеної системи, розмежування доступу тощо) з ймовірністю P_1, яка уже визначена раніше.

2. Подолано засоби контролю та поновлення цілісності інформації відповідного вузла і засоби захисту від спеціального впливу на інформацію по технічним каналам. Ймовірність такої події P_5 можна визначити з виразу:

$$P_5 = P_{\text{зсп}} \times P_{\text{кпц}}, \qquad (12)$$

де:

$P_{\text{зсп}}$ – ймовірність подолання засобів захисту від спеціального впливу на інформацію по технічним каналам;

$P_{\text{кпц}}$ – ймовірність подолання засобів контролю та поновлення цілісності інформації вузлів центрального, регіонального, місцевого рівнів АС.

3. Подолано засоби фільтрації пакетів, блокування засобів генерації безперервних запитів, спроб підбору паролів та т.п. і засоби канального захисту інформації телекомунікаційної мережі. Ймовірність такої події P_6 можна визначити з виразу

$$P_5 = P_{\text{зб}} \times P_{\text{ззк}}, \qquad (13)$$

де:

$P_{\text{зб}}$ – ймовірність подолання засобів блокування засобів генерації безперервних запитів, спроб підбору паролів тощо;

$P_{\text{ззк}}$ – ймовірність подолання засобів канального захисту інформації в телекомунікаційної мережі.

Тоді ймовірність подолання засобів забезпечення доступності $q_{n3} = 1 - p_{\text{вз}}$, де $p_{\text{вз}}$ – ймовірність виявлення і усунення загроз доступності, можна знайти з виразу:

$$q_{n3} = 1 - (1 - P_1)(1 - P_5)(1 - P_6) = 1 - \\ - \left[1 - P_{\text{уд}}\left[1 - \left(1 - P_{\text{ood}}\right)(1 - P_{\text{oc}})\right]\right] \times \left[1 - \right. \\ \left. - P_{\text{зсп}}P_{\text{кпц}}\right][1 - P_{\text{зб}}P_{\text{ззк}}]. \qquad (14)$$

Для оцінки ймовірності порушення доступності шляхом переводу ресурсу в режим штучної відмови необхідно визначити інтенсивність потоку впливів на доступність ресурсу. Для цього скористаємося відомим з [5] виразом для розрахунку результуючої інтенсивності загроз з урахуванням спеціального впливу по технічним каналам та проріджения (фільтрації) впливів засобами їх виявлення та усунення

$$\lambda_{\text{рз}} = \left(\lambda_{\text{шi}}\left(1 - p_{\text{уд}}\right) + \lambda_{\text{i}} + \lambda_{\text{сп}}P_{\text{кпц}}P_{\text{зсп}}\right)(1 - \\ -p_{\text{вз}}) = \left(\lambda_{\text{шi}}P_{\text{уд}} + \lambda_{\text{i}} + \lambda_{\text{сп}}P_{\text{кпц}}P_{\text{зсп}}\right)q_{n3}, \qquad (15)$$

де: змінні $P_{\text{кпц}}$, $P_{\text{зсп}}$, q_{n3} мають раніше визначений зміст; $\lambda_{\text{рз}}$ – результуюча інтенсивність загроз захищеному ресурсу: $\lambda_{\text{шi}}$ – інтенсивність штучних впливів через засоби управління доступом; $p_{\text{уд}}$ – ймовірність неподолання кіберзагрозами засобів управління доступом; λ_{i} – інтенсивність природних впливів; $\lambda_{\text{сп}}$ – інтенсивність спеціальних впливів по технічним каналам.

При такому підході інтенсивність запитів на використання ресурсів ССП можна визначити як суму інтенсивності справжніх запитів $\lambda_{\text{сз}}$ та результуючої інтенсивності загроз захищеному ресурсу:

$$\lambda_{\text{рз}}: \lambda_{\text{з}} = \lambda_{\text{сз}} + \lambda_{\text{рз}}. \qquad (16)$$

Тоді ймовірність порушення доступності можна визначити як ймовірність того, що кількість запитів на часовому інтервалі, тривалість якого дорівнює тривалості циклу управління $\text{T}_{\text{упр}}$ ІС, перевищить допустиму, або як ймовірність того, що на певний часовий інтервал, довжина якого $t_{\text{кр}}$, попаде більше ніж один запит. Розглянемо останній варіант, вважаючи розподіл ймовірностей таких подій пуассоновським. Для цього варіанту вираз для розрахунку ймовірності порушення доступності можна записати у вигляді:

$$q_{\text{з}} = 1 - p_0 - p_1 = 1 - \\ -\left(1 + \lambda_{\text{з}}t_{\text{кр}}\right)exp\left(-\lambda_{\text{з}}t_{\text{кр}}\right), \qquad (17)$$

де p_0 та p_1 – ймовірності відсутності подій і наявності рівно однієї події на інтервалі $t_{\text{кр}}$ відповідно.

Змінну $t_{\text{кр}}$ при цьому слід розглядати як середній час використання захищеного ресурсу в умовах обслуговування ІС усіх можливих запитів (для інформаційних об'єктів це – контроль цілісності, при необхідності її поновлення, виконання програмного засобу, читання чи запис інформації та все таке інше). Визначення величини $t_{\text{кр}}$ виходить за рамки даної роботи, хоча в якості першого, грубого, наближення можна використати значення $t_{\text{кр}} = (T_{ki} - \Delta T_{ki})/n_{io}$, де n_{io} – кількість інформаційних об'єктів, що потребують використання на інтервалі часу $(T_{ki} - \Delta T_{ki})$. При цьому, якщо середнє значення часу використання ресурсу перевищить середнє

значення часового інтервалу між сусідніми запитами (інтенсивність запитів перевищує інтенсивність обслуговування), то кількість будь-яких запитів в черзі на використання ресурсу буде зростати до нескінченності, що є ознакою штучної відмови захищеного ресурсу. Тобто умову, коли слід розглядати як умову переходу захищеного ресурсу в режим штучної відмови

$$1/\lambda_{pз} \leq t_{kp}. \quad (18)$$

ВИСНОВКИ

Розглянуті моделі дозволяють, по-перше, запропонувати вирази для оцінки залишкового ризику при захисті ресурсів базових характеристик безпеки у вигляді ймовірностей їх порушення та сформувати умову переходу захищеного ресурсу в режим штучної відмови.

По-друге, зробити висновок про те, що для забезпечення базових характеристик безпеки за рахунок унеможливлення доступу до інформації та модифікації неавторизованим користувачем змісту інформаційного об'єкту необхідно застосовувати засоби (апаратурні чи програмні) для управління доступом, для контролю та поновлення цілісності, для фільтрації пакетів, блокування засобів генерації безперервних запитів та т.п., засоби управління фізичним доступом, охоронної сигналізації та організаційного обмеження доступом.

По-третє, з останнього витікає необхідність застосування для забезпечення доступності інформаційних об'єктів, на відміну від моделі взаємодії засобів реалізації загроз та засобів забезпечення цілісності, замість засобів лише контролю цілісності – засобів контролю та поновлення цілісності з відповідними механізмами, оскільки використання ресурсу з порушеною цілісністю є порушенням доступності ресурсу, як властивості його захищеності.

Окрім того, на відміну від захисту від порушення конфіденційності та цілісності слід передбачати і можливість недопущення переводу ресурсу в режим штучної відмови - порушення доступності об'єкту за рахунок унеможливлення вчасного використання того чи іншого ресурсу авторизованим користувачем, тобто необхідно передбачати механізми запобігання постійного чи занадто тривалого використання цього ресурсу чи засобів його отримання порушником (установка квот – кількості звернень поспіль, допустимої тривалості чи допустимих часових інтервалів використання ресурсу, установка приорітетів на використання ресурсів та інше), механізми забезпечення стійкості та відновлення процесів в умовах збоїв, механізми резервування інформаційних об'єктів, механізми аналізу потоків запитів від суб'єктів ІС, контролю та поновленню цілісності інформаційних об'єктів тощо.

ЛІТЕРАТУРА

[1] Браіловський М.М. Аналіз кібербезпеки у сучасних умовах. Монографія. / М.М. Браіловський, С.В. Зибін, А.А. Кобозєва, В.О. Хорошко, Ю.Є. Хохлачова. – К.: ТОВ ЦП "Компринт", 2021. – 360 с.

[2] Корченко А.Г. Анализ и оценивание рсиков информационной безопасности / Корченко А.Г., Архипов А.Е.,Казмирчук С.В. - Л: ООО ”Лазурий-Полиграф”, 2013. – 275 с.

[3] Бармен Скотт. "Разработка правил информационной безопасности" – М: Вильямс, 2002. – 208 с.

[4] Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. / Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. / За заг. ред. докт. техн. наук, проф. В.Б. Толубко. – К.: ДУТ, 2015. – 288 с.

[5] Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: підручник / Бурячок В.Л., Гулак Г.М., Толубко В.Б..– К.: ТОВ "СІКГРУП Україна", 2015. – 449с.

[6] Дубов Д. В. Кібербезпека : світові тенденції та виклики для України / Д. В. Дубов, М. А. Ожеван. – К. : НІСД, 2011. – 30 с.

[7] Лунтовський А.О., Климаш М.М. Інформаційна безпека розподілених систем. Монографія. – Львів: Національний університет "Львівська політехніка", 2014. – 480 с.

[8] Шорошев В.В. Теоретичні і практичні аспекти організації і побудови архітектури захищених комп'ютерних систем ОВС України: монографія / В. В. Шорошев ; Держ. ун-т інформ.-комунікац. технологій, Навч.-наук. ін-т захисту інформації. – К. : ДУІКТ, 2011. – 256 с.

MODELS FOR ASSESSMENT OF RESIDUAL RISK IN INFORMATION SYSTEM

To ensure the basic characteristics of the security of information system resources by preventing unauthorized users from accessing information and disclosing its content, it is necessary to use the means (hardware or software) of access administration, physical access control, protection against information leaks through technical channels, cryptographic means transformation (for encryption and decryption of

closed information, as well as means of generation and distribution of keys), means of security signaling and organizational access restriction, etc. In the work, models of the process of interaction of means of cyber-attacks with means of cyber protection were developed to ensure the basic characteristics of the security of resources of information systems in which, due to the amount of residual risk and variation in the mode of operation or unauthorized use of means of storage of information carriers ration and thereby violating its integrity, accessibility and confidentiality, allows to provide a quantitative and qualitative assessment of the state of cyber security. A model of the process of the interaction of protection means is also presented, in which, due to the use of the model of the process of the interaction of means of cyber-attacks with means of cyber protection and the decomposition of the basic security characteristics of information system resources and taking into account the relevant indicators of the basic security characteristics in the process of cyber protection of information system resources, it is possible to increase the accuracy of the dynamic assessment of efficiency dependence from the intensity of the effects of cyberattacks. The proposed cyber protection models make it possible to block cyber-attacks in information systems even before they start to act on the system. In this way, cyber defense can use its resources more effectively, which does not need to respond to every warning, since there can also be false warnings. The considered models make it possible to propose expressions for assessing the residual risk when protecting resources of basic safety characteristics in the form of probabilities of their violation and form the conditions for the transition of the protected resource to the mode of artificial failure.

Keywords: cyber security, information systems, cyber-attacks, security of resources, ensuring cyber security.

Хорошко Володимир Олексійович, доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.

Khoroshko Volodymyr, doctor of technical sciences, professor, professor of the department of security of information technologies of the National Aviation University.
E-mail: professor_va@ukr.net.
Orcid ID: 0000-0001-6213-7086.

Хохлачова Юлія Євгеніївна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Khokhlachova Yuliia, candidate of technical sciences, associate professor, associate professor of the department of security of information technologies of the National Aviation University.
E-mail: yuliiahohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

Погорелов Володимир Володимирович, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Pogorelov Volodymyr, Candidate of Technical Sciences, Associate Professor of the Department of Security of Information Technologies of the National Aviation University.
E-mail: volodymyr.pogorelov@gmail.com.
Orcid ID: 0000-0002-6100-1504.

Аясрах Ахмад Расмі Алі, аспірант кафедри безпеки інформаційних технологій Національного авіаційного університету.

Ayasrah Ahmad, graduate student of the Department of Security of Information Technologies of the National Aviation University.
E-mail: ahmadaesr@gmail.com.
Orcid ID: 0000-0003-4392-1806.

DOI: 10.18372/2410-7840.24.16933
УДК:336.71:004.056

ОЦІНКА РІВНЯ БЕЗПЕКИ В КІБЕРФІЗИЧНИХ СИСТЕМАХ

Сергій Погасій

У статті наведений новий підхід оцінки ризиків та формування превентивних заходів безпеки на основі моделі Лотки-Вольтери. Запропоновані моделі безпеки кіберфізичних систем: "хижак-жертва" з урахуванням обчислювальних можливостей і спрямованості цільових кібератак, "хижак-жертва" з урахуванням можливої конкуренції зловмисників по відношенню до "жертви", "хижак-жертва" з урахуванням взаємозв'язків між "видами жертв" і "видами хижаків", "хижак-жертва" з урахуванням взаємозв'язків між "видами жертв" і "видами хижаків" дозволяють забезпечити погляд на можливість формування вектору загроз, а також їх залежність від розвитку цифрових