© Skurativskyi A. Cybersecurity requirements management method for software implementation in business // *Ukrainian Scientific Journal of Information Security, 2025, vol. 31, issue 3, pp. 135-141.* ©

DOI: 10.18372/2225-5036.31.21158

МЕТОД УПРАВЛІННЯ ВИМОГАМИ КІБЕРБЕЗПЕКИ ПРИ ВПРОВАДЖЕННІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ У БІЗНЕСІ

Анатолій Скуратівський

Державний університет «Київський авіаційний інститут», м. Київ, Україна

СКУРАТІВСЬКИЙ Анатолій Анатолійович
Рік та місце народження: 1983 р., м. Київ
Освіта: Національний авіаційний університет
Посада: аспірант
Наукові інтереси: IT-системи, DevSecOps, кібербезпека, програмне забезпечення
Публікації: більше 10 наукових публікацій
Email: a.skurativskyi@gmail.com
ORCID ID: 0009-0000-0566-2394

Анотація. *В статті проаналізовано сучасні стандарти та підходи до управління вимогами кібербезпеки і визначено їхні обмеження у статичних моделях. Запропоновано метод динамічного управління вимогами кібербезпеки, який передбачає циклічний процес ініціалізації, моніторингу, переоцінювання та оптимізації вимог із урахуванням змін середовища й загроз. Метод спрямований на підвищення ефективності захисту, раціональне використання ресурсів і забезпечення балансу між рівнем безпеки та функціональними можливостями системи.*

Ключові слова: вимоги, кібербезпека, метод, програмне забезпечення, управління вимогами кібербезпеки.

Вступ. Управління вимогами кібербезпеки при впровадженні ПЗ суттєво залежить від галузевої специфіки, характеру бізнес-процесів, регуляторних вимог, допустимого рівня ризику та потенційних наслідків інцидентів. На відміну від універсальних підходів, галузево (секторально) орієнтоване управління вимогами кібербезпеки передбачає адаптацію методів пріоритезації, оцінювання ризиків і розподілу ресурсів відповідно до контексту застосування ПЗ. У фінансових установах вимоги кібербезпеки мають високий пріоритет через критичність конфіденційності, цілісності та доступності даних. Основна увага приділяється управлінню доступом, ідентифікації та автентифікації, моніторингу транзакцій і аудиту дій користувачів. Для цієї галузі характерні жорсткі регуляторні обмеження та низька толерантність до ризику, що зумовлює домінування превентивних контролів і високі витрати на виконання вимог кібербезпеки. У промислових і інфраструктурних системах управління вимогами кібербезпеки орієнтоване насамперед на забезпечення безперервності та безпеки технологічних процесів. Тут пріоритет надається вимогам стійкості, відновлення після інцидентів та ізоляції критичних компонентів. Особливістю є необхідність узгодження вимог кібербезпеки з вимогами функціональної безпеки та обмеженими можливостями оновлення ПЗ.

Для корпоративних бізнес-систем управління вимогами кібербезпеки здійснюється в умовах обмеженого бюджету та швидких циклів розробки. Пріоритети вимог часто змінюються залежно від бізнес-цілей, ринкових умов і моделей загроз. У таких системах важливу роль відіграє баланс між витратами на безпеку та допустимим рівнем ризику, що потребує формалізованих методів оптимізації та підтримки прийняття рішень. У хмарних середовищах управління вимогами кібербезпеки ускладнюється розподіленою архітектурою, динамічним масштабуванням та розподілом відповідальності між провайдером і замовником. Пріоритетними стають вимоги до контролю доступу, ізоляції середовищ, моніторингу та відповідності стандартам. Характерною особливістю є необхідність постійного перегляду вимог у відповідь на зміну конфігурацій і моделей використання сервісів.

Аналіз показує, що універсальне управління вимогами кібербезпеки без урахування галузевого контексту є неефективним. Різні галузі вимагають різних стратегій пріоритезації вимог, рівнів деталізації контролів і підходів до оцінювання ризиків. Це обґрунтовує доцільність використання адаптивних методів управління вимогами кібербезпеки, які здатні враховувати галузеві особливості, обмеження ресурсів і динаміку загроз.

Різні типи середовищ потребують різних стратегій пріоритезації вимог, рівнів автоматизації та методів оцінювання ризиків. Це обґрунтовує доцільність використання адаптивних і формалізованих моделей управління вимогами кібербезпеки, здатних динамічно враховувати зміну умов функціонування ПЗ. Отже, середовище орієнтоване управління вимогами кібербезпеки може передбачати такі типи середовищ за основу:

У локальних середовищах управління вимогами кібербезпеки ґрунтується на повному контролі інфраструктури з боку організації. Пріоритетними є вимоги до управління доступом, сегментації мережі, резервного копіювання та аудиту дій користувачів. Характерною особливістю є відносна стабільність архітектури, що дозволяє застосовувати статичні (не динамічні) або напівдинамічні моделі пріоритезації вимог. Разом із тим, значні капітальні витрати та обмежені ресурси зумовлюють необхідність оптимізації виконання вимог кібербезпеки з урахуванням бюджету.

У хмарних середовищах управління вимогами кібербезпеки ускладнюється розподіленою природою ресурсів, динамічним масштабуванням і моделлю спільної відповідальності між постачальником послуг та

замовником. Основну увагу приділяють вимогам до ідентифікації та автентифікації, контролю доступу, ізоляції середовищ, моніторингу та відповідності стандартам. Пріоритети вимог у таких середовищах змінюються в часі, що зумовлює необхідність динамічного управління вимогами та регулярного перегляду їхньої важливості.

Гібридні середовища поєднують локальні та хмарні компоненти, що створює додаткову складність для управління вимогами кібербезпеки. Особливістю є необхідність узгодження вимог між різними доменами безпеки, забезпечення захищених каналів обміну даними та єдиної політики управління доступом. У таких умовах зростає роль інтегрованих моделей оцінювання ризиків, здатних враховувати взаємозалежності між компонентами системи та потенційні каскадні наслідки інцидентів.

У сервіс-орієнтованих і мікросервісних архітектурах управління вимогами кібербезпеки здійснюється в умовах високої динамічності та великої кількості взаємодіючих компонентів. Пріоритетними стають вимоги до безпеки API, автентифікації між сервісами, контролю конфігурацій і моніторингу взаємодій. Особливістю є необхідність локальної пріоритезації вимог для окремих сервісів із подальшим узгодженням на рівні всієї системи.

Для розподілених середовищ, що включають віддалених користувачів, філії або мобільні компоненти, управління вимогами кібербезпеки орієнтоване на захист каналів зв'язку, контроль ідентичності та забезпечення цілісності даних. Додатковим чинником є висока невизначеність загроз, що потребує адаптивних методів оцінювання ризиків і гнучкого перерозподілу ресурсів між вимогами. Характеризується підвищеними вимогами до конфіденційності, цілісності та доступності інформації, що зумовлено нормативними, договірними або внутрішніми організаційними обмеженнями. До таких середовищ належать системи, що обробляють комерційну таємницю, персональні дані, фінансову інформацію або інші чутливі дані бізнесу. Управління вимогами кібербезпеки в таких умовах потребує суворої формалізації правил доступу, детального аудиту дій користувачів та обмеження розповсюдження даних як на рівні інфраструктури, так і на рівні ПЗ. Особливістю управління вимогами кібербезпеки в середовищах з обмеженим доступом є необхідність точного визначення пріоритетів між вимогами безпеки та бізнес-функціональністю. Пріоритетними стають вимоги до ідентифікації та автентифікації користувачів, управління привілеями, журналювання подій безпеки та забезпечення контролю цілісності даних. Водночас такі середовища часто мають жорсткі обмеження на зміну архітектури та використання зовнішніх сервісів, що підвищує значущість оптимізаційних методів управління вимогами кібербезпеки з урахуванням обмежених ресурсів.

Крім того, для середовищ обробки даних з обмеженим доступом характерною є необхідність постійного підтвердження відповідності вимогам стандартів і регуляторних актів, що зумовлює потребу в динамічному перегляді вимог кібербезпеки з урахуванням змін у загрозах, бізнес-процесах та нормативній базі. Таким чином, у цьому випадку ефективне управління вимогами кібербезпеки повинно базуватися на формалізованих моделях оцінювання ризиків і підтримки прийняття рішень, здатних забезпечити баланс між рівнем захисту, вартістю реалізації та допустимими обмеженнями функціонування ПЗ.

Аналіз джерел та постановка завдання

Сучасні міжнародні стандарти і рекомендовані практики у галузі кібербезпеки (документи NIST, PCI DSS, MITTRE, GDPR та інші [1-6]) визначають вимоги, які необхідно виконати як при побудові систем, так і під час їх удосконалення з точки зору безпеки (після тестувань та аудитів безпеки).

Крім описаних у вступі підходів (галузево- та середовище орієнтованого управління вимогами кібербезпеки) на сьогодні виділяють також ризик-(загрозо-) орієнтовані підходи, а також стандартизований і орієнтований на дані підходи, що відображено в [7-10].

Традиційні підходи до управління вимогами кібербезпеки, як правило, ґрунтуються на статичному формуванні набору вимог, що призводить до зниження ефективності захисту та нераціонального використання ресурсів. Це обґрунтовує необхідність розроблення методу динамічного управління вимогами кібербезпеки, здатного адаптуватися (перебудовуватися) до змін умов функціонування ПЗ, саме це і є *метою цієї роботи*.

Розроблення методу динамічного управління вимогами кібербезпеки

Метод динамічного управління вимогами кібербезпеки реалізується в п'ять основних етапів, а саме:

1) ініціалізація вимог кібербезпеки відповідно до нормативних документів і стандартів;

2) визначення тригерів динамічного оновлення вимог кібербезпеки;

3) моніторинг змін у середовищі впровадження ПЗ та актуальних загроз;

4) кореляція та переоцінювання вимог кібербезпеки з урахуванням виявлених змін і оновлень ризиків;

5) оптимізація розподілу ресурсів між вимогами кібербезпеки з урахуванням оновлених пріоритетів і обмежень;

6) формування зворотного зв'язку та ініціація наступного циклу управління вимогами.

Розглянемо більш детально кожен з етапів цього методу, а для початку визначимо і формалізуємо базові множини параметрів *REQ, SFT, ACT, THR, SRC* у момент часу $t \subseteq T$ за допомогою виразів (1) – (5):

$$REQ_{(t)} = \left\{\bigcup_{i=1}^{n} REQ_i\right\} = \{REQ_1, REQ_2, \dots, REQ_{n(t)}\}, \quad (1)$$

де $REQ_i \subseteq REQ\left(i = \underline{1,n}\right)$ – множина вимог кібербезпеки, визначених певним нормативним документом в заданий момент часу $t \subseteq T$.

$$SFT_{(t)} = \left\{\bigcup_{i=1}^{m} SFT_i\right\} = \{SFT_1, SFT_2, \dots, SFT_{m(t)}\}, \quad (2)$$

де $SFT_i \subseteq SFT\left(i = \underline{1,m}\right)$ – множина модулів ПЗ (застосунків, сервісів, програм), яке впроваджується в заданий момент часу $t \subseteq T$.

$$ACT_{(t)} = \left\{\bigcup_{i=1}^{k} ACT_i\right\} = \{ACT_1, ACT_2, \dots, ACT_{k(t)}\}, \quad (3)$$

де $ACT_i \subseteq ACT\left(i = \underline{1,k}\right)$ – множина активів компанії (дані, функції, сервіси тощо), що впроваджує ПЗ в заданий момент часу $t \subseteq T$.

$$THR_{(t)} = \left\{\bigcup_{i=1}^{q} THR_i\right\} = \left\{THR_1, THR_2, \dots, THR_{q(t)}\right\}, \quad (4)$$

де $THR_i \subseteq THR\left(i = \underline{1,q}\right)$ – множина загроз кібербезпеки (кіберзагроз), які мають вплив на зміну вимог кібербезпеки в заданий момент часу $t \subseteq T$.

$$SRC_{(t)} = \left\{\bigcup_{i=1}^{p} SRC_i\right\} = \left\{SRC_1, SRC_2, \dots, SRC_{p(t)}\right\}, \quad (5)$$

де $SRC_i \subseteq SRC\left(i = \underline{1,p}\right)$ – множина джерел змін вимог кібербезпеки в заданий момент часу $t \subseteq T$, що можуть бути пов'язані з інцидентами, проведенням аудиту, зміною архітектури чи законодавства тощо (при $p = 4$).

Перейдемо до базових етапів реалізації запропонованого метода, використовуючи для більш грунтовного розуміння підхід, використаний для формалізації моделі управління вимогами кібербезпеки при впровадженні ПЗ в [2]:

Етап 1. Ініціалізація вимог кібербезпеки відповідно до нормативних документів і стандартів

Відповідно до описаного в [2] підходу, при $n = 3$ вираз (1) у момент часу $t = 0$ матиме наступний вигляд (6):

$$REQ_{(0)} = \left\{\bigcup_{i=1}^{3} REQ_i\right\} = \{REQ_1, REQ_2, REQ_3\} = \{NIST, ISO, MITRE\}, \quad (6)$$

де $REQ_1 = NIST$ – це множина вимог кібербезпеки зі стандарту NIST 800-53, $REQ_2 = ISO$ – це множина вимог кібербезпеки зі стандарту ISO 22316 (в частині resilience-вимог, інтерпретованих для ПЗ / процесів), а $REQ_3 = MITRE$ – це множина вимог кібербезпеки з MITRE ATT&CK (threat-driven requirements).

Тоді початкова множина вимог в момент часу $t = 0$, з урахуванням описаного в [2] підходу матиме вигляд (7):

$$REQ_{(0)} = REQ_1 \cup REQ_2 \cup REQ_3 = NIST \cup ISO \cup MITRE, \quad (7)$$

Далі, введемо функцію нормалізації початкової множини вимог $REQ_{(0)}$, що задана виразом (8):

$$\varphi = REQ_1 \cup REQ_2 \cup REQ_3 \to U, \quad (8)$$

де U – це уніфікований простір опису вимог, що вводиться для синхронізації вимог кібербезпеки, які можуть бути представлені у різному вигляді в різних нормативних документах..

Тоді уніфіковане подання початкової множини вимог $REQ_{(0)}$ можна представити наступним чином (9):

$$\widetilde{REQ_{(0)}} = \left\{REQ \in REQ_{(0)}\right\}. \quad (9)$$

Далі, на наступному етапі, нам потрібно визначити тригери динамічного оновлення вимог кібербезпеки.

Етап 2. Визначення тригерів динамічного оновлення вимог кібербезпеки

Під «тригерами» у нашому випадку будемо розуміти певні типи подій (див. вираз (10)), які спричиняють оновлення / зміну вимог кібербезпеки при впровадженні ПЗ в бізнесі.

Нехай множина тригерів динамічного оновлення вимог кібербезпеки, що корелюється з множиною $SRC_{(t)}$ (5) джерел змін вимог (тобто $p = 4$), задана наступним виразом (10):

$$\begin{aligned}\Omega &= \left\{\bigcup_{i=1}^{p} \Omega_i\right\} = \{\Omega_1, \Omega_2, \dots, \Omega_n\} = \left\{\bigcup_{i=1}^{4} \Omega_i\right\} \\ &= \{\Omega_1, \Omega_2, \Omega_3, \Omega_4\} \\ &= \{INCIDENT, AUDIT, ARCHITECTURE, LEGISLATIO\end{aligned} \quad (10)$$

де $\Omega_i \subseteq \Omega\left(i = \underline{1,p}\right)$ – множина тригерів динамічного оновлення вимог кібербезпеки, а відповідно $\Omega_1 = INCIDENT$ – це множина інцидентів, які виникають і впливають на зміну вимог кібербезпеки, $\Omega_2 = AUDIT$ – це множина аудитів, за результатами проведення яких необхідно змінювати вимоги кібербезпеки, $\Omega_3 = ARCHITECTURE$ – це множина змін архітектури системи, що має вплив на зміну вимог кібербезпеки, $\Omega_4 = LEGISLATION$ – це відповідні зміни законодавства, що впливають на зміну вимог кібербезпеки при впровадженні ПЗ в бізнесі.

Таким чином, певна подія в момент часу $t \subseteq T$ є кортежем параметрів, визначених виразами (5) та (10), який можна представити у вигляді (11):

$$E_{(t)} = \langle \Omega, SRC, \Delta(t) \rangle, \quad (11)$$

де $\Delta(t)$ – це опис зміни вимог кібербезпеки.

Індикатор спрацювання тригера можна визначити таким чином:

$$\delta_\Omega(t) = \begin{cases} 1, \text{якщо } E_{(t)} \in \Omega \\ 0, \text{в іншому випадку} \end{cases}. \quad (12)$$

Динамічна зміна (оновлення) вимог кібербезпеки активується за умови (13):

$$\delta(t) = \bigvee_{\Omega_i \subseteq \Omega} \delta_\Omega(t) = 1. \quad (13)$$

Далі, на наступному етапі методу, формалізуємо процес моніторингу змін у середовищі впровадження ПЗ.

Етап 3. Моніторинг змін у середовищі впровадження ПЗ та актуальних загроз

Моніторинг здійснюється неперервно або з визначеною періодичністю та охоплює технічні, організаційні й безпекові (загрозові) аспекти функціонування системи. Стан середовища впровадження ПЗ у момент часу $t \subseteq T$ можна представити у вигляді сукупності основних характеристик (14):

$$K_{(t)} = \langle SFT_{(t)}, ACT_{(t)}, THR_{(t)}, BUD_{(t)}, REG_{(t)} \rangle, \quad (14)$$

де параметри $SFT_{(t)}, ACT_{(t)}, THR_{(t)}$ визначаються відповідно до виразів (2), (3) та (4), а $BUD_{(t)}, REG_{(t)}$ –

параметри, що означають бюджетні ресурси і регуляторні вимоги відповідно.

Таке представлення (14) дозволяє відобразити середовище не як окремі диференційовані компоненти (чинники), а як єдиний керований об'єкт.

Формалізацію ж змін середовища впровадження ПЗ у момент часу $t \subseteq T$ можна представити у вигляді дельти стану:

$$\Delta K_{(t)} = K_{(t)} - K_{(t-1)}. \quad (15)$$

Враховуючи (14) – (15), зміни модулів ПЗ, активів, загроз, бюджетних ресурсів і регуляторних вимог представимо відповідно:

$$\begin{gathered}\Delta SFT_{(t)}=SFT_{(t)} - SFT_{(t-1)};\\ \Delta ACT_{(t)}=ACT_{(t)} - ACT_{(t-1)};\\ \Delta THR_{(t)}=THR_{(t)} - THR_{(t-1)};\\ \Delta BUD_{(t)}=BUD_{(t)} - BUD_{(t-1)};\\ \Delta REG_{(t)}=REG_{(t)} - REG_{(t-1)}.\end{gathered} \quad (16)$$

Для прикладу, при $\Delta SFT_{(t)} = \emptyset$ змінено модулі програмного забезпечення, при $\Delta ACT_{(t)} = \emptyset$ спостерігається зміна активів, $\Delta THR_{(t)} = \emptyset$ означає появу нових або модифікованих загроз, $\Delta BUD_{(t)} = \emptyset$ означає зміну доступних бюджетних ресурсів, а при $\Delta REG_{(t)} = \emptyset$ спостерігається зміна регуляторних вимог.

На наступному етапі, з урахуванням результатів перших трьох етапів методу, необхідно здійснити корелювання та оновлення оцінок (переоцінювання) вимог кібербезпеки з урахуванням змін.

Етап 4. Кореляція та переоцінювання вимог кібербезпеки з урахуванням виявлених змін і оновлень ризиків

Метою цього етапу є встановлення та актуалізація взаємозв'язків між вимогами кібербезпеки, елементами ПЗ та актуальними загрозами з урахуванням виявлених змін у середовищі впровадження.

Для реалізації цього етапу використаємо теорію графів [11], Байєсові мережі [12] та теорію множин [13].

Крок 4.1. Визначимо орієнтований зважений граф:

$$G_{REQ_{(t)}} = (V_{REQ_{(t)}}, E_{REQ_{(t)}}, W_{REQ_{(t)}}), \quad (17)$$

де $V_{REQ_{(t)}} = REQ_{(t)}$ – вершини графа (вимоги), $E_{REQ_{(t)}} \subseteq V_{REQ_{(t)}} \times V_{REQ_{(t)}}$ – множина залежностей, $W_{REQ_{(t)}} = \left\{w_{ij_{(t)}}\right\}$ – ваги залежностей $w_{ij_{(t)}} \in [0;1]$.

Якщо існує ребро $(REQ_i \to REQ_j)$, то виконання вимоги REQ_i впливає на виконання вимоги REQ_j.

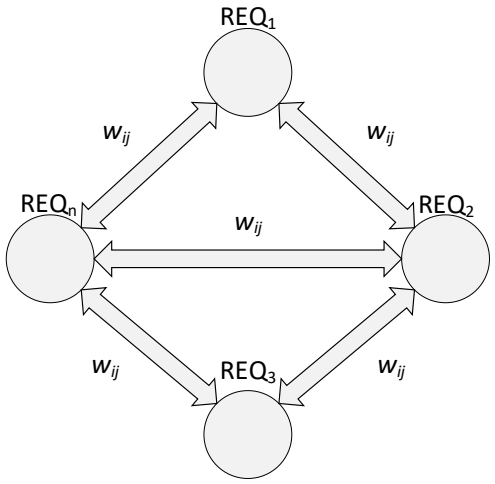

Рис. 1. Схематичне відображення графу $G_{REQ_{(t)}}$ (17)

Далі представимо граф $G_{REQ_{(t)}}$ у матричній формі, сформувавши матрицю суміжності зазначеного графа (17):

$$A_{(t)} = \left[a_{ij_{(t)}}\right],\ a_{ij_{(t)}} = \begin{cases} w_{ij_{(t)}}, (REQ_i, REQ_j) \in E_{REQ_{(t)}} \\ 0, \text{інакше.} \end{cases} \quad (18)$$

Крок 4.2. Корелювання з актуальними загрозами

Враховуючи (4), задано множину кіберзагроз $THR_{(t)}$, які мають вплив на зміну вимог кібербезпеки під час впровадження ПЗ. Введемо матрицю покриття $G_{RT_{(t)}} = \left[g_{ij_{(t)}}\right]\ (i = \underline{1,n}), \left(j = \underline{1,q}\right)$, яка фактично відображатиме зниження ризику від кіберзагроз за рахунок виконання відповідних вимог:

$$G_{RT_{(t)}} = \left| g_{11_{(t)}}\ g_{12_{(t)}}\ \dots\ g_{1q_{(t)}}\ g_{21_{(t)}}\ g_{22_{(t)}}\ \dots\ g_{2q_{(t)}}\ \dots\ \dots\ \dots\ \dots\ g_{n1_{(t)}}\ g_{n2_{(t)}}\ \dots\ g_{nq_{(t)}} \right|, \quad (19)$$

де кожен елемент $g_{ij_{(t)}} = [0;1]$ характеризує ступінь, з яким вимога REQ_i знижує ризик від кіберзагрози THR_i.

Таким чином, ймовірність реалізації кіберзагрози $THR_{(t)}$ за результатами моніторингу (14) – (16) у момент часу $t \subseteq T$ можна представити наступним чином:

$$p_{k_{(t)}} = P\left(O_{(t)}\right), \quad (20)$$

де $O_{(t)}$ – це множина спостережуваних подій та параметрів середовища впровадження ПЗ, отриманих на етапі моніторингу (інциденти, результати аудиту, зміни архітектури, законодавчі зміни).

Враховуючи (10) у момент часу $t \subseteq T$ ця множина може бути представлена таким чином: $O_{(t)} = \left\{INCIDENT_{(t)}, AUDIT_{(t)}, ARCHITECTURE_{(t)}, LEGISLATION_{(t)}\right\}$.

Крок 4.3. Оцінювання залишкового ризику

Позначимо ступінь реалізації (виконання) вимоги REQ_i у момент часу $t \subseteq T$ як $x_{i_{(t)}} \in [0;1]$ (тобто при значенні «0» вимога не виконана, а при значенні «1» відповідно виконана) тоді залишковий ризик можна визначити за виразом (21) таким чином:

$$\rho_{i_{(t)}} = \left(\sum_{j=1}^{q} \quad g_{ij_{(t)}} p_{k_{(t)}}\right) \cdot \left(1 - x_{i_{(t)}}\right). \tag{21}$$

Крок 4.4. Врахування важливості вимоги

На основі визначеного графа (17) та матриці (18) можна визначити зважений ступінь $d_{i_{(t)}} = \sum_{j=1}^{n} \quad a_{ij_{(t)}}$ (сумарний вплив вимоги REQ_i на інші вимоги) та відповідно нормалізований вплив:

$$\hat{d}_{i_{(t)}} = \frac{d_{i_{(t)}}}{max_j d_{j_{(t)}}} \in [0;1], \left(i = \underline{1,n}\right), \left(j = \underline{1,q}\right). \tag{22}$$

Тобто, чим більше інших вимог залежать від вимоги REQ_i і чим більша вага цих залежностей, тим більшим є параметр $d_{i_{(t)}}$. Крім того, $max_j d_{j_{(t)}}$ – максимальний зважений ступінь серед усіх вимог, до того ж при $\hat{d}_{i_{(t)}} = 1$ вимога REQ_i є найбільш структурно значущою (важливою), а при $\hat{d}_{i_{(t)}} \approx 0$ вимога REQ_i майже не впливає на інші, тобто не є структурно значущою.

Цей показник враховує системну взаємозалежність вимог, каскадний ефект їх реалізації, архітектурну критичність. Тобто не оцінюється вимога ізольовано, а враховується її роль у структурі всієї системи.

Крок 4.5. Оновлення пріоритету вимоги

Пріоритет вимоги REQ_i у заданий момент часу $t \subseteq T$ з урахуванням (21) – (22) можна представити таким чином:

$$\pi_{i_{(t)}} = \alpha\rho_{i_{(t)}} + \beta u_{i_{(t)}} + \gamma\hat{d}_{i_{(t)}}, \tag{23}$$

де $u_{i_{(t)}}$ – це регуляторна важливість вимоги REQ_i, α, β, γ – це нормовані вагові коефіцієнти, що відображають відносну значущість структурного (залишкового) ризику, регуляторної важливості (критичності) та нормалізований вплив (каскадний ефект) відповідно. До того ж, обмеження $\alpha + \beta + \gamma = 1$ забезпечує інтерпретованість моделі та стабільність масштабування інтегрального показника пріоритету.

У результаті вектор пріоритетів виглядатиме наступним чином:

$$\Pi_{(t)} = \left\{\pi_{1_{(t)}}, \pi_{2_{(t)}}, \dots, \pi_{n_{(t)}}\right\}. \tag{24}$$

На наступному етапі, з урахуванням результатів попередніх чотирьох етапів методу, буде оптимізовано розподіл ресурсів між вимогами REQ_i з урахуванням оновлених пріоритетів $\pi_{i_{(t)}}$ та відповідних обмежень.

Етап 5. Оптимізація розподілу ресурсів між вимогами кібербезпеки з урахуванням оновлених пріоритетів і обмежень

Цільова функція матиме вигляд (25), тобто фактично максимізується сумарна інтегральна корисність реалізованих вимог REQ_i:

$$max \sum_{i=1}^{n} \quad \pi_{i_{(t)}} x_{i_{(t)}}, \tag{25}$$

де $\pi_{i_{(t)}}$ визначено в (23), а $x_{i_{(t)}} \in [0;1]$ – це бінарний параметр, що відображає прийняття рішення щодо забезпечення вимоги REQ_i (див. крок 4.3).

При цьому обмеження ресурсів:

$$\sum_{i=1}^{n} \quad c_{i_{(t)}} x_{i_{(t)}} \leq BUD_{(t)}, \tag{26}$$

де $c_{i_{(t)}} > 0$ – це ресурсна вартість забезпечення однієї вимоги REQ_i, а змінна $BUD_{(t)}$ визначена на 3 етапі методу і відображає сукупні бюджетні ресурси.

Якщо i-та вимога є залежною, тобто виконується тільки після виконання j-тої вимоги, то $x_{i_{(t)}} \leq x_{j_{(t)}}$ і відповідно для множини попередників, враховуючи (17):

$$PRE_{i_{(t)}} = \left\{j \in V_{REQ_{(t)}} : (i,j) \in E_{REQ_{(t)}}\right\}. \tag{27}$$

Таким чином, отримуємо оптимальний вектор (28), який визначає множину вимог для реалізації у момент часу $t \subseteq T$, отриманий з урахуванням пріоритетів, ресурсних обмежень та залежностей графа:

$$X^*(t) = \left\{x^*_{1_{(t)}}, x^*_{2_{(t)}}, \dots, x^*_{n_{(t)}}\right\}, \tag{28}$$

де $x^*_{i_{(t)}} \in [0;1]$ – це оптимальне значення параметру $x_{i_{(t)}}$, що отримане в результаті оптимізаційної задачі.

Останній етап цього методу описує формування зворотнього звязку та ініціацію наступного циклу управління вимогами кібербезпеки при впровадження ПЗ.

Етап 6. Формування зворотного зв'язку та ініціація наступного циклу управління вимогами

Для кожної вимоги REQ_i визначається її поточний стан виконання:

$$s_{i_{(t+1)}} = g(s_{i_{(t)}} + x^*_{i_{(t)}}), \tag{29}$$

$s_{i_{(t)}}$ – ступінь реалізації вимоги REQ_i.

Далі, на основі оновленого стану уточняється показник нормалізованого впливу $\hat{d}_{i_{(t+1)}} = h(s_{i_{(t+1)}})$ і за потреби актуалізуються структурні $(\rho_{i_{(t)}})$ та регуляторні $(u_{i_{(t)}})$ оцінки.

Таким чином, враховуючи вирази (23) та (24), новий вектор пріоритетів матиме вигляд:

$$\pi_{i_{(t+1)}} = \alpha\rho_{i_{(t+1)}} + \beta u_{i_{(t+1)}} + \gamma\hat{d}_{i_{(t+1)}}. \tag{30}$$

$$\Pi_{(t+1)} = \left\{\pi_{1_{(t+1)}}, \pi_{2_{(t+1)}}, \dots, \pi_{n_{(t+1)}}\right\}. \tag{31}$$

Наступний цикл управління ініціюється, якщо виконується хоча б одна з наступних умов:

1) зміна пріоритетів перевищує поріг ε;

2) з'явилися нові вимоги REQ_i або змінилися обмеження ресурсів $BUD_{(t)}$;

3) завершено поточний період планування.

Таким чином, метод набуває ітераційного характеру – результати оптимізації впливають на стан системи, що, у свою чергу, формує оновлені пріоритети та ініціює новий цикл управління вимогами. Це забезпечує адаптивність до змін середовища та ресурсних обмежень.

Структурна схема методу динамічного управління вимогами кібербезпеки відображена на рис. 2, а псевдокод його реалізації міститься на рис. 3.

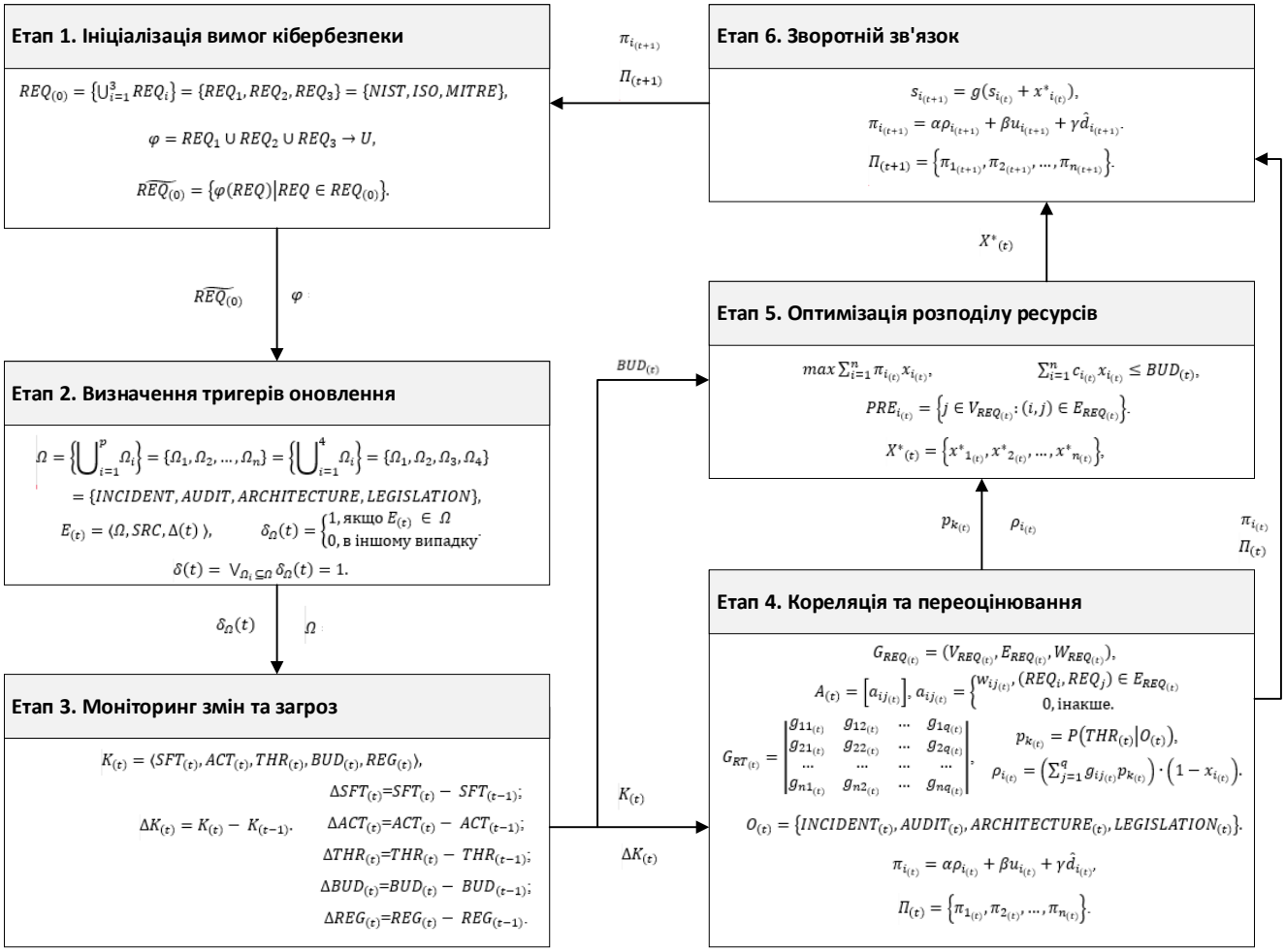

Рис. 2. Схема розробленого методу

```
Initialize t ← 0
Compute structural importance ρ_i from graph G
Compute deviation ∂_i from state s_i
Compute priorities π_i(t) = α ρ_i + β u_i + γ ∂_i

repeat
    // Resource allocation
    Solve:
        maximize Σ π_i(t) x_i
        subject to:
            Σ c_i x_i ≤ B
            x_i ≤ x_j  for all dependencies j → i
            x_i ∈ {0,1}

    Obtain optimal plan X*(t)

    // Feedback update
    Update state s_i(t+1) based on X*(t)
    Recompute deviation ∂_i(t+1)
    Recompute priorities π_i(t+1)

    t ← t + 1
until  ||Π(t) - Π(t-1)|| ≤ ε
```

Рис. 3. Псевдокод практичної реалізації методу

Висновки. Проаналізовано основні підходи до управління вимогами кібербезпеки при впровадженні ПЗ. Зокрема, розглянуто галузево орієнтоване управління вимогами кібербезпеки, яке передбачає адаптацію методів пріоритезації, оцінювання ризиків і розподілу ресурсів відповідно до контексту застосування ПЗ. Крім того, різні типи середовищ потребують різних стратегій пріоритезації вимог, рівнів автоматизації та методів оцінювання ризиків. Це обґрунтовує доцільність використання адаптивних і формалізованих моделей управління вимогами кібербезпеки, здатних динамічно враховувати зміну умов функціонування ПЗ. Отже, середовище орієнтоване управління вимогами кібербезпеки є актуальним підходом.

Розроблено метод динамічного управління вимогами кібербезпеки, який за рахунок ініціалізації вимог кібербезпеки відповідно до нормативних документів і стандартів, визначення тригерів динамічного оновлення вимог кібербезпеки, моніторингу змін у середовищі впровадження ПЗ та актуальних загроз, кореляції та переоцінювання вимог кібербезпеки з урахуванням виявлених змін і оновлень

ризиків, оптимізації розподілу ресурсів між вимогами кібербезпеки з урахуванням оновлених пріоритетів і обмежень, формування зворотного зв'язку та ініціації наступного циклу управління вимогами, дає змогу забезпечити інтегровану оцінку їх структурної, регуляторної та динамічної значущості з подальшою формалізацією управлінського рішення через оптимізаційну модель розподілу ресурсів та ітераційний механізм зворотного зв'язку, що дозволяє інтегрувати топологічні та станові характеристики системи, максимізувати ефект від використання бюджету, регулярно оновлювати пріоритети, врахувати нові вимоги кібребезпеки при впровадженні ПЗ, а також забезпечити адаптацію системи до зміни ресурсних або нормативних умов.

Практична цінність методу полягає у створенні формалізованого адаптивного механізму управління вимогами кібербезпеки, який забезпечує обгрунтований вибір пріоритетів, оптимальний розподіл ресурсів та підвищення системної стійкості інформаційно-комунікаційних систем. Запропонований метод формалізований у вигляді псевдокоду та може бути реалізований у:

- системах підтримки прийняття рішень [14];
- програмних засобах управління кіберризиками [15];
- корпоративних GRC-платформах [16];
- автоматизованих системах планування тощо [17].

Список використаних джерел

[1] *National Institute of Standards and Technology Special Publication 800-53*, Rev. 5, 492 pages (September 2020), https://doi.org/10.6028/NIST.SP.800-53r5

[2] *ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection – Information security management systems – Requirements,* Ed. 3, 2022, 19 pages.

[3] IT Governance Publishing; Stephen Hancock, *PCI DSS Version 4.0.1: A guide to the payment card industry data security standard,* Packt Publishing, 2025.

[4] W. Wodo, D. Stygar, PSD2 Compliant Hardware Token for Digital Banking, *62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS),* Riga, Latvia, 2021, pp. 1-6.

[5] W. -T. Tsai, J. -N. Luo and C. -L. Chou, Integrating Tree Structures with the MITRE ATT&CK Framework for APT Detection, *2025 9th International Conference on Cryptography, Security and Privacy (CSP)*, Okinawa, Japan, 2025, pp. 139-143, doi: 10.1109/CSP66295.2025.00031.

[6] IT Governance Publishing; IT Governance Privacy Team, *EU General Data Protection Regulation (GDPR): An implementation and compliance guide,* Packt Publishing, 2025.

[7] Davis A., Overmyer S., Jordan K., Caruso J., Ashi F., Dinh A., Kincaid G., Ledeboer G., Reynolds P., Sitaram P. and others. Identifying and measuring quality in a software requirements specification. In: *Proceedings First International Software Metrics Symposium, IEEE,* 2019, pp. 141-152.

[8] Гнатюк С., Сидоренко В., Скуратівський А. Модель управління вимогами кібербезпеки при впровадженні програмного забезпечення, *Електронне фахове науково видання «Кібербезпека: освіта, наука, техніка»,* 2025, 4(28), с. 715-726. https://doi.org/10.28925/2663-4023.2025.28.841

[9] Петренко М.А. Управління безпекою діяльності e-commerce підприємств, *кваліфікаційна робота другого (магістерського) рівня*, Харків, 2022, 91 с.

[10] Alexander I. F., Stevens R. Writing better requirements. Pearson Education. Breach Level Index, 2019, 427 p.

[11] H. A. Dawood, Graph Theory and Cyber Security, *2014 3rd International Conference on Advanced Computer Science Applications and Technologies*, Amman, Jordan, 2014, pp. 90-96, doi: 10.1109/ACSAT.2014.23.

[12] Q. Yu and Z. Li, A Bayesian Model Averaging Method for Software Reliability Assessment, *2020 Asia-Pacific International Symposium on Advanced Reliability and Maintenance Modeling (APARM)*, Vancouver, BC, Canada, 2020, pp. 1-5, doi: 10.1109/APARM49247.2020.9209504.

[13] T. J. Mathew and E. Sherly, A Review on Soft Set-Based Theories Relevant to Decision Making in Computer Science, *2019 Third International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, India, 2019, pp. 395-399, doi: 10.1109/ICISC44355.2019.9036419.

[14] R. Kuceba and L. Kieltyka, Criteria classification Intelligent Decision Support Systems, *2009 ICCAS-SICE*, Fukuoka, Japan, 2009, pp. 5351-5355.

[15] P. J. G. Guerra and D. A. Sepulveda Estay, An Impact-wave Analogy for Managing Cyber Risks in Supply Chains, *2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, Bangkok, Thailand, 2018, pp. 61-65, doi: 10.1109/IEEM.2018.8607563.

[16] S. Stapleton, *Top 18 GRC (Governance, Risk & Compliance) Tools in 2025,* Published 24.10.2025, https://pathlock.com/blog/grc/list-of-top-grc-tools-and-softwares

Skurativskyi A. Cybersecurity requirements management method for software implementation in business. The article analyzes modern standards and approaches to cybersecurity requirements management and identifies their limitations within static models. A method for dynamic cybersecurity requirements management is proposed, which involves a cyclic process of initialization, monitoring, reassessment, and optimization of requirements, taking into account changes in the environment and evolving threats. The method is aimed at improving protection effectiveness, ensuring efficient resource utilization, and maintaining a balance between security levels and system functionality.

Keywords: requirements, cybersecurity, method, software, cybersecurity requirements management.

Скуратівський Анатолій Анатолійович, аспірант Державного університету «Київський авіаційний інститут».

Skurativskyi Anatolii, PhD student at the State University "Kyiv Aviation Institute".