УДК 004.72.056.52:004.4
DOI: 10.31673/2409-7292.2024.010007

Захаржевський А. Г., Толкачов М. Ю., Дженюк Н. В., Погасій С. С., Глухов С. І.

МЕТОД ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ НА ОСНОВІ СЕМІОТИЧНОЇ МОДЕЛІ КІБЕРПРОСТОРУ

Предметом дослідження у статті є процеси забезпечення захисту інформаційних ресурсів у кіберфізичному просторі. Мета – розробка моделі щодо реалізації методу захисту інформації у кіберфізичному просторі. В основу розробки покладено семіотичну модель кіберпростору. Задача – розробка ефективних стратегій захисту інформаційних ресурсів та керування кібербезпекою у кіберпросторі з урахуванням соціальних та перцептивних аспектів. Використані методи: методи аналітичного моделювання та нечіткої логіки. Отримані наступні результати. Показано, що складна, різностороння подача інформації у мережі вимагає комплексного підходу із розділенням змішаного контенту інформації на взаємопов'язані рівні. Запропоновано семіотичний підхід, який дозволяє більш глибоко аналізувати взаємодію між людиною та технологіями, що особливо важливе для розуміння та керування складними системами інформаційної безпеки. Розроблена шестирівнева модель кіберпростору з методом оцінки рівня безпеки для кожного з рівнів розробленої моделі та запропоновано інтегральний показник потенційних загроз для власників мережевих інформаційних ресурсів. Проведено верифікацію розробленої моделі. Розроблені семіотична модель кіберпростору та інтегральний показник потенційних загроз дають змогу покращити моніторинг та керування кібербезпекою власників мережевих інформаційних ресурсів шляхом врахування різноманітних факторів, включно з урахуванням соціальних та перцептивних аспектів, що є ключовим фактором для розробки ефективних стратегій захисту інформаційних ресурсів у кіберпросторі.

Ключові слова: кіберфізичний простір, кібербезпека, захист інформаційних ресурсів, інтегральний показник, семіотична модель.

Вступ

Бурхливе зростання інформаційних ресурсів та технологій сприяє зростанню атак на інформаційно-комунікаційні, кіберфізичні та соціокіберфізичні системи. Оцінка рівня захищеності та захист мережевого трафіку стає критично важливою задачею в епоху глобальної цифровізації. З огляду на різноманітність та обсяг наборів даних, які передаються мережами, слід зазначити, що традиційні підходи до кібербезпеки, які сфокусовані тільки на технічних аспектах захисту, виявляються недостатніми [1–4]. У міжнародних стандартах по кібербезпеці Standard ISO/IEC 27032:2023 [5, 6] з урахуванням тенденцій розвитку глобальної мережі Інтернет визначено поняття кіберпростору та кібербезпеки. Кіберпростір – середовище, яке являє собою наслідки результатів взаємодії людей, програмного забезпечення та послуг у Інтернеті за допомогою технологій, пристроїв та мереж, що під'єднані до неї, яких не існує у будь-якої фізичної формі. У цьому ж стандарті поняття кібербезпека визначено через поняття кіберпростір. Кібербезпека – це безпека у кіберпросторі [5, 6]. Крім того, у рекомендації X.1205 МСЕ-Т кібербезпека визначено як систему управління ризиками у кіберпросторі, що пов'язана із мережевою, прикладною, Інтернет-безпекою та безпекою критичної інформаційної інфраструктури.

Семіотика, що акцентує свою увагу на знаках, символах та їх використанні для передачі та інтерпретації інформації, стає актуальною у контексті кібербезпеки, де інтерпретація даних та комунікація інформації щодо загроз безпеці грає ключову роль. Семіотичний підхід дозволяє більш глибоко аналізувати взаємодію між людиною та технологіями, що особливо важливе для розуміння та керування складними системами інформаційної безпеки. Семіотична модель дозволяє створювати більш глибоке та всеосяжне розуміння у оцінці загроз, що стає ключовим для розробки ефективних стратегій кіберзахисту і керування складними системами інформаційної безпеки.

Для опису інформації у рамках пов'язаних концепцій Данні-Інформація-Знання запропоновано структуру, яка візуалізує зв'язки цих різних термінів (рис. 1). Вона демонструє взаємозв'язок між семіотикою та використанням знаків під час обробки інформації [7, 8].

Ця структура [9] є базисом для комплексної оцінки захищеності мережевих ресурсів, що надає нові можливості для більш докладного розуміння динаміки кіберзагроз і впливу людського фактору на безпеку мережевих систем. Зокрема, вона дає змогу усвідомити, як інформація про кіберзагрози сприймають і інтерпретують користувачі і фахівці та використовують її під час розробки більш ефективних стратегій кіберзахисту для підвищення загального рівня безпеки. Причому, застосування комплексного підходу із поділом на взаємопов'язані рівні дозволяє запобігти горизонтальному розповсюдженню атак у мережі та звести до мінімуму наданої шкоди.

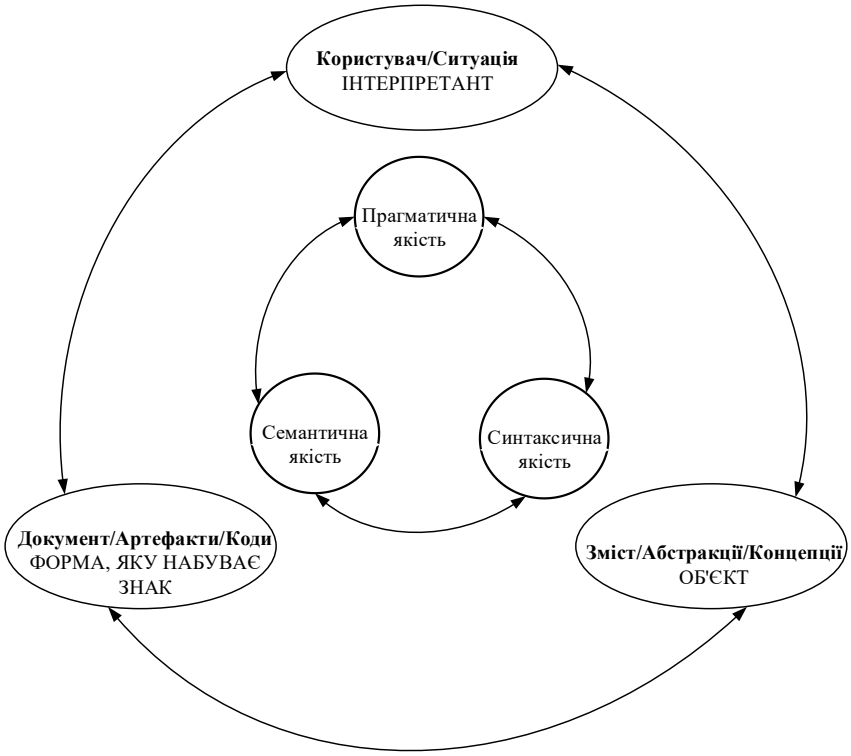

Рис 1. Семіотичний трикутник, що ілюструє порівняння концепцій Пірса, Бакленда та Хуанга

Таким чином застосування семіотичної моделі при оцінці рівня захисту мережевих ресурсів дозволяє окрім аналізу технічних вразливостей інформаційних ресурсів, враховувати ще й результати взаємодії користувачів із системами безпеки, що забезпечує більш глибоке розуміння динаміки кіберзагроз та ефективність прийнятих заходів щодо забезпечення безпеки систем кіберпростору.

Аналіз літературних джерел та формулювання проблеми.

В [10] розроблено кілька моделей знакового процесу або семіозису на основі трьох універсальних категорій: первинність, вторинність і третинність. Все, що однозначно і незалежно від усього іншого, є первинність. Це категорія відчуття, чистої якості або можливості. Вторинність – це категорія двох сутностей або, взагалі, категорія відносин або реакцій без якого-небудь закону або причини. Людська свідомість, наприклад, має справу з реакціями між внутрішнім і зовнішнім світом. Третинність – це посередницький елемент між двома сутностями. Третинність виникає, коли між двома речами є зв'язок, пов'язаний з мисленням і/або створенням звички. Це категорія представлення, звички, комунікації/посередництва, закону і знакових процесів, що не означає, що знаки не важливі для перших двох категорій.

Теорія знаків була більш детально розроблена в сучасній семіотиці, але її потенціал досі не був повністю реалізований. У [11] уточнюється, що комунікація складається не з інформації, а скоріше з використання знаків, які трактуються на декількох рівнях. Початковий рівень включає в себе елементарну взаємодію, сприяючі смисловому обміну (головним чином, через сигнали). Наступний рівень полягає в інтуїтивних знакових взаємодіях, що сприяють живій і емоційній комунікації про важливі аспекти життя. Відмінною особливістю цієї роботи є опис формування третього рівня – поля смислів, яке соціально-комунікативна система використовує як фундамент для модулювання свідомого лінгвістичного значення. Цей вищий рівень, відрізняючись підвищеною абстрактністю, доступний тільки людині.

Опираючись на фундаментальні роздуми семіотичного підходу, у [12] описані оновлення класичного семіотичного підходу до нової реальності, щоб інтегрувати його з досягненнями в області системної науки, кібернетики, прагматичної лінгвістики та управління документацією. У роботі [13] розроблена структура для інтеграції (біо)семіотичних, (другого порядку) кібернетичних і системних теорій в універсальне підґрунтя для інформаційних, когнітивних і комунікаційних наук. Відмінною особливістю цієї публікації є те, що в кіберсеміотиці використовується класифікація знаків Пірса, щоб досягти розуміння процесу індексації.

Кіберсеміотика прагне надати трансдисциплінарну основу для наукових досліджень у галузі інформації, пізнання та комунікації, які проводяться в природничих, технічних та соціальних науках, а також в гуманітарних дисциплінах. Вона спирається на два вже сформованих міждисциплінарних підходи: з одного боку, на кібернетику та теорію систем, включаючи інформаційну теорію та науку, а з іншого – на пірсовську семіотику, що включає феноменологію та прагматичні аспекти лінгвістики. Кіберсеміотика намагається поєднати нові парадигми сучасного світу людського сприйняття та впливу з системами обробки та оцінки в захисті інформації, та штучного інтелекту (AI).

Виходячи з джерела [14], розвиток систем на базі штучного інтелекту тягне за собою зростання інтересу злочинців до їх використання в недобросовісних цілях. Існуючі методи управління ризиками не завжди адекватно оцінюють потенційні загрози, пов'язані з AI. В той же час, при правильному контролі, AI може ефективно протистояти загрозам безпеці, згідно з [15]. Легкість доступу до інформації з відкритих джерел та необмежені можливості AI спрощують збір даних для організації цілеспрямованих атак. Використання технологій, таких як машинне навчання, підвищує ефективність та агресивність атак на соціокіберфізичні системи, роблячи можливими масштабні та автоматизовані дії.

Дані, які передаються соціокіберфізичними системами, та отримувана інформація вимагають різних рівнів безпеки та ефективних методів обробки. Це включає в себе нові аспекти кібербезпеки, пов'язані з соціальним впливом, сприйняттям, образами, емоціями та прийняттям рішень, як згадується в [16].

Згідно з [9], NIST видав спеціальний посібник щодо ідентифікації та управління упередженістю в AI. Цей посібник не є остаточним рішенням для усунення упередженості AI, але він спрямований на виявлення ключових проблем та надання першого кроку в розробці докладного соціально-технічного посібника для боротьби з упередженістю AI. Він пропонує чітку та стандартизовану базу для виявлення та управління упередженістю в AI, комплексний підхід до її ідентифікації, практичний посібник з впровадження структури в різних організаціях, а також інструменти та методи для виявлення та усунення упередженості в AI. Це може допомогти організаціям створювати більш надійні та прозорі AI системи. Однак, публікація може бути недоступна для непрофесіоналів в галузі AI, структура може виявитися занадто приписувальною для деяких організацій, а також публікація не надає інструкцій щодо вимірювання ефективності методів зменшення упередженості та не фокусується на усуненні кореневих причин упередженості в суспільстві та даних.

У контексті покращення вимірювань якості даних у [17] запропонована концептуальна модель, яка використовує семіотичні рівні для визначення способів досягнення цілей

покращення якості. У [8] розроблений набір метрик на основі семіотичної теорії для аудиту онтологій. Інші дослідження використовували категорії якості даних, похідні від семіотичних рівнів. У [18], використовуючи семіотичну теорію з суб'єктивними та об'єктивними точками зору на якість даних, застосовуються правила цілісності для відповідності структурних даних або метаданих для класифікації вимірювань якості даних. Семіотичні вимірювання якості даних групувалися відповідно до "зовнішньої відповідності референту" [18]. У [19] використана семіотична теорія для аналізу вимірювань якості даних, пов'язуючи рівні інформаційної піраміди з рівнями вимірювань якості даних [20]. Рівні інформаційної піраміди зв'язані з рівнями вимірювань в [21], сімнадцять вимірювань були згруповані на кожному з чотирьох семіотичних рівнів (емпірика, синтаксис, семантика і прагматика). У [22] висвітлюються три основні проблеми, пов'язані з захистом кіберфізичних систем. Ці проблеми включають в себе: розуміння потенційних загроз та наслідків атак, визначення унікальних характеристик кіберфізичних систем, що відрізняють їх від традиційної інформаційної безпеки, та розробку специфічних механізмів захисту для кіберфізичних систем. Зокрема, розглядаються механізми безпеки для запобігання атакам, їх виявлення та реагування на них, а також для забезпечення стійкості системи та стримування можливих атак.

Робота виділяється створенням моделі противника, що допомагає усвідомити загальний обсяг проблеми та оцінити можливі ризики. У ній представлені профілі різних можливих порушників, включаючи їх мотивації та доступні ресурси. Аналіз поведінкових аспектів зловмисників зроблений і в роботах [23, 24].

У промисловості мережеві власники використовують управління кіберфізичними системами (CPS), яке базується на одній або декількох контрольних мережах, які часто інтегровані з фізичними датчиками та виконавчими пристроями. Це відрізняє їх від традиційних IT-систем з точки зору безпеки. Системи SCADA, ключові у сучасній промисловості, піддаються ризику через зв'язок з Інтернетом, роблячи їх вразливими для кібератак [25]. Дослідження, про яке йде мова, не просто класифікує атаки, але також пов'язує їх зі стандартами безпеки. Сучасні гібридні атаки на рівні державних систем не обмежуються пошкодженням окремих машин або порушенням роботи корпоративних систем. Вони націлені на інфраструктуру, важливу для економіки, національної оборони та повсякденного життя [26, 27].

В іншому дослідженні була запропонована класифікація атак, що складається з чотирьох вимірів: вектора атаки, основної мети, вразливостей та корисних навантажень [28]. Ця класифікація дозволяє враховувати як функціонування мережі, так і аспекти, пов'язані з кібератаками. Автори також представили методологію оцінювання ризиків інформаційної безпеки, що пов'язує активи, вразливості, загрози та елементи управління. Цей підхід використовує послідовність матриць для відображення кореляції між різними елементами при аналізі ризику, допомагаючи пріоритетизувати елементи управління на основі активів організації [29]. Додатково, обговорювалися та класифікувалися кіберінциденти залежно від сектору, джерела та впливу інцидентів в [30]. Це дослідження є прикладом того, як процес збору інформації про кіберінциденти може бути використано для розуміння загроз та покращення організаційної готовності до кібератак.

Мета роботи та завдання дослідження

Метою роботи є розробка методу захисту мережевих джерел інформації у кібефізичному просторі на ґрунті багаторівневої семіотичної моделі.

Для вирішення поставленої мети розглянуто такі завдання: проаналізувати різносторонню подачу інформації; запропонувати семіотичний підхід, який дозволяє більш глибоко аналізувати взаємодію між людиною та технологіями; розробити модель кіберпростору з методом оцінки рівня безпеки для кожного з рівнів розробленої моделі та запропоновано інтегральний показник потенційних загроз для власників мережевих інформаційних ресурсів; провести верифікацію розробленої моделі.

© Захаржевський, А. Г., Толкачов, М. Ю., Дженюк, Н. В., Погасій, С. С., & Глухов, С. І. (2024). Метод захисту інформаційних ресурсів на основі семіотичної моделі кіберпростору. Сучасний захист інформації, 1(57), 57–68. https://doi.org/10.31673/2409-7292.2024.010007.

Розробка моделі захисту інформації у кіберпросторі

Інформація, що циркулює у мережах кіберпростору, є особливим видом комунікабельних знаків, які використовують у спілкуванні для створення та обміну програмними, протокольними і сформованими службовими повідомленнями. При цьому частина інформаційного трафіку є засобом взаємодії документів створених різною мовою, що призначені для опанування людиною, а не комп'ютером. Для усвідомленої обробки даних слід застосовувати інтелектуальне керування для уточнення і розшифрування змісту інформації. Семіотика вирішує питання формування смислу. Тому її покладено на основу для розуміння понять інформації, смислу, пізнання, комунікації та їх адаптації до завдань оцінки кіберзахисту мережі, складовими якої є змістовно пов'язані данні. При цьому, застосовуючи метод розбиття загальної моделі (Рис.1) на відповідні рівні семіотики, отримуємо адаптовану модель для різних контекстів (Рис.2).

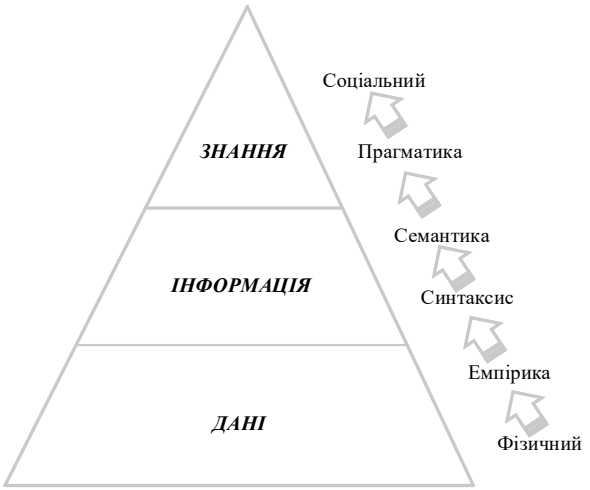

Рис 2. Семіотичні рівні та ієрархія дані-інформація-знання

Рівні семіотики дозволяють розрізнити різні аспекти якості даних, для вирішення яких слід застосовувати спеціальні навички [31, 32]. Вони дають змогу розширити аналіз за межі традиційних технічних аспектів та включити складовими оцінки сприйняття, контекст та соціальні наслідки загроз. Багаторівневий підхід ґрунтується на фізичному, емпіричному, синтаксичному, семантичному, прагматичному та соціальному рівнях [20, 33, 34]. Такий підхід дозволяє враховувати різні аспекти загроз та їх взаємодію (Рис. 3). У якості ключових метрик для оцінки використовують рейтинг вразливостей (CVE – Common Vulnerabilities and Exposures) та індикатор компроментації (IOC – Indicators of Compromise).

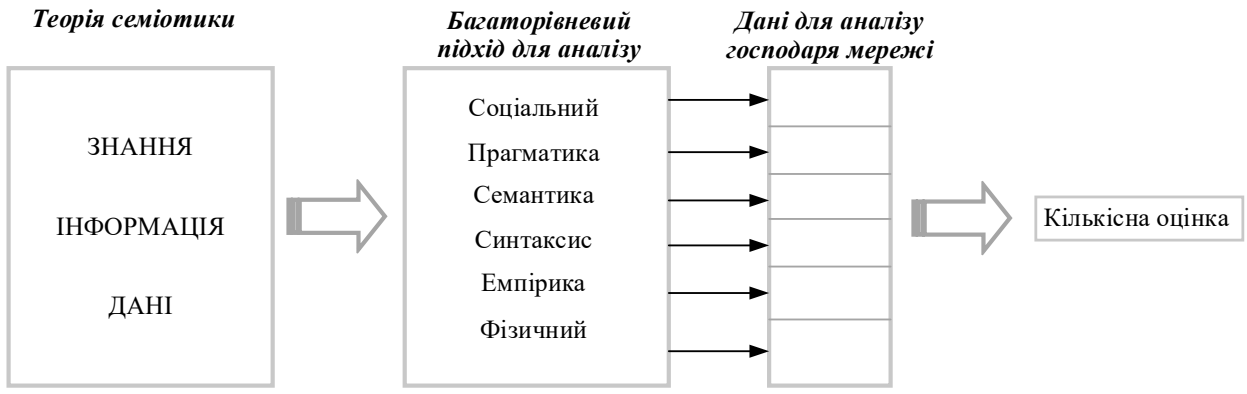

Рис.3. Багаторівневий підхід

© Захаржевський, А. Г., Толкачов, М. Ю., Дженюк, Н. В., Погасій, С. С., & Глухов, С. І. (2024). Метод захисту інформаційних ресурсів на основі семіотичної моделі кіберпростору. Сучасний захист інформації, 1(57), 57–68. https://doi.org/10.31673/2409-7292.2024.010007.

До індикаторів компрометації IOC відносять підказки або докази того, що мережа або система була зламана. Їх визначають незвичайна поведінка мережевого трафіку, несподіване встановлення програмного забезпечення, входи користувачів із ненормальних місць та велика кількість запитів до одного й того ж ресурсу. Ці індикатори сигналізують про підозрілу активність у мережі та відхилення у нормальній діяльності в моделях поведінки. Кількісно їх представляють у відсотках змін у об'ємі трафіка. Причому, їх позитивне значення вказує на збільшення підозрілої чи шкідливої активності.

CVE – це система реєстрації і класифікації відомих вразливостей у програмному забезпеченні та обладнанні. Це стандартний метод для загального позначення вразливостей та їх розповсюдження у базах даних безпеки. Вона надає унікальний ідентифікатор для кожної вразливості, що дозволяє обмінюватися інформацією про них. Числові показники вразливостей зазвичай знаходяться у межах 0 – 10 одиниць. Так низька вразливість знаходиться у межах 0 … 3,9; середня – 4,0 … 6,9; висока – 7 … 8,9; критична – 9,0 … 10. Ці оцінки допомагають визначити пріоритети під час усунення вразливостей.

Для оцінки різних аспектів безпеки запропоновано шестирівневу модель.

Фізичний рівень (CVE Rating) використовує данні про рейтинг можливостей, який базується на реальних кількісних вимірюваних вразливостей. Кількість та рівень вразливостей CVE, які впливають на фізичні компоненти, визначає наступне співвідношення:

$$F_{physical}(CVE) = \sum_{i=1}^{n} w_i \cdot CVE_i, \quad (1)$$

де: CVE_i – рівень ризику i-ї вразливості;

w_i – вага, що відображає рівень вразливості.

Емпіричний рівень (Normalized IOC) визначає виміри у мережі через індикатори компрометації, які вказують на наявність шкідливої активності. Параметром є частота визначення IOC, що визначає наступне співвідношення:

$$P_{IOC}(N) = e^{-\lambda \cdot \sum_{j=1}^{n} w_j \cdot IOC_j}, \quad (2)$$

де: IOC_j – кількість виявлень j-го IOC;

$P_{IOC}(N)$ – ймовірність виявлення шкідливої активності в мережі;

n – загальна кількість різних видів IOC;

w_j – ваговий коефіцієнт для j-го виду IOC, що відображає його значимість або вплив на безпеку мережі;

λ – коефіцієнт, що показує загальний вплив частоти визначення IOC на надійність системи.

Синтаксичний рівень визначає кількість і рівень впливу синтаксичних похибок, що пов'язані з IOC. Його рівень визначає наступне співвідношення:

$$C_{syntax}(IOC) = \frac{1}{1+e^{\left(b_0+\sum_{k=1}^{p} b_k \cdot IOC_k\right)}} \quad , \quad (3)$$

де: IOC_k – вплив k-го IOC на синтаксичну структуру;

b_k – ваговий коефіцієнт, що віддзеркалює ступінь впливу.

Семантичний рівень визначає загальну кількість і важливість системи реєстрації вразливостей у програмному забезпеченні та обладнанні. Кількісну характеристику цього рівня визначає наступне співвідношення.

$$V_{semantic}(CVE) = \sum_{i=1}^{q} v_i \cdot CVE_i \quad , \quad (4)$$

де: CVE_i – рівень важливості i-ї вразливості IOC на синтаксичну структуру;

v_i – коефіцієнт впливу на семантичну валідність.

Прагматичний рівень визначає ефективність засобів протидії атаці або зламу мережі чи системи. Його рівень визначає наступне співвідношення:

$$U_{pragmatic}(IOC_{counter}) = \int_0^R p(r)dr \ , \tag{5}$$

де: $IOC_{counter}$ – засоби протидії;

$p(r)$ – імовірність вдалої протидії в залежності від ресурсів r.

Соціальний рівень визначає узгодженість моделі та забезпеченні соціального консенсусу під час її використання. Його рівень визначає наступне співвідношення:

$$S_{social}(d,r) = 1 - \sum_{i=1}^{k} \delta(d_i, r_i) \ , \tag{6}$$

де: d – пропозиції системи аналізу по соціальному контенту;

r – відгуки кінцевих хостів користувачів;

δ – функція розходження між пропозиціями та відгуками;

k – кількість розглянутих пропозицій та відгуків.

При цьому слід зазначити, що кількісні значення запропонованих рівнів моделі вимірюють у відносних одиницях, які знаходяться у межах 0 … 10 та визначають на ґрунті експертного аналізу даних.

Розробка інтегрального показника захищеності мережевих ресурсів

З метою визначення загального стану кібербезпеки запропоновано використовувати інтегральний показник, що враховує зважене середнє показників усіх запропонованих рівнів семіотичної моделі кіберпростору.

$$\begin{aligned} Q_{cybersecurity} = {} & \frac{w_{physical} \cdot F_{physical}(CVE) + w_{empirical} \cdot P_{empirical}(IOC) +}{w_{physical} + w_{empirical} + w_{syntax} + w_{semantic} + w_{pragmatic} + w_{perception} + w_{social}} \\ & \frac{+w_{syntax} \cdot C_{syntax}(IOC) + w_{semantic} \cdot V_{semantic}(CVE) +}{w_{physical} + w_{empirical} + w_{syntax} + w_{semantic} + w_{pragmatic} + w_{perception} + w_{social}} \\ & + \frac{w_{pragmatic} \cdot U_{pragmatic}(IOC_{counter}) + w_{perception} \cdot P_{perception}(CVE, IOC) +}{w_{physical} + w_{empirical} + w_{syntax} + w_{semantic} + w_{pragmatic} + w_{perception} + w_{social}} \\ & + \frac{w_{social} \cdot S_{social}(IOC_{resp}, CVE_{resp})}{w_{physical} + w_{empirical} + w_{syntax} + w_{semantic} + w_{pragmatic} + w_{perception} + w_{social}} \end{aligned} \tag{7}$$

де: $Q_{cybersecurity}$ – інтегрований показник якості кібербезпеки;

$w_{physical}$, $w_{empirical}$, w_{syntax}, $w_{semantic}$, $w_{pragmatic}$, $w_{perception}$, w_{social} – ваги відповідних рівнів;

$F_{physical}(CVE)$, $P_{empirical}(IOC)$, $C_{syntax}(IOC)$, $V_{semantic}(CVE)$, $U_{pragmatic}(IOC_{counter})$, $P_{perception}(CVE, IOC)$, $S_{social}(d,r)$ – показники рівнів.

Таким чином, впровадження інтегрального показника захисту інформаційного простору $Q_{cybersecurity}$ дає загальну метрику для оцінки та порівняння рівня кібербезпеки різних власників.

Верифікація моделі захисту інформації у кіберпросторі

Верифікацію моделі для оцінки рівня кібербезпеки власників мережі (Рис. 4) зроблено на основі даних звіту Cisco Talos за 2023 р. про загальнодоступні вразливості, який містить

© Захаржевський, А. Г., Толкачов, М. Ю., Дженюк, Н. В., Погасій, С. С., & Глухов, С. І. (2024). Метод захисту інформаційних ресурсів на основі семіотичної моделі кіберпростору. Сучасний захист інформації, 1(57), 57–68. https://doi.org/10.31673/2409-7292.2024.010007.

172 загальнодоступні вразливості. Вибірку зроблено по електронній пошті та найбільш активним власникам мереж.

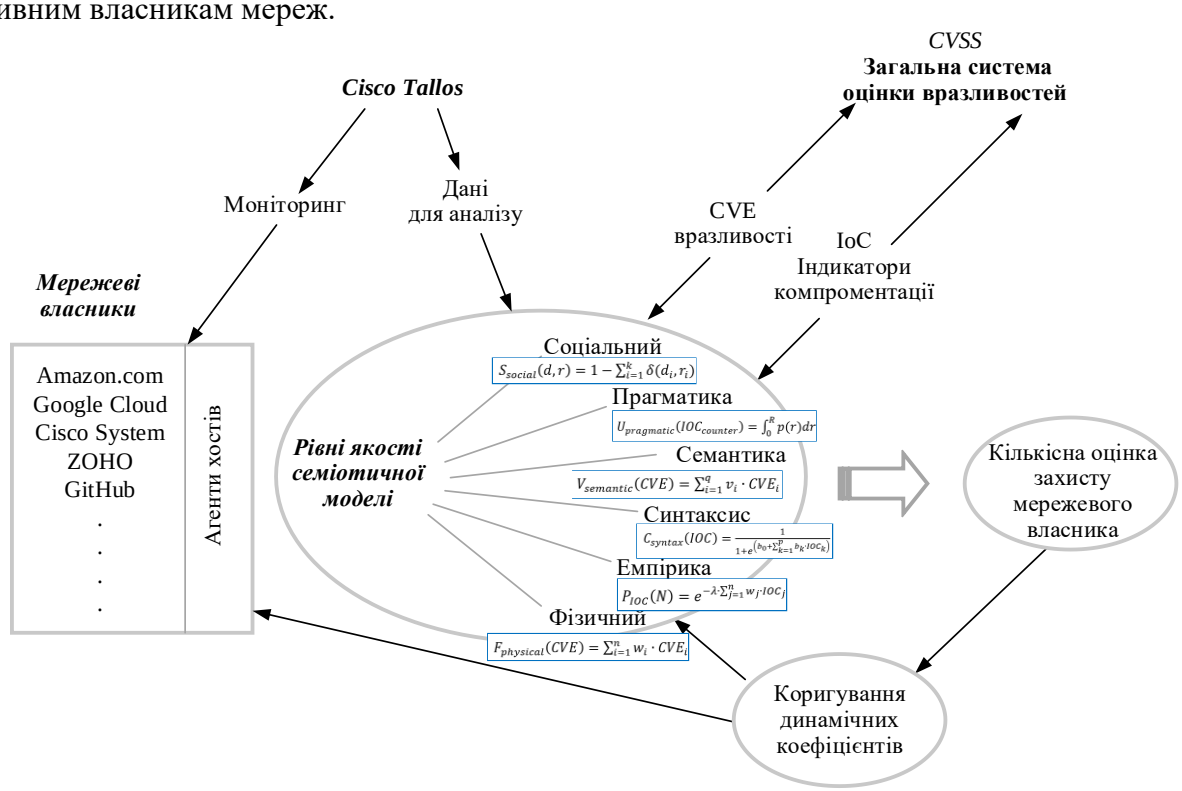

Рис.4. Модель для оцінки рівня кібербезпеки власників мережі.

Для кожного власника мережі було використано спрощену версію інтегрального показника захищеності мережевих ресурсів, за якою значення ваги усіх рівнів вважають однаковими, а значення кожного рівня пропорційна його рейтингу загроз CVE та відсотковій зміні IOC. Таким чином інтегральний показник захисту інформаційного простору набирає наступного вигляду:

$$Q_{cybersecurity} = \frac{1}{7}(CVE + norm(IOC) + norm(IOC) + CVE + norm(IOC) + \\ +(CVE + norm(IOC)) + norm(IOC)) \quad (8)$$

де: *norm (IOC)* являє собою нормалізоване значення IOC, яке змінюється у межах 0…10.

Нормалізацію здійснюють шляхом пропорційного відображення різниці між поточним значенням та мінімумом із співставленням її результату діапазону 0…10. Верифікацію моделі зроблено на 20 власниках мереж та зведені до таблиці 1.

У кожній стрічці таблиці наведено аналіз рівня кібербезпеки для кожного окремого власника мережі. Також туди включено значення рейтингу загроз CVE, відсоткові зміни індикаторів компрометації IOC, нормалізований IOC, показники по кожному з рівнів та загальний інтегрований показник якості кібербезпеки.

У таблиці 1 наведені данні мають наступні значення та розмірність.

1. Network Owner містить найменування власників мережевих ресурсів. Це текстові данні, які являють собою найменування компаній або організацій.

2. CVE Rating (Common Vulnerabilities and Exposures – CVE) містить рейтинг вразливостей для кожного з власника мережевих ресурсів. Ці значення відображають рівень вразливостей у відповідності з загальноприйнятою шкалою CVE, причому більш високі значення відображають більш високий рівень ризику або вразливості.

3. IOC Change (%) (Indicators of Compromise – IOC) відображає відсоткові зміни індикаторів компрометації для кожного власника мережевих ресурсів. Збільшення значень вказує на збільшення підозрілої або шкідливої активності.

Таблиця 1

Аналіз рівня кібербезпеки окремого власника мережі

Network Owner	CVE Rating	Normalized IOC	Physical Level	Empirical Level	Syntactic Level	Semantic Level	Pragmatic Level	Social Level	Cybersecurity Quality Score
Conquest Telecomunicacoes Ltda	7.8	1.236	7.8	1.236	4.518	7.8	1.236	4.518	4.05
Amazon.com	7.5	1.72	7.5	0.0172	3.7586	7.5	0.0172	3.7586	3.22
Google Cloud	7.4	1	7.4	0.01	3.705	7.4	0.01	3.705	3.18
Cisco Systems Ironport Division	7.3	2.64	7.3	0.0264	3.6632	7.3	0.0264	3.6632	3.14
Amazon.com	7.3	2.76	7.3	0.0276	3.6638	7.3	0.0276	3.6638	3.14
Servicenow	7.2	1.56	7.2	0.0156	3.6078	7.2	0.0156	3.6078	3.09
Cisco Systems Ironport Division	7.2	1.88	7.2	0.0188	3.6094	7.2	0.0188	3.6094	3.1
Telecom Italia Business	7.2	5.2	7.2	0.0052	3.6026	7.2	0.0052	3.6026	3.09
HostUS	7.2	1.6	7.2	0.016	3.608	7.2	0.016	3.608	3.09
Salesforce.com Inc. (SALESF-3)	7.1	1.6	7.1	0.016	3.558	7.1	0.016	3.558	3.05
Dedibox SAS	7.1	6.8	7.1	0.0068	3.5534	7.1	0.0068	3.5534	3.05
CyberU	7.1	10.0	7.1	10.0	8.55	7.1	10.0	8.55	8.76
ZOHO	7.1	0.0684	7.1	0.0684	3.5842	7.1	0.0684	3.5842	3.08
Proofpoint Inc. USA	7.1	10.0	7.1	10.0	8.55	7.1	10.0	8.55	8.76
Proofpoint Inc. Europe	7.1	0.0312	7.1	0.0312	3.5656	7.1	0.0312	3.5656	3.06
GitHub Campus	7.0	0.0208	7.0	0.0208	3.5104	7.0	0.0208	3.5104	3.01
GitHub Eportal	7.0	0.016	7.0	0.016	3.508	7.0	0.016	3.508	3.01
Accelya World SLU	7.0	0.0156	7.0	0.0156	3.5078	7.0	0.0156	3.5078	3.01
Google	7.0	0.0148	7.0	0.0148	3.5074	7.0	0.0148	3.5074	3.01
Verizon Internet Services	7.0	0.0148	7.0	0.0148	3.5074	7.0	0.0148	3.5074	3.01

4. Normalized IOC – це нормалізовані значення IOC, що приведені до єдиної шкали від 0…10, де 0 відповідає відсутності змін, а 10 – максимальним змінам.

5. *Physical Level* використовує таку ж саму шкалу, що і CVE Rating, оскільки вона напряму відповідає цьому показнику.

6. *Empirical Level* здійснює оцінку емпіричного рівня безпеки, який відповідає нормалізованому значення IOC та використовує шкалу від 0 до 10, відображаючи рівень виявлених IOC.

7. *Syntactic Level* відображає синтаксичний рівень безпеки, який включає як фізичні вразливості, так і визначені індикатори компрометації, значення яких знаходиться у межах від 0 до 10.

8. *Semantic Level* відображає глибину розуміння та інтерпретації загроз. Значення коефіцієнтів знаходиться у межах від 0 до 10.

© Захаржевський, А. Г., Толкачов, М. Ю., Дженюк, Н. В., Погасій, С. С., & Глухов, С. І. (2024). Метод захисту інформаційних ресурсів на основі семіотичної моделі кіберпростору. Сучасний захист інформації, 1(57), 57–68. https://doi.org/10.31673/2409-7292.2024.010007.

9. *Pragmatic Level* пов’язаний із практичними аспектами визначення та реагування на загрози, використовуючи шкалу від 0 до 10.

10. Social Level розраховано як середнє значення між CVE та нормалізованим IOC. Він відображає вплив загроз на соціальні аспекти організації, використовуючи шкалу від 0 до 10.

11. Cybersecurity Quality Score – це інтегрований показник якості, що розрахований як середнє усіх рівневих оцінок. Це комплексна метрика, яка оцінює загальний стан кібербезпеки власника мережевих ресурсів. Рівень визначає шкала від 0 до 10, що забезпечує уніфікований засіб оцінки загального стану кібербезпеки.

Для моделювання використовувався застосунок на мові Python 3.x через його широку підтримку та багату екосистему бібліотек. У процесі моделювання використовувалися такі бібліотеки:

Pandas: Ця бібліотека надає зручні структури даних та функції для аналізу та маніпуляції даними. У цій програмі вона використовувалася для створення та обробки DataFrame, який містив дані про мережних власників, рейтинги загроз та IOC.

NumPy: Pandas тісно інтегрований з NumPy і багато операцій з даними використовують можливості NumPy для оптимізації обчислень.

SciPy: Для складних математичних чи статистичних обчислень бібліотека SciPy пропонує додаткові інструменти для оптимізації, вирішення рівнянь та іншого.

Обговорення результатів верифікації моделі.

Отримані результати верифікації моделі для оцінки рівня кібербезпеки власників мережі дозволяють сформувати об'єктивну оцінку рівня кіберзахисту 20 реальних власників інформаційних ресурсів із застосуванням семіотичного підходу (Табл. 1). Крім цього, аналіз показує, що ефективність системи кібербезпеки залежить не лише від технічних аспектів, але й від того, як інформація інтерпретується, використовується та впливає на соціальні аспекти. Запропонований підхід з використанням розділення змішаного контенту інформації на взаємопов’язані рівні дозволяє підвищити рівень об'єктивності оцінки комплексування цільових (змішаних) атак із комплексними загрозами.

Семіотичний підхід підкреслює важливість залучення людини в процеси кібербезпеки, включаючи розуміння та інтерпретацію інформації, що є критично важливим для ефективного управління ризиками. Потреба у комплексному аналізі різних рівнів інформації підтверджує, що для ефективного управління кібербезпекою необхідно інтегрувати технічні, семантичні, прагматичні та соціальні аспекти.

Сформований математичний апарат дозволяє враховувати формування інтегрованого підходу до оцінки кібербезпеки, що включає різні рівні: від фізичних аспектів (CVE Rating) до більш абстрактних, таких як вплив на соціальні аспекти (Social Level). Різні рівні оцінки в таблиці відображають, як технічні аспекти безпеки (наприклад, фізичний рівень) взаємодіють з більш людськими аспектами (наприклад, соціальний рівень). Це вказує на те, що ефективне керування кібербезпекою вимагає уваги до обох аспектів.

Поділ на різні рівні дозволяє глибше аналізувати як технічні, так і контекстуальні аспекти кібербезпеки. Наприклад, показник CVE Rating (фізичний рівень) не завжди корелює з загальним рівнем кібербезпеки (Cybersecurity Quality Score), що вказує на необхідність розгляду інших рівнів для повного розуміння стану безпеки.

Ці рівні не існують ізольовано, а взаємодіють між собою. Наприклад, високий рівень вразливостей (CVE Rating) без ефективного моніторингу індикаторів компрометації (Normalized IOC) може призвести до недооцінки реальних загроз. Жоден одиничний показник не може повністю оцінити стан кібербезпеки. Для повного аналізу стану кібербезпеки організацій потрібно розглядати не лише кількісні, але й якісні аспекти інформації, що включає її структуру, контекст та взаємозв'язки на різних рівнях. Інтегроване розуміння різних рівнів забезпечує більш точну оцінку загроз та вразливостей.

© Захаржевський, А. Г., Толкачов, М. Ю., Дженюк, Н. В., Погасій, С. С., & Глухов, С. І. (2024). Метод захисту інформаційних ресурсів на основі семіотичної моделі кіберпростору. Сучасний захист інформації, 1(57), 57–68. https://doi.org/10.31673/2409-7292.2024.010007.

Запропонований підхід у майбутньому сприятиме поліпшенню контролю та управління в галузі кібербезпеки, забезпечуючи розгляд різних аспектів, включаючи соціальні фактори. Крім цього, він дозволяє більш ефективно впроваджувати політики безпеки, що враховують різноманітність бізнес-процесів, корпоративну культуру та регуляторні вимоги. У підсумку, семіотичний підхід забезпечує більш глибоке розуміння складності кіберпростору та дозволяє розробляти більш ефективні, цілісні та адаптивні стратегії захисту інформаційних ресурсів у різних сферах ІТ-технологій.

Висновки

За результатами аналізу існуючих методів захисту інформаційних ресурсів у кіберпросторі з метою підвищення рівня безпеки мережевих систем запропоновано застосування семіотичної моделі. Семіотичний підхід дозволяє більш глибоко аналізувати взаємодію між людиною та технологіями, що особливо важливе для розуміння та керування складними системами інформаційної безпеки. Показано, що складна, різностороння подача інформації у мережі вимагає комплексного підходу із розділенням змішаного контенту інформації на взаємопов'язані рівні. Визначено якості семіотики для оцінки рівня кіберзахисту та потенційних загроз для власників інформаційних ресурсів, які є складовими розробленої шостирівневої моделі та розроблена оцінка рівня безпеки для кожного з рівнів. Розроблено інтегральний показник захищеності мережевих ресурсів та здійснено оцінку рівня кіберзахисту 20 реальних власників інформаційних ресурсів. Проведено верифікацію розробленої моделі. Таким чином розроблена модель дає змогу покращити моніторинг та керування кібербезпекою шляхом врахування різноманітних факторів, включно з урахуванням соціальних та перцептивних аспектів, що є ключовим фактором для розробки ефективних стратегій захисту інформаційних ресурсів у кіберпросторі.

Перелік посилань

1. Broadband Search: "Key Internet Statistics in 2023 (Including Mobile)"., https://datareportal.com/reports/digital-2023-global-overview-report.

2. A Method of Protecting Information in Cyberphysical Space / N. Dzheniuk, S. Yevseiev, B. Lazurenko, O. Serkov, O. Kasilov // Advanced Information Systems. – 2023. – Volume 7, Number 4. – P. 80-85 **doi:** https://doi.org/10.20998/2522-9052.2023.4.11.

3. Спосіб генерації широкосмугового імпульсного сигналу та антена для його реалізації / Серков О.А., Бреславець В.С. Перова І.Г. Толкачов М.Ю. Чурюмов Г.І. // Патент України на винахід № 120554 С2, МПК H01Q 21/06, H01Q 13/08, Опубл. 26.12.2019, Бюл. № 24, заявка № а 2018 03104; від 26.03.2018.

4. The Order of Formation of Information Signals in IIoT /Alla Jammine, Serkov Alexandr, Bogdan Lazurenko, Nait-Abdesselam Farid // IJCSNS International Journal of Computer Science and Network Security, VOL.23 No.3, pp. 139-143. http://paper.ijcsns.org/07_book/202303/20230314.pdf.

5. Standard ISO/IEC 27032:2023. Cybersecurity. Guidelines for Internet security, (2023). Released: 28.06.2023, available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-2:v1:en.

6. ITU-T X.1205:2008. Cybersecurity overview, (2008), Geneva: ITU-T, 2008. 162 p., available at: www.itu.int/ITU-T.

7. Laptiev, O., Biehun, A., Hohoniants, S., Lisnevskyi, R., Pravdyvyi, A., Lazarenko, S. Method of detecting signals of means of covert obtaining of information on the basis of approximation of T-spectrum. The Intelligent Control System for infocommunication networks. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 10, Oktober 2020, pp. 6835-6841.

8. Burton-Jones, A., Storey, V.C., Sugumaran, V. and Ahluwalia, P. A semiotic metrics suite for assessing the quality of ontologies. Data & Knowledge Engineering. 2005; 55: 84-102.

9. NIST Special Publication 1270 proposes a framework for identifying and managing bias in artificial intelligence. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270-draft.pdf .

10. Peirce at Signo: Theoretical Semiotics on the Web, Louis Hébert, director, supported by U. of Québec. Theory, application, exercises of Peirce's Semiotics and Esthetics. English, French.

11. Brier, S. Cybersemiotics: A New Foundation for a Transdisciplinary Theory of Consciousness, Cognition, Meaning and Communication // Biosemiotics. – Dordrecht: Springer Netherlands, 2012-11-20. – С. 97 – 126. –ISBN 9789400754188, 9789400754195.

12. Brier, S. Cybersemiotics: Why Information Is Not Enough!. – University of Toronto Press, 2008. – 498 с. – ISBN 0802092209. – ISBN 9780802092205.

13. Cobley, P. Cybersemiotics and Human Modelling (англ.) // Entropy. – 2010/9. – Vol. 12, iss. 9. – P. 2045–2066. – doi:10.3390/e12092045.

14. Goldstein, J. A., Sastry, G., Musser, M., DiResta, R., Gentzel, M., and Sedova, K. 'Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations'. Georgetown University's Center for Security and Emerging Technology, OpenAI, Stanford Internet Observatory, January 2023. https://cdn.openai.com/papers/forecasting-misuse.pdf.

15. NIST AI 100-1 Artificial Intelligence Risk Management Framework (AI RMF 1.0) (January 2023). https://doi.org/10.6028/NIST.AI.100-1.

16. Wang, L. Sun, and Zhu, H., «Defining Social Engineering in Cybersecurity», IEEE Access, vol. 8, стр. 85094–85115, 2020, doi: 10.1109/ access.2020.2992807.

17. Наконечний, В., Лаптєв, О., Погасій, С., Лазаренко, С., Мартинюк, Г. Відбір джерел з неправдивою інформацію методом бджолиної колонії. Наукоємні технології. Інформаційні технології, кібербезпека. Том 52 № 4 (2021) стр.330-337. DOI: https://doi.org/10.18372/2310-5461.52.16379.

18. Lindland, O.I., Sindre, G. and Solvberg, A. Understanding quality in conceptual modeling. Software, IEEE. 1994; 11: 42-9.

19. Price, R. and Shanks, G. A semiotic information quality framework: development and comparative analysis. Journal of Information Technology. 2005; 20: 88-102.

20. Tejay, G., Dhillon, G. and Chin, A.G. Data quality dimensions for information systems security: A theoretical exposition. Security Management, Integrity, and Internal Control in Information Systems. Springer, 2006, p. 21-39].

21. Huang, H. (2018). Big data to knowledge – Harnessing semiotic relationships of data quality and skills in genome curation work. Journal of Information Science, 44(6), 785-801. https://doi.org/10.1177/0165551517748291.

22. Lester, J. and Wllace, C. Fundamentals of information studies: Understanding information and its environment. Neal-Schuman Publishers, Inc., 2007.

23. C´ardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., and Sastry, S. "Challenges for securing cyber physical systems". In Workshop on future directions in cyber-physical systems security, vol. 5, 2009.

24. Milov, O., Korol, O., and Khvostenko, V. "Development of the Classification of the Cyber Security Agents Bounded Rationality." Системи управління, навігації та зв'язку. Збірник наукових праць 4, no. 56 (September 11, 2019): 82–90. http://dx.doi.org/10.26906/sunz.2019.4.082.

25. Evseev, S. (2017), "Model narushytelia prav dostupa v avtomatyzyrovannoi bankovskoi systeme na osnovesynerhetycheskoho podkhoda" [A model of access rights violator in an automated banking system based on a synergistic approach], Informational security, No. 2(26), pp. 110-120.

26. Dell security annual threat report. https://software.dell.com/docs/2015-dell-security-annual-threat-report-white-paper-15657.pdf.

27. Hansman, S. and Hunt, R. (2005) 'A taxonomy of network and computer attacks', Computers and Security, Vol. 24, No. 1, pp.31-43 [online] http://goo.gl/hJBy5h.

28. Goel, S. and Chen, V. (2005) 'Information security risk analysis – a matrix-based approach', Proceedings of the Information Resource Management Association (IRMA) International Conference, San Diego, CA, pp.1-9.

29. Kjaerland, M. (2006) 'A taxonomy and comparison of computer security incidents from the commercial and government sectors', Computers and Security, Vol. 25, No. 7, pp.522-538 [online] http://linkinghub.elsevier.com/retrieve/pii/S0167404806001234. (accessed 10 May 2020).].

30. Stamper, R. The semiotic framework for information systems research. Information systems research: Contemporary approaches and emergent traditions. 1991: 515-28.

31. Boell, S.K. and Cecez-Kecmanovic, D. Attributes of Information. Americas Conference on Information System. Lima, Peru: AIS eLibrary, 2010.

32. Yevseiev, S., Milov, O., Dzheniuk, N., Tolkachov, M., Voitko, T., Prygara, M., Voropay, N., Shpak, O., Volkov, A., Lezik, O. (2023). Development of a multi-loop security system of information interactions in socio-cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 5 (9 (125)), p. 53–74. doi: https://doi.org/10.15587/1729-4061.2023.289467.

33. Yevseiev, S., Tolkachov, M., Shetty, D., Khvostenko, V., Strelnikova, A., Milevskyi, S., & Golovashych, S. (2023). The concept of building security of the network with elements of the semiotic approach. ScienceRise, (1), 24-34. https://doi.org/10.21303/2313-8416.2023.002828.

34. Беркман, Л.Н., Барабаш, О.В., Ткаченко, О.М., Мусієнко, А.П., Лаптєв, О.А., Свинчук, О.В. Інтелектуальна система управління для інфокомунікаційних мереж. Системи управління навігації і зв'язку. Том 3. №69. 2022. С 54–59. https://doi.org/10.26906/SUNZ.2022.3.

Надійшла 25.01.2024