e-ISSN 1607-3274 Радіоелектроніка, інформатика, управління. 2019. № 2
p-ISSN 2313-688X Radio Electronics, Computer Science, Control. 2019. № 2

УДК 519.863

МЕТОД РОЗРАХУНКУ ОПТИМАЛЬНОСТІ ВИТРАТ НА ІНФОРМАЦІЙНУ ТА КІБЕРБЕЗПЕКУ

Романюков М. Г. – аспірант кафедри Інформатики та управління захистом інформаційних систем Одеського національного політехнічного університету, Одеса, Україна.

АНОТАЦІЯ

Актуальність. Досліджено загальну математичну модель за участю двох протиборчих сторін (нападника та захисника). Встановлено, що досліджувана модель дозволить отримати практичні результати по розрахунку оптимального коефіцієнту витрат на інформаційну та кібербезпеку об'єкту інформаційної діяльності.

Мета роботи. Отримати метод по розрахунку оптимального коефіцієнту витрат на інформаційну та кібербезпеку об'єктів інформаційної діяльності, де циркулює інформація з обмеженим доступом.

Метод. Полягає у розробці ігрової моделі з двома протиборчими сторонами та алгоритму для забезпечення гарантованого результату по показнику втрат від атак зі сторони захисту. При цьому кількість засобів захисту та число атак можуть вимірюватись десятками, а в окремих випадках навіть сотнями. Для вирішення поставленої задачі даним методом використовується критерій оптимальності Вальда із вирішенням задачі булевого програмування, оскільки проектуючи систему захисту, необхідно забезпечити гарантований результат при будь-яких умовах.

Результати. Отримано практичні результати по розрахунку оптимального коефіцієнту витрат на інформаційну та кібербезпеку об'єктів інформаційної діяльності, де циркулює інформація з обмеженим доступом.

Висновки. Таким чином, отриманий метод дозволить отримати практичні результати по розрахунку оптимального коефіцієнту витрат на інформаційну та кібербезпеку об'єктів інформаційної діяльності, де циркулює інформація з обмеженим доступом. Важливим є врахування всіх методів та засобів захисту у тому числі методів і засобів соціального інжинірингу, що створюють найнебезпечніший канал витоку інформації з обмеженим доступом. Роботу даного методу було підтверджено експериментально на прикладі загроз соціального інжинірингу та побудовано відповідні графіки залежностей як упереджених так і не упереджених збитків від даного виду атак.

КЛЮЧОВІ СЛОВА: інформаційна та кібербезпека, методи розрахунку оптимальності витрат, булеве програмування.

АБРЕВІАТУРИ

OSINT – open source intelligence (моніторинг відкритих та відносно-відкритих джерел);

ЗЗІ – засоби захисту інформації;

ІзОД – Інформація з обмеженим доступом;

КР – кіберрозвідка;

ІТС – інформаційно-телекомунікаційна система;

МР – мережева розвідка;

РсТ – розвідка систем комунікацій;

СІ – соціальна інженерія.

НОМЕНКЛАТУРА

A – перелік можливих загроз;

B – перелік можливих засобів захисту;

$C^{(3)}(x)$ – вартість використаних засобів захисту;

$C_j^{(3)}x_j$ – вартість j-го засобу захисту;

$C^{(H)}(y)$ – вартість використаних засобів нападу;

$C_i^{(H)}(y_i)$ – вартість i-того засобу нападу;

$C_{\max}^{(3)}$ – максимальна сума, яку може витратити сторона захисту;

$C_{\max}^{(H)}$ – максимальна допустима вартість, яку може витратити сторона нападу;

i – порядковий номер засобу нападу;

j – порядковий номер засобу захисту;

$P_{\text{н.з}}, P_{\text{у.з.}}$ – вартість витрат захисника у випадку неупередженого $P_{\text{н.з}}$ і упередженого $P_{\text{у.з.}}$ захисту;

M – множина допустимих значень засобів захисту;

N – множина допустимих значень засобів нападу;

p_{ij} – можливі імовірності i-тої загрози для j-го захисту;

$P_н$ – вартість витрат нападника;

U_{MinMax} – мінімальне значення максимально можливих витрат зі сторони захисту;

$U^{\max}(\vec{Y})$ – максимально можливий збиток з боку захисту;

U_{Max} – максимально можливі сумарні витрати обох гравців;

$U^{\text{пред}}(\vec{X},\vec{Y})$ – упереджений збиток з боку захисту;

$U_i, \forall_{i\in n}$ – середній збиток від неупередженої i-тої загрози за даний період часу;

u_i – витрати нападника на i-ий метод нападу;

$\vec{X}$ – вектор булевих змінних для сторони захисту;

$X_{\text{Re}c}$ – рекурсивні значення вектора $\vec{X}$;

$\vec{X}_{\text{наст.}}$ – вектор допустимих значень для сторони захисту для наступного рівня решітки для режиму оптимізації;

$U(\vec{X},\vec{Y})$ – реальні збитки для сторони захисту;

$\vec{X}_{\text{next}}$ – вектор допустимих значень для сторони захисту для наступного рівня решітки;

DOI 10.15588/1607-3274-2019-2-18

Y_{next} – вектор допустимих значень для сторони нападу для наступного рівня решітки;

$\vec{Y}$ – вектор булевих змінних для сторони нападу;

$Y_{\text{Rec}2}$ – рекурсивні значення вектора $\vec{Y}$;

$\vec{Y}_{\text{наст.}}$ – вектор допустимих значень для сторони нападу для наступного рівня решітки для режиму оптимізації;

(доп.) $\min_{x\in\Delta x}$ – мінімальне значення допустимих значень вектора $\vec{X}$;

(доп.) $\max_{y\in\Delta y}$ – максимальне значення допустимих значень вектора $\vec{Y}$;

(доп.)$U(\vec{X},\vec{Y})$ – збиток нанесений захиснику з урахуванням упереджених мір захисту.

ВСТУП

Забезпечення інформаційної безпеки є важливим завданням для будь-якої системи захисту, оскільки від збереження конфіденційності, цілісності та доступності інформаційних ресурсів багато в чому залежать якість і оперативність прийняття технічних рішень та ефективність їх реалізації.

«В умовах різних форм власності завдання забезпечення інформаційної безпеки повністю лягає на плечі підприємців, керівників організацій, різних комерційних структур. За підрахунками американських фахівців, втрата 20% інформації веде до розорення організації протягом місяця в 60 випадках зі 100. Інформація є основою для прийняття рішень людиною і від її достовірності, повноти та системної організованості залежить ризик прийняття неефективних і небезпечних рішень [1]».

Існує проблема відставання захисту від прискореного збільшення кількості інцидентів з інформаційною безпекою. Дослідження компанії IBM показали, що розмір найбільш прийнятних витарт на кібербезпеку складає у межах 9,8–13,7% від IT-бюджету організації. Даний показник починає зростати пропорційно інтеграції безпеки на всіх рівнях IT-інфраструктури [2].

Об'єкт дослідження – процеси організації інформаційної та кібербезпеки інформації з обмеженим доступом на об'єктах інформаційної діяльності.

«Про важливість інформаційного та кіберпростору свідчить поява концепцій ведення боротьби у них, а також створення у Збройних силах багатьох країн світу спеціальних структур, призначених для ведення такої боротьби. Такий стан справ, а також глибинні зміни у відношенні більшості держав земної кулі до власної інформаційної та, як наслідок, кібернетичної безпеки фактично зумовлюють необхідність здійснення конкретних кроків [3]».

Предмет досліджень – методи розрахунку оптимальності витрат на інформаційну та кібербезпеку об'єктів інформаційної діяльності.

Так, питання розробки загальної математичної моделі по вибору оптимального засобу забезпечення кібербезпеки об'єктів інформаційної діяльності від реалізації будь-яких видів загроз та належного функціонування кожного методу інформаційної та кібербезпеки з урахуванням методів соціального інжинірингу, залишається не вирішеним.

Мета роботи: розробка методу розрахунку оптимальності витрат на інформаційну та кібербезпеку у тому числі з урахуванням методів соціальної інженерії, щодо захисту інформації що циркулює на об'єктах інформаційної діяльності.

1 ПОСТАНОВКА ЗАДАЧІ

Дано множини можливих загроз безпеці та засобів захисту інформації від цих загроз безпеці, а також вартості реалізації кожної загрози $C_i^{(H)} \geq 0, \forall_{i\in N}$ і кожного засобу захисту $C_j^{(3)} \geq 0, \forall_{i\in M}$. Для сторони захисту вводимо булеву змінну $x_j \in \{0,1\}, \forall j \in M$, а для сторони нападу булеву змінну $y_i \in \{0,1\}, \forall i \in N$. Необхідно розробити ігрову математичну модель з двома протиборчими сторонами та алгоритми ефективного захисту інформації з гарантованим результатом за показником збитків від атак з боку захисту. Для забезпечення необхідного рівня захищеності інформації доцільно з боку захисту використати критерій оптимальності Вальда, тому що саме він забезпечує гарантований результат при самих непередбачуваних обставинах. Так як під час вибору засобів захисту вирішується мінімізація можливих збитків, то даний критерій перетворюється у мінімаксний критерій. Таку задачу можна вирішити за допомогою булевого програмування з лінійними обмеженнями. Обмеження на максимальну вартість засобів захисту описується нерівністю $\sum_j {}_{jeM} C_j^{(3)} x_j \leq C_{\max}^{(3)}$, а обмеження на максимальну вартість використовуваних для атак ресурсів $\sum_i {}_{ieN} C_i^{(H)} y_j \leq C_{\max}^{(H)}$.

2 ОГЛЯД ЛІТЕРАТУРИ

На сьогодні існують досить відомі моделі реалізації процесу інформаційної та кібербезпеки, однак їм властивий ряд недоліків.

Модель оцінки кібербезпеки на основі теорії ігор для передових промислових систем [4]. У даній моделі показано, що теорія ігор може бути застосована в області виробництва для визначення надійності системи від впливу кіберзагроз та аналізу різних методів захисту від цього класу атак. У даній роботі розглядаються сторона захисту та нападу у тому розумінні, що вони володіють певною інформацією про один одного стосовно характеру їх дій, у той час, як при реальному рівні кібербезпеки це далеко не так у більшості випадків. Окрім того, категоризація кібербезпеки як гри з нульовою сумою не враховує того факту,

DOI 10.15588/1607-3274-2019-2-18

що мотивація дій кожного з гравців може відрізнятися у часі. Так як витрати сторони захисту не обов'язково відповідають витратам сторони нападу, то слід розглядати задану гру, як гру з ненульовою сумою.

Модель Гордона-Лоєба, що розглядається у роботі [5], дозволяє вирішити важливу проблему для всіх зацікавлених організацій: скільки необхідно інвестувати у дільність, пов'язану з організацією інформаційної та кібербезпеки. Дана модель забезпечує інтуїтивну структуру, яку легко зрозуміти за допомогою множини спеціальних кроків для отримання інвестиційного рівня організації інформаційної та кібербезпеки. Як і при застосування всіх підходів до прийняття інвестиційних рішень, існують обмеження на застосування вказаної моделі при прийнятті рішень про відповідний рівень витрат на інформаційну та кібербезпеку. По-перше, це нечіткість пов'язана з оцінкою інформації, яку організація намагається захистити і ймовірністю того, що інформація буде порушена. По-друге, не забезпечує якісні аспекти рішення (наприклад, організації загальної стратегії по відношенню до витрат на кібербезпеку), які повинні бути розглянуті першочергово перед тим, як приймати остаточне рішення відносно відповідного рівня витрат на кібербезпеку. При цьому необхідно обов'язково використовувати і економічні моделі, як доповнення до моделі Гордона-Лоєба.

Приведені математичні моделі [6] ймовірності кіберінцидентів у якості функцій інвестицій безпеки та можливі застосування цих моделей для аналізу витрат і доцільності цих витрат на кібербезпеку для зниження втрат протягом року. Однак ці моделі не враховують необхідність моделювання у часі і ефект кіберзахисту, виявлення та пом'якшення їх наслідків. Також відсутня кількісна оцінка ризиків і взаємозв'язок з кібербезпекою при поширенні інформації з обмеженим доступом.

Модель, що описується у працях [7–9], реалізує свій розвиток на принципі оптимального управління, але при цьому ресурсами, розподіл яких необхідно обов'язково врахувати між суб'єктами інформаційного протиборства, нехтує. Модель [10] не враховує інформаційний конфлікт у його динамічному прояві. У роботах [11–14] пропонуються статистичні моделі, без врахування подальшого розвитку інформаційного конфлікту у його динаміці. Модель, що реалізується у [15], досить загальна та не повною мірою відповідає практичним вимогам, оскільки якість її успішної реалізації прямо залежить від професійної кваліфікації експерта з інформаційної та кібербезпеки.

3 МАТЕРІАЛИ І МЕТОДИ

Для розв'язання даного роду проблем, необхідною умовою є формування достатнього понятійного апарату, з метою належного оцінювання загроз для інформаційного та кіберпростору.

Так під розвідкою ІТС слід розуміти цілеспрямований пошук з метою подальшого добування з ІТС інформації, що цікавить нападника стосовно протиборчої сторони(захисника). У вітчизняних та закордонних фахівців склалась наступна класифікація способів ведення розвідки (ІТС) (рис. 1): МР, РсТ та КР [3].

У відповідності до [16] силами і засобами РсТ та МР добувається відповідно до 8% та до 7% інформації, що цікавить атакуючих. Однак, останнім часом дедалі більшого розповсюдження набула саме КР, за допомогою якої може добуватись до 90% інформації з обмеженим доступом, яка у свою чергу за методом ведення поділяється на технічну, програмну, розвідку методами так званої СІ, а також розвідку шляхом моніторингу відкритих або відносно відкритих електронних джерел (рис. 2).

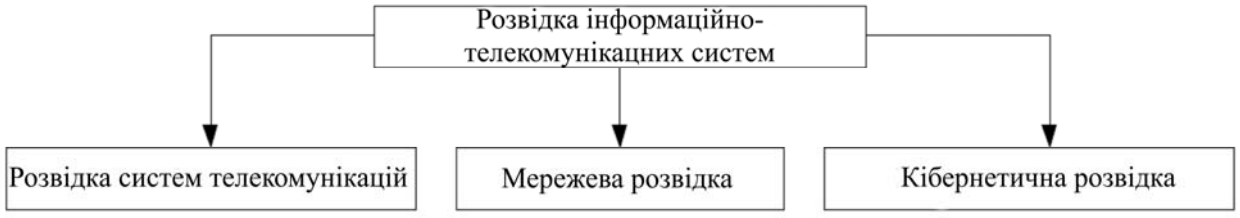

Рисунок 1 – Способи ведення розвідки в ІТС

Рисунок 2 – Склад методів ведення кіберрозвідки

DOI 10.15588/1607-3274-2019-2-18

Аналізуючи дану класифікацію, звернемо увагу саме на методи соціальної інженерії (людський фактор), оскільки враховуючи думку міжнародних фахівців [17–20], проводячи аналіз інцидентів інформаційної кібербезпеки [21] та збору даних щодо впливу соціальної інженерії на бізнес [22–24] даний клас методів представляє найбільшу зацікавленість у реалізації з боку зловмисника, навіть у науковому світі [25, 26].

Чіткої класифікації методів розрахунку оптимальності витрат на інформаційну та кібербезпеку об'єктів інформаційної діяльності не існує, однак існують різні підходи по моделюванню ситуації протиборства двох конфліктуючих сторін. Так, аналізуючи різні критерії оптимальності, такі як Лапласа, Вальда, Гурвіца або Севіджа, з точки зору забезпечення стану захищеності інформації стороною захисту слід використовувати саме критерій оптимальності Вальда, оскільки саме він забезпечує реалізацію так званої «песимістичної стратегії», що гарантує отримання гарантованого результату для системи захисту навіть при найгірших умовах [27].

Модель антагоністичної гри досліджує практичну залежність тривалості роботи розроблених алгоритмів від розмірності поставленої задачі, а також оцінку похибки роботи наближеного алгоритму.

Вибір ЗЗІ забезпечується вибором таких параметрів:

– показника вартості ЗЗІ;

– показника, що задає можливий запобіжний збиток (показник ефективності).

Вирішення даного роду задач здійснюється за допомогою булевого програмування. Така математична модель дозволяє досягти гарантованого результату по показнику збитків від атак з боку захисту. В даному випадку кількість атак можуть вимірюватись десятками, а в деяких випадках навіть сотнями. Під час моделювання даного типу гри, кожен із її учасників вирішує свою задачу булевого програмування. Оскільки при виборі засобів захисту вирішується мінімізація можливих збитків, то критерій Вальда перетворюється у мінімаксний критерій:

$$(\text{доп})\min_{x\in\Delta x}(\text{доп})\max_{y\in\Delta y}(\text{доп})U(\vec{X},\vec{Y}) \qquad (1)$$

Необхідністю є розробка точних та наближених алгоритмів, які дозволяють знаходити розв'язки по заданому критерію. Серед таких методів у булевому програмуванні завжди можна виділити метод повного перебору. Для розв'язку задач мінімізації витрат на інформаційну та кібербезпеку об'єкту інформаційної діяльності доцільно використовувати метод неявного перебору на векторній решітці. Основа методу полягає в наступному: між булевими векторами $\vec{X}$ (або $\vec{Y}$), які мають різні значення компонент, можна ввести відношення домінування. Відношення домінування встановлюється між будь-якими двома векторами, які відрізняються значеннями тільки одного елемента. Для реалізації алгоритмів перебору на векторній решітці зручно використовувати рекурсивні алгоритми по правилу «1 домінує 0».

Використання точних методів у булевому програмуванні вимагає дотримуватись певних обмежень. Вартість використаних засобів захисту можна представити у вигляді:

$$C^{(з)}(x)=\sum\nolimits_{jeM} C_j^{(3)}x_j. \qquad (2)$$

При цьому сторона захисту обмежена в засобах і може витратити на захист деяку максимальну суму $C_{\max}^{(з)}$. Тоді обмеження на максимальну вартість засобів захисту визначається нерівністю:

$$\sum\nolimits_{jeM} C_j^{(3)}x_j \le C_{\max}^{(3)}. \qquad (3)$$

Аналогічно для сторони нападу вводимо обмеження на максимальну вартість ресурсів, які можуть бути виділені на проведення атак зловмисником:

$$\sum\nolimits_{ieN} C_i^{(H)}y_i \le C_{\max}^{(H)}, \qquad (4)$$

Стартовий точний алгоритм методу неявного перебору на решітці, побудованої за правилом «1 домінує 0» має наступні кроки [28]:

1. Задаємо початкове рішення, яке складається з усіх одиниць $\vec{X}=\|1,1...1\|$, тобто всі засоби захисту в автоматизованій системі будуть застосовуватись для захисту від тих чи інших загроз (масив x розмірності m). Припускаємо, що $U_{\text{MinMax}}\to\infty$, тобто затрати на захист максимальні.

2. Виконання рекурсивного алгоритму зондування розв'язку $\vec{X}$ за принципом «1 домінує 0».

3. Після роботи алгоритму зондування значення показника для першого гравця, що здійснює вибір засобів захисту знайдене по критерію мінімаксу (1), буде дорівнювати U_{MinMax} і отримане рішення буде записане у масиві X_{Rec}, а рішення другого гравця у масиві $Y_{\text{Rec}2}$.

Рекурсивний алгоритм зондування рішення $\vec{X}$ (масиву X) розмірності m по правилу «1 домінує 0»:

1. Якщо рішення $\vec{X}$ допустиме у відповідності з обмеженням (3), то задаємо початкове рішення $\vec{Y}$, що складається з усіх одиниць $\vec{Y}=\|1,1...1\|$ (масив Y розмірності n) та припускаючи $U_{\text{Max}}\to 0$, переходимо до наступного кроку, а в протилежному випадку переходимо до кроку 5.

2. Виконання рекурсивного алгоритму зондування рішення $\vec{Y}$ по правилу «1 домінує 0».

3. Якщо $U_{\text{Max}}<U_{\text{MinMax}}$, то допускаємо, $U_{\text{MinMax}}=U_{\text{Max}}$ і зберігаємо рішення Y_{Rec} у масиві $Y_{\text{Rec}2}$ (рекордне рішення по критерію мінімаксу), зберігаємо значення масиву X в масиві $X_{\text{Rec}2}$ (рекордне рішення по критерію мінімакс).

4. Алгоритм завершує роботу.

DOI 10.15588/1607-3274-2019-2-18

5. Отримуємо повний вектор наступного рівня решітки в циклі $\vec{X}_{\text{next}}$ (масив x розмірності m) для кожного $\vec{X}_{\text{next}}$ записуємо рекурсивний алгоритм зондування $\vec{X}$ по правилу «1 домінує 0». Якщо таких рішень не існує, то алгоритм завершує свою роботу. При цьому число розглянутих вершин решітки буде меншим, якщо буде менше число недопустимих рішень, які визначаються обмеженнями (3) та (4). Співвідношення числа допустимих і недопустимих рішень залежить від відношення суми коефіцієнтів $\sum_{jeM} C_j^{(3)} x_j$, до $C_{\max}^{(3)}$ для обмеження (3) і відношення суми коефіцієнтів $\sum_{ieN} C_i^{(H)} y_i$ до $C_{\max}^{(H)}$, для обмеження (4).

Рекурсивний алгоритм зондування рішення $\vec{Y}$ (масив Y розмірності n) по правилу «1 домінує 0»:

1. Якщо рішення $\vec{Y}$ допустиме у відповідності з обмеженням (4), то обчислюємо значення реального збитку для сторони захисту:

$$U(\vec{X},\vec{Y}) = U^{\max}(\vec{Y}) - U^{\text{пред}}(\vec{X},\vec{Y}) = \\ = \sum_{i\in N} u_i y_i - \sum_{i\in N} u_i y_i \max_{j\in M}\left[p_{ij} x_j\right]. \quad (5)$$

Переходимо до наступного кроку, в протилежному випадку переходимо до кроку 3 рекурсивного алгоритму зондування рішення $\vec{X}$ (масиву X) розмірності m по правилу «1 домінує 0».

2. Якщо $U > U_{\text{Max}}$, то припускаємо, що $U_{\text{Max}} = U$ і зберігаємо рішення в масиві Y_{Rec} (рекордне значення по критерію максимум) і алгоритм завершує роботу.

3. Отримуємо новий вектор нового рівня решітки в циклі Y_{next} (масив Y розмірності n); для кожного Y_{next} запускаємо рекурсивний алгоритм зондування $\vec{Y}$ по правилу «1 домінує 0». Якщо таких рішень не існує, алгоритм завершує свою роботу. Розглядаючи рекурсивний алгоритм зондування рішення $\vec{X}$ (масиву X розмірності m) згідно пункту 5 і рекурсивний алгоритм зондування рішення $\vec{Y}$ (масиву Y розмірності n) згідно пункту 3 по правилу (1 домінує 0), встановлено, що число розглянутих вершин решітки буде меншим, якщо буде менше число недопустимих рішень, які визначаються обмеженнями (3) та (4). Співвідношення числа допустимих і недопустимих рішень залежить від відношення суми коефіцієнтів $\sum_{j\in M} C_j^{(3)} x_j$, до $C_{\max}^{(3)}$ для обмеження (3) і відношення суми коефіцієнтів $\sum_{i\in N} C_i^{(H)} y_i$ до $C_{\max}^{(H)}$, для обмеження (4).

Приведені рішення для сторони захисту [8] $\vec{X} = \|1,1,0,1,1,0,0,0,1,1\|$ і для сторони нападу $\vec{Y} = \|1,0,1,1,1,1,1,1,0,0,1\|$ є далеко не оптимальними. Враховуючи значення елементів матриці ймовірностей упереджених наслідків i-тої загрози за допомогою j-того засобу захисту $P = \|p_{ij}\|$ (табл. 1), а також дані з табл. 2 та приведені вище рішення для $\vec{X}$ та $\vec{Y}$ можна зробити висновок, що прогнозовані загрози під номерами 5, 6, 8 навряд чи будуть задіяні зі сторони нападу, так як для їх усунення будуть використані засоби захисту у кількості 6, 7, 6 одиниць відповідно. Крім того, недоцільно застосовувати засоби захисту під №1, 9, 10, так як вони не дозволяють ефективно позбутися можливих загроз у кількості 8, 9, 10 одиниць відповідно.

Таблиця 1 – Засоби захисту від загроз безпеці, вартості їх реалізації та можливості запобігання

Засоби захисту ($B = \{b_1, b_2, ...b_m\}$)	Вартість реалізації ($C_i^{(3)}, \forall j \in M$), доларів США	Можливість (імовірність) попередження загрози ($p_{ij}, \forall i \in N, \forall j \in M$)										
		Номера загроз з таблиці 2										
		1	2	3	4	5	6	7	8	9	10	11
Звичайний антивірус	500	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,9	0,8	0,9	0,0
Програмний продукт для шифрування та дешифрування даних	1000	0,6	0,7	0,9	0,0	0,8	0,6	0,0	0,0	0,0	0,0	0,0
Засіб для захисту від мережевих вторгнень, шкідливих програм та спаму	650	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,7	0,6	0,8	0,0
Засіб виявлення вторгнень та несанкціонованого доступу до інформації	350	0,0	0,0	0,0	0,6	0,5	0,4	0,8	0,1	0,0	0,0	0,4
Засіб, що активує міжмережевий екран, антивірус і засоби виявлення вторгнень	850	0,0	0,0	0,0	0,7	0,5	0,4	0,7	0,1	0,6	0,7	0,6
Комплекс шифрування	10000	0,7	0,8	0,9	0,0	0,7	0,1	0,0	0,0	0,0	0,0	0,0
Засоби захисту інформації від несанкціонованого доступу	600	0,0	0,0	0,0	0,0	0,5	0,6	0,0	0,8	0,8	0,0	0,0
Пристрої електронного замикання	3500	0,0	0,0	0,0	0,0	0,6	0,5	0,0	0,9	0,9	0,0	0,0
Засоби захисту даних від злому або крадіжки жорстких дисків, ноутбука чи флеш-носія	450	0,9	0,0	0,0	0,0	0,0	0,8	0,0	0,0	0,0	0,0	0,0
Засоби захисту від DDos-атак	1000	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0
Виділено коштів ($C_{\max}^{(3)}$)	18900											

DOI 10.15588/1607-3274-2019-2-18

Оптимальний розв'язок по заданому алгоритму оптимізації який раніше не використовувався $\vec{X} = \|0,1,0,1,1,1,1,1,0,0\|$ та $\vec{Y} = \|1,1,1,1,0,0,1,0,0,1,1\|$ можна досягти, якщо зняти обмеження (3) і ввести вектори $\vec{X}$ та $\vec{Y}$ початкового рівня решітки. Для вказаних векторів необхідно знайти елементи наступного рівня решітки – нові вектори $\vec{X}_{\text{наст.}}$ та $\vec{Y}_{\text{наст.}}$ і для кожного з них запустити рекурсивні алгоритми зондування $\vec{X}$ та $\vec{Y}$ по правилу «1 домінує 0». Такий цикл слід повторювати доти, доки будуть існувати рішення. З отриманих рішень обираємо оптимальне, яке відповідає мінімаксному критерію (2). Таким чином, оптимізований алгоритм спрощує процес розрахунку та скорочує загальний час обчислення поставленої задачі.

4 ЕКСПЕРИМЕНТИ

Основні загрози соціального інжинірингу від небажаного витоку інформації, можливі збитки за період шість місяців та умовні затрати соціальних інженерів-зловмисників на проведення відповідних атак за цей же період, приведені у табл. 3 [29].

В табл. 4 приведені методи захисту від загроз, які задані своїми номерами відповідно до табл. 3. Орієнтовні ціни задають конфігурацію методів захисту об'єкту інформаційної діяльності, де циркулює ІзОД [29, 30].

Таблиця 2 – Збитки від не запобігання атакам та вартості їх реалізації

Загрози $(A = \{a_1, a_2, ...a_n\})$	Збитки від не запобігання $(u_i, \forall\, i \in N)$, доларів США	Вартість реалізації загрози для порушника $(c_i^{(H)}, \forall\, i \in N)$, доларів США
Витік інформації з обмеженим доступом з мережі по каналам зв'язку (email, web і т.п.)	165600	1650
Прослуховування зовнішніх каналів зв'язку зловмисниками	16650	1650
Пасивне прослуховування каналів зв'язку, що проходять поза межами контрольованої території	165600	875
Перехват інформації на лініях зв'язку, з використанням різного роду аналізаторів мережевого трафіку	16650	875
Модифікація, видалення чи підміна даних користувачів в інформаційному потоці	83300	1500
Перехват ідентифікуючої інформації (паролів) з метою подальшого її використання для обходу засобів мережевої ідентифікації	83300	1650
Статистичний аналіз мережевого трафіку з метою виявлення вразливостей	16650	875
Впровадження несанкціонованого, неправомірного чи шкідливого програмного коду (віруси, троянські програми, тощо)	16650	650
Аналіз та модифікація програмного забезпечення	250000	8300
Логічні «бомби», що пересилаються по email	16650	850
Атаки на відмову в обслуговуванні проти зовнішніх хостів	16650	350
Всього виділено коштів на реалізацію загроз $(C_{\max}^{(H)})$	19225	

Таблиця 3 – Збитки від соціотехнічних атак та вартість їх реалізації.

№ з/п	Загрози	Збитки від не упередження, грн.	Вартості від реалізації загрози нападника, грн.
1.	Електронна пошта (e-mail)	500000	90000
2.	Телефонний зв'язок	500000	30000
3.	Аналіз сміття	50000	10000
4.	Особисті підходи	30000	6000
5.	Реверсивна соціальна інженерія	120000	15000

Таблиця 4 – Методи захисту від загроз безпеці, вартості їх реалізації та ймовірності упередження загроз в інтервалі шести місяців

№ з/п	Методи захисту	Вартості реалізації, грн.	Можливості (імовірності) упередження загрози				
			Номера загроз (по таблиці 2)				
			1	2	3	4	5
1	Законодавчі	10000	0,1	0,1	0,2	0,5	0,1
2	Морально-етичні	12000	0,4	0,4	0,6	0,4	0,2
3	Організаційно-адміністративні	5000	0,6	0,5	0,0	0,0	0,2
4	Організаційно-технічні	7000	0,5	0,4	0,0	0,0	0,3
5	Інформаційні	15000	0,6	0,4	0,5	0,4	0,7
6	Організаційно-економічні	100000	0,1	0,1	0,5	0,4	0,2
7	Інженерно-технічні	20000	0,1	0,1	0,5	0,2	0,1

DOI 10.15588/1607-3274-2019-2-18

Для вирішення задачі вибору методів захисту, необхідно використати точний алгоритм задачі булевого програмування. Враховуючи вихідні дані в табл. 3 та 4, отримуємо рішення для сторони захисту $\vec{X} = |0,1,1,1,1,0,1|$ і для сторони нападу $\vec{Y} = \|1,1,0,0,1\|$. Це означає, що обрані методи захисту за номерами 2,3,4,5,7 із табл. 4 і методи нападу 1,2,5 із табл. 3. Рішення задачі є оптимальним для сторони захисту, так як використання інформаційних методів дозволяє з достатньою імовірністю усунути всі можливі загрози соціального інжинірингу. При цьому загальна сума витрат на упереджений захист інформації складає 59000 грн., у той час як витрати нападника досягають 135000 грн., тобто маємо виграш більш ніж у 2 рази. У даному випадку можливо з високою імовірністю усунути всі можливі загрози соціального інжинірингу. Найбільш вразливими для користувача є електронна пошта, телефонний зв'язок і реверсивна соціальна інженерія.

5 РЕЗУЛЬТАТИ

Побудуємо відповідні графіки для наглядного представлення отриманих результатів (Рис.3). Координатні осі побудовані у вигляді десяткових логарифмічних функцій $\lg(P_{\text{н.з}}; P_{\text{у.з.}})$ і $\lg P_{\text{н}}$.

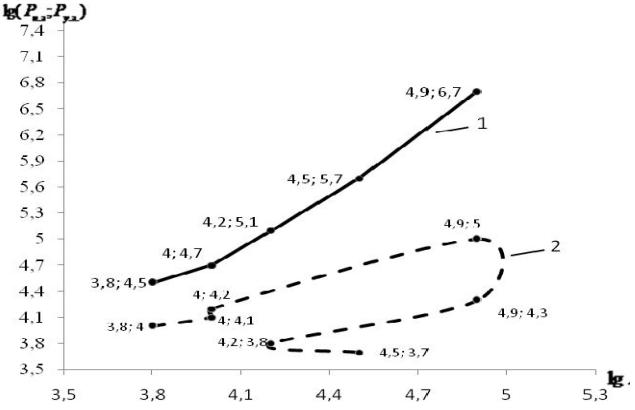

Рисунок 3 – Графіки залежностей збитків $P_{\text{н.з}}; P_{\text{у.з.}}$ від соціотехнічнихатак $P_{\text{н}}$:1 – неупереджені збитки $P_{\text{н.з}}$; 2 – упереджені збитки $P_{\text{у.з.}}$

6 ОБГОВОРЕННЯ

Питання вирішення інформаційного протиборства двох конфліктуючих сторін з використанням принципу гарантованого результату (нападника та захисника) вирішувалось у багатьох дослідженнях, наприклад [31]. Однак, у даному дослідженні встановлено, що кількість атак може вимірюватись десятками, а в деяких випадках навіть сотнями. При моделюванні даного типу гри, кожен з її учасників вирішує свою задачу булевого програмування. Для забезпечення максимально можливого рівня захисту інформації доцільно з боку захисту використати критерій Вальда, що забезпечує гарантований результат при будь-яких умовах.

У ході дослідження даної моделі, встановлено, що найбільші збитки від неупереджених атак нападника, пов'язані із методами і засобами соціального інжинірингу (людський фактор) витоку інформації з обмеженим доступом.

Було проведено відповідні дослідження та розрахунки і отримано практичні результати (рис. 3), де графік 1 показує значне зростання затрат $(P_{\text{н.з}})$ у випадку неупереджених дій захисника при зростанні вартості затрат нападника $(P_{\text{Н}})$. Графік 2 показує значне зменшення затрат $(P_{\text{у.з.}})$ у випадку попереднього застосування стороною захисту відповідних методів захисту $(1)-(7)$ відповідно до затрат при неупереджених діях захисника $(P_{\text{н.з}})$. Графічна залежність під номером 2 відповідає оптимальному варіанту вибору методів захисту, у тому числі від соціотехнічних атак.

ВИСНОВКИ

У роботі вирішено актуальну на сьогоднішній день задачу по розробці методу розрахунку оптимальності витрат на інформацію та кібербезпеку об'єкту інформаційної діяльності.

Наукова новизна отриманих результатів полягає у врахуванні всіх методів та засобів захисту як від упереджених так і від неупереджених атак.

Вперше розроблено ефективний метод розрахунку оптимальності витрат на інформаційну та кібербезпеку об'єктів інформаційної діяльності з урахуванням всіх методів та засобів у тому числі враховуючи найнебезпечніший клас методів соціальної інженерії.

Кількість засобів захисту та число атак можуть обчислюватись десятками, а в окремих випадках навіть сотнями. Для вирішення поставленої задачі даним методом використовувався критерій оптимальності Вальда з вирішенням задачі булевого програмування, що призвело до отримання гарантованого результату при будь-яких умовах для сторони захисту.

Практична цінність по використанню даного методу дозволить отримати конкретні результати по розрахунку оптимальних витрат на інформаційну та кібербезпеку об'єктів інформаційної діяльності, де циркулює інформація з обмеженим доступом.

Використання даного методу у підрозділах інформаційної та кібербезпеки під час побудови комплексних систем захисту інформації та комплексів технічного захисту інформації дозволить оптимізувати процес вибору методів захисту, при цьому заощадити володільцю ІзОД до 2 разів коштів, передбачених бюджетом організації на інформаційну та кібербезпеку.

У подальшому необхідно здійснити вартісну оцінку найбільш ефективних методів захисту, прогнозуючи ймовірні загрози соціального інжинірингу.

DOI 10.15588/1607-3274-2019-2-18

ПОДЯКИ

Роботу виконано у рамках дисертаційного дослідження на кафедрі Інформатики та управління захистом інформаційних систем Одеського національного політехнічного університету. Автор висловлює подяку науковому керівнику, кандидату технічних наук, доценту кафедри Кононовичу В. Г., за корисні зауваження під час обговорення статті та кандидату фізико-математичних наук, старшому науковому співробітнику Панасенку Б.В. за участь у експериментах.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Заячук Я. І. Аналіз та оцінка ризиків інформаційної безпеки локальної обчислювальної мережі / Я. І. Заячук // Восточно-Европейский журнал передовых технологий. – 2012. – № 4/9(58). – С. 40.
2. Collins D. How Much Should I Spend on Cyber Security? [Electronic resource] – 2018. – Available at: https://www.edts.com/edts-blog/how-much-should-i-spend-on-cyber-security.
3. Бурячок В. Л. Соціальна інженерія як метод розвідки інформаційно-телекомунікаційних систем / В. Л. Бурячок, О. Г. Корченко, Л. В. Бурячок // Захист інформації. – 2012. – № 4. – С. 5–8. DOI: 10.18372/2410-7840.14.3471
4. Zarreh A. A game theory based cybersecurity assessment model for advanced manufacturing systems / [A. Zarreh and others]; 46th SME North American Manufacturing Research Conference, Texas, USA. – 2018. – June 18–22 – P. 1255–1264.
5. Gordon Lawrence A. Investing in Cybersecurity: Insights from the Gordon-Loeb Model / Lawrence A. Gordon, Martin P. Loeb, Lei Zhou // Journal of Information Security. – 2016. – № 7. – P. 49–59. DOI: 10.4236/jis.2016.72004
6. Shaun W. Optimal Level And Allocation Of Cybersecurity Spending: Model And Formula. [Electronic resource] – 2017. – Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3010029. DOI: 10.2139/ssrn.3010029
7. Ігнатов В. О. Динаміка інформаційних конфліктів в інтелектуальних системах / В. О. Ігнатов, М. М. Гузій // Проблеми інформатизації та управління. – 2005. – Вип. 15. – С. 88–92.
8. Игнатов В. А. Оптимальное управление скаляризацией векторных критериев в конфликтующих системах / В. А. Игнатов, М. М. Гузий // Проблеми інформатизації та управління. – 2004. – Вип. 11. – С. 118–126.
9. Игнатов В.А. Оптимальное управление информационной безопасностью / В. А. Игнатов, М. М. Гузий // Проблеми інформатизації та управління. – 2004. – Вип. 14. – С. 71–74.
10. Безопасность информации в автоматизированных системах [Електронний ресурс] – 2003. – Режим доступу: http://www.studentlibrary.ru/book/ISBN5279025607.html.
11. Кількісно-якісна оцінка рівня інформаційної безпеки / [М. М. Браіловський та ін.] // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2006. – № 9 (103). – Ч. 1. – С. 14–17.
12. Андреев В. И. Количественная оценка защищенности технических объектов с учетом их функционирования / В. И. Андреев, В. С. Козлов, В. А. Хорошко // Захист інформації. – 2004. – № 2. – С. 47–50.
13. Козлов В. С. Количественная оценка защищенности информации / В. С. Козлов, В. А. Хорошко // Захист інформації. – 2003. – № 4. – С. 67–73.
14. Козлова К. В. Кількісна оцінка захисту радіоелектронних об'єктів (РЕО) / К. В. Козлова, В. О. Хорошко // Захист інформації. – 2007. – № 1. – С. 30–32.
15. The Common Criteria for Information Technology Security Evaluation: ISO/IEC 15408-1:2009. – [Effective from 2009-12]. – Geneve: ISO, 2009. – 65 p.
16. Бурячок В. Л. До питання організації та проведення розвідки у кібернетичному просторі / В. Л. Бурячок, Г. М. Гулак, В. О. Хорошко // Наука і оборона. – 2011. – № 2. – С. 19– 23.
17. Transformation of information and social-psychological security paradigms (Part 1) / [S. Gnatyuk, V. Gnatyuk, V. Kononovich, I. Kononovich] // Informatics and mathematical methods in simulation. – 2016. – Vol. 6, No. 3. – P. 227–239.
18. Mitnik K. The Art of Deception: Controlling the Human Element of Security / Kevin U. Mitnik, William L. Simon, Steve Wozniak. – Wiley, 2002. – P. 304.
19. Goldschmidt M. Social Engineering is the new norm in hacking [Electronic resource] – 2018. – Available at: https://www.cso.com.au/article/634433/social-engineering-new-norm-hacking/.
20. Widdowson A. Human Factors in Rail Cyber Security [Electronic resource] – 2017. – Available at:https://www.thalesgroup.com/sites/default/files/database/document/201806/CyberinHFpaperV3.pdf.
21. IBM Security services 2014 Cyber Security Intelligence Index [Electronic resource]. – 2014. – Available at: https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf.
22. Zelazny F. Here's what happens during a social engineering cyber-attack [Electronic resource] / F. Zelazny. – 2018. – Available at: https://www.techrepublic.com/article/heres-what-happens-during-a-social-engineering-cyber-attack/.
23. Santavy J. 7 Social engineering attacks on small business [Electronic resource] / J. Santavy. – 2018. – Available at: https://wuvavi.com/2018/09/05/social-engineering/
24. The risk of social engineering on information security a survey of it professionals [Electronic resource] – 2011. – Available at:https://www.stamx.net/files/The-Risk-of-Social-Engineering-on-Information-Security.pdf.
25. Dadkhah M. Social engineering in academic world [Electronic resource] / M. Dadkhah, A. Quliyeva. – 2014. – Available at: https://www.researchgate.net/publication/272159213_Social_engineering_in_academic_world.
26. Jalalian M. Hijacked Journals and Predatory Publishers: Is There a Need to Re-Think How to Assess the Quality of Academic Research? [Electronic resource] / M. Jalalian, H. Mahboobi. – 2014. – Available at: http://wjst.wu.ac.th/index.php/wjst/article/view/1004. DOI: 10,14456 / WJST.2014.16
27. Абденов А. Ж. Выбор средства эффективной защиты с помощью методов теории игр / А. Ж. Абденов, Р. Н. Заркумова // Вопросы защиты информации. – 2010. – № 2. – С. 26–31.
28. Быков А. Ю. Задача выбора средств защиты информации в автоматизированных системах на основе модели антагостической игры / А. Ю. Быков, Н. О. Алтухов,

DOI 10.15588/1607-3274-2019-2-18

А. С. Сосенко. // Инженерный Вестник. – 2014. – № 4. – С. 525–542.
29. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа] ; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. – К. : ДУТ, 2015. – 288 с.
30. Табаков А.Б. Разработка моделей оптимизации средств защиты информации для оценки страхования информационных рисков / А. Б. Табаков // Политематический сетевой научный журнал Кубанского аграрного университета. – 2005. – № 12. – С. 1–11.
31. Nakonechnyi O. Best-mean estimates in models of information confrontation / O. Nakonechnyi, P. Zinko // Problems of decision making under uncertainties: 24 Intern. Conf., 1–5 sept. 2014. – Cesky Rudolec. – P. 114–115.

Стаття надійшла до редакції 04.12.2018.
Після доробки 28.02.2019.

УДК 519.863

МЕТОД РАСЧЕТА ОПТИМАЛЬНОСТИ ЗАТРАТ НА ИНФОРМАЦИОННУЮ И КИБЕРБЕЗОПАСНОСТЬ

Романюков Н. Г. – аспирант кафедры Информатики и управления защитой информационных систем Одесского национального политехнического университета, Одесса, Украина.

АННОТАЦИЯ

Актуальность. Исследована общая математическая модель с участием двух противоборствующих сторон (нападающего и защитника). Установлено, что исследуемая модель позволит получить практические результаты по расчету оптимального коэффициента затрат на информационную и кибербезопасность объекта информационной деятельности.

Метод. Заключается в разработке игровой модели с двумя противоборствующими сторонами и алгоритма для обеспечения гарантированного результата по показателю потерь от атак со стороны защиты. При этом количество средств защиты и число атак могут измеряться десятками, а в отдельных случаях даже сотнями. Для решения поставленной задачи данным методом используется критерий оптимальности Вальда с решением задачи булевого программирования, поскольку проектируя систему защиты, необходимо обеспечить гарантированный результат при любых условиях.

Результаты. Получены практические результаты по расчету оптимального коэффициента затрат на информационную и кибербезопасность объекта информационной деятельности, где циркулирует информация с ограниченным доступом.

Выводы. Таким образом, полученный метод позволит получить практические результаты по расчету оптимального коэффициента затрат на информационную и кибербезопасность объектов информационной деятельности, где циркулирует информация с ограниченным доступом. Важно учитывать все методы и средства защиты в том числе методы и средства социального инжиниринга, которые создают опасный канал утечки информации с ограниченным доступом. Работу данного метода была подтверждена экспериментально на примере угроз социального инжиниринга и построены соответствующие графики зависимостей как предвзятых так и не предвзятых убытков от данного вида атак.

КЛЮЧЕВЫЕ СЛОВА: информационная и кибербезопасность, методы расчета оптимальности затрат, булевое программирование.

UDC 519.863

METHOD OF CALCULATION OF OPTIMALITY OF INFORMATION AND CYBER SECURITY EXPENSES

Romanyukov M. G. – Postgraduate Student of the Department of Computer Science and Information Management of the Odessa National Polytechnic University, Odessa, Ukraine.

ABSTRACT

Context. The general mathematical model with participation of two opposing sides (attacker and defender) is investigated. It is established that the model under study will provide practical results in calculating the optimal cost factor for the information and cybersecurity of an object of information activity.

Method. It comes in the development of a game model with two opposing sides and an algorithm to provide a guaranteed result on the loss of protection from attack attacks. At the same time, the number of means of protection and the number of attacks can be measured by dozens, and in some cases even hundreds. To solve the problem, this method uses the Wald's optimality criterion to solve the Boolean problem, since designing a security system requires the guaranteed result under all conditions.

Results. Practical results are obtained on the calculation of the optimal cost factor for information and cybersecurity of an information activity object, where circular information with limited access circulates.

Conclusions. Thus, the obtained method will allow obtaining practical results in calculating the optimal cost factor for the information and cybersecurity of information activity objects, where circular information with limited access is circulated. It is important to consider all methods and means of protection, including methods and tools for social engineering, which create a dangerous channel for leakage of information with limited access. The work of this method was confirmed experimentally by the example of threats to social engineering and constructed the corresponding graphs of dependencies of both prejudiced and not prejudiced losses from this type of attack.

KEYWORDS: informational and cybersecurity, methods of calculation of cost optimality, boolean programming.

DOI 10.15588/1607-3274-2019-2-18

REFERENCES

1. Zaiachuk Y. I. Analiz ta otsinka ryzykiv informatsiinoi bezpeky lokalnoi obchysliuvalnoi merezhi, *Vostochno-Evropeiskyi zhurnal peredovukh tekhnolohyi*, 2012, No. 4/9(58), P. 40.
2. Collins D. How Much Should I Spend on Cyber Security? [Electronic resource], 2018, Available at: https://www.edts.com/edts-blog/how-much-should-i-spend-on-cyber-security.
3. Buriachok V. L., Korchenko O. H., Buriachok L. V. Sotsialna inzheneriia yak metod rozvidky informatsiino-telekomunikatsiinykh system, Zakhyst informatsii, 2012, No. 4, pp. 5–8. DOI: 10.18372/2410-7840.14.3471
4. Zarreh A. and others A game theory based cybersecurity assessment model for advanced manufacturing systems, *46th SME North American Manufacturing Research Conference*. Texas, USA, 2018, June 18–22, pp. 1255–1264.
5. Gordon Lawrence A., Martin P. Loeb, Lei Zhou Investing in Cybersecurity: Insights from the Gordon-Loeb Model, *Journal of Information Security*, 2016, No. 7, pp. 49–59. DOI: 10.4236/jis.2016.72004
6. Shaun W. Optimal Level And Allocation Of Cybersecurity Spending: Model And Formula. [Electronic resource], 2017, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3010029. DOI: 10.2139/ssrn.3010029
7. Ignatov V. O., GuzIy M. M. DinamIka InformatsIynih konflIktIv v Intelektualnih sistemah, *Problemi Informatizatsii ta upravlinnya*, 2005, Vyp. 15, pp. 88–92.
8. Ignatov V. A., Guziy M. M. Optimalnoe upravlenie skalyarizatsiey vektornyih kriteriev v konfliktuyuschih sistemah, *Problemi Informatizatsii ta upravlinnya*, 2004, Vyp. 11, pp. 118–126.
9. Ignatov V. A., Guziy M. M. Optimalnoe upravlenie informatsionnoy bezopasnostyu, *Problemi Informatizatsii ta upravlinnya*, 2004, Vyp. 14, pp. 71–74.
10. Bezopasnost informatsii v avtomatyzyrovannuh systemah [Elektronnyi resurs], 2003, Rezhym dostupu: http://www.studentlibrary.ru/book/ISBN5279025607.html.
11. BraIlovskiy M. M. ta in. KIlkisno-yakisna otsinka rivnya Informatsiynoi bezpeki *Visnik ShIdnoukrayinskogo natsionalnogo universitetu Imeni Volodimira Dalya*, 2006, No. 9 (103), Ch. 1, pp. 14–17.
12. Andreev V. I., Kozlov B. C., Horoshko V. A. Kolichestvennaya otsenka zaschihyonnosti tehnicheskih ob'ektov s uchotom ih funktsionirovaniya, *Zahist Informatsii*, 2004, No. 2, pp. 47–50.
13. Kozlov B. C., Horoshko V. A. Kolichestvennaya otsenka zaschischonnosti informatsii, *Zahist Informatsii*, 2003, No. 4, pp. 67–73.
14. Kozlova K. V., Horoshko V. O. Kilkisna otsinka zahistu radioektronnih ob'ektiv (REO), *Zahist Informatsiyi,* 2007, No. 1, pp. 30–32.
15. The Common Criteria for Information Technology Security Evaluation: ISO/IEC 15408-1:2009. [Effective from 2009-12]. Geneve: ISO, 2009, 65 p.
16. Buryachok V. L., Gulak G. M., Horoshko V. O. Do pitannya organizatsii ta provedennya rozvidki u kibernetichnomu prostori, *Nauka i oborona,* 2011, No. 2, pp. 19– 23.
17. Gnatyuk S. Gnatyuk V. , Kononovich V. , Kononovich I. Transformation of information and social-psychological security paradigms (Part 1), *Informatics and mathematical methods in simulation,* 2016, Vol. 6, No. 3, pp. 227–239.
18. Mitnik K., William L. Simon, Steve Wozniak The Art of Deception: Controlling the Human Element of Security. Wiley, 2002, P. 304.
19. Goldschmidt M. Social Engineering is the new norm in hacking [Electronic resource], 2018, Available at: https://www.cso.com.au/article/634433/social-engineering-new-norm-hacking/.
20. Widdowson A. Human Factors in Rail Cyber Security [Electronic resource], 2017, Available at:https://www.thalesgroup.com/sites/default/files/database/document/2018-06/CyberinHFpaperV3.pdf.
21. IBM Security services 2014 Cyber Security Intelligence Index [Electronic resource], 2014, Available at: https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf.
22. Zelazny F. Here's what happens during a social engineering cyber-attack [Electronic resource], 2018, Available at: https://www.techrepublic.com/article/heres-what-happens-during-a-social-engineering-cyber-attack/.
23. Santavy J. 7 Social engineering attacks on small business [Electronic resource], 2018, Available at: https://wuvavi.com/2018/09/05/social-engineering/
24. The risk of social engineering on information security a survey of it professionals [Electronic resource], 2011, Available at:https://www.stamx.net/files/The-Risk-of-Social-Engineering-on-Information-Security.pdf.
25. Dadkhah M., Quliyeva A. Social engineering in academic world [Electronic resource], 2014, Available at: https://www.researchgate.net/publication/272159213_Social_engineering_in_academic_world.
26. Jalalian M., Mahboobi H. Hijacked Journals and Predatory Publishers: Is There a Need to Re-Think How to Assess the Quality of Academic Research? [Electronic resource], 2014, Available at: http://wjst.wu.ac.th/index.php/wjst/article/view/1004. DOI: 10,14456 / WJST.2014.16
27. Abdenov A. Zh., Zarkumova R. N. Vyibor sredstva effektivnoy zaschityi s pomoschyu metodov teorii igor, *Voprosyi zaschityi informatsii,* 2010, No. 2, pp. 26–31.
28. Byikov A. Y., Altuhov N. O., Sosenko A. S. Zadacha vyibora sredstv zaschityi informatsii v avtomatizirovannyih sistemah na osnove modeli antagosticheskoy igryi, *Inzhenernyiy Vesnik*, 2014, No. 4, pp. 525–542.
29. Buryachok V. L., Tolubko V. B., Horoshko V. O., Tolyupa S. V.; za zag. red. d-ra tehn. nauk, profesora V. B. Tolubka Informatsiyna ta kiberbezpeka: sotsiotehnichniy aspekt: pidruchnik. Kiev, DUT, 2015, 288 p.
30. Tabakov A.B. Razrabotka modeley optimizatsii sredstv zaschityi informatsii dlya otsenki strahovaniya informatsionnyih riskov, *Politematicheskiy setevoy nauchnyiy zhurnal Kubanskogo agrarnogo universiteta*, 2005, No. 12, pp. 1–11.
31. Nakonechnyi O., Zinko P. Best-mean estimates in models of information confrontation, *Problems of decision making under uncertainties: 24 Intern. Conf., 1–5 sept. 2014,* Cesky Rudolec, pp. 114–115.

DOI 10.15588/1607-3274-2019-2-18