УДК 004.094

О.В. Ізмайлова[1],
канд. техн. наук, доцент
ORCID: 0000-0002-2905-1827
Г.В. Красовська[2],
канд. техн. наук, доцент
ORCID: 0000-0003-1986-6130
К.К. Красовська[3],
PhD
ORCID: 0000-0002-3468-8064
[1]Київський національний університет будівництва і архітектури, м. Київ
[2]Київський національний університет імені Тараса Шевченка, м. Київ
[3]SoftServe Poland

МОДУЛЬ ОЦІНКИ ОЧІКУВАНИХ ВТРАТ В СИСТЕМІ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БУДІВЕЛЬНОЇ КОМПАНІЇ

У статті розглядається проблема ефективності оцінки очікуваних втрат будівельної компанії при реалізації загроз інформаційної безпеки. Пропонується один з шляхів часткового розв'язання цієї проблеми на основі удосконалення відповідного модуля системи управління ризиками, що надає користувачу людино-машинний інструментарій експертного оцінювання очікуваних втрат. При цьому передбачено вибір та застосування ефективного сценарію оцінювання за поточних ситуаційних умов прийняття рішень. Для забезпечення роботи модуля визначено інформаційно-логічні зв'язки між етапами оцінювання та запропоновано підхід до формування різних сценаріїв оцінювання. Крім того, для підвищення точності результатів та гнучкості запропонованого алгоритму забезпечено можливість вибору сценарію оцінювання користувачем з відповідною роллю. Оскільки в роботі розглядається задача багатокритерійного оцінювання, формалізовано ієрархію критеріїв, а також враховано вагу їх впливу на результати обчислень, враховано можливість реалізації різних типів загроз для різних інформаційних активів (ІА) підприємства. Оцінка наслідків реалізації загроз інформаційної безпеки може здійснюватися на різних ієрархічних рівнях з урахуванням, між іншим, показників порушення конфіденційності, цілісності та доступності інформації. При розробці логіко-математичного апарату застосовуються методи безпосереднього експертного оцінювання, аналізу ієрархій, Дельфи, лінійної згортки критеріїв, ймовірнісного моделювання. З метою формалізації суджень експертів використовується якісно-кількісна шкала. Визначено необхідні ролі експертів для проведення ефективного оцінювання. Узагальнення оцінок експертів здійснюється за умови контролю достатності міри логічності та розсіювання думок кожного експерта, у відповідності встановленим вимогам до міри узгодженості думок групи експертів, оцінки та формалізованого врахуванням міри їх компетентності.

Ключові слова: BIM-технологія, BIM-модель, корпоративна інформаційна система управління життєвим циклом будівлі (КІС ЖЦ), система управління ризиками, інформаційний актив, загроза інформаційній безпеці, очікувані втрати, укрупнена та комплексна оцінка втрат, експертне оцінювання.

Вступ. В галузі будівництва кінець XX століття знаменувався появою принципово нової ідеї – реалізації всіх етапів життєвого циклу (ЖЦ) будівлі від самих ранніх (створення концепцій проекту) до робочого проектування, будівництва, супроводження, експлуатації та зносу на основі єдиної інформаційної моделі будівлі BIM (Building Information Modeling), технології її колективного поступового створення та загального використання [1]. BIM-модель є інформаційною основою реалізації корпоративної (інтегрованої) інформаційної системи управління життєвим циклом будівлі (КІС ЖЦ), де кожна функціональна складова: система, підсистема або комплекс задач може бути розроблена індивідуально залежно від вимог предметної області.

Актуальним при створенні КІС ЖЦ на різних управлінських рівнях є побудова та удосконалення системи управління ризиками, головна задача якої – забезпечити та оптимізувати за встановленими критеріями результати знайденого компромісу між двома пріоритетними потребами: прозорість та доступність для всіх користувачів єдиної інформаційної моделі, з одного боку, і гарантія захищеності даних та надійний рівень інформаційної та кібернетичної безпеки, з іншого боку.

В сучасних умовах, управління ризиками дедалі більше віддаляється від жорсткої цільової установки їх уникнення та мінімізації і спрямовується на формування компромісних варіантів рішень – можливості прийняття певного рівня ризику та його використання на користь підприємства. Значна увага в управлінні ризиками надається питанню пошуку ефективного балансу між витратами на захист даних та очікуваними втратами, що пов’язані з можливістю реалізації загроз, зокрема, інформаційної безпеки. Вирішальними вимогами до якісного розв’язання цього питання є забезпечення достовірності, оперативності, ресурсної спроможності реалізації, гнучкості до змін в умовах неповної визначеності даних.

Аналіз досліджень і публікацій. Серед сучасних теоретичних та практично-орієнтованих публікацій існує значна кількість робіт, що розглядають проблеми ефективної оцінки очікуваних втрат в результаті реалізації загроз як вагому складову удосконалення системи управління ризиками. Високу міру актуальності цієї задачі в період створення та експлуатації КІС ЖЦ обґрунтовано в роботі [2], де проаналізовані поточні умови та властивості загроз та ризиків в галузі будівництва.

Аналіз сучасних напрямків досліджень показує, що оцінювання можливого збитку відходить від стандарту врахування тільки фінансових втрат, а також вимагає використання великих об’ємів статистичних даних які збираються з різноманітних джерел. Математичні моделі та методи оцінки ризиків визначено у Керівництві з проведення оцінювання ризиків NIST SP 800-30 та методології оцінки ризиків OWASP [3]. Вони передбачають оцінювання рівня втрат та імовірності реалізації ризику за якісною шкалою без її кількісної інтерпретації. В більш складних методах, таких як OCTAVE, Allegro, MEHARY, Magerit [4] оцінка збитку проводиться за основі єдиного узагальнюючого показника, що передбачає різні типи втрат, але без їх формальної структуризації і, як наслідок, без врахування різноаспектного впливу загрози на різні критерії оцінювання втрат.

Підтвердження значного позитивного впливу на удосконалення результатів оцінювання на основі структуризації оцінок втрат за багатьма критеріями

представлено в [5, 6]. В роботі [6] проведені експериментальні дослідження шляхів удосконалення багатокритерійного підходу до оцінювання. В її основу закладені можливості багатокритерійної експертної оцінки втрат на основі метода безпосереднього оцінювання та методу аналізу ієрархій, структуризації різних рівнів наслідків реалізації загрози очікуваних збитків і розгляд їх як ймовірнісних величин. Передбачено врахування різних рівнів ієрархії критеріїв та ваги їх впливу на результати обчислень. Узагальнення оцінок експертів здійснюється з контролем достатності міри логічності та розсіювання думок кожного експерта, відповідності встановленим вимогам до міри узгодженості думок групи експертів, оцінки та формалізованого врахуванню міри їх компетентності. Для практичної реалізації підходу, що пропонується, розроблений людино-машинний інструментарій – функціональний модуль системи управління ризиками, що побудований на основі зв'язаної бази моделей експертного оцінювання з застосуванням сучасних можливостей систем підтримки прийняття рішень (СППР) в умовах слабкої структуризації процесів та концептуальної невизначеності.

Спираючись на проведений аналіз літературних джерел та результатів експериментального дослідження авторів [6], був визначений напрямок подальшого удосконалення інструментарію оцінки втрат. Реалії прийняття рішень в різних ситуаційних умовах доступності даних, різних задачах оцінювання, з різними існуючими ресурсними, часовими та інформаційними обмеженнями визначають доцільність альтернативного сценарного підходу оцінки втрат. Кожний сценарій повинен відображати обрані користувачем умови прийняття рішень з множини наданих йому можливих альтернатив налаштування роботи функціонального модуля оцінки втрат.

Постановка завдання. На основі BIM-моделі в КІС ЖЦ функціонує фіксований набір інформаційних систем (ІС) $i \in I = \{1,2,\dots,k^*\}$. Кожна ІС має множину інформаційних активів: $A_i = \left\{a_1^i, a_2^i, \dots, a_s^i, \dots, a_{s_i'}^i\right\}, i \in I$. Інформаційний актив – це інформація або ресурс (інформаційний, технічний, програмний), що підлягає захисту на підприємстві, його інформаційних мережах та системах.

Для кожної ІС $i \in I$ на певний час відома скінчена множина можливих загроз: $Z_i = \left\{z_1^i, z_2^i, \dots, z_l^i, \dots, z_{l_i'}^i\right\}, i \in I$.

Для проведення оцінки збитків при реалізації загроз по інформаційних активах при реалізації окремих альтернатив оцінювання встановлюється множина критеріїв оцінювання втрат: $F = \left\{f_1, \dots, f_j, \dots, f_{j^*}\right\} = \left\{f_j, j \in J\right\}, J = \{1,2, \dots, j^*\}$

Визначається: $E_i^p = \{e_1^i, e_p^i, \dots, e_{p^*}^i\}$, $p \in P = \{1,2,\dots,p^*\}$ – множина експертів, що приймають участь в оцінюванні.

Для кожного експерта може бути заданий показник його компетентності K_i^p, що може враховуватись при формуванні групи експертів, а також при обчисленні фінальних узагальнених оцінок очікуваних втрат. При проведенні експертних оцінок ставиться задача оптимізувати достовірність експертного оцінювання в умовах невизначеності даних і необхідності передбачення наслідків реалізації загрози.

Експерту надається можливість проводити оцінку очікуваних втрат на основі єдиної якісно-кількісної шкали оцінювання, що включає 7 рівнів:

– W_1 – суто оптимістичні збитки (невпливові та надзвичайно низькі збитки, що не змінять загальний стан системи);

– W_2 – оптимістичні збитки (мало впливові – низькі збитки, які можуть змінити загальний стан системи, але не вплинуть на її функціонування);

– W_3 – низькі збитки (збитки із незначним впливом, які можуть змінити загальний стан системи та навіть незначним чином погіршити її функціонування);

– W_4 – середні збитки (збитки із середньо зваженим впливом, які можуть змінити загальний стан системи та її функціонування, але при цьому відновлення роботи займає незначний час);

– W_5 – високі збитки (збитки із суттєвим впливом, змінюють загальний стан системи та значно впливають на її функціонування, час відновлення нормального стану системи достатньо великий);

– W_6 – песимістичні збитки (збитки зі значним впливом, можуть кардинальним чином змінити загальний стан системи, надзвичайно впливають на її функціонування, час та можливість відновлення складно прогнозувати, але відновлення можливе);

– W_7 – суто песимістичні оцінки (збитки з глобальним впливом – надзвичайно високі, що можуть спричинити повний колапс системи, відновлення стабільної роботи майже неможливо).

Оскільки запропонована градація являє собою певну якісну шкалу, встановлюються шкала структуризації переваг для кожного рівня W_i (рис. 1), тобто їх граничні та середні значення в межах від 0 до 1 $\{W_i^{min}, W_i^{mid}, W_i^{max}\}$, де $W_i^{mid} = {W_i^{min} + W_i^{max}}/{2}$.

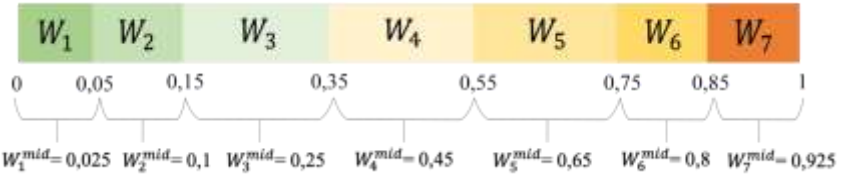

Рис. 1. Якісно-кількісна шкала оцінювання втрат

При реалізації модуля оцінки очікуваних втрат розв'язується слабко структурована задача прийняття рішень, що передбачає вирішальне місце людини в процесі прийняття рішень. Застосовуючи існуючу термінологію системного аналізу, передбачений наступні типи ролей спеціалістів, що будуть приймати участь в його реалізації:

– особа, що приймає рішення (ОПР) – відповідальний співробітник або підрозділ будівельної компанії, що приймає рішення про вибір варіанту оцінювання, організацію і оцінку їх наслідків;

– експерт – це спеціаліст у будівельній галузі та (або) спеціаліст в створенні та експлуатації інформаційних галузевих систем, що володіє інформацією про ситуацією, що розглядається, але не несе прямої відповідальності за результати її розв'язання;

– аналітик (консультант, дослідник) – спеціаліст в галузі інформаційних безпеки, що приймав участь в розробці чи впровадженню системи та займається її супроводженням.

Вибір одного з альтернативних сценаріїв оцінювання є прерогативою ОПР. При цьому йому надається можливість покроковим шляхом проаналізувати доцільність застосування наступних альтернатив:

– оцінювання на основі єдиного укрупненого показника очікуваних втрат **або** на основі комплексного оцінювання, що передбачає врахування різних критеріїв втрат;

– оцінювання втрат з врахуванням узагальнюючої оцінки наслідків реалізації загрози **або** на основі врахування наслідків реалізації загрози з точки зору порушення конфіденційності (К), цілісності (Ц) та доступності даних (Д).

– надання можливості оцінювання очікуваних втрат як детермінованої величини **або** передбачення можливості відбуття різних рівнів очікуваних втрат з встановленою ймовірністю.

Модуль оцінки очікуваних збитків базується на системному застосуванні можливостей наступних методів: експертного оцінювання (метод аналізу ієрархій (МАІ) Сааті , метод безпосереднього оцінювання, метод ранжирування, метод Дельфі), лінійної згортки критеріїв та оцінки критеріїв як дискретних випадкових величин.

Мета статті проаналізувати підхід до побудови модуля оцінки очікуваних витрат в системі управління ризиками інформаційної безпеки КІС ЖЦ будівельної компанії, що надає користувачу можливість застосування альтернативних сценаріїв прийняття рішень на основі системно зв’язаної бази моделей експертного оцінювання.

Основна частина. Розглянемо етапи роботи модуля оцінки очікуваних втрат при реалізації загрози на визначеному інформаційному активі. Інформаційно-логічні зв’язки між різними етапами та алгоритм формування різних сценаріїв оцінювання представлено у вигляді діаграми діяльності на рис. 2.

Етап1. Формування групи експертів. Перед ОПР ставиться задача формування групи експертів $E_i^p = \{e_1^i, e_p^i, \dots, e_{p^*}^i\}$, $p \in P = \{1,2,\dots,p^*\}$, що будуть приймати участь на різних етапах оцінювання. По кожному експерту визначені дані його ідентифікації, спеціалізація та рівень компетентності K_i^p для вирішення задач даного класу в рамках визначеної інформаційної системи.

Етап 2. Вибір інформаційного активу (ІА). Вибір інформаційного активу проводиться ОПР, порядок розгляду активу встановлюється з врахуванням міри його цінності. Обраний ОПР a_s^i стає об’єктом подальшого оцінювання.

Етап 3. Встановлення типу загрози. Для кожної ІС $i \in I$ на певний час визначена скінчена множина можливих загроз: $Z_i = \left\{z_1^i, z_2^i, \ldots, z_l^i, \ldots, z_{l_i'}^i\right\}, l \in l'$. Вибір типу загрози з врахуванням міри її критичності проводиться ОПР.

Етап 4. Вибір варіанту оцінювання втрат експертами. На вибір ОПР надаються два альтернативних варіантів оцінки очікуваних втрат**:** укрупнене або комплексне оцінювання витрат.

Укрупнений варіант передбачає оцінку втрат групою експертів на основі єдиного узагальнюючого всі види витрат показника. Його оцінка проводиться без формалізованої структуризації думок експертів по окремих критеріях, які є складовими агрегованого показника очікуваних втрат.

Комплексний варіант оцінки передбачає оцінку втрат на основі врахуванням різних типів втрат. Наприклад, «фінансовий збиток», «репутаційний збиток», «можливість функціонування інформаційної системи», «зниження конкурентних переваг» тощо.

При обох альтернативних варіантах експертне оцінювання пропонується проводити на основі якісно-кількісної шкали оцінювання (див. рис. 1).

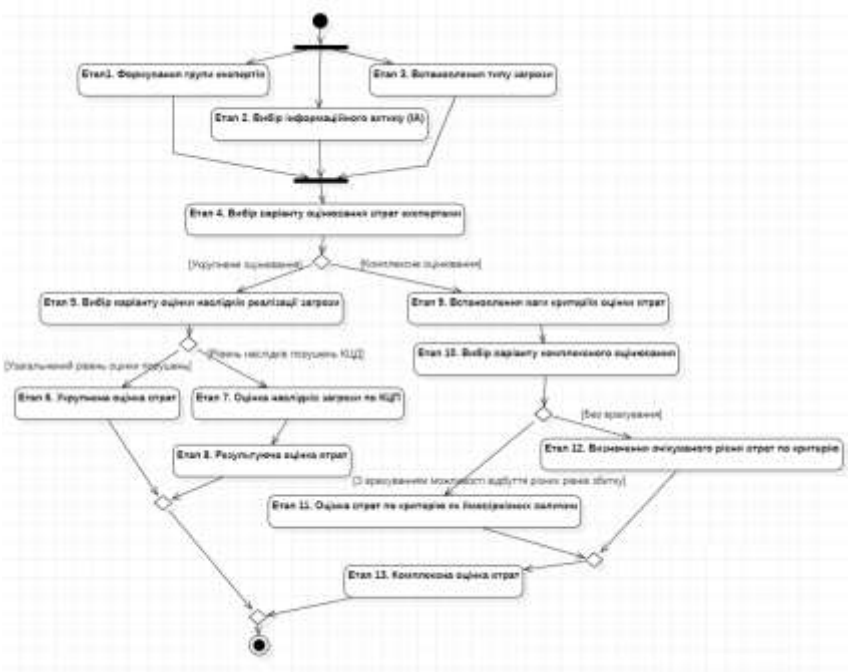

Рис. 2. Алгоритм формування різних сценаріїв оцінювання модуля оцінки очікуваних втрат

Етап 5. Вибір варіанту оцінки наслідків реалізації загрози. ОПР на цьому етапі деталізує правила оцінки втрат як єдиного узагальнюючого показника. Передбачено два альтернативні варіанти вибору. Перший (етапи 6-8) – оцінка наслідків реалізації загрози на узагальненому рівні W_s^l. Другий (етапи 9-13) – очікувані втрати розглядаються на основі трьох показників: порушення конфіденційності інформацій (К) $W_{s\text{К}}^l$, порушення її цілісності (Ц) $W_{s\text{Ц}}^l$ та порушення її доступності (Д) $W_{s\text{К}}^l$.

Етап 6. Укрупнена оцінка втрат. Кожний експерт повинен оцінити на основі встановленої шкали оцінювання (див. рис. 2) очікуваний їм рівень втрат при реалізації загрози на визначеному інформаційному активі W_{sr}^{lp}. При виборі експертом рівня витрат W_r^{mid} встановлюється значення укрупненого показника:

$$W_{sr}^{lp} = W_r^{mid}. \quad (1)$$

На основі встановлених оцінок кожного експерта проводиться узагальнення результатів. При узагальненні передбачене застосування логіко-математичних процедур, що виключають можливість врахування даних з суттєвим розкидом експертних оцінок, і спрямовані на знаходження реального компромісу в оцінках експертів з урахуванням думок і рівня компетентності кожного з них [6, 7, 8]. При досягненні достатнього рівня узгодженості оцінок експертів, встановлюється оцінка очікуваних втрат у вигляді укрупненого показника:

$$W_s^l = \sum_{p=1}^{p^*} W_{sr}^{lp} \times \alpha_p, \quad (2)$$

де α_p – відносний пріоритет *p*-того експерта:

$$\alpha_p = \frac{K_i^p}{\sum_{p=1}^{p^*} K_i^p}. \quad (3)$$

Етап 7. Оцінка наслідків загрози по КЦП. Змістовна особливість реалізації етапу полягає в тому, що експерту надається можливість оцінки очікуваних втрат за правилами, що визначені на етапі 7, але з деталізацією оцінки очікуваних втрат при реалізації від порушення конфіденційності інформацій (К) $W_{s\text{К}}^l$, її цілісності (Ц) $W_{s\text{Ц}}^l$ та доступності (Д) $W_{s\text{К}}^l$.

Етап 8. Результуюча оцінка втрат. Встановлюється значення узагальнюючого показника оцінки втрат з врахуванням різних типів наслідків реалізації загрози:

$$W_{s\text{КЦД}}^l = \max_{\text{КЦД}}\{W_{s\text{К}}^l, W_{s\text{Ц}}^l, W_{s\text{К}}^l\}. \quad (4)$$

Етап 9. Встановлення ваги критеріїв оцінки втрат. При реалізації комплексного підходу до оцінювання очікуваних втрат експерту пропонується надати свої оцінки наслідків реалізації загрози з врахуванням різних критеріїв. Наприклад, оцінити вплив реалізації загрози на фінансовий стан підприємства, негативний вплив на його конкурентоспроможність тощо. На цьому етапі ставиться задача оцінки порівняльної значущості – ваги критеріїв для подальшого її врахуванням при проведенням комплексної оцінки. Для цього експерту надається встановлена ОПР ієрархічна структура критеріїв f_j, *j=1,…J.* Оцінка ваги критеріїв β_j базується на застосуванні можливостей метода аналізу ієрархій. При цьому експерт проводить порівняльну парну оцінку значущості критеріїв різних ієрархічних рівнів.

Постановка задачі оцінки ваги критеріїв та логіко-математичний апарат її реалізації, що враховує оцінки різних експертів, і перевіряє міру логічності та узгодженості оцінок різних експертів, наведений авторами в роботах [6, 7, 8]. Доцільність застосування МАІ [9] в якості базового інструментарію побудови моделі обґрунтовувалась наступними можливостями методу, що суттєво впливають на достовірність результатів оцінювання:

– гнучка ієрархічна структура подання критеріїв оцінювання, надає можливість користувачу, відповідно до ситуаційних умов роботи компанії, вносити зміни як до складу критеріїв оцінювання, так і до рівнів декомпозиції критеріїв;

– розширення інтервалу оцінювання. Якщо більшість методів експертного порівняльного оцінювання (наприклад, парних порівнянь та ранжирування) надають можливість експерту встановити тільки факт переваги одного об'єкта над іншим, МАІ дозволяє врахувати різні рівні переваг;

– допускає порушення умови повної узгодженості оцінок експерта, що в умовах виконання встановлених обмежень, розширює шкалу оцінювання і уточнює результати оцінок.

Етап 10. Вибір варіанту комплексного оцінювання. Передбачаються два альтернативні варіанти оцінювання втрат: перший – детермінована оцінка по кожному критерію очікуваних втрат (етап 12); другий (етап 11) – аналіз наслідків очікуваних втрат як ймовірного результату. Це передбачає надання можливості експерту встановлення декількох можливих рівнів наслідків реалізації загрози та визначення очікуваної ймовірності їх відбуття.

Етап 11. Оцінка втрат по критерію як ймовірнісних величин. Оскільки при оцінюванні експерт працює в умовах неповної визначеності даних, його думка базується не тільки на існуючих знаннях про задачу прийняття рішень в даних умовах, а і потребує проведення професійного інтуїтивного аналізу багатофакторних майбутніх наслідків реалізації загрози. При цьому необхідно враховувати різні ситуаційні умови функціонування системи та різні сценарії реалізації загроз інформаційної безпеки. Для цього в модулі передбачено формалізований інструментарій визначення експертом різних варіантів наслідків реалізації загрози, оцінювання ймовірності їх відбуття та врахування впливу на узагальнену оцінку очікуваних збитків.

Детальний опис логіко-математичного апарату реалізації цього етапу наведений в роботі [6]. В цій статті надано загальну характеристику підходу до реалізації. Етап включає три послідовні процеси. Перший – оцінка експертами ймовірності відбуття кожного рівня втрат (див. рис. 2) по встановленій множині критеріїв $\Upsilon^{l}_{sr j_p}$. Його реалізація базується на базових можливостях методу аналізу ієрархій. При оцінюванні експерт може виключити з оцінювання непередбачені їм рівні втрат і навіть зупинитися на одному можливому, з його точки зору, рівні. Другий – перевірка міри узгодженості думок різних експертів та узагальнення їх оцінок на основі показника Υ^{l}_{srj}:

$$\Upsilon^{l}_{srj} = \sum_{p=1}^{p^*} \Upsilon^{l}_{sr j_p} \times \alpha_p \ . \qquad (5)$$

Третій – встановлення значення очікуваних втрат по критерію. Враховуючи ймовірнісний характер оцінювання, пропонується визначати в якості базового

показник математичного сподівання випадкової величини втрат по критерію MW_{sj}^{l}:

$$MW_{sj}^{l} = \sum_{r=1}^{7} W_{j}^{mid} \times \Upsilon_{srj}^{l}. \quad (6)$$

Етап 12. Визначення очікуваного рівня втрат по критерію. Кожен експерт повинен обрати по кожному критерію на основі встановленої шкали оцінювання (див. рис. 2) очікуваний ним рівень втрат при реалізації загрози на визначеному інформаційному активі W_{sr}^{lp}. Узагальнена оцінка очікуваних втрат по кожному критерію, що враховує оцінки різних експертів, визначається наступним чином:

$$W_{sj}^{l} = \sum_{p=1}^{p^*} W_{sr}^{lp} \times \alpha_{p}. \quad (7)$$

Етап 13. Комплексна оцінка втрат. Комплексна оцінка втрат визначається за двома альтернативними варіантами. **Перший** передбачає оцінку очікуваних втрат по кожному критерію нижчого рівня ієрархічної декомпозиції при врахування можливості відбуття різних рівнів наслідків реалізації загрози MW_{sj}^{l} (при реалізації варіанту розгляд очікуваних втрат як ймовірної величини (етап 11)), **другий** встановлює значення W_{sj}^{l} – при детермінованій оцінці наслідків реалізації загрози (етап 12). В першому та другому випадку комплексну оцінку передбачається задавати у вигляді двох показників: $W_{s}^{l} = \{W_{s}^{l\,mid}, W_{s}^{l\,max}\}$.

Перший $W_{s}^{l\,mid}$ визначає середнє зважене значення комплексного показника, що встановлюється як узагальнений критерій за рахунок зведення багатокритеріальної задачі до скалярної шляхом згортання значень по кожному критерію з врахуванням ваги кожного критерію при визначенні втрат на основі метода лінійної згортки:

$$W_{s}^{l\,mid} = \begin{cases} \sum_{j=1}^{J} MW_{sj}^{l} \times \beta_{j} - \text{ перший варіант оцінювання;} \\ \sum_{j=1}^{J} W_{sj}^{l} \times \beta_{j} - \text{ другий варіант оцінювання.} \end{cases} \quad (8)$$

Показник $W_{s}^{l\,mid}$ може бути єдиним показником для попереднього етапу оцінювання тільки за умови незначного розсіювання оцінки втрат за різними критеріями. При аналізі майбутніх наслідків загрози часто виникає ситуація, коли значний ризик втрат за одним критерієм може компенсуватися за рахунок іншого. Вважається доцільним подання ОПР показника $W_{s}^{l\,max}$, щоби зосередити його увагу при узагальненні оцінок на найбільш негативно впливовому (максимальному значенні) очікуваного критерію оцінювання втрат:

$$W_{s}^{l\,max} = \begin{cases} \max_{j}\{MW_{sj}^{l}\}, j = 1, \dots J - \text{ перший варіант оцінювання;} \\ \max_{j}\{W_{sj}^{l}\}, j = 1, \dots J - \text{другий варіант оцінювання.} \end{cases} \quad (9)$$

Висновки:

1. В статті представлено підхід до побудови модуля оцінки очікуваних витрат в системі управління ризиками інформаційної безпеки КІС ЖЦ будівельної компанії шляхом надання можливості застосування альтернативних сценаріїв оцінювання.

2. Запропоновано технологія функціонування модуля, що побудована як людино-машинний інструментарій оцінювання, що визначає інформаційно-логічні зв'язки між різними етапами роботи та алгоритм формування різних сценаріїв оцінювання.

3. Запропонований підхід, моделі та методи, які використовуються при

оцінюванні очікуваних витрат спрямовані на підвищення вірогідності отриманих результатів. Це досягається за рахунок того, що користувачу надається можливість вибору найбільш доцільного та ефективного сценарію оцінювання. При цьому враховуються цілі та задачі оцінювання, доступність та міра визначеності базових даних, існуючими ресурсними, часовими та інформаційними обмеженнями при прийнятті рішень. Вибір варіанту обробки є прерогативою ОПР.

4. Особливістю побудови модуля є те, що для прийняття рішення ОПР отримує можливість керуватися результатами аналізу міри розсіювання експертних оцінок і впливати на вірогідність результатів з метою їх удосконалення та пошуку раціонального компромісу.

Список літератури:

1. Николаев В.П. Новейшие методы и информационные технологии управления в строительстве. URL: http://www. infobud.com.ua

2. Хлапонін Ю.І., Ізмайлова О.В. Підхід до забезпечення захисту корпоративних інформаційних систем в будівництві. *Управління розвитком складних систем*. 2017. Вип. 31. С. 126-131.

3. Кожедуб Ю. Реалізація процесного підходу до керування ризиками інформаційної безпеки в документах NIST. *Information Technology and Security*. July-December 2017. Vol. 5. Iss. 2 (9), С. 76-89

4. Корченко О.Г., Казмірчук С.В., Ахметов Б.Б., Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія, Київ, ЦП «Компринт», 2017 435 с.

5. Dudykevych V., Prokopyshyn I., Chekurin V., Opirskyy I., Lakh Y., Kret T., Ivanchenko Y., & Ivanchenko I. A multicriterial analysis of the efficiency of conservative information security systems. *Eastern-European Journal of Enterprise Technologies*, vol. 3(9(99), P. 6–13, 2019. https://doi.org/10.15587/1729-4061.2019.166349

6. Izmailova, O., Krasovska, H., Krasovska, K., & Zaslavskyi, V. (2020). Assessing the Variety of Expected Losses upon the Materialisation of Threats to Banking Information Systems. *Information & Security: An International Journal*, 45, 89–118. https://doi.org/10.11610/isij.4506

7. Ізмайлова О.В., Пида С.В., Мельник І.М., Красовська К.К. Підвищення достовірності оцінок значущості критеріїв при визначенні ринкової вартості об'єктів нерухомості. *Управління розвитком складних систем*. 2017. Вип. 29. С. 109-118.

8. Khlaponin, Y., Izmailova, O., Qasim, N. H., Krasovska, H., & Krasovska, K. (2021). Management Risks of Dependence on Key Employees: Identification of Personnel. *Cybersecurity Providing in Information and Elecommunication Systems*, 2923, 295–308. http://ceur-ws.org/Vol-2923/paper33.pdf.

9. Saaty, T.L., & Vargas, L.G. (2013). Decision making with the Analytic Network Process: Economic, political, social and technological applications with benefits, opportunities, costs and risks. https://link.springer.com/book/10.1007/0-387-33987-6

References:

1. Nykolaev, V.P. (2016). Noveishye metody i informatsyonnye tekhnolohii upravlenia v stroitelstve. Available at: http://www. infobud. com. ua/ru [in Russian]
2. Khlaponin, Yu. & Izmailova, O. (2017). Approach to providing the protection of corporate information systems in construction. *Management of Development of Complex Systems*, 31, 126 – 131 [in Ukrainian].
3. Kozhedub, Yu. (2017). Implementation of the process approach to managing risk of information security in the NIST documents. *Information Technology and Security*, 5(2), 76 – 89 [in Ukrainian].
4. Korchenko, O.H., Kazmirchuk, S.V., Akhmetov, B.B. (2017). Prykladni systemy otsiniuvannia ryzykiv informatsiinoi bezpeky. TsP «Komprynt» [in Ukrainian].
5. Dudykevych, V., Prokopyshyn, I., Chekurin, V., Opirskyy, I., Lakh, Y., Kret, T., Ivanchenko, Y., & Ivanchenko, I. (2019). A multicriterial analysis of the efficiency of conservative information security systems. *Eastern-European Journal of Enterprise Technologies*, 3(9 (99), 6–13. https://doi.org/10.15587/1729-4061.2019.166349
6. Izmailova, O., Krasovska, H., Krasovska, K., & Zaslavskyi, V. (2020). Assessing the Variety of Expected Losses upon the Materialisation of Threats to Banking Information Systems. *Information&Security: An International Journal*, 45, 89–118. https://doi.org/10.11610/isij.4506
7. Izmaylova, O., Melnyk, I., Pyda, S., Krasovska, K. (2017). Improving the reliability of estimates of criteria significance while determining the market value of the residential property. *Management of Development of Complex Systems*, 29, 121 – 128 [in Ukrainian].
8. Khlaponin, Y., Izmailova, O., Qasim, N. H., Krasovska, H., & Krasovska, K. (2021). Management Risks of Dependence on Key Employees: Identification of Personnel. *Cybersecurity Providing in Information and Elecommunication Systems*, 2923, 295–308. Retrieved November 22, 2022, available at http://ceur-ws.org/Vol-2923/paper33.pdf.
9. Saaty, T.L., & Vargas, L.G. (2013). Decision making with the Analytic Network Process: Economic, political, social and technological applications with benefits, opportunities, costs and risks. Available at: https://link.springer.com/book/10.1007/0-387-33987-6.

O. Izmailova, H. Krasovska, K. Krasovska

Module for expected losses assessing in the information security risk management system of a construction company

The article examines the problem of the expected losses effective assessment in a construction company upon materialization of information security threats. One of the ways to partially solve this problem is proposed. It is suggested to improve the capabilities of the respective module of the risk management system, which provides the user with a human-machine toolkit for expert assessment of expected losses. This toolkit consists of several stages. The toolkit considers the most effective evaluation scenario given the existing situational decision-making conditions. In order to ensure the operation of the module, the informational and logical connections between the evaluation stages are also defined and the apparatus for the formation of various evaluation scenarios is designed. In addition, to increase the accuracy of the results and

increase the flexibility of the proposed algorithm, the possibility of selecting the evaluation scenario by the user with the appropriate role is provided. Since the paper considers the problem of multi-criteria evaluation, the hierarchy of criteria is formalized, and the weight of their influence on the calculation results is also taken into account. When building a logical-mathematical apparatus, the possibility of realizing various types of threats to various information assets (IA) of the enterprise is also considered. The assessment of the consequences of information security threats can be carried out at different levels: general and distributed, taking into account various indicators such as violations of confidentiality, integrity and availability of information. The methods of direct expert evaluation, analytic hierarchy process (AHP), Delphi, linear convolution of criteria, probabilistic modeling are used in the development of the logico-mathematical apparatus. A qualitative-quantitative scale is used to formalize expert judgments. The necessary roles of experts for effective evaluation have been defined. Summarization of experts' assessments is carried out with control of the adequacy of the degree of logic and dispersion of the opinions of each expert, in accordance with the established requirements for the degree of agreement of the opinions of a group of experts. Competence of the experts is also taken into account during assessment.

Keywords: BIM – technology, BIM-model, corporate information system for building lifecycle management (CIS LM), risk management system, information asset (IA), information security threat, expected losses, aggregated and comprehensive losses assessment, expert assessment.

Посилання на статтю

APA: Izmailova, O., Krasovska, H., & Krasovska, K. (2022). Module for expected losses assessing in the information security risk management system of a construction company. *Shliakhy pidvyshchennia efektyvnosti budivnytstva v umovakh formuvannia rynkovykh vidnosyn*, 50 (1), 81-92.

ДСТУ: Ізмайлова О.В., Красовська Г.В., Красовська К.К. Модуль оцінки очікуваних втрат в системі управління ризиками інформаційної безпеки будівельної компанії. *Шляхи підвищення ефективності будівництва в умовах формування ринкових відносин*. 2022. № 50 (1). С. 81-92.