КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (12), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.12.96107
УДК 005.336.1:004.056

Чубаєвський Віталій Іванович
кандидат політичних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет, м.Київ, Україна
ORCID ID: 0000-0001-8078-2652
chubaievskyi_vi@knute.edu.ua

Лахно Валерій Анатолійович
доктор технічних наук, професор, завідувач кафедри комп'ютерних систем та мереж
Національний університет біоресурсів і природокористування України, м.Київ, Україна
ORCID ID: 0000-0001-9695-4543
lva964@gmail.com

Криворучко Олена Володимирівна
доктор технічних наук, професор, завідувач кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет, м.Київ, Україна
ORCID ID: 0000-0002-7661-9227
kryvoruchko_ev@knute.edu.ua

Касаткін Дмитро Юрійович
кандидат педагогічних наук, доцент, доцент кафедри комп'ютерних систем та мереж
Національний університет біоресурсів і природокористування України, м.Київ, Україна
ORCID ID: 0000-0002-2642-8908
dm_kasat@ukr.net

Десятко Альона Миколаївна
PhD in Computer Sciences, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет, м.Київ, Україна
ORCID ID: 0000-0003-2860-2188
desyatko@knute.edu.ua

Блозва Андрій Ігорович
кандидат педагогічних наук, доцент, доцент кафедри комп'ютерних систем та мереж
Національний університет біоресурсів і природокористування України, м.Київ, Україна
ORCID ID: 0000-0002-4377-0916
andriy.blozva@nubip.edu.ua

ЕФЕКТИВНІСТЬ МЕТОДИКИ РОЗРАХУНКУ ПОКАЗНИКІВ ІНВЕСТИЦІЙ В СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТІВ ІНФОРМАТИЗАЦІЇ

Анотація. У статті проведено аналіз публікацій за проблематикою оцінки інвестицій в інформаційну безпеку об'єктів безпеки інформатизації. Обґрунтовано можливість і необхідність отримання необхідних даних, що сприяють достовірній оцінці ефективності заходів, спрямованих на підвищення інформаційної безпеки компанії. У процесі дослідження застосовано методи імітаційного моделювання. Пропонується методика розрахунку показників від інвестиційних заходів в рамках підвищення метрик ІБ ОБІ. Описано конкретний приклад застосування імітаційного моделювання. У запропонованій методиці передбачена оцінка попередження шкоди від кібератаки. Як базисний показник розрахунку економічного ефекту від інвестування в засоби захисту інформації (ЗЗІ) прийнятий розмір попередження шкоди від кібератаки. Запропоноване імітаційне моделювання дало можливість врахувати відносну невизначеність реальної ситуації з ІБ ОБІ. Проведені дослідження нададуть можливість практикам у сфері інформаційної безпеки отримувати за допомогою викладеного в роботі підходу формулювати обґрунтовані рішення по підвищенню ефективності інвестиційних проектів в сфері інформаційної безпеки для ОБІ. На

відміну від існуючих, у запропонованій методиці враховані як прямі, так і непрямі чинники інвестиційних проектів в сфері ІБ ОБІ.

Ключові слова: інформаційна безпека; захист інформації; невизначеність; методика імітаційного моделювання, процес інвестування; методика; попереджені збитки

ВСТУП

Відповідно до загальноприйнятої точки зору, характерною для більшості фахівців в області інформаційної безпеки (ІБ), сформувалася думка, що інвестування в ІБ і її концепція для конкретного об'єкта інформатизації (ОБІ) будуть ефективним якщо забезпечити виконання вимог державних нормативних документів і стандартів. Така точка зору сформувалася на основі, єдиної загальновизнаної методики оцінки економічного ефекту від інвестування в ІБ ОБІ [1, 2]. Зауважимо, що в даному контексті проблематики оцінювання ефективності інвестування в ІБ ОБІ розуміється перевищення вартісної оцінки кінцевого результату відповідних заходів над сумарними розмірами інвестицій тобто сукупними витратами фінансових ресурсів на ІБ ОБІ в перебігу фіксованого періоду часу [3].

Постановка проблеми. Складність оцінювання реального ефекту від інвестування в ІБ ОБІ обумовлюється досить великим переліком специфічних для сектора захисту інформації та кібернетичної безпеки чинників. Загалом, відзначимо лише істотний вплив на ефективність інвестування в ІБ ОБІ таких факторів як 1) постійно мінливий ландшафт кіберзагроз; 2) різноваріантність стратегії і тактики атакуючої сторони (комп'ютерних зловмисників); 3) швидкий розвиток технічних засобів захисту інформації (ЗІ) і кібербезпеки (КБ) ін. У свою чергу, відповідно до базових постулатів теорії оцінки ефективності систем, відомо, що якість засобів ЗІ (далі ЗЗІ), може проявлятися лише під час реального цільового застосування на ОБІ. Саме ця обставина дає можливість об'єктивно оцінювати ефективність їх застосування, а, отже, і результативність інвестицій в ЗЗІ на ОБІ [4,5].

Додаткова складність при оцінюванні ефективності інвестування в ІБ ОБІ пов'язана з невизначеністю результатів функціонування ЗЗІ. На етапі проектування ЗЗІ присутні фактори невизначеності. Наприклад, пов'язані з тим, що може скластися така ситуація, при якій сторона захисту ОБІ витратить сотні тисяч у.о. або навіть мільйони на захист від складних націлених кібератак, а атакуючої стороні часто досить вдатися до невеликих витратах («інвестицій в кібератаку») застосуємо методи соціальної інженерії. Така тактика застосування методів соціальної інженерії в ряді випадків допомагала обходити найсучасніші ЗЗІ [6]. Таким чином, під час реалізації проектів в сфері ІБ рівень функціональності ЗЗІ може знизиться. Отже, з точки зору методології моделювання ефективності інвестування в ІБ ряд функціональних метрик ЗЗІ не може бути тотожним виражений і описаний детермінованими показниками.

Зауважимо, що в ході багатокритеріальної оптимізації ЗЗІ також виконується оцінювання рівня гарантій ІБ в залежності від особливостей ОБІ (наприклад, банк, промислове підприємство, сфер торгівлі або освіти і т.п.). Цей рівень в досить великій мірі залежить від розміру потенційно запобігання шкоди для інформаційних масивів ОБІ. В такому випадку, виникає нове завдання, пов'язане з отриманням чисельної оцінки ризику для ОБІ. Тобто, стороні захисту необхідно володіти уявленням про розподіл випадкових величин збитку в разі атаки. У такій ситуації традиційно застосовують методи імітаційного моделювання. Як альтернативний підхід також використовують результати активного аудиту ІБ (або ЗЗІ) для аналізованого ОБІ.

Аналіз останніх досліджень і публікацій. У роботах [7, 8] було показано, що когнітивні моделі дають можливість в цілому аналізувати ЗЗІ для ОБІ. Автори в своїх моделях здійснюють вибір комплексів заходів щодо вдосконалення ЗЗІ. Крім того, можна визначати спрямованість необхідних дій на ситуацію з ЗІ. Авторами розглянута процедура вибору метрик ІБ, які здатні охарактеризувати розвиток ситуації в перспективі. На думку авторів [8,9] значущістю когнітивного моделювання є можливість обліку не тільки якісних, а й кількісних показників ЗЗІ. Як недолік такого підходу можна відзначити лише сценарні прогнози розвитку ситуації.

В [10] авторами в ході моделювання розглядався часовий чинник в процесі інвестування в ІБ ОБІ. Проаналізовано тактика захисту, яку автори назвали «чекай і дивися». Тобто, стороні захисту слід обмежити надмірне інвестування коштів в ЗЗІ та ІБ (або в авторській термінології КБ), виходячи з уже досягнутого результату. Безсумнівною перевагою такого підходу слід визнати можливість брати до уваги невизначеність настання того моменту часу, коли, виходячи з наявних даних про атаку, можна гнучко збільшувати (або зменшувати) розміри інвестиційних коштів на ЗЗІ для пом'якшення наслідки атаки. Відповідно, даний підхід на не позбавлений суб'єктивності. Адже, на думку авторів [10], єдиний спосіб отримати інформацію про атаку це фіксація факту атаки. Лише після цього, сторона захисту повинна відреагувати і виділити фінансовий ресурс (далі ФР) на ІБ ОБІ. Недоліком цього підходу є те, що він заснований на структурі з дискретним часом атаки, а це призводить до необхідності повторно проводити розрахунки в разі зміни ситуації і метрик ІБ ОБІ. Автори [10] вказують, що традиційні методи оцінювання інвестиційних проектів, як правило, занижують їх вартість.

Резюмуючи вищевикладене, можна констатувати, що:

1) ефективність заходів, спрямованих на підвищення ступеня захищеності і ІБ ОБІ не може бути обґрунтована лише на основі детермінованих оцінок;

2) ефективність заходів, спрямованих на підвищення захисту ОБІ і поліпшення його ІБ вимагає задіяння імовірнісних характеристик. До таких можна, зокрема, віднести функцію розподілу показників попередженої в результаті деструктивних дій зловмисників шкоди для ОБІ.

Мета статті. - Розробка методики розрахунку показників від інвестицій в системи інформаційної безпеки об'єкта інформатизації.

Для досягнення мети вирішуються такі завдання:

вдосконалення методики розрахунку показників від інвестиційних заходів в рамках підвищення метрик ІБ ОБІ на основі базисного показника - розмір попередженої шкоди від кібератаки;

застосування методів імітаційного моделювання для конкретного прикладу розрахунку ефективності інвестування в ІБ ОБІ з урахуванням як прямих, так і непрямих факторів інвестиційних проектів в сфері ІБ ОБІ.

МЕТОДИКА ДОСЛІДЖЕННЯ

У процесі розрахунку економічної ефективності від інвестицій в ІБ ОБІ, як правило, використовують дві наступні змінні. Відповідно, отриманий в ході впровадження засобів і заходів по ІБ результат, зведений до фінансового показника по витратам на впроваджувані засоби і заходи щодо забезпечення ІБ.

Фактичним кінцевим результатом впровадження засобів щодо забезпечення ІБ можна вважати розмір (в грошовому еквіваленті), що відповідає попереджуваним

ISSN 2663 - 4023

втратам (попереджуваній шкоді від кібератак). Цей параметр можна формалізувати наступним чином:

$$D_i = D_i^{'} - D_i^{''}, \quad (1),$$

де $D_i^{'}, D_i^{''}$ – збиток від атак, відповідно до і після впровадження засобів і заходів по ІБ.

Фактично, розмір попереджуваної шкоди від кібератак відображає частку недоотриманого прибутку, через те, що не було впроваджені відповідні засоби і заходи по ІБ протидії загрозам.

Тоді сумарний розмір попереджуваної шкоди від кібератак визначимо:

$$P = \sum_{i=1}^{n} P_i + R_i, \quad (2),$$

де R_i - величина безпосередньо повертаються фінансових ресурсів. Відповідно, такими ресурсами можуть бути, наприклад, кошти, які в були б стягнені в якості штрафних санкцій стосовно працівників, які порушили політику ІБ компанії і т.п.

Використання подібного комбінованого підходу передбачає наступну послідовність дій для моделювання (наприклад, імітаційного) розміру попереджуваної шкоди від кібератак:

Крок 1. Розбиваємо потенційні втрати (збитки) на групи. Як критерій такого розбиття можна застосовувати категорійний розподіл інцидентів ІБ за ступенем небезпеки для ОБІ, застосовуючи типові метрики ІБ [10];

Крок 2. На підставі наявної статистики кіберінцидентів по ОБІ та використовуючи СППР або експертів виконуємо оцінку значення величини втрат (попереджуваної шкоди) для кожного інциденту. Ця величина може варіювати від мінімального (min), до і максимального (max) значення. Подібний крок виконується як до, так і після реалізації заходів щодо посилення ІБ ОБІ;

Крок 3. Застосовуючи попередньо обраний закон розподілу, створити модель величини втрат (до і після впровадження заходів і засобів ІБ);

Крок 4. Розрахувати сумарне значення попереджуваної шкоди від кібератак на підставі попередніх кроків 1-3;

Крок 5. Розрахувати статистичні характеристики для величин, на основі яких була створена модель, а також підсумкові показники економічної ефективності впроваджених коштів і проведених заходів щодо посилення ІБ ОБІ.

Для візуалізації результату розрахунку доцільно побудувати гістограму розподілу результуючого значення попереджуваної шкоди від кібератак, або гістограму інтегрального відсотку розподілу попереджуваної шкоди від кібератак. Точний підбір закону розподілу сумарного результуючого значення попереджуваної шкоди від кібератак дозволить досить точно оцінювати ймовірні характеристики в будь-якому місці гістограми або по відношенню до інтервалу, який аналізується.

Таким чином, імовірнісна характеристика попереджуваної шкоди від кібератак може бути прийнята в якості обґрунтованого критерію ефективності заходів, спрямованих на підвищення ІБ ОБІ.

Більш трудомістким завданням є визначення конкретних розмірів витрат на забезпечення ІБ ОБІ. Такі витрати включають в себе такі статті витрат:

- утримання відділу ІБ ОБІ;
- витрати на закупівлю, експлуатацію, ремонт і апаратно-програмних ЗЗІ;
- інше

Крім того, під час розрахунку ефективності інвестування в ІБ ОБІ обов'язково слід врахувати важливість інформаційних активів в бізнес-процесах компанії. Розрахувати цей параметр можна застосувавши таку залежність:

$$S_j = C/Y, \quad (3),$$

Де: S_j – важливість j-го інформаційного активу в бізнес процесах компанії;

C – вартість j-го інформаційного активу;

Y – величина капіталу, вкладеного в експлуатацію j-го інформаційного активу.

Коли мова йдеться про оцінку ефективності чи іншого ЗЗІ слід брати до уваги і таку категорію параметрів як ризики порушення ІБ ОБІ. Ризик може бути одиничним, суб'єктивним, сукупним [9].

Відповідно, кожен з цих видів ризику може бути розрахований наступним чином:

Одиничний ризик (R_i):

$$R_i = p_i \cdot d_i, \quad (4),$$

де p_i – ймовірність того, що зловмисник реалізує загрозу ІБ ОБІ;

d_i – збиток від i-ї загрози для ІБ ОБІ;

Суб'єктивний ризик (R_{sub}):

$$R_{sub} = N_R/Y, \quad (5)$$

де N_R – сумарна кількість всіх ризиків;

Y – кількість актуальних ризиків;

Сукупний ризик (Q):

$$Q = \sum_{i=1}^{n} R_i + R_{sub}, \quad (6)$$

де n – загальне число кіберзагроз для ІБ ОБІ.

Проаналізувавши низку публікацій [8-10] більшість дослідників орієнтовані на оцінювання ризиків порушення ІБ за локальними ознаками. Якщо узагальнити дані публікації (Таб. 1), то можна помітити, що в основному застосовуються такі моделі: Cost Benefit Analysis - CBA, Net Present Value - NPV, Profitability Index - PI, Internal Rate of Return - IRR [8].

Таблиця 1

Моделі для оцінки витрат на ІБ ОБІ

№	Модель	Переваги	Недоліки
1	DCF	1. Комплексний підхід при оцінюванні витрат на ІБ. 2. Облік всіх етапів життєвого циклу компонентів ЗЗІ, а також бізнес-процесів компанії.	Модель статична. До уваги не прийняті можливі зміни ситуації з ІБ, наприклад, під час тривалої атаки.

ISSN 2663 - 4023

2	PI	1. Достатня кореляція моделі з типовими методами бухгалтерського обліку. 2. Простота і швидкість отримання результатів оцінки інвестування в ІБ.	1. Не береться до уваги інфляція. 2. Неадаптивність
3	NPV	1. Можливість обліку різної вартості ресурсів для підвищення ступеня ІБ ОБІ. 2. Прийнято до уваги позиція і інтереси інвестора.	1. Частину ресурсів неможливо оцінити в грошовому еквіваленті. 2. Прив'язка моделі до показників вартості компанії.

В даний час найбільш популярні наступні моделі для оцінки витрат на ІБ: NPV (Net Present Value) і DCF (Discounted Cash Flow). Не зважаючи на переваги та недоліки кожного з цих методів і моделей [8, 9], зауважимо, що багато моделей, самі по собі орієнтовані лише на економічний аспект оцінки ефективності.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Отримані на підставі реалізації кроків 1-5 результати можна використовувати в сукупності з будь-яким із методів (CBA, NPV, PI, IRR і ін.). Такий комбінований підхід дозволить власникам інформаційних ресурсів компанії (ОБІ) з гарантійною імовірністю отримати різні сценарії (від песимістичних до оптимістичних) результатів інвестування в ІБ ОБІ. При цьому основна обчислювальна робота може бути перекладена на інтелектуальні інформаційні системи, наприклад, СППР (Рис. 1.)

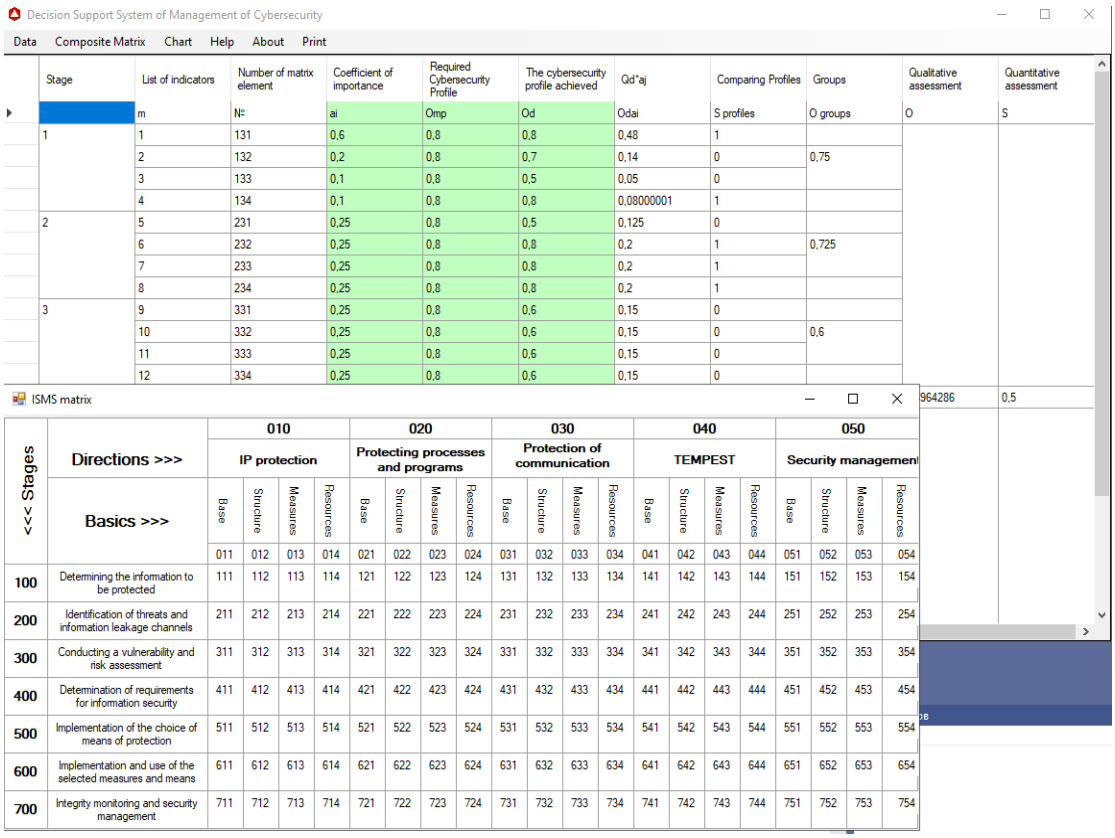

Рис. 1. Загальний вигляд інтерфейсу інтелектуальної системи для оцінювання ефективності заходів, спрямованих на забезпечення ІБ ОБІ

ISSN 2663 - 4023

Блок-схема алгоритму функціонування підсистеми «Оцінювання ефективності заходів, спрямованих на забезпечення ІБ ОБІ» на рис. 2.

Розглянемо приклад варіанту оцінювання ефективності заходів, спрямованих на забезпечення ІБ ОБІ.

Припустимо, що є проєкт по підвищенню ступеня ІБ ОБІ. У тестовому прикладі проєкт може включати в себе наступні заходи (Рис. 2).

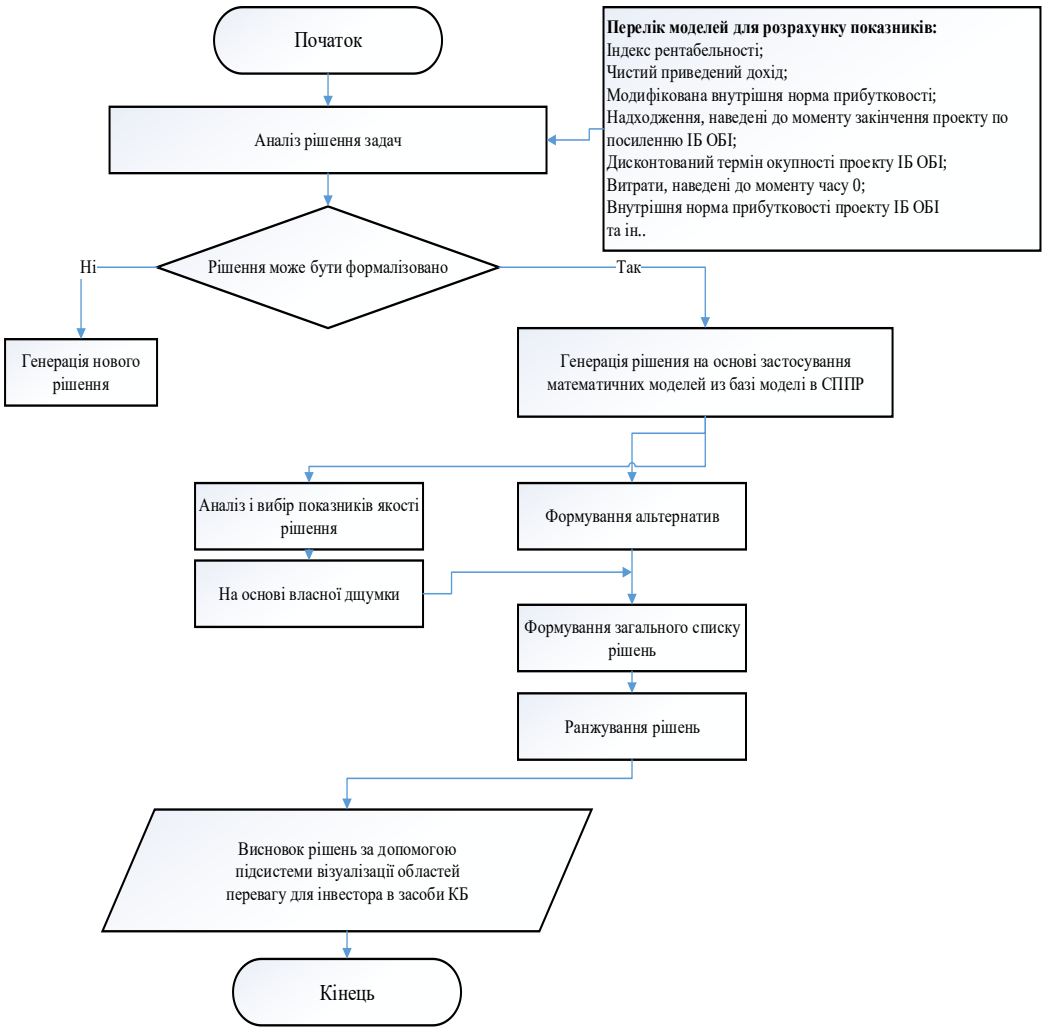

Рис. 2. Блок-схема алгоритму функціонування підсистеми СППР «Оцінювання ефективності заходів, спрямованих на забезпечення ІБ ОБІ»

Для розрахунку показників чистого приведеного доходу (NPV), індексу рентабельності (PI), внутрішньої норми прибутковості (IRR), модифікованої внутрішньої норми прибутковості (MIRR), дисконтованого терміну окупності проекту (DPB) використаємо вже проведені дослідження[4], а також формулами (1) - (6). Необхідно отримати результати для трьох сценарних результатів розрахунку з метою прийняття обґрунтованого рішення про доцільність інвестування в проекти ІБ.

ISSN 2663 - 4023

Таблиця 2

Витрати і можливі надходження коштів в результаті проведення заходів щодо підвищення ІБ ОБІ

Заходи щодо підвищення рівня ІБ ОБІ	Витрати, тис. у.е.	Надходження, тис. у.е.			
		Позначення	Min (мінімальне)	Mid (Найвирогідніший)	Max (Максимальне)
M1 (технічні, наприклад, придбання нового файєрвола)	65	P1	160	270	420
M2 (організаційні, наприклад, тренінги для співробітників відділу ІБ)	35	P2	90	170	300
M3 (інші)	20	P3	50	100	190
Сума	**120**		**300**	**540**	**910**

Описову статистику підсумкового розподілу суми попереджуваної шкоди від кібератак представлено в табличній формі (Таб. 3)

Таблиця 3

Результати розрахунку описової статистики для надходжень коштів в результаті проведені заходів по підвищенню ІБ ОБІ

Показник	Позначення	Значеннння
Середнє значення	μ	33,9
Стандартна помилка	δ	0,74
Стандартне відхилення	σ	7,4
Дисперсія вибірки	Ω	470,2
Min значення	Min	5
Max значення	Max	35,1

Результати моделювання для різних сценаріїв інвестиційного процесу в ІБ ОБІ для тестового прикладу наведено в таблиці 4.

Таблиця 4

Оцінка ефективності проектів з підвищення ІБ ОБІ для різних сценаріїв

Сценарії	Позначення	Надходження за період, тыс. у.е.
Песимістичний	S_{pes}	31
Найбільш ймовірний	S_{mp}	45
Оптимістичний	S_{op}	62

На фінальному етапі тестування по кожному із сценаріїв визначаємо показники ефективності проєкту підвищення ІБ (табл.5).

Аналіз результатів розрахунків, дозволив зробити такий висновок (для заданих вхідних даних), що всі сценарії крім песимістичного задовольняють умови схвалені з боку керівництва компанії проєкту з інвестування в ЗЗІ та заходи, спрямовані на підвищення рівня ~~и~~ ІБ. Для того, щоб керівництву компанії прийняти остаточне рішення про доцільність інвестування коштів в ІБ, слід визначити близькість кожного з розглянутих сценаріїв до гіпотетичного ідеального проєкту. Це можна реалізувати застосувавши, наприклад, такі метрики як Евклідова відстань або кореляцію Пірсона. В такому випадку необхідно виконати нормування показника чистого приведеного доходу (NPV) для відповідного сценарію. Нормування необхідно виконувати по відношенню до максимального значення.

Ідеальним можна вважати проєкт інвестування в ІБ якщо сценарій відповідає таким показникам: $NPV = 2; PI = 2; MIRR = 1.$

Таблиця 5

Показники ефективності ІТ-проекту за сценаріями

Показник ефективності інвестиційного проекту в ІБ ОБІ	Позначення параметра	Варіант сценарію		
		S_{pes}	S_{mp}	S_{op}
Індекс рентабельності	PI	0,85	1,2	1,11
Чистий наведений дохід	NPV	9,2	27,0	13,3
Модифікована внутрішня норма прибутковості	$MIIR$	0,12	0,18	0,17
Надходження, наведені до моменту закінчення проєкту щодо посилення ІБ ОБІ	FPI	189,0	196,0	161,3
Дисконтований термін окупності проекту ІБ ОБІ	DPB	3,7	2,4	1,79
Витрати, наведені до моменту часу $t = 0$	PVO	120	120	120
Внутрішня норма прибутковості проєкту ІБ ОБІ	IIR	0,14	0,22	0,18

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Провівши аналіз існуючих наукових джерел стосовно інвестиційних проєктів інформаційної безпеки (ІБ) об'єктів інформатизації (ОБІ), обґрунтовано можливість і необхідність отримання необхідних даних, що сприяють достовірній оцінці ефективності заходів, спрямованих на підвищення ІБ (КБ) компанії. Запропоновано методику розрахунку показників щодо інвестиційних заходів в рамках підвищення метрик ІБ ОБІ на конкретному прикладі. У запропонованій методиці передбачено оцінка попереджуваної шкоди від кібератаки. Як базисний показник розрахунку економічного ефекту від інвестування в ЗЗІ прийнято розмір попереджуваної шкоди від кібератаки.

Розрахунок ефективності інвестування в ІБ ОБІ методами імітаційного моделювання, дав можливість врахувати відносну невизначеність реальної ситуації з ІБ ОБІ. Відповідно, проведені дослідження допоможуть фахівцям-практикам у сфері ІБ отримувати, за допомогою викладеного в роботі підходу, обґрунтовані рішення для підвищення ефективності інвестиційних проєктів в сфері ІБ для ОБІ. На відміну від існуючих, у запропонованій методиці враховані як прямі, так і непрямі чинники інвестиційних проєктів в сфері ІБ ОБІ. Дане дослідження є затребуваним на часі та потребує подальшої роботи в напрямку моделювання системи оцінювання ефективності захисту корпоративної інформації.

ISSN 2663 - 4023

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Pieters, W., Probst, C. W., Lukszo, Z., & Montoya, L. (2014). Cost-effectiveness of security measures: A model-based framework. In *Approaches and processes for managing the economics of information systems* (pp. 139-156). IGI global.
2. Brangetto, P., & Aubyn, M. K. S. (2015). Economic aspects of national cyber security strategies. *Brangetto P., Aubyn MK-S. Economic Aspects of National Cyber Security Strategies: project report. Annex*, *1*(9-16), 86.
3. Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: uncertainties, risks and cyber security. *Procedia computer science*, *149*, 65-70.
4. Chronopoulos, M., Panaousis, E., & Grossklags, J. (2017). An options approach to cybersecurity investment. *IEEE Access*, *6*, 12175-12186.
5. Hallman, R. A., Major, M., Romero-Mariona, J., Phipps, R., Romero, E., Slayback, S. M., & San Miguel, J. M. (2021). Determining a Return on Investment for Cybersecurity Technologies in Networked Critical Infrastructures. *International Journal of Organizational and Collective Intelligence (IJOCI)*, *11*(2), 91-112.
6. Nagurney, A., & Shukla, S. (2017). Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research*, *260*(2), 588-600.
7. Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018). Simulations in cyber-security: a review of cognitive modeling of network attackers, defenders, and users. *Frontiers in psychology*, *9*, 691.
8. Gonzalez, C., Ben-Asher, N., & Morrison, D. (2017). Dynamics of decision making in cyber defense: Using multi-agent cognitive modeling to understand cyberwar. In *Theory and Models for Cyber Situation Awareness* (pp. 113-127). Springer, Cham.
9. Maqbool, Z., Pammi, V. C., & Dutt, V. (2019). Behavioral Cybersecurity: Investigating the influence of Patching Vulnerabilities in Markov Security Games via Cognitive Modeling. *IJCSA*, *4*(1), 185-209.
10. Gordon, L., Loeb, M., Lucyshyn, W. (2003). Information security expenditures and real options: A wait-and-see approach, *Computer Security Journal*, *19*(2), 1-7.
11. Majd, S, Pindyck, R. (1987). Time to build, option value, and investment decisions, *Journal of Financial Economics*, *1*(1), 7-27.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (12), 2021
ISSN 2663 - 4023

Vitaliy Chubaievskyi
Candidate of Political Sciences, Associate Professor of Department of Software Engineering and Cyber Security
Kyiv National University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0001-8078-2652
chubaievskyi_vi@knute.edu.ua

Valerii Lakhno
Doctor of Technical Sciences, Professor of Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0001-9695-4543
lva964@gmail.com

Olena Kryvoruchko
Doctor of Engineering Sciences, Professor, Head of Department of Software Engineering and Cyber Security
Kyiv National University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0002-7661-9227
kryvoruchko_ev@knute.edu.ua

Dmytro Kasatkin
Candidate of Pedagogical Sciences, Associate Professor, Associate Professor of Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine Kyiv, Ukraine
ORCID ID: 0000-0002-2642-8908
dm_kasat@ukr.net

Alona Desiatko
PhD in Computer Sciences, Associate Professor of Department of Software Engineering and Cyber Security
Kyiv National University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0003-2860-2188
desyatko@knute.edu.ua

Andrii Blozva
Candidate of Pedagogical Sciences, Associate Professor, Associate Professor of Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine Kyiv, Ukraine
ORCID ID: 0000-0002-4377-0916
andriy.blozva@nubip.edu.ua

EFFICIENCY OF THE INDICATORS INVESTMENT CALCULATION METHOD IN THE INFORMATION SECURITY SYSTEM OF INFORMATION OBJECTS

Abstract. The article analyzes publications on the evaluation of investments in information security (IS) of objects of informatization (OBI). The possibility and necessity of obtaining the necessary data have been substantiated, contributing to a reliable assessment of the effectiveness of measures aimed at increasing the company's IS. In the study process, the modelling methods have been used. A methodology is proposed for calculating indicators from investment activities in the context of increasing IS metrics of OBI. A specific example of such simulation is described. The proposed methodology provides an assessment of the damage prevention from a cyber-attack. The amount of the damage prevention from a cyber-attack is taken as a basic indicator for calculating the economic effect of investing in information security tools (IST). The performed simulation modelling allowed taking into account the relative uncertainty of the real situation with IS of OBI. The conducted study will help practitioners in the field of IS to obtain informed decisions to increase the efficiency of investment projects in the field of IS for OBI, using the approach outlined in the study. Unlike the existing ones, the proposed methodology takes into account both direct and indirect factors of investment projects in the field of IS of OBI.

Keywords: information security; information protection; uncertainty; investment process; methodology; damage prevention.

ISSN 2663 - 4023

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Pieters, W., Probst, C. W., Lukszo, Z., & Montoya, L. (2014). Cost-effectiveness of security measures: A model-based framework. In *Approaches and processes for managing the economics of information systems* (pp. 139-156). IGI global.
2. Brangetto, P., & Aubyn, M. K. S. (2015). Economic aspects of national cyber security strategies. *Brangetto P., Aubyn MK-S. Economic Aspects of National Cyber Security Strategies: project report. Annex*, *1*(9-16), 86.
3. Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: uncertainties, risks and cyber security. *Procedia computer science*, *149*, 65-70.
4. Chronopoulos, M., Panaousis, E., & Grossklags, J. (2017). An options approach to cybersecurity investment. *IEEE Access*, *6*, 12175-12186.
5. Hallman, R. A., Major, M., Romero-Mariona, J., Phipps, R., Romero, E., Slayback, S. M., & San Miguel, J. M. (2021). Determining a Return on Investment for Cybersecurity Technologies in Networked Critical Infrastructures. *International Journal of Organizational and Collective Intelligence (IJOCI)*, *11*(2), 91-112.
6. Nagurney, A., & Shukla, S. (2017). Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research*, *260*(2), 588-600.
7. Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018). Simulations in cyber-security: a review of cognitive modeling of network attackers, defenders, and users. *Frontiers in psychology*, *9*, 691.
8. Gonzalez, C., Ben-Asher, N., & Morrison, D. (2017). Dynamics of decision making in cyber defense: Using multi-agent cognitive modeling to understand cyberwar. In *Theory and Models for Cyber Situation Awareness* (pp. 113-127). Springer, Cham.
9. Maqbool, Z., Pammi, V. C., & Dutt, V. (2019). Behavioral Cybersecurity: Investigating the influence of Patching Vulnerabilities in Markov Security Games via Cognitive Modeling. *IJCSA*, *4*(1), 185-209.
10. Gordon, L., Loeb, M., Lucyshyn, W. (2003). Information security expenditures and real options: A wait-and-see approach, *Computer Security Journal*, *19*(2), 1-7.
11. Majd, S, Pindyck, R. (1987). Time to build, option value, and investment decisions, *Journal of Financial Economics*, *1*(1), 7-27.