информации как необходимый элемент совершенствования государственной системы правовой информации и формирования единого информационно-правового пространства государства / Современные компьютерные технологии в системах правовой информации. Тезисы конференции.- Минск, 21 – -22 ноября 2002 г. / http://pravo.by/conf/ Report/ r_35.htm. ***25.*** *Кашинский Ю. И., Сатолина М. Н., Сокол С. Ф., Славин Б. С. Образовательные процессы в сфере правовой информатизации // там же/ r_37.htm.* ***26.*** *Славин Б. С. Вопросы правового образования: специализация "Правовая информатизация"/ http://www.ifap.ru/pi/06/r13.htm.* ***27.*** *Уотермен Д. Руководство по экспертным системам: Пер. с англ.- М.:Мир, 1989.- 388 с.* ***28.*** *Алиев Р. А., Абдикеев Н. М., Шахназаров М. М. Производственные системы с искусственным интеллектом. - М.: Радио и связь, 1990.- 264 с. 29. Блюменау Д. И. Информация и информационный сервис. - Л.: Наука, 1989.- 192 с.* ***30.*** *Швець М. Я, Гладківська О., Цимбалюк В. С. Взаємозв'язок інформаційної безпеки з правовою інформатикою // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – 2005.- Вип. 11 - С. 6 – 13.* ***31.*** *Закон України від 4 лютого 1998 року № 74/98-ВР "Про Національну програму інформатизації". 32. Законом України від 02 .10. 1992 р. №2657-XII "Про інформацію".* ***33.*** *Закон України від 31. 05. 2005 р. № 2594-IV "Про захист інформації в інформаційно-телекомунікаційних системах".* ***34.*** *Закон України від 22. 05. 2003 № 851-IV "Про електронні документи та електронний документообіг".* ***35.*** *Закон України від 22. 05. 2003 р. № 852-IV "Про електронний цифровий підпис".* ***36.*** *Закон України від 18 листопада 2003 року № 1280-IV "Про телекомунікації".* ***37.*** *Гутман Е. Н., Радиванович Н. Н. Перспективы развития эталонного и иных банков данных правовой информации Республики Беларусь / Современные компьютерные технологии в системах правовой информации. Тезисы конференции. – Минск, 21 – 22 ноября 2002г. / http://pravo.by/conf/Report/r_30.htm* ***38.*** *Орлов П. И., Громыко И. А., Носов В. В., Логвиненко Н. Ф. Общая парадигма защиты информации // Защита информации. Конфидент.- 2003. № 1 (49) -с. 14 – 18.* ***39.*** *Курбацкий А. Н., Чеушев В. А., Радиванович Н. Н., Муравьев А. К., Кочергов Е. Г. Логическая разметка правовых актов при формировании государственного ресурса правовой информации / Современные компьютерные технологии в системах правовой информации. Тезисы конференции.- Минск, 21 – 22 ноября 2002 г. http://pravo.by/conf/Report/r_42.htm.* ***40.*** *Клир Дж. Системология. Автоматизация решения системных задач: Пер. с англ.-М.: Радио и связь, 1990.- 554 с.* ***41.*** *Построение экспертных систем (Под ред. Ф. Хейес-Рота, Д. Уотермена, Д. Лената) - М.: Мир, 1987.- 434 с.* ***42.*** *Корнеев В. В., Гареев А. Ф., Васютин С. В., Райх В. В. Базы данных. Интеллектуальная обработка информации. - М.: "Нолидж", 2000.- 352 с.* ***43.*** *Электронной Москве не доплатили? // http://www.cnews.ru/newtop/index.shtml.2006/01/26/194999.*

ДК 515.142.33:004.056

ДОСЛІДЖЕННЯ СИСТЕМИ КОМП'ЮТЕРНОЇ БЕЗПЕКИ ЗА ДОПОМОГОЮ Q-АНАЛІЗУ

Оксана Григораш
НТУУ «КПІ», Фізико-технічний факультет

Анотація: **Проаналізовано структуру системи комп'ютерної безпеки, зв'язки між окремими її компонентами за допомогою одного із методів системного аналізу – Q-аналізу; визначені найбільш дієві заходи захисту та найбільш небезпечні загрози КС.**

Summary: **In the article with the help of one out of method systematical analysis – Q-analysis was realization analyze of computer security structure, was realization analyze connection with separate their components. Also was determine the most effective actions of defense and the most dangerous menaces in computers system.**

Ключові слова: **Системи комп'ютерної безпеки, Q-аналіз.**

Збільшення об'ємів інформації, що зберігається, обробляється та передається в комп'ютерних системах, територіальна розподіленість їх обчислювальних мереж приводять до збільшення потенційно можливої кількості навмисних та ненавмисних порушень безпеки інформації, можливих каналів або уразливих ланок несанкціонованого проникнення в мережі з метою зчитування, копіювання, підробки програмного забезпечення, текстової та іншої інформації. Тому якість, надійність та безпечність інформаційного обміну – це ті критерії, які повинні лежати в основі всіх комп'ютерних систем. А створення безпечної комп'ютерної системи стало однією із пріоритетних задач для всіх – як державних так і недержавних структур.

І Побудова множин механізмів захисту КС та її загроз

Метод Q-аналізу вивчає закономірності зв'язків і відносин між елементами системи і є бінарним методом. Необхідність класифікації загроз інформаційної безпеки комп'ютерних систем обумовлена тим, що архітектура сучасних засобів автоматизованої обробки інформації, організаційна, структурна та функціональна побудова інформаційно-обчислюваних систем та мереж, технології та умови автоматизованої обробки інформації такі, що інформація, що накопичується, зберігається та оброблюється, підпадає під випадковий вплив великого числа загроз. Тому для аналізу системи комп'ютерної безпеки потрібно дослідити дві множини, елементи яких взаємопов'язані та становлять її основу: множину механізмів захисту безпеки та множину загроз безпеці.

Визначимо ці множини наступним чином.

Множина заходів і механізмів захисту КС

1. **Фізичні –** пристрої, інженерні побудови та організаційні заходи, які ускладнюють чи унеможливлюють проникнення зловмисників до джерела захищеної інформації. Позначимо цей елемент множини механізмів захисту як Y_1.
2. **Апаратні –** механічні, електричні, електронні та інші пристрої, необхідні для захисту інформації від витоку та розголошення і протидії технічним розвідкам (Y_2).
3. **Програмні –** система спеціальних програм, що включаються в склад загального та спеціального програмного забезпечення, реалізують виконання критеріїв захищеності інформації (цілісність, конфіденційність, доступність, гарантії, спостережність):

a. ідентифікація, автентичність та авторизація технічних засобів, задач, масивів та користувачів (Y_3);
b. реєстрація дій, небезпечних для КС (Y_4);
c. визначення прав технічних засобів, задач та користувачів (Y_5);
d. контроль розмежування доступу до ресурсів мережі (визначення таблиці правил доступу) (Y_6);
e. розмежування прав доступу користувачів системи (Y_7);
f. забезпечення логічної та фізичної цілісності даних (Y_8);
g. блокування комп'ютера (Y_9);
h. контроль роботи технічних засобів та користувачів (Y_{10});
i. реєстрація роботи засобів та користувачів при обробці інформації з обмеженим доступом (Y_{11});
j. знищення інформації в пристроях пам'яті після завершення роботи (Y_{12});
k. захист інформації від несанкціонованого доступу (Y_{13});
l. сигналізація про несанкціоновані дії (Y_{14});
m. підтримка потоку повідомлень фіктивною інформацією (Y_{15});
n. керування маршрутизацією (Y_{16});
o. підтвердження достовірності (Y_{17});
p. керування доступом (забезпечення доступу до ресурсів відповідно до таблиці правил) (Y_{18});
q. протоколювання та аудит (аналіз адекватності функціонування системи політики безпеки) (Y_{19});
r. допоміжні програми різного призначення (Y_{20});
s. контроль роботи механізмів захисту (Y_{21}).

2. Криптографічні – технічні та програмні засоби шифрування:

a. шифрування даних (Y_{22});
b. цифровий підпис (Y_{23});
c. маскування та перетворення інформації (Y_{24});
d. шифрування даних, що передаються незахищеними каналами (Y_{25});

e. шифрування трафіку (Y_{26}).

3. Правові – нормативно-правові акти, що регламентують порядок роботи з інформацією з обмеженим доступом, відповідальність за його порушення (Y_{27}).

4. Організаційні – заходи адміністративного характеру, які визначають процеси функціонування системи обробки інформації, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб ускладнити або унеможливити реалізацію загроз системі безпеки (Y_{28}).

Таким чином, множину механізмів захисту комп'ютерної системи можна записати як $Y = \{Y_1, Y_2, ..., Y_{28}\}$.

Множина загроз безпеці КС

1. **Несанкціонований доступ (НСД, unauthorized access)** полягає в отриманні користувачем доступу до об'єкта, на який у нього немає дозволу відповідно до прийнятої в організації політики безпеки **(**найбільш розповсюджений вид комп'ютерних злочинів**)**:

a. навмисне викриття (X_1);

b. перегляд залишку даних (X_2);

c. помилка людини (X_3);

d. апаратно-програмна помилка (X_4);

e. перехоплення (X_5);

f. крадіжка (X_6);

g. прослуховування (X_7);

h. аналіз випромінювань (X_8);

i. аналіз трафіка (X_9);

j. використання «прихованих каналів» (X_{10});

k. нав'язування невірного маршруту (X_{11}).

2. **Обман** – обставина або подія, яка може спричинити отримання повноважним суб'єктом викривлених даних, що приймаються ним як вірні:

a. маскарад (X_{12});

b. атака «злом системи» (X_{13});

c. фальсифікація (X_{14});

d. підміна даних (X_{15});

e. вставка (X_{16});

f. відмова джерела (X_{17});

g. відмова одержувача (X_{18}).

3. **Руйнування** – обставина або подія, яка перешкоджає або припиняє коректне функціонування системних служб та реалізацію ними необхідних дій:

a. руйнування системи (шкідництво) (X_{18});

b. руйнування даних (псування) (X_{20});

c. підробка з точки зору псування (X_{21});

d. використання шкідливих програм (X_{22});

4. **Захват (узурпація).** Обставина або подія, в результаті якої керування службами системи та її функціонування перейшло до незаконного суб'єкту:

a. незаконне присвоєння (X_{23});

b. атака типу «збирання сміття» (X_{24});

c. зловживання (X_{25});

d. підробка з точки зору суб'єкта злочину (X_{26}).

Отже, множина загроз має вигляд $X = \{X_1, X_2, ..., X_{26}\}$.

Зазначимо, що деякі елементи побудованих нами множин можуть перетинатися за змістом своїх характеристик, але не накладаються повністю.

II Аналіз структури та взаємозв'язків елементів системи комп'ютерної безпеки

Задамо відношення λ між множинами елементів системи безпеки *Y* і *X* як підмножину декартового добутку X×Y, де λ⊂ X×Y. Множина заходів і механізмів безпеки КС $Y = \{Y_1, Y_2, ..., Y_{28}\}$ пов'язана відношенням λ з множиною загроз безпеці КС $X = \{X_1, X_2, ..., X_{26}\}$, якщо для кожної пари цілих чисел *(i, j)*, де *i*=1, 2... 28, *j*=1, 2, ..., 26 можна дати однозначну відповідь на запитання Q (англ., question, query – запитання, запит), *чи спроможний даний механізм* Y_i *вплинути на запобігання або нейтралізацію комп'ютерної загрози* X_j .

Відношення між множинами елементів системи безпеки КС можна записати у вигляді **матриці інцидентності** $\Delta = (\lambda_{ik})$, де

$\lambda_{ik} = 1$, якщо $(Y_i, X_k) \in \lambda$ – *i*-тий та *k*-тий елементи множин пов'язані відношенням **λ**,

$\lambda_{ik} = 0$, якщо $(Y_i, X_k) \notin \lambda$ - не пов'язані відношенням.

Проаналізував структуру взаємозв'язків системи безпеки КС, побудували матрицю інцидентності (табл. 1). Наприклад, $\lambda_{15,13}$=0, оскільки підтримка потоку повідомлень фіктивною інформацією (Y_{15}) не може запобігти злому системи шляхом використання чужих прав авторизації (X_{13}), проте цю загрозу можна попередити шляхом шифрування даних, що захищаються (Y_{22}), тому $\lambda_{22,13}$=1.

Таблиця 1 – Матриця інцидентності безпеки комп'ютерної системи (Δ)

	X1	X2	X3	X4	X5	X6	X7	X8	X9	X10	X11	X12	X13	X14	X15	X16	X17	X18	X19	X20	X21	X22	X23	X24	X25	X26
Y1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1
Y2	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	1	1	1	1	1	1	1	1
Y3	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Y4	1	1	1	1	1	0	1	0	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Y5	1	1	1	1	1	0	1	0	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Y6	1	1	1	1	1	0	0	0	0	1	0	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1
Y7	1	1	1	1	1	0	0	1	0	1	0	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1
Y8	1	1	1	1	1	1	1	1	0	0	0	1	1	1	1	1	0	1	0	0	0	1	1	1	1	1
Y9	1	1	1	1	0	1	0	0	0	0	0	1	1	0	0	0	0	0	1	1	1	1	1	1	1	1
Y10	1	1	1	1	1	1	1	1	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Y11	1	1	1	1	1	0	1	1	0	1	0	1	1	1	1	1	0	0	0	0	0	1	1	1	1	1
Y12	0	1	0	1	0	0	1	0	0	0	0	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1
Y13	1	1	1	1	1	0	1	0	0	1	0	1	1	1	1	1	0	1	0	0	0	1	1	1	1	1
Y14	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1
Y15	0	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Y16	0	0	0	0	1	0	1	1	0	1	1	0	0	0	0	0	0	1	0	0	0	1	0	1	0	0
Y17	1	1	1	1	1	0	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Y18	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1
Y19	1	1	1	1	1	0	1	0	0	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Y20	0	0	1	1	1	0	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Y21	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

	X1	X2	X3	X4	X5	X6	X7	X8	X9	X10	X11	X12	X13	X14	X15	X16	X17	X18	X19	X20	X21	X22	X23	X24	X25	X26
Y22	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	0	1	0	0	0	1	1	1	1	1
Y23	0	0	0	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1	1	1
Y24	0	0	1	1	1	1	1	0	1	0	0	1	1	1	1	1	0	1	0	0	0	1	1	1	1	1
Y25	0	0	0	0	1	0	1	1	1	0	1	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0
Y26	0	0	0	0	1	0	1	1	1	1	1	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0
Y27	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Y28	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1

Відношення λ породжує симплексний комплекс безпеки КС $K_Y(X;\lambda)$ (під структурою відношення λ розумітимемо саме цей комплекс).

Аналогічно, якщо Y є множиною вершин, то λ^{-1} є зв'язаним комплексом, в якому X_k є симплекси. Відношення λ^{-1} між X та Y існує тоді і тільки тоді, коли між Y_i і X_i існує відношення λ. Зауважимо, що у даному випадку матрицею інцидентності для λ^{-1} є матриця Δ^T, яку можна одержати за допомогою операції транспортування Δ.

Для подальшого аналізу структури безпеки КС введемо поняття *q*-зв'язку. Оскільки симплексний комплекс є множиною симплексів, з'єднаних між собою за допомогою спільних граней, то за характеристику зв'язку можна брати величину грані, спільної для двох симплексів. Але нас цікавить комплекс у цілому, тому більш доцільно використати при цьому поняття ланцюга зв'язку, який віддзеркалює той факт, що два симплекси можуть і не мати спільної грані, але можуть бути зв'язані за допомогою послідовності проміжних симплексів.

Будемо вважати, що задана пара симплексів σ_p, $\sigma_r \in K$ зв'язана у ланцюг, якщо існує скінчена послідовність симплексів $\sigma_{a_1}, \sigma_{a_2}, ..., \sigma_{a_n}$, що:

1. σ_{a_1} – грань симплекса σ_p;
2. σ_{a_n} – грань симплекса σ_r;
3. σ_{a_i} і $\sigma_{a_{i+1}}$ – відокремлені спільною гранню, наприклад, σ_{β_i}, для *i=1,...,(n-1).*

Вважатимемо, що цей ланцюг зв'язку є ***q*-зв'язком**, якщо *q* є найменшим з цілих чисел $\{a_1, \beta_1, \beta_2, ..., \beta_{n-1}, a_n\}$.

Очевидно, що симплекс σ_p повинен розглядатися як *p*-зв'язаний сам із собою, незважаючи на те, що не може бути (*p+1*)-зв'язаним ні з яким іншим симплексом.

Процес виділення найбільших частин комплексу *K*, які *q*-зв'язані для всіх значень *q* від 0 до *dim K*, передбачає виділення симплексів із *K* на кожному рівні *q*. Таким чином, можна ввести на симплексах із *K* відношення γ_q, що визначається таким чином: $(\sigma_p, \sigma_r) \in \gamma_q$ тоді і тільки тоді, коли симплекс σ_p *q*-зв'язаний із σ_r. Це відношення γ_q рефлексивне, симетричне і транзитивне, а тому є відношенням еквівалентності. Класи еквівалентності для відношення γ_q є елементами фактор-множини (K/γ_q) і визначають розбиття комплексу *K*. Позначимо число елементів множини (K/γ_q) через Q_q; воно дорівнює кількості різних *q*-зв'язаних компонент у *K*. Ця операція називається **Q-аналізом** комплексу *K*, а вектор $Q = (Q_{\dim K}, ..., Q_1, Q_0)$ – першим структурним вектором комплексу.

Алгоритм знаходження значень *q* для спільних граней усіх пар симплексів безпеки КС у *K* і алгоритм одержання значень Q_q використовує матрицю інцидентності Δ, що визначає *K*. Таким чином, для знаходження *q*-спільних граней усіх пар *Y*-симплексів у $K_Y(X;\lambda)$ необхідно:

1. скласти матрицю $\Delta\Delta^T$ розміром (*m*×*m*);
2. дослідити матрицю $\Delta\Delta^T - \Omega$, де $\Omega = (\omega_{ij})$, а $\omega_{ij} = 1$ для всіх *i, j*=1,2,…,*m*.

Цілі числа на діагоналі є розмірностями симплексів *Y*, а Q-аналіз здійснюється перевіркою інших

комбінацій стовпчиків та рядків. Таким чином, маємо *dim K*=25, оскільки Y_{21}, Y_{27} – симплекси розмірності 25 і проаналізувавши матрицю *q*-значень симплексів комплексу $K_Y(X;\lambda)$ маємо:

при *q*=25 Q=1 $\{Y_{21}, Y_{27}\}$;

при *q*=23 Q=1 $\{Y_1, Y_{10}, Y_{14}, Y_{21}, Y_{27}\}$;

при *q*=22 Q=1 $\{Y_{17}, Y_{18}, Y_{21}, Y_{27}\}$;

при *q*=21 Q=1 $\{Y_1, Y_4, Y_5, Y_{10}, Y_{14}, Y_{17}, Y_{18}, Y_{19}, Y_{20}, Y_{21}, Y_{27}\}$;

при *q*=20 Q=1 $\{Y_3, Y_4, Y_5, Y_{10}, Y_{14}, Y_{17}, Y_{18}, Y_{19}, Y_{20}, Y_{21}, Y_{27}, Y_{28}\}$;

при *q*=19 Q=1 $\{Y_1, Y_4, Y_5, Y_{14}, Y_{17}, Y_{18}, Y_{19}, Y_{20}, Y_{28}\}$;

при *q*=18 Q=1 $\{Y_1, Y_3, Y_8, Y_{10}, Y_{14}, Y_{18}, Y_{20}, Y_{21}, Y_{22}, Y_{28}\}$;

при *q*=17 Q=1 $\{Y_1, Y_2, Y_7, Y_8, Y_{10}, Y_{11}, Y_{13}, Y_{14}, Y_{17}, Y_{18}, Y_{19}, Y_{21}, Y_{22}, Y_{27}\}$;

при *q*=16 Q=1 $\{Y_1, Y_3, Y_4, Y_5, Y_6, Y_7, Y_8, Y_{10}, Y_{11}, Y_{13}, Y_{14}, Y_{17}, Y_{18}, Y_{19}, Y_{21}, Y_{22}, Y_{24}, Y_{27}, Y_{28}\}$;

при *q*=15 Q=1 $\{Y_1, Y_2, Y_3, Y_6, Y_7, Y_8, Y_{10}, Y_{11}, Y_{13}, Y_{14}, Y_{20}, Y_{22}, Y_{24}\}$;

при *q*=14 Q=1 $\{Y_{18}, Y_{19}, Y_{20}, Y_{21}, Y_{27}, Y_{28}\}$;

при *q*=13 Q=1 $\{Y_2, Y_4, Y_5\}$;

при q=11 Q=1 $\{Y_2, Y_8, Y_9, Y_{10}, Y_{11}, Y_{12}, Y_{13}, Y_{14}, Y_{17}, Y_{18}, Y_{19}, Y_{21}, Y_{22}\}$;

при q=10 Q=1 $\{Y_2, Y_6, Y_7, Y_9, Y_{11}, Y_{12}, Y_{13}, Y_{20}, Y_{24}, Y_{28}\}$;

при q=7 Q=1 $\{Y_{16}, Y_{20}, Y_{21}, Y_{26}, Y_{27}\}$;

при q=6 Q=1 $\{Y_1, Y_2, Y_{10}, Y_{14}, Y_{16}, Y_{17}, Y_{18}, Y_{26}\}$;

при q=5 Q=1 $\{Y_{16}, Y_{22}, Y_{23}, Y_{25}, Y_{26}\}$;

при q=4 Q=1 $\{Y_8, Y_{10}, Y_{11}, Y_{13}, Y_{17}, Y_{18}, Y_{19}, Y_{24}, Y_{25}, Y_{26}\}$;

при q=3 Q=1 $\{Y_3, Y_4, Y_5, Y_7, Y_{11}, Y_{13}, Y_{15}, Y_{19}, Y_{25}, Y_{26}, Y_{28}\}$.

Аналіз для $K_X(Y;\lambda^{-1})$ виконується дослідженням матриці $\Delta^T\Delta - \Omega'$, де Ω' – матриця розміром ($n \times n$), що складається з одиниць. Таким чином, для комплексу $K_X(Y;\lambda^{-1})$ маємо *dim K*=25, оскільки X_5, X_{22} – симплекси розмірності 25 і при *q*=23Q=1 $\{X_{23}, X_{24}, X_{25}, X_{26}\}$;

при *q*=22 Q=1 $\{X_4, X_{12}, X_{13}, X_{23}, X_{24}, X_{25}, X_{26}\}$;

при *q*=20 Q=1 $\{X_4, X_5, X_{12}, X_{13}, X_{14}, X_{15}, X_{16}, X_{23}X_{24}, X_{25}, X_{26}\}$;

при *q*=19 Q=2 $\{X_2, X_3, X_4, X_7, X_{12}, X_{13}, X_{23}, X_{24}, X_{25}, X_{26}\}, \{X_5, X_{14}, X_{15}, X_{16}, X_{22}\}$;

при *q*=18 Q=2 $\{X_1, X_7, X_{12}, X_{13}\}, \{X_2, X_3, X_{14}, X_{15}, X_{16}\}$;

при *q*=17 Q=3 $\{X_1, X_2, X_3, X_5\}, \{X_7, X_{14}, X_{15}, X_{16}\}, \{X_5, X_{10}, X_{18}, X_{22}\}$;

при *q*=14 Q=1 $\{X_4, X_{12}, X_{13}, X_{18}, X_{19}, X_{20}, X_{21}, X_{22}, X_{23}, X_{24}, X_{25}, X_{26}\}$;

при *q*=12 Q=1 $\{X_1, X_2, X_3, X_7, X_{19}, X_{20}, X_{21}\}$;

при *q*=11 Q=1 $\{X_4, X_5, X_6, X_8, X_{11}, X_{12}, X_{13}, X_{14}, X_{15}, X_{16}, X_{17}, X_{22}, X_{23}, X_{24}, X_{25}, X_{26}\}$;

при *q*=9 Q=2 $\{X_1, X_2, X_3, X_6, X_8\}, \{X_{17}, X_{18}, X_{19}, X_{20}, X_{21}\}$;

при *q*=8 Q=1 $\{X_6, X_{11}, X_{19}, X_{20}, X_{21}\}$.

Таким чином, за даними симплексними комплексами $K_Y(X;\lambda)$ і $K_X(Y;\lambda^{-1})$, які відображають структуру відношень у системі безпеки КС, можна визначити, як ланцюги зв'язку з'єднують заходи

безпеки Y_i та загрози безпеці КС X_j.

Для кожного значення розмірності q=0,1,…,*dim K* ми отримали число різних класів еквівалентності Q_q. **Структурний вектор** відношень механізмів захисту КС має вигляд:

Q={0,0,0,1,1,1,1,1,1,0,0,1,1,0,1,1,1,1,1,1,1,1,1,1,1,1,1,1},

а для відношень загроз:

Q={0,0,0,0,0,0,0,0,1,2,0,1,1,0,1,0,0,3,2,2,1,0,1,1,0,0}.

Існування на рівні q більше, ніж одної компоненти, означає, що існує декілька еквівалентних за характеристиками зв'язності множин. Наявність цих множин означає, що при їх одночасному використанні, дані множини будуть тільки перешкоджати дії один одного.

За допомогою структурних векторів можна отримати і порівняти ступінь складності комплексів відношень елементів множин безпеки КС. Для цього використаємо формулу:

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

де N=*dim K* – розмірність комплексу *K*, а Q_i – *i*-та компонента структурного вектора *Q*, отриманого в результаті застосування *q*-аналізу. Таким чином, $\phi_{мех.зах} = 0{,}8917$, а $\phi_{загроз} = 0{,}7664$, що свідчить про більшу складність механізмів захисту КС. Тобто набагато важче побудувати таку систему захисту КС, яка б змогла забезпечити захист від усіх загроз, ніж побудувати таку систему загроз, завдяки якій з деякою ймовірністю можна будо подолати будь-яку систему безпеки.

III Ексцентриситет системи комп'ютерної безпеки

За допомогою Q-аналізу дослідили загальну структуру зв'язаності елементів захисту та загроз системи комп'ютерної безпеки. Проаналізуємо індивідуальні властивості симплексів та їх вплив на структуру зв'язаності системи безпеки КС. З цією метою введемо поняття **ексцентриситету**, яке є мірою ізоляції симплексів один від одного:

$$Ecc(Y_i) = (\hat{q} - \overset{\vee}{q})/(\overset{\vee}{q} + 1),$$

де $\hat{q}$ – це dim P_i у *K*, *а* $\overset{\vee}{q}$ – це найменше значення рівня q, при якому P_i стає зв'язаною.

Поняття ексцентриситету віддзеркалює як відносну важливість даного симплекса для комплексу безпеки КС загалом (через його розмірність), так і його важливість як ланцюга зв'язку (через максимальне число його вершин, що також належать до будь-якого іншого симплекса). Таким чином, ексцентриситет дає можливість побачити й оцінити, наскільки «щільно» кожний симплекс вкладений у комплекс.

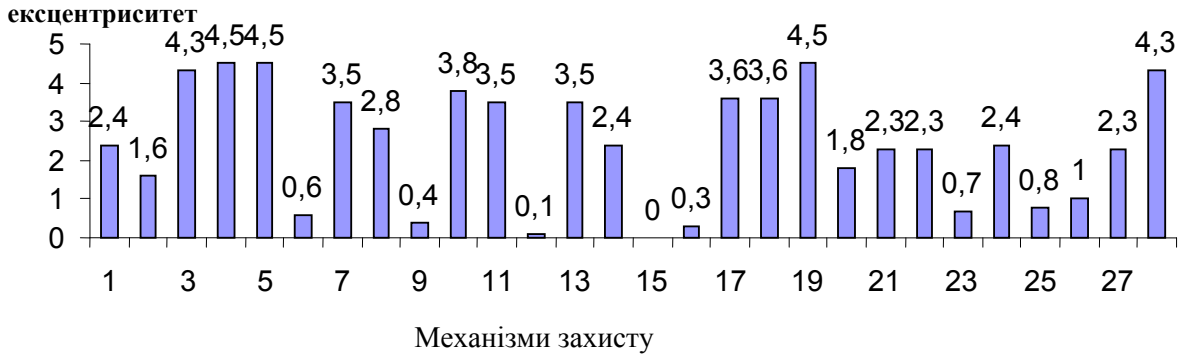

Рисунок 1 – Величини ексцентриситетів механізмів безпеки комп'ютерних систем

З рис. 1 видно, що найбільший ексцентриситет механізмів безпеки КС 4,5 мають: реєстрація (Y_4); визначення прав технічних засобів, задач та користувачів (Y_5); протоколювання та аудит (Y_{19}). Трохи меншу величину ексцентриситету (рівну 4,3) мають ідентифікація, автентичність та авторизація технічних

засобів, задач, масивів і користувачів (Y_3) та організаційні заходи захисту КС (Y_{28}). Тобто, ці механізми захисту є найбільш дієвими.

Аналогічний аналіз можна виконати для множини загроз. Результати розрахунків ексцентриситетів наведено на рис. 2.

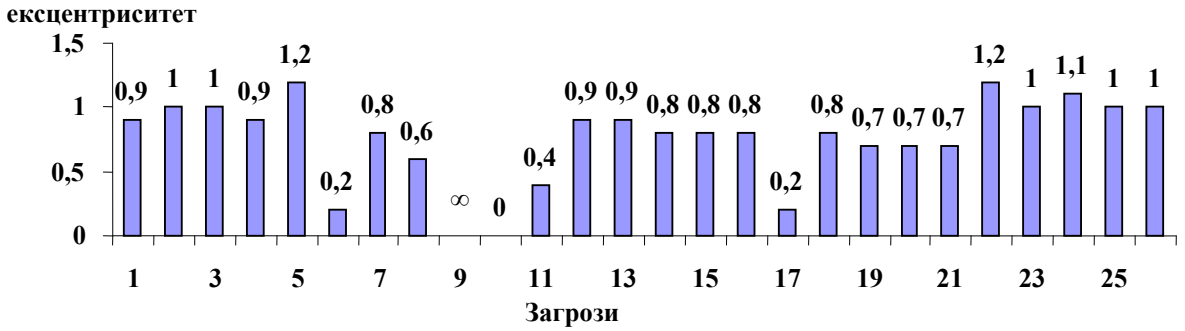

Рисунок 2 – Величини ексцентриситетів загроз безпеці комп'ютерних систем

Найбільшу величину – 1,2 – мають перехоплення і використання шкідливих програм (ці загрози складають найбільшу небезпеку і застосовуються найчастіше), а аналіз трафіка (∞) є некерованою загрозою, тобто не існує визначеної системи захисту від цієї загрози.

Зазначимо, що *величини ексцентриситетів для комплексу механізмів безпеки КС більші порівняно з аналогічними величинами комплексу загроз*, що свідчить про більш високу стійкість та керованість елементів множини механізмів захисту КС.

IV Висновки

Результати дослідження становлять не тільки науковий інтерес, але мають також і певне практичне значення для розробки захищених комп'ютерних систем.

Запропонований підхід до аналізу структури системи комп'ютерної безпеки дозволив визначити переліки заходів, мінімально необхідні для захисту комп'ютерних систем від визначеної кількості загроз, а також переліки загроз, із застосуванням яких можна подолати певну кількість механізмів захисту.

Контроль роботи засобів захисту та правові заходи є необхідними для захисту від загроз усіх типів, що розглядаються. Найбільш дієвими механізмами захисту є ідентифікація, автентичність, авторизація та визначення прав технічних засобів, задач, масивів і користувачів; реєстрація дій, небезпечних для комп'ютерних систем; аналіз адекватності застосування політики безпеки; організаційні заходи захисту.

Найбільш небезпечними є загрози безпосереднього несанкціонованого доступу до захищених даних, які циркулюють між повноважними відправниками та одержувачами (перехоплення), використання шкідливих програм та спостереження за іменами характеристик систем зв'язку, які передають дані (аналіз трафіка).

Для злому комп'ютерної системи досить ймовірні атаки із застосуванням кількох загроз одночасно, тому система захисту повинна розроблятися таким чином, щоб бути готовою до протидії відразу декільком загрозам.

Множина механізмів захисту комп'ютерної системи більш стійка і керована порівняно з множиною загроз. Тому побудувати систему комп'ютерної безпеки, яка б змогла забезпечити захист від усіх загроз набагато важче, ніж побудувати такий алгоритм атаки комп'ютерної системи, завдяки якому з деякою ймовірністю можна буде подолати будь-яку систему безпеки.

Література: ***1.*** *Качинський А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи – К.., 2004.* ***2.*** *Касти Дж. Большие системы. Связность, сложность и катастрофы. – м. Мир – 1982.* ***3.*** *Саати Т. Принятие решений. Метод анализа иерархий. – М.: Радио и связь – 1993.* ***4.*** *Гайкович В., Першин А. Безопасность электронных банковских систем.* ***5.*** *Петров А. А. Компьютерная безопасность – Москва. 2000.*