DOI: 10.18372/2410-7840.20.12805
УДК 004.056.53

ВИКОРИСТАННЯ Q-АНАЛІЗУ ДЛЯ ВИЗНАЧЕННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Олег Козленко

У статті розглянуто застосування методів структурного аналізу систем для дослідження функціонування та визначення системи захисту інформації в ІТС з орієнтацією на найбільш поширені варіанти сценаріїв витоку інформації та на особливості культури інформаційної безпеки. Компанія Verizon щорічно у своїх дослідженнях в області безпеки інформації ділять усі інциденти витоку інформації на дев'ять сценаріїв, які стали основою для побудови відповідної множини елементів захисту та загроз. Небезпеку також становить людський фактор, який не завжди пов'язаний з нестачею або недосконалістю заходів захисту, але завжди пов'язан з недотриманням вимог політики безпеки Дослідження людських чинників в області інформаційної безпеки все більше привертають увагу, тому що мають значний вплив на інформаційну безпеку в цілому і окремо на інсайдерську її складову. Організації страждають від випадкових або навмисних помилок співробітників, незважаючи на наявність політики безпеки і необхідних технологій. За допомогою Q-аналізу представлені основні принципи побудови моделі зв'язаності забезпечення захисту інформації в ІТС на прикладі двох множин: множини загроз і множин заходів щодо захисту, розраховані числові значення ексцентриситетів. Математичний апарат Q-аналізу дозволяє здійснювати дослідження топологічних, інформаційних і функціональних властивостей забезпечення захисту інформації в ІТС. На основі дослідження структурної зв'язності системи з'являється можливість провести формальну оцінку її рівня функціональності, що визначає здатність до поглинання зовнішніх несприятливих факторів за рахунок внутрішніх ресурсів. Системний характер дозволив зробити висновок, що елементи двох множин забезпечення захисту інформації в ІТС - взаємопов'язані і складають основу системи забезпечення їх безпеки. Дані розрахунки можуть бути використані подальшого визначення загальної формальної оцінки захищеності організації і побудова системи захисту інформації в ІТС повинна рахуватися за результатами даного аналізу.

Ключові слова: *Q-аналіз, сценарії витоку інформації, культура інформаційної безпеки, загрози інформації, рівень культури інформаційної безпеки.*

Вступ

Процес побудови забезпечення захисту інформації в ІТС у зв'язку з високою деталізацією її структури, зокрема, елементів, впливових факторів, відношень між ними, вимагає для аналізу та дослідження цієї структури застосування різних практик. Q-аналіз виявився особливо корисним для вирішення завдань, пов'язаних із складними системами, такими як ті, що створюються при обробці медичних зображень. Ця методика вимагає строгого визначення наборів даних та їхніх зв'язків та заохочує до вивчення наслідків в системі. Мета роботи полягає у використанні Q-аналізу та визначення критеріїв зв'язності системи захисту інформації в ІТС для подальшого аналізу системи захисту ІТС. Наукова новизна цієї роботи у застосуванні Q-аналізу для системи захисту інформації в ІТС з орієнтацією на особливості культури інформаційної безпеки та сценаріїв витоку інформації та представлені основні принципи побудови моделі зв'язаності забезпечення захисту інформації в ІТС на прикладі двох множин: множини загроз і множин заходів щодо захисту, розраховані числові значення ексцентриситетів.Метою роботи є математичний опис зв'язаності елементів системи забезпечення інформаційної безпеки за допомогою теорії алгебри топології (Q-аналізу). Метод оцінки структурної зв'язності, що базується на математичному апараті Q-аналізу, здатний в значній мірі прискорити вирішення завдань, пов'язаних з оцінкою захищеності системи.

Сценарії витоку інформації та культура інформаційної безпеки

Однією з складових аналізу інформаційних систем є визначення елементів забезпечення захисту інформації в ІТС. Для визначення елементів захисту системи від витоку інформації потрібно знати можливі загрози для цільової системи та відповідно необхідні дії захисту [1].

Компанія Verizon щорічно проводить дослідження в області безпеки інформації [12, 13, 14, 15] і доводять доцільність поділу інцидентів витоку інформації на дев'ять можливих сценаріїв: вторгнення в точки продажу (POS-вторгнення), атаки на веб-застосунки, злочинне ПЗ, кібер-шпіонаж, скимери платіжних карток, фізична крадіжка або втрата, різні помилки, інсайдерські атаки та DOS-атаки [12, 13, 14, 15].

У звітах про витоки даних в період за 2014-2017 роки компанія Verizon виділила відповідні загрози для кожного з вищезазначених сценаріїв. Спираючись на цю інформацію та фактори, які Verizon виділила у звіті про витоки інформації за 2014 рік [12], множина елементів захисту для вищезазначених сценаріїв складається з:

– "інвентаризація" ПЗ;
– відсутність непотрібного ПЗ, облікових записів, портів та ін.;
– оновлення та патчі;
– цілісність системних файлів;
– антивірусні програми;
– оновлення захисних програм;
– DEP, ASLR, EMET;
– тестування веб-застосунків;
– закритість матеріалів для розробленого ПЗ;
– резервне копіювання;
– тренінги по ІБ для співробітників;
– перевірка працівників;
– фільтрування трафіку;
– відокремлення сервісів;
– контроль адміністраторів;
– складні паролі;
– відсутність паролів за замовчуванням;
– чорні та білі списки IP;
– подвійна автентифікація;
– протокол Netflow;
– журнал подій;
– аккаунт-менеджмент;
– централізована автентифікація;
– моніторинг входів;
– шифрування;
– відсутність конфіденційних даних у відкритому тексті;
– DLP-система;
– робота з інцидентами;
– ролі при інцидентах;
– сегментація мережі;
– відеоспостереження;
– перевірка терміналів;
– попередження користувачів;
– ефективний дизайн.

Не всі загрози безпосередньо залежать від технічних особливостей систем. Як зазначено у [6] користувачі, умисно або через нестачу знання, є найбільшою загрозою для інформаційної безпеки. У роботі [8] Сіпонен зазначає, що без необхідних знань та співпраці користувачів з відділом безпеки або менеджменту адекватні засоби безпеки стають неефективними.

У існуючій літературі культура інформаційної безпеки (КІБ) є важливою складовою у забезпеченні безпеки інформаційних активів організацій. У таких работах як [2] автор визначає КІБ як поведінку,цінності та припущення, які забезпечують безпеку інформації, дослідники у [4] визначають КІБ як систему, у якій взаємодіють мотивація, спрямування, знання та ментальні моделі. Ван Нікерк та Вон Солмс у своїй роботі [11] пропонують концептуальну модель культури інформаційної безпеки. Ця модель спрямована на визначення взаємодії між різними елементами, які складають культуру інформаційної безпеки. Досліди, які були проведені у [7] допомагають розкласти поняття «КІБ» на складові. Тим самим, «КІБ» можливо визначити наступними складовими:

– «Персонал»:
  – «Кадрова безпека»;
  – «Міра прийняття КБ»;
– «Керівництво»:
  – «Управлінська готовність»;
  – «Координованість»:
    – «Співпраця з відділом ІБ»;
    – «Співпраця з менеджментом».

Методика використання Q-аналізу для визначення захищенності інформаційної системи

Техніка Q-аналізу забезпечує алгебраїчну топологічну структуру для зменшення даних, що полегшує макроскопічну концептуалізацію системи. З цією метою можна знизити такі показники як рівень зв'язності, ексцентриситет та складність. Q-аналіз передбачає відносно прості розрахунки, коли визначаються приблизні множини та оцінюються їх співвідношення [3].

Сила зв’язку між елементами системи безпеки відіграє значну роль у визначенні ступення взаємодії між елементами. У разі відсутності зв’язку між елементами сама система буде вразлива до атак. Системний характер досліджуваної області дав змогу визначити множину загроз та мір захисту, які повязані за допомогою відношення λ і є основою системи [3].

Відповідно, λ є відношенням декартового добутку множин X та Y, де $X=\{x_1,x_2,\ldots,x_{13}\}$ – множина загроз системи, яка складається з:

x_1 - Атаки на веб-застосунки;
x_2 - DOS-атаки;
x_3 - Інсайдерські атаки;
x_4 - Різні помилки;
x_5 - Фізична крадіжка або втрата;
x_6 - Скримери платіжних карток;
x_7 - Кібер-шпигунство;
x_8 - Злочинне ПЗ;
x_9 - POS-вторгнення;
x_{10} - Кадрова безпека;
x_{11} - Міра прийняття КБ;
x_{12} - Управлінська готовність;

x_{13} – Координованість.

Y = {y_1,y_2,…,y_{37}} – множина мір захисту і складається з:

y_1 - Тестування веб-застосунків;

y_2 - Закритість матеріалів для розробленого ПЗ;

y_3 - Оновлення та патчі;

y_4 - Подвійна автентифікація;

y_5 - Робота з інцидентами;

y_6 - Ролі при інцидентах;

y_7 - DLP-система;

y_8 - Журнал подій;

y_9 - Аккаунт-менеджмент;

y_{10} - Централізована автентифікація;

y_{11} - Моніторинг входів;

y_{12} - Контроль адміністраторів;

y_{13} – Відсутність конфіденційних даних у відкритому вигляді;

y_{14} - Резервне копіювання;

y_{15} - Шифрування;

y_{16} - Відео-спостереження;

y_{17} - Перевірка терміналів;

y_{18} - Попередження користувачів;

y_{19} - Ефектиний дизайн;

y_{20} - Тренінги по ІБ для співробітників;

y_{21} - Перевірка працівників;

y_{22} - Сегментація мережі;

y_{23} - Інвентарізація ПЗ;

y_{24} - Чорні та білі списки IP;

y_{25} - Антивірусні програми;

y_{26} - Оновлення захисних програм;

y_{27} - DEP, ASLR, EMET;

y_{28} - Немає непотрібного ПЗ облікових записів, портів;

y_{29} - Цілісність системних файлів;

y_{30} - Фільтрування трафіку;

y_{31} - Журнал подій;

y_{32} - Протокол NetFlow;

y_{33} - Відокремлення сервісів;

y_{34} - Складні паролі;

y_{35} - Відсутність паролів за замовчуванням;

y_{36} - Співпраця з відділом ІБ;

y_{37} - Співпраця з менеджментом.

Тобто елемент декартового добутку (Y_i,X_k) показує, що Y_i знаходиться у відношенні λ з X_k, якщо λ=1 у данному випадку та λ = 0 навпаки [9].

Відношення між елементами множин X та Y можна представити у вигляді матриці інцидентності $\Delta = (\lambda_{ik})$, де λ_{ik}=1, якщо (Y_i,X_k) ∈ λ та λ_{ik}=0 навпаки. Таблиця 1 зображає отриману матрицю інцидентності, на основі дослідження.

Відношення λ породжує симплиційний комплекс $K_y(X;\lambda)$, де елементи множини Y розглядаються як вершини, а елементи множини X – як симплекси. Значення N є розмірністю комплекса K (dimK) й означає максимальну размірність σ_p ∈ K. Множина X також називається множиною вершин комплексу $K_y(X;\lambda)$. Також, кожний симплекс σ_p ∈ K відповідає хоч б одному Y_n ∈ Y. Симплеціальний комплекс $K_y(X;\lambda)$ складається з множини симплексів, звязних між собою гранями, тобто загальними вершинами [9].

Аналогічно, якщо Y є множиною вершин, то λ^{-1} є звязний комплекс в якому X_k – симплекси [3,10].

Поняття Q-зв'язку визначається наступним чином - пара симплексів σ_p, σ_r ∈ K звязана, якщо існує послідовність симплексів σ_{a1} , σ_{a2}, ... σ_{ah}, таких, що:

1) σ_{a1} - грань симлекса σ_p;

2) σ_{ah} - грань симлекса σ_r;

3)σ_{a1} та σ_{ah} мають спільну грань $\sigma_{\beta i}$, для i=1,…,(h-1).

Вважатимемо, що цей зв'язок є Q-зв'язним, якщо q – найменше з цілих чисел (a1,β1,…,ah)[9].

Структурний вектор Q, який є безпосереднім результатом Q-аналізу, може бути використаний для отримання додаткової інформації про зв'язок.

Алгоритм отримання q-загальних граней [9,10] усіх пар Y-симплексов в $K_y(X;\lambda)$ [4]:

1. Скласти матрицю $\Delta\,\Delta^T$ розмірністю (m x m).

2. Визначити $\Delta\,\Delta^T$ - Ω , де Ω=(ω_{ij}) , а ω_{ij} = 1 для i, j = 1 , 2, ... , m.

За допомогою структурних векторів можливо отримати та порівняти міру (числове значення) складності компексів відношень. Для цього необхідно скористатися формулою [3]:

$$\varphi(K)=\frac{2\left[\sum_{i=0}^{N}(i+1)Q_i\right]}{(N+1)(N+2)},$$

де N=dimK – размірність комлекса K; Q_i – i-та компонента структурного вектора Q, отриманого за допомогою Q-аналізу.

Оскільки індивідуальні властивості симплексів можуть мати важливе значення для вирішення задач, необхідно визначити ступінь інтегрованості кожного симплексу у структурі всього комплексу. Для цього є поняття ексцентиристету, яке виражає ступінь ізоляції симлексів друг від друга. Це поняття відображає як відносну важливість даного симлексу до комлексу, так і значимість симлексу як звязного елементу. Ексцентриситет симплексу визначається за допомогою наступної формули [3]:

$$Ecc(\sigma) = \frac{\hat{q} - \check{q}}{\check{q} + 1},$$

де $\hat{q}$= dimPi , $\check{q}$- найбільше значення q, при якому Pi стає звязним з іншим Pj.

Отриманий структурний вектор за матрицею інцидентності з таблиці 1 має такий вигляд:

Q=(0,0,0,0,0,0,0,0,0,3,8,6,37).

Отримані значення $Ecc(\sigma)$для множин X та Y представлены у таблицях 2 та 3.

Таблиця 1

Матриця інцидентності для множин загроз та мір захисту

	X1	X2	X3	X4	X5	X6	X7	X8	X9	X10	X11	X12	X13
Y1	1	0	0	0	0	0	0	0	0	0	0	0	0
Y2	1	0	0	0	0	0	0	0	0	0	0	0	0
Y3	1	0	0	0	0	0	1	1	0	0	0	0	0
Y4	1	0	0	0	0	0	1	1	1	0	0	0	0
Y5	0	1	0	0	0	0	0	0	0	1	1	1	0
Y6	0	1	0	0	0	0	0	0	0	1	1	1	0
Y7	0	1	1	1	0	0	0	0	0	0	0	0	0
Y8	0	0	1	0	0	0	0	0	0	0	0	0	0
Y9	0	0	1	0	0	0	0	0	0	0	0	0	0
Y10	0	0	1	0	0	0	0	0	0	0	0	0	0
Y11	0	0	1	0	0	0	0	0	0	0	0	0	0
Y12	0	0	1	0	0	0	0	0	1	0	0	1	0
Y13	0	0	1	1	1	0	0	0	0	0	0	0	0
Y14	0	0	0	0	1	0	0	0	0	0	0	0	0
Y15	0	0	0	0	1	0	0	0	0	0	0	0	0
Y16	0	0	0	0	0	1	0	0	0	0	0	0	0
Y17	0	0	0	0	0	1	0	0	0	0	0	0	0
Y18	0	0	0	0	0	1	0	0	0	0	0	0	0
Y19	0	0	0	0	0	1	0	0	0	0	0	0	0
Y20	0	0	0	0	0	0	1	0	0	1	1	0	0
Y21	0	0	0	0	0	0	1	0	0	1	1	1	0
Y22	0	0	0	0	0	0	1	0	0	0	0	0	0
Y23	0	0	0	0	0	0	1	1	0	0	0	0	0
Y24	0	0	0	0	0	0	1	1	0	0	0	0	0
Y25	0	0	0	0	0	0	0	1	1	0	0	0	0
Y26	0	0	0	0	0	0	0	1	1	0	0	0	0
Y27	0	0	0	0	0	0	0	1	1	0	0	0	0
Y28	0	0	0	0	0	0	0	1	0	0	0	0	0
Y29	0	0	0	0	0	0	0	1	0	0	0	0	0
Y30	0	0	0	0	0	0	0	0	1	0	0	0	0
Y31	0	0	0	0	0	0	0	0	1	1	0	0	0
Y32	0	0	0	0	0	0	0	0	1	0	0	0	0
Y33	0	0	0	0	0	0	0	0	1	0	0	0	0
Y34	0	0	0	0	0	0	0	0	1	1	0	1	0
Y35	0	0	0	0	0	0	0	0	1	1	0	1	0
Y36	0	0	0	0	0	0	0	0	0	0	0	0	1
Y37	0	0	0	0	0	0	0	0	0	0	0	0	1

Висновки

В роботі було проаналізовані сценарії витоку інформації, які були отримані з звітів щодо витоку інформації за 2014 - 2017 роки та особливості культури інформаційної безпеки, яка має відношення до загроз, пов'язаних з людськими чинниками. В результаті проведеного аналізу було визначено необхідні множини та відношення для проведення Q-аналізу. Це дозволить ефективно управляти процесом прийняття рішень, поліпшить управління існуючими слабкими зв'язками. Наведені вище розрахунки свідчать про те, що система безпеки має надзвичайно високий рівень комплексності. Для того, щоб два симплекса з безлічі загроз або механізмів захисту належали одній q-зв'язковий компоненті комплексу K, необхідна наявність ланцюга проміжних симплексів, що зв'язують їх, тобто самий «слабкий» з них повинен мати розмірність велику або рівну q, то це означає, що загрозу не зможе нейтралізувати певний механізм запобігання, а рішення виниклої проблеми можливе шляхом системного поєднання заходів щодо попередження руйнування системи.

Таблиця 2

Основні значення ексцентриситетів для множини мір захисту

Y - множина мір захисту	$Ecc(\sigma)$
y_1 - Тестування веб-застосунків	0
y_2 - Закритість матеріалів для розробленого ПЗ	0
y_3 - Оновлення та патчі	0
y_4 - Подвійна автентифікація	0,33
y_5 - Робота з інцидентами	0
y_6 - Ролі при інцидентах	0
y_7 - DLP-система	0,5
y_8 - Журнал подій	0
y_9 - Аккаунт-менеджмент	0
y_{10} - Централізована автентифікація	0
y_{11} - Моніторинг входів	0
y_{12} - Контроль адміністраторів	0
y_{13} - Відсутність конфіденційних даних у відкритому вигляді	0,5
y_{14} - Резервне копіювання	0
y_{15} - Шифрування	0
y_{16} - Відео-спостереження	0
y_{17} - Перевірка терміналів	0
y_{18} - Попередження користувачів	0
y_{19} - Ефектиний дизайн	0
y_{20} - Тренінги по ІБ для співробітників	0,33
y_{21} - Перевірка працівників	0
y_{22} - Сегментація мережі	0
y_{23} - Інвентарізація ПЗ	0
y_{24} - Чорні та білі списки IP	0
y_{25} - Антивірусні програми	0
y_{26} - Оновлення захисних програм	0
y_{27} - DEP, ASLR, EMET	0
y_{28} - Немає непотрібного ПЗ облікових записів, портів	0
y_{29} - Цілісність системних файлів	0
y_{30} - Фільтрування трафіку	0
y_{31} - Журнал подій	0
y_{32} - Протокол NetFlow	0
y_{33} - Відокремлення сервісів	0
y_{34} - Складні паролі	0
y_{35} - Відсутність паролів за замовчуванням	0
y_{36} - Співпраця з відділом ІБ	0
y_{37} - Співпраця з менеджментом	0

Таблиця 3

Основні значення ексцентриситетів для множини загроз

X - множина загроз	$Ecc(\sigma)$
x_1 - Атаки на веб-застосунки	1
x_2 - DOS-атаки	0,5
x_3 - Інсайдерські атаки	6
x_4 - Різні помилки	0
x_5 - Фізична крадіжка або втрата	2
x_6 - Скримери платіжних карток	-1
x_7 - Кібер-шпигунство	1
x_8 - Злочинне ПЗ	1,25
x_9 - POS-вторгнення	1,75
x_{10} - Кадрова безпека	0,75
x_{11} - Міра прийняття КБ	0
x_{12} - Управлінська готовність	0,2
x_{13} – Координованість	-1

ЛІТЕРАТУРА

[1]. О. Архипов, "Щодо методики ідентифікації та оцінювання активів системи інформаційних те-хнологій", *Захист інформації*, №1 (50), С.42-47, 2011.

[2]. G. Dhillon, *Managing information system security*, London: Macmillan, 1997.

[3]. A. Goicoechea, D. Hansen, L. Duckstein, *Multiobjective Decision Analysis with Engineering and Business Applications*, IWiley, New York, 1982.

[4]. T. Helokunnas, R. Kuusisto, "Information security culture in a value net", *In: Engineering Management Conference, IEMC'03 on Managing Technologically Driven Organizations: The Human Side of Innovation and Change*, New York: IEEE Press, P. 190-194, 2003.

[5]. K. Mitnick, W. Simon, *The art of deception: controlling the human element of security*, Wiley Publishing, P. 3, 2002.

[6]. A. Potiy, D. Pilipenko, I. Rebriy, "The prerequisites of information security culture development and an approach to complex evaluation of its level", *Радіоелектронні і комп'ютерні системи,* no. 5, P. 72-77, 2012.

[7]. M. Siponen, "Five dimensions of information security awareness", *Computers and Society*, 2001.

[8]. Y. Svirezhev, D. Logofet, *Stability of Biological Communities*, Mir, Moscow ,1978.

[9]. F. Szidarovszky, M. Gershon, L. Duckstein, *Techniques for Multiobjective Decision Making in Systems Management*, Elsevier, New York, 1986.

[10]. J. Van Niekerk, R. Von Solms, "Information security culture: A management perspective", *Computers* & *Security*, p.478, 2010.

[11]. 2014 Data Breach Investigation Report, Verizon Enterprise Solutions, 2013

[12]. 2015 Data Breach Investigation Report, Verizon Enterprise Solutions, 2014

[13]. 2016 Data Breach Investigation Report, Verizon Enterprise Solutions, 2015
[14]. 2017 Data Breach Investigation Report, Verizon Enterprise Solutions, 2016

ИСПОЛЬЗОВАНИЕ Q-АНАЛИЗА ДЛЯ ОПРЕДЕЛЕНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

В статье рассмотрено применение методов структурного анализа систем для исследования функционирования и определения системы защиты информации в ИТС с ориентацией на наиболее распространенные варианты сценариев утечки информации и особенности культуры информационной безопасности. Компания Verizon ежегодно в своих исследованиях в области безопасности информации делят все инциденты утечки информации на девять сценариев, которые стали основой для построения соответствующей множества элементов защиты и угроз. Опасность также представляет человеческий фактор, который не всегда связан с недостатком или несовершенством мер защиты, но всегда связан с несоблюдением требований политики безопасности Исследование человеческих факторов в области информационной безопасности все больше привлекают внимание, так как имеют значительное влияние на информационную безопасность в целом и отдельно на инсайдерскую ее составляющую. Организации страдают от случайных или преднамеренных ошибок сотрудников, несмотря на наличие политики безопасности и необходимых технологий. С помощью Q-анализа представлены основные принципы построения модели связанности обеспечения защиты информации в ИТС на примере двух множеств: множества угроз и множеств меры по защите, рассчитанные числовые значения эксцентриситетов. Математический аппарат Q-анализа позволяет проводить исследования топологических, информационных и функциональных свойств обеспечения защиты информации в ИТС. На основе исследования структурной связности системы появляется возможность провести формальную оценку ее уровня функциональности, определяет способность к поглощению внешних неблагоприятных факторов за счет внутренних ресурсов. Системный характер позволил сделать вывод, что элементы двух множеств обеспечения защиты информации в ИТС - взаимосвязаны и составляют основу системы обеспечения их безопасности. Данные расчеты могут быть использованы дальнейшего определения общей формальной оценки защищенности организации и построение системы защиты информации в ИТС должна считаться по результатам данного анализа.

Ключевые слова: Q-анализ, сценарии утечки информации, культура информационной безопасности, угрозы информации, уровень культуры информационной безопасности.

USING OF THE Q-ANALYSIS FOR THE DETERMINING PROTECTION OF THE INFORMATION SYSTEM

Article proposes application of methods of structural analysis of systems for the study of the functioning and definition of the information security system with focus on the most common variants of information leakage scenarios and on the features of the information security culture. Verizon annually divides information leakage incidents into nine scenarios that have become the basis for security features and threats sets for this analysis. Human factor is also a great danger, which is not always associated with deficiencies or imperfections of security measures, but is always linked to non-compliance with security policy requirements. Human factor in information security field is increasingly attracting attention because it has a significant impact on information security as a whole and separately for its insider component. Organizations suffer from accidental or deliberate employee errors, despite the availability of security policies and the necessary technologies. Using Q-analysis, the basic principles of constructing a communications model for providing information security in information system are presented in the example of two sets: set of threats and sets of security measures, numerical values of eccentricities are calculated. The mathematical apparatus of Q-analysis allows to study the topological, informational and functional properties of information security protection in information security. On the basis of the study of structural connectivity of the system there is an opportunity to carry out a formal assessment of its level of functionality, which determines the ability to absorb external adverse factors at the expense of internal resources. The systemic nature allowed us to conclude that the elements of the two sets of information security protection in information system are interconnected and form the basis of the system for ensuring their safety. These calculations can be used to further determine the overall formal assessment of the security of the organization and the construction of the information security system in information system should be based on the results of this analysis.

Keywords: Q-analysis, information leakage scenarios, information security culture, information threats, level of information security culture.

Козленко Олег Віталійович, аспірант кафедри інформаційної безпеки Фізико-технічного інституту НТУУ «Київський політехнічний інститут імені Ігоря Сікорського».
Email: education.kozlenko@gmail.com.
Козленко Олег Витальевич, аспирант кафедры информационной безопасности Физико-технического института НТУУ «Киевский политехнический институт имени Игоря Сикорского».
Kozlenko Oleh, p.h.d student of the Department of Information Security of the Physical-Technical Institute of the NTUU "Igor Sikorsky Kiev Polytechnic Institute**".**