УДК 519.6+625.1

КАЧИНСЬКИЙ А.Б., *доктор технічних наук, професор*
ВАРИЧЕВА Д.І., студентка 2 курсу ФТІ НТУУ “КПІ”
СВИРИДЕНКО С.В., студентка 2 курсу ФТІ НТУУ “КПІ”

КІЛЬКІСНІ ОЦІНКИ ПРІОРИТЕТІВ СИСТЕМИ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Анотація. *Запропоновано алгоритм вибору раціональної структури системи кібернетичної безпеки з елементами потенційних кіберзагроз в умовах високої ймовірності їх реалізації. Алгоритм базується на аналізі ієрархічних структур. Розглядаються основні кібернетичні загрози й оцінки локальних і глобальних пріоритетів системи кібернетичної безпеки.*

Ключові слова: *кібербезпека, кіберзагрози, ризики, метод аналізу ієрархій, попарні порівняння, загрози, локальні і глобальні пріоритети.*

Аннотация. *Предложен алгоритм выбора рациональной структуры системы кибернетической безопасности с элементами потенциальных киберугроз в условиях высокой вероятности их реализации. Алгоритм базируется на анализе иерархических структур. Рассматриваются основные кибернетические угрозы и оценки локальных и глобальных приоритетов системы кибернетической безопасности.*

Ключевые слова: *кибербезопасность, киберугрозы, риски, метод анализа иерархий, попарные сравнения, угрозы, локальные и глобальные приоритеты.*

Summary. *The algorithm of a choice of rational cyber security structure with elements of potential cyber threats in a high probability of their realization is proposed. The algorithm is based on the analysis of hierarchical structures. The article discusses the basic cyber threats and evaluation of local and global priorities of cyber security.*

Keywords: *cyber security, cyber threats, risks, hierarchy analysis method, pairwise comparisons, threats, local and global priorities.*

Постановка проблеми. Сучасні вимоги до систем забезпечення кібернетичної безпеки, узгодженої взаємодії її елементів, передбачають наявність пріоритетних заходів, спрямованих на гарантування необхідного рівня їх захисту.

В останні роки з’явилися публікації, присвячені розв’язанню даної проблеми, зокрема, див. [1 – 11]. В основі цих методів знаходиться метод аналізу ієрархій (далі – МАІ).

Проте, оцінка локальних та глобальних пріоритетів забезпечення кібернетичної безпеки потребує подальших досліджень.

Метою статті є розробка алгоритму структури системи кібернетичної безпеки (далі – СКБ), де основними її елементами є потенційні кіберзагрози, що існують в умовах високої ймовірності їх реалізації.

Виклад основного матеріалу. Ієрархічне уявлення про СКБ використовується для опису того, як впливають зміни пріоритетів (відповідних внесків) на нижніх рівнях на пріоритети елементів верхніх рівнів. Ієрархічні структури надають більше інформації про склад та функції системи нижніх рівнів, забезпечують розгляд чинників і їх цілей на вищих рівнях. Алгоритм застосування МАІ заснований на послідовній реалізації чотирьох принципів: ідентичності, дискримінації, синтезу локальних та глобальних пріоритетів [7].

Принцип ідентичності: декомпозиція системи кібернетичної безпеки.

Передбачає структурування у вигляді ієрархії, і є першим етапом застосування МАІ для прийняття рішень у важкоформалізованих ситуаціях, що стосуються СКБ.

Система кібернетичної безпеки – це функціональна система, що відображає процес взаємодії трьох основних компонентів: безпеку, загрози та ризик. Ці компоненти визначають стан захищеності важливих інтересів особи, суспільства та держави.

У нашому випадку ієрархічна модель системи кібернетичної безпеки (Рис. 1) розглядається як цілеспрямована інформаційно-управлінська структура з обов’язковим урахуванням ієрархічних рівнів її організації: перший рівень – кібернетична безпека, другий рівень – загрози, третій рівень – ризики. При цьому функції управління розподілені між супідрядними рівнями, і організація всієї системи підпорядкована певній меті – дотримання визначеного рівня безпеки. Вважається, що елементи кожного рівня СКБ незалежні. Окрім того, ієрархія будувалася з вершини.

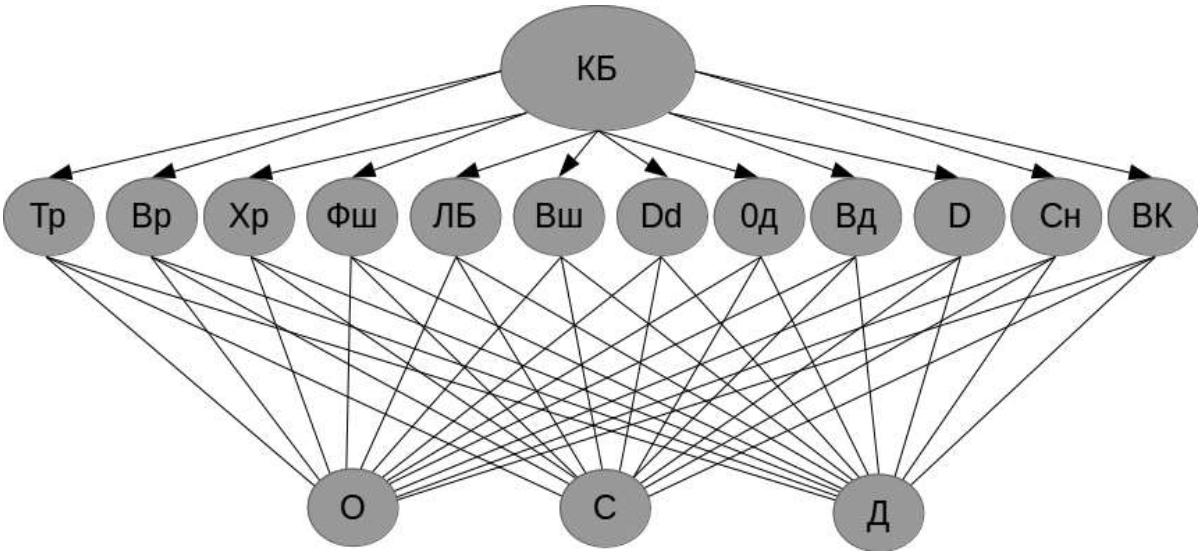

Рис. 1. Ієрархічна модель системи кібернетичної безпеки

На рисунку: 1 рівень – кібернетична безпека (КБ);
2 рівень – загрози (Тр - троян, Вр - вірус, Хр - хробак, Фш - фішинг, Лб - логічні бомби, Вш - вішинг, Dd - DDoS атаки, 0Д - атака нульового дня, Вд - відмичка, D- DoS-атака, Сн - сніффер, Вк - воєнне катання);
3 рівень – ризики загроз (О - особа; С - суспільство; Д - держава).

Зробимо деякі зауваження:

- очевидно, що модель значно спрощена: залежно від питання, на яке хочемо дістати відповідь, можна було би визначити більше елементів та ієрархічних рівнів. Тут запропонована ієрархічна модель з урахуванням відповідності до нашого розуміння проблеми кібернетичної безпеки;
- у пропонованій моделі не врахований той очевидний факт, що не тільки критерії екологічної безпеки впливають на альтернативи, але й альтернативи впливають на критерії. На нашу думку, цей зворотній зв’язок не суттєвий для даної проблеми.

Принцип дискримінації: порівняльні міркування у системі кібернетичної безпеки.

Після ієрархічної структуризації проблеми центральне питання в термінах методу аналізу ієрархій щодо проблеми кібернетичної безпеки такє: як відчутно впливають окремі чинники нижчого рівня ієрархії на вершину – загальну мету? Нерівномірний вплив усіх факторів на мету призводить до необхідності визначення інтенсивності впливу (пріоритетів) цих факторів.

Відповісти на ці питання можна за допомогою принципу дискримінації. Згідно нього визначення пріоритетів чинників найнижчого рівня щодо мети можна звести до послідовності завдань визначення пріоритетів для кожного рівня, а кожне таке завдання – до послідовності попарних порівнянь.

Розгляд даної проблеми доречно розпочати зі з’ясування ключових понять, що пов’язані з реалізацією принципу декомпозиції.

Кібернетична безпека (кібербезпека) – це стан захищеності життєво важливих інтересів особи, суспільства та держави від зовнішніх і внутрішніх загроз, джерелом яких є кібернетичний простір.

Важливу роль при забезпеченні кібернетичної безпеки відіграє класифікація загроз на окремі види відповідно до чітко визначених критеріїв, що допомагає гарантувати необхідний рівень захисту основних об’єктів.

Кібернетичні загрози (кіберзагрози) – це прогнозовані, але не контрольовані явища, події та процеси, що відбуваються в кібернетичному просторі, і можуть завдати значних збитків матеріальним і духовним цінностям особи, суспільства та держави.

Аналіз численних джерел і літератури з проблем кібернетичної безпеки свідчить про те, що нині відсутній єдиний підхід щодо класифікації цього складного та багатобічного явища [5; 6; 9]. Ми зупинилися на тих типах кіберзагроз, що були наведені у доповіді Конгресу США їх розвідувальними службами [6], а також у роботах [1; 2; 10].

Відповідно до стандарту міжнародного союзу електрозв’язку (ITU-T) E.408 [ITU-T. Recommendation E.408. Telecommunication Network Security Requirement, 2004] кількісна оцінка ризику загрози інформаційній безпеці у мережі зв’язку, визначається двома характеристиками – ймовірністю реалізації загрози та збитками, що виникають при її реалізації.

Під кібернетичними ризиком ми розуміємо наступне.

Кібернетичний ризик (кіберризик) – це прогнозована векторна величина збитку, що пов’язана із реалізацією кібернетичної загрози, і дорівнює добутку ймовірності її реалізації на ймовірність величини можливого збитку від даної загрози.

Ризик є кількісною мірою безпеки. Його оцінка при проектуванні, дослідженні й експлуатації мережі дозволяє приділяти найбільшу увагу забезпеченню захисту від кіберзагроз, що є найбільш небезпечними [3].

Можливості використання принципу дискримінації в різних ситуаціях, пов’язаних із формуванням і вибором альтернатив, наведені в роботах [7; 8]. Одначе принциповою тут є оцінка ступеню близькості позитивної обернено-симетричної матриці до узгодженої, можна за значенням показника індексу узгодженості (I_y), що обчислюється за формулою:

$$I_y = \frac{\lambda max \quad n}{n \quad 1};$$

де: n – порядок матриці, λ_{max} – її найбільше власне число.

Крім того, для таеих цілей використовується так зване відношення узгодженості:

$$B_y = \frac{Iy}{M(Iy)};$$

де: $M(I_y)$ – середнє значення індексу узгодження випадковим чином складеної матриці парних порівнянь.

Позитивна обернено-симетрична матриця є узгодженою тоді і тільки тоді, коли порядок матриці та її найбільше власне максимальне значення збігаються ($n = \lambda_{max}$)

У неузгоджених обернено-симетричних матрицях $\lambda_{max} \neq n$, практично $\lambda_{max} > n$. Тому $I_y > 0$ та $B_y > 0$. На практиці вважають, що якщо $B_y \leq 0{,}1$, то можна бути задоволеним ступенем узгодженості матриці.

Принцип синтезу локальних пріоритетів системи кібернетичної безпеки.

У нашій моделі перший рівень ієрархії має одну мету: кібернетична безпека. Значення її пріоритету приймається рівним одиниці.

Другий рівень ієрархії нараховує дванадцять видів загроз. Пріоритети цих загроз розраховуються за допомогою матриці попарних порівнянь загроз щодо кібернетичної безпеки у спосіб порівняння елементів другого рівня ієрархії відносно першого рівня.

Матриця попарних порівнянь, що заснована на шкалі важливості Т. Сааті, має наступний вигляд:

Безпека	**Тр**	**Вр**	**Хр**	**Фш**	**ЛБ**	**Вш**	**Dd**	**0д**	**Вд**	**D**	**Сн**	**ВК**
Тр	1	2	3	3	4	6	7	7	8	9	9	9
Вр	1/2	1	2	3	3	5	6	6	8	8	9	9
Хр	1/3	1/2	1	2	3	4	5	5	6	7	7	8
Фш	1/3	1/3	1/2	1	2	3	4	5	5	7	7	8
ЛБ	1/4	1/3	1/3	1/2	1	2	3	4	4	5	5	7
Вш	1/6	1/5	1/4	1/3	1/2	1	2	2	3	5	5	6
Dd	1/7	1/6	1/5	1/4	1/3	1/2	1	2	3	3	5	6
0д	1/7	1/6	1/5	1/5	1/4	1/2	1/2	1	2	2	3	4
Вд	1/8	1/8	1/6	1/5	1/4	1/3	1/3	1/2	1	2	2	3
D	1/9	1/8	1/7	1/7	1/5	1/5	1/3	1/2	1/2	1	2	3
Сн	1/9	1/9	1/7	1/7	1/5	1/5	1/5	1/3	1/2	1/2	1	2
ВК	1/9	1/9	1/8	1/8	1/7	1/6	1/6	1/4	1/3	1/3	1/2	1

Локальні пріоритети показують відносну силу, величину, бажаність кожного окремого елемента системи кібернетичної безпеки. Як показали розрахунки, найбільший локальний пріоритет щодо кібербезпеки у порівнянні з іншими кіберзагрозами має троян – 0,25. На другому і третьому місцях віруси та хробаки, глобальні пріоритети яких відповідно дорівнюють 0,20 і 0,15. Заслуговують уваги також фішинг з глобальними пріоритетами 0,12, логічні бомби – 0,08, а також вішинг – 0,06 Для решти кіберзагроз глобальні пріоритети наступні: DDoS-атаки – 0,04, атака нульового дня – 0,04, відмичка – 0,025, DoS-атака – 0,019, сніффер – 0,015, воєнне катання – 0,011.

Основним завданням третього етапу MAI є визначення локальних пріоритетів ризиків об’єктів захисту для кібербезпеки через проміжний другий рівень – загрози за допомогою матриць попарних порівнянь щодо цих загроз. У такий спосіб за допомогою групи матриць парних порівнянь, для вище наведених загроз, послідовно формуємо множину локальних пріоритетів третього рівня щодо ризиків особи, суспільства та держави.

Значення локальних пріоритетів ризиків об’єктів захисту щодо зазначених загроз наведені на Рис. 2 – 13, а загальний їх розподіл в системі кібернетичної безпеки – на Рис. 14.

Троянська програма (або “троян”) – це різновид комп’ютерних програм або шкідливий код, візначальною особливістю якого є здатність, на відміну від вірусів і черв’яків, що поширюються мимоволі, виконувати свої функції зі строго визначеною метою.

Тр	О	С	Д
О	1	3	7
С	1/3	1	5
Д	1/7	1/5	1

λ_{max} =12,784.
I_y = 0,07
B_y = 0,1 – матриця узгоджена.

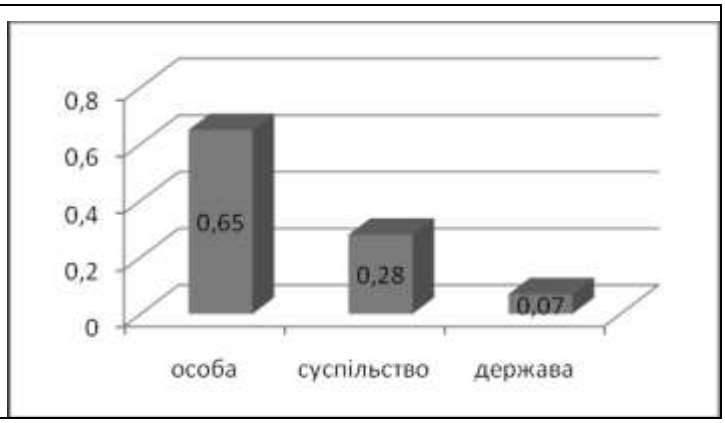

Рис. 2. Локальні пріоритети ризиків об’єктів захисту щодо загрози “троянська програма”

Вірус – вид шкідливого програмного забезпечення, що здатне створювати власні копії та впроваджувати свій код в інші програми, системні області пам’яті, завантажувальні сектори.

Вр	О	С	Д
О	1	3	5
С	1/3	1	4
Д	1/5	¼	1

λ_{max}=3,1
I_y = 0,05
B_y = 0,075 - матриця узгоджена

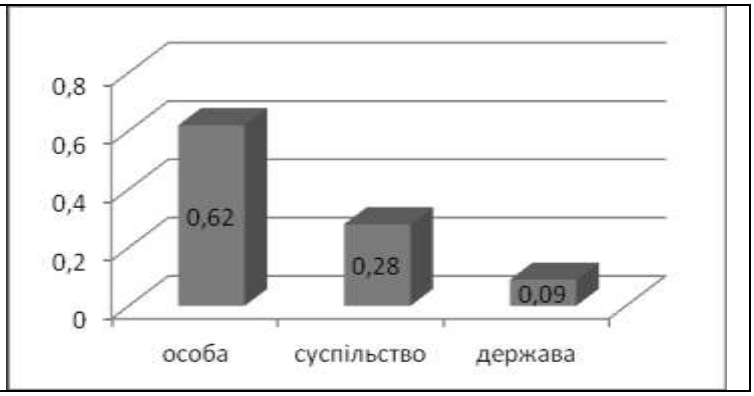

Рис. 3. Локальні пріоритети ризиків об’єктів захисту щодо загрози “вірус”

Хробак – різновид шкідливої програми, яка самостійно розповсюджується через локальні і глобальні комп’ютерні мережі.

Хр	О	С	Д
О	1	1	5
С	1	1	5
Д	1/5	1/5	1

λ_{max}=3,1
I_y= 0,05
B_y = 0,075 -матриця узгоджена.

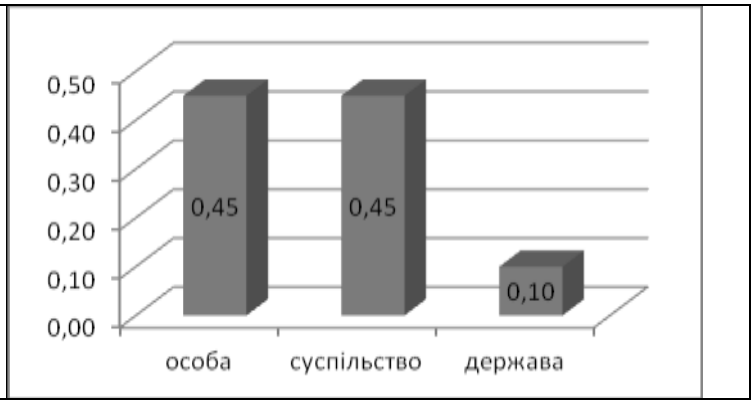

Рис. 4. Локальні пріоритети ризиків об’єктів захисту щодо загрози “хробак”

Фішинг – вид Інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувача за допомогою методів соціальної інженерії.

Фш	О	С	Д
О	1	3	7
С	1/3	1	5
Д	1/7	1/5	1

λ_{max}=3,04
I_y = 0,02
B_y = 0,03 - матриця узгоджена

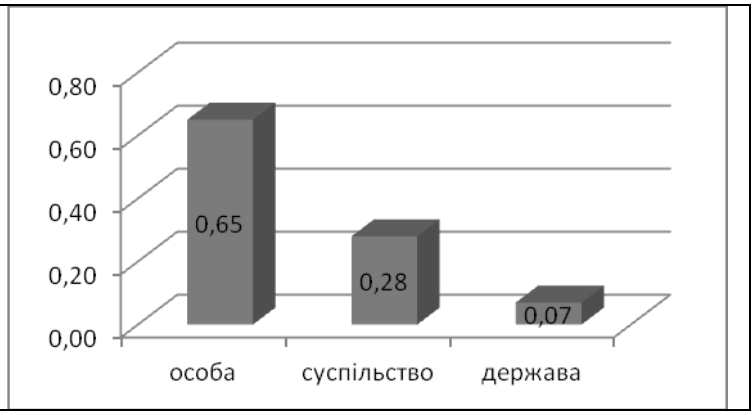

Рис. 5. Локальні пріоритети ризиків об’єктів захисту щодо загрози “фішинг”

Логічна бомба (англ. logic bomb) – загроза покликана припиняти або виводити з ладу програмні продукти, що забезпечує штатний режим роботи даного об’єкта або організації у спосіб введення спеціального сконструйованого коду, що може бути задіяний у визначений момент часу за певних умов.

ЛБ	О	С	Д
О	1	3	9
С	1/3	1	5
Д	1/9	1/5	1

λ_{max}=3,01
I_y = 0,005
B_y = 0,075 - матриця узгоджена

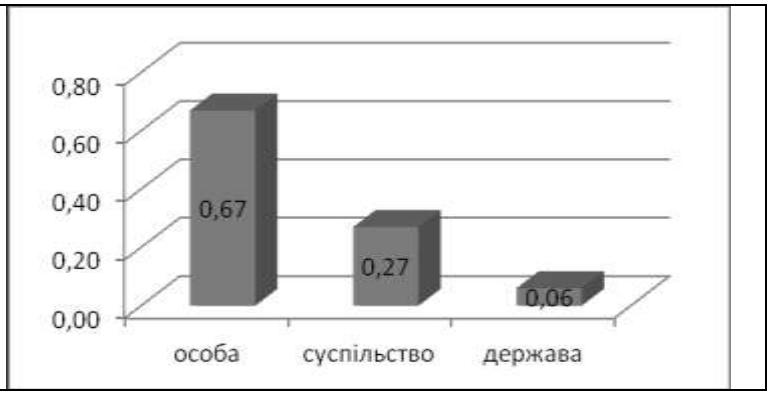

Рис. 6. Локальні пріоритети ризиків об’єктів захисту щодо загрози “логічна бомба”

Вішинг (vishing – voice phishing) названий так за аналогією з фішингом – поширеним мережевим шахрайством. Подібність назв підкреслює той факт, що принципової різниці між вішингом і фішингом немає. Основна відмінність вішингу в тому, що він так чи інакше здійснюється по телефону.

Вш	О	С	Д
О	1	1/5	3
С	5	1	7
Д	1/3	1/7	1

λ_{max}=3,125
I_y = 0,0625
B_y = 0,09 - матриця узгоджена

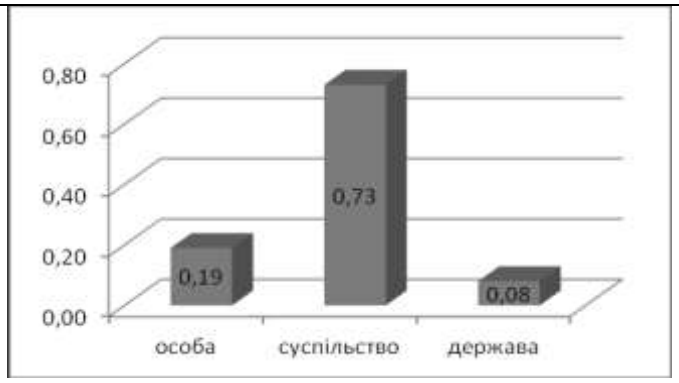

Рис. 7. Локальні пріоритети ризиків об’єктів захисту щодо загрози “вішинг”

DDoS-атака – спосіб атаки на комп’ютерні системи ідентичні DoS-атаці, що відбувається одночасно з багатьох скоординованих пристроїв, за домовленістю або взятими під контроль вірусними програмами.

Dd	О	С	Д
О	1	3	7
С	1/3	1	5
Д	1/7	1/5	1

λ_{max}=3,04
I_y = 0,02
B_y = 0,03 -матриця узгоджена

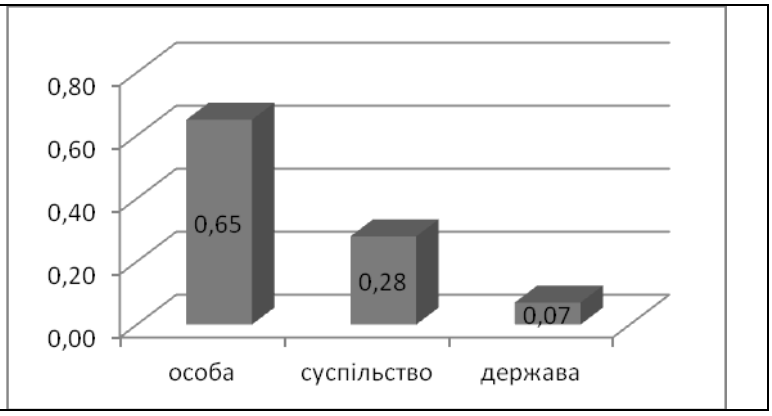

Рис. 8. Локальні пріоритети ризиків об’єктів захисту щодо загрози DDoS-атака

Атака 0 дня – це напад, що відбувається раніше першого дня (в “нульовий” день) розуміння розробником наявної уразливості, означаючи, що у розробника не було жодної можливості розповсюдити патч безпеки серед користувачів програмного забезпечення.

0д	О	С	Д
О	1	3	7
С	1/3	1	5
Д	1/9	1/5	1

λ_{max}=3,04
I_y = 0,02
B_y = 0,03 -матриця узгоджена

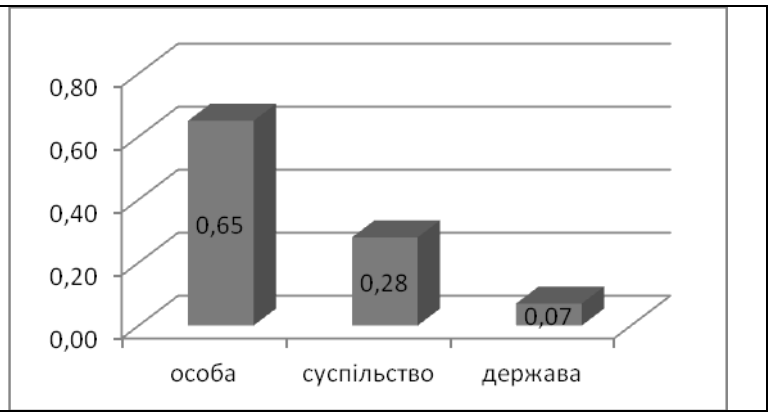

Рис. 9. Локальні пріоритети ризиків об’єктів захисту щодо загрози “атака 0 дня”

Відмичка – загроза, покликана перебрати контроль над комп’ютером жертви або мережею комп’ютерів за допомогою реєстру або файлу у спосіб застосування замаскованого програмного продукту, з наперед заданими шкідливими кодами.

Вд	О	С	Д
О	1	3	9
С	1/3	1	4
Д	1/9	1/4	1

λ_{max}=3,03
I_y= 0,015
B_y = 0,02 - матриця узгоджена

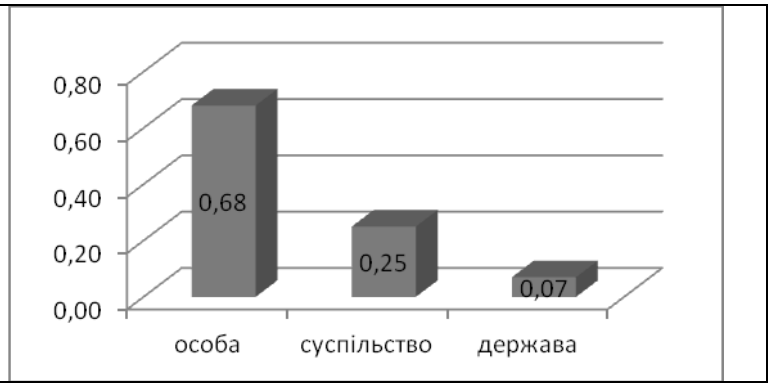

Рис. 10. Локальні пріоритети ризиків об’єктів захисту щодо загрози “відмичка”

DoS-атака – спосіб атаки на комп’ютерні системи, що спрямована на порушення штатного їх функціонування шляхом переповнення ресурсу комп’ютера, внаслідок чого здійснюється його перевантаження.

D	О	С	Д
О	1	5	5
С	1/5	1	6
Д	1/5	1/6	1

λ_{max}=3.1
I_y= 0,05
B_y = 0,07 - матриця узгоджена

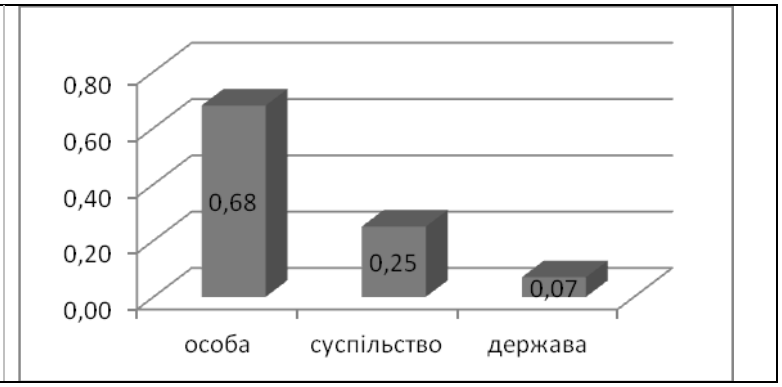

Рис. 11. Локальні пріоритети ризиків об’єктів захисту щодо загрози DoS-атака

Аналізатор трафіку або “сніффер” (англ. to sniff – “нюхати”) – програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу, або тільки аналізу мережного трафіку, призначеного для інших вузлів.

Сн	О	С	Д
О	1	3	9
С	1/3	1	5
Д	1/9	1/5	1

λ_{max}=3,01
I_y = 0,005
B_y = 0,075 - матриця узгоджена

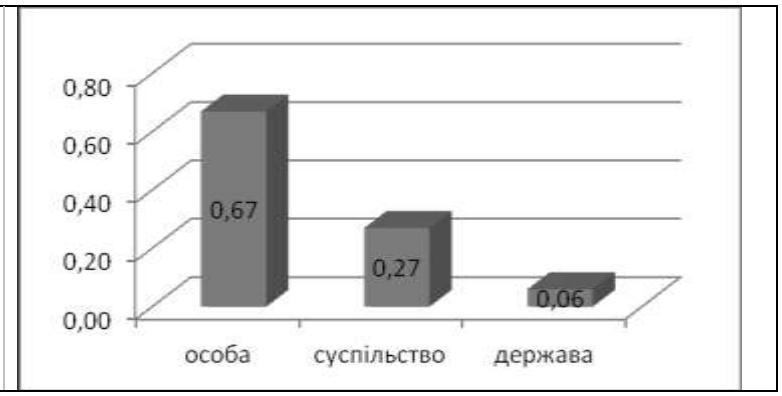

Рис. 12. Локальні пріоритети ризиків об’єктів захисту щодо загрози “сніффер”

Воєнне катання (англ. wardriving) – процес пошуку і злому вразливих точок доступу безпровідних мереж Wi-Fi людиною або групою осіб, оснащених переносним комп’ютером з Wi-Fi-адаптером. При цьому для просторового пошуку та локалізації точки використовується транспортний засіб (звідси і назва – воєнне катання).

ВК	О	С	Д
О	1	2	3
С	1/2	1	3
Д	1/3	1/3	1

λ_{max}=3,07
I_y = 0,035
B_y = 0,05 - матриця узгоджена

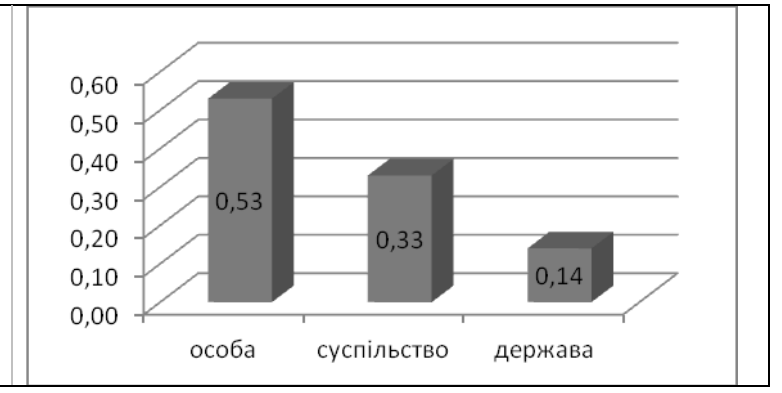

Рис. 13. Локальні пріоритети ризиків об’єктів захисту щодо загрози “вардрайвінг”

Легко побачити, що найбільш уразливою з усіх об’єктів кібербезпеки є особа. Нині важко знайти людину, яка не стикалась би з комп’ютерними загрозами. Зазвичай значна їх частина навіть не здогадується про існування шкідливих програм на їх комп’ютерах. За оцінкою Symantec Corporation на кінець 2015 року жертвами хакерів стали 594 мільйона людей. Збиток від атак в середньому складає $ 358 на одну людину.

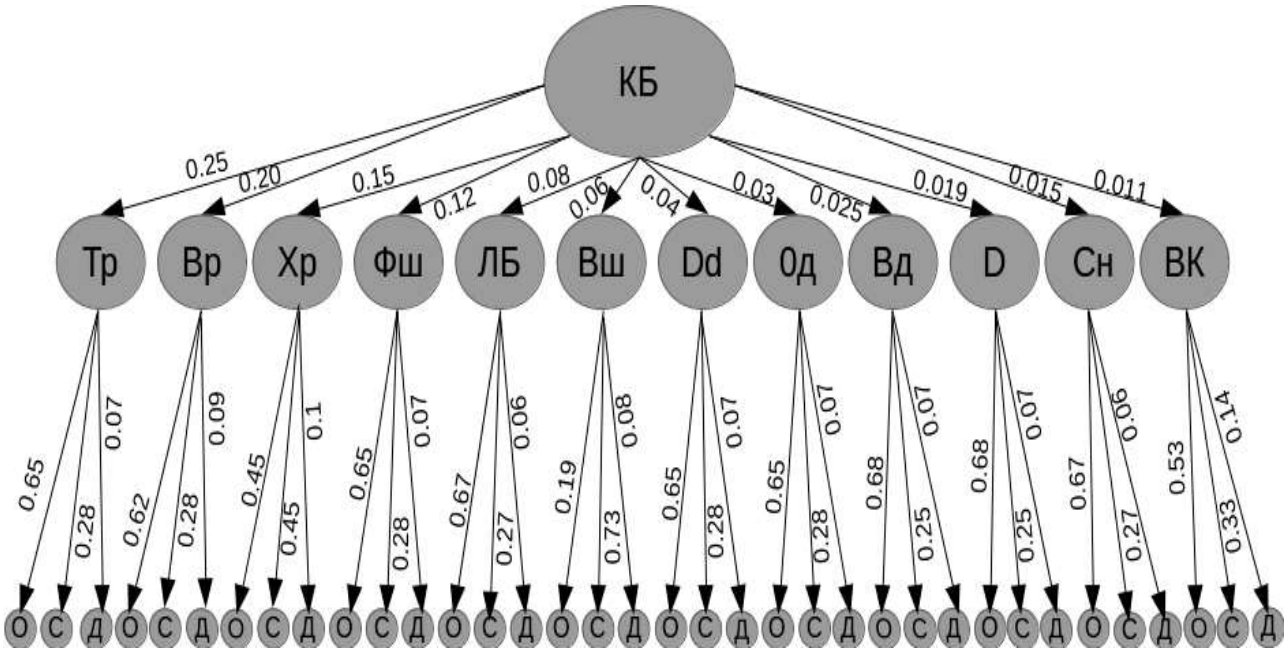

Рис. 14. Розподіл пріоритетів в системі кібернетичної безпеки.

Разом з матрицями парних порівнянь ми отримали міри оцінок відхилення від узгодженості, які в узагальненому вигляді подані в Табл. 1.

Таблиця 1.

Узгодженість пріоритетів ієрархії системи кібербезпеки України

Рівні	**Пріоритети**	**n**	**λ_{max}**	**I_y**	**B_y**
1	КБ	12	12,784	0,07	0,1
2	Тр	3	3,04	0,02	0,03
	Вр	3	3,1	0,05	0,075
	Хр	3	3,1	0,05	0,075
	Фш	3	3,04	0,02	0,03
	ЛБ	3	3,01	0,005	0,0075
	Вш	3	3,125	0,0625	0,09
	Dd	3	3,04	0,02	0,03
	0д	3	3,04	0,02	0,03
	Вд	3	3,03	0,015	0,02
	D	3	3,1	0,05	0,07
	Сн	3	3,01	0,005	0,0075
	ВК	3	3,07	0,035	0,05

Аналіз даної таблиці показав, що не для всіх матриць парних порівнянь індекс узгодженості дорівнює величині розмірів матриці чи має незначні відхилення від неї. Особливо це стосується таких матриць, як: для рівня 2 – матриця загроз щодо кібербезпеки держави; для рівня 3 – матриця об’єктів захисту для кібербезпеки України.

Показники індексів узгодженості ІУ та відношення узгодженості для цих матриць також дещо більші (величина ВУ має бути 10 % або меншою). Якщо ВУ знаходиться за цими межами, то у таких випадках теорія МАІ рекомендує переглянути завдання спочатку і перевірити свої міркування щодо матриці парних порівнянь. Зазначені матриці ми не переглядали, оскільки [7]:

- в окремих випадках можна припустити величину ВУ понад 20 %, але не більше;
- як вважає сам Т. Сааті, у порівняно великих матрицях, розміри яких, наприклад, від 7 до 9, важко досягти високого рівня узгодженості;
- на нашу думку, ті рівні узгодженості, що ми отримали, відповідають тому ризику, який супроводжує роботу з неузгодженими результатами.

Якщо це не покращить узгодженості, то, ймовірно, завдання необхідно більш точно структурувати, тобто згрупувати аналогічні елементи під більш значущими критеріями, хоча для перегляду може бути необхідною тільки сумнівна частина ієрархії.

Для покращення узгодженості можна пошукати додаткову інформацію з даної проблеми і переглянути дані, що використовувалися при побудові шкали.

Принцип синтезу глобальних пріоритетів системи кібернетичної безпеки.

Оскільки глобльаний пріоритет першого рівня дорівнює 1, то, починаючи з другого рівня, глобальні пріоритети синтезуються вниз. Для чого локальні пріоритети множаться на пріоритет відповідного критерію, що знаходиться на вищому рівні, й сумуються з кожним елементом відповідно до критеріїв, на які впливає цей елемент. Процедура продовжується до самого низу. Таким чином вектор локальних пріоритетів другого рівня множиться на 1, що дає цей самий вектор, але вже глобальних пріоритетів другого рівня (див. Табл. 9).

Таблиця 9.

Глобальні пріоритети другого рівня системи кібернетичної безпеки

1	Трояни	0,25
2	Віруси	0,20
3	Хробаки	0,15
4	Фішинг	0,12
5	Логічні бомби	0,08
6	Вішинг	0,06
7	DDoS	0,04
8	Атака 0 дня	0,04
9	Відмичка	0,025
10	DoS	0,019
11	Сніффер	0,015
12	Воєнне катання	0,011

З Табл. 9 видно, що “трояни” для кібернетичної безпеки держави мають найвищий пріоритет (0,25) у порівнянні з іншими загрозами. У деяких троянських програм ці функції добре приховані, тож користувач може і не підозрювати, що його комп’ютер уже “заражений”. Основне завдання троянської програми – звернути на себе увагу користувача

і змусити його запустити цю програму. За даними Лабораторії Касперського більшість троянів спрямовано на користувачів ПК, ніж на організації та державні установи [11].

Троянські програми виконують безліч завдань: порушують роботу інших програм (аж до зависання комп’ютера, яке вирішується лише перезавантаженням); незалежно від власника пропонують в якості стартової сторінки спам-посилання, рекламу або порносайти; поширюють по комп’ютеру користувача порнографію та перетворюють мову текстових документів у бінарний код

Як правило, віруси (глобальний пріоритет – 0,20) у своєму коді несуть додатковий шкідливий функціонал: бекдори, кейлогери, шпигуни, ботнети. Віруси здатні завдати шкоди файловій системі, отримати доступ до конфіденційної інформації, вивести з ладу устаткування(наприклад за допомогою логічної бомби).

За допомогою хробаків (глобальний пріоритет – 0,15) можна зробити збій у системах і мережах, так як вони споживають великий обсяг оперативної пам'яті і забивають пропускну спроможність мереж. Черв’як може надіслати свої копії всім контактам користувача з адресної книги, і далі буде розповсюджуватися в геометричній прогресії. Хробак порушує роботу інших програм та завдає шкоди користувачу шахрайством.

Як правило, за допомогою фішингу (глобальний пріоритет – 0,12) користувачеві надсилається лист з важливою для нього інформацією (наприклад про блокування банківської карти) та відповідним фішинговим посиланням на сторінку, яка запропонує ввести свої персональні дані. Переважно метою атаки є дані банківських рахунків, логіни й паролі на важливих для користувача сайтах.

Логічні бомби (глобальний пріоритет – 0,08) здатні отримати доступ до конфіденційної інформації, вивести з ладу устаткування. Вони можуть спричинити втрату персональної інформації, репутації особи, міжнародного іміджу, конфіденційної інформації. З їх допомогою можна “викликати катастрофи на атомних станціях, відкривати греблі для затоплення населених пунктів, відключати диспетчерське обладнання з метою виклику авіакатастроф”. У результаті впливу “логічної бомби” може постраждати цивільне населення.

Вішингова атака (глобальний пріоритет – 0,06) здатна завдати фінансових збитків користувачеві, викрасти конфіденційну інформацію організації. Вона дозволяє створювати бази паролів та отримувати несанкціонований доступ від викраденого імені.

DDoS-атаки (глобальний пріоритет – 0,04) найчастіше здійснюються для комерційної вигоди, адже для організації DDoS-атаки потрібні сотні тисяч комп’ютерів, а такі величезні матеріальні та часові витрати може дозволити собі далеко не кожен. Для організації DDoS-атак зловмисники використовують спеціальну мережу комп’ютерів – ботнет. “Лабораторія Касперського” регулярно проводить дослідження, які показують, що від DDoS-атак найбільше страждає сфера Інтернет-торгівлі, фінансовий сектор і IT-компанії.

Загроза атаки 0 дня (глобальний пріоритет – 0,04) наразі призвела до того, що багато авторів шкідливого ПЗ фокусують свої зусилля саме на виявленні невідомих вразливостей в програмному забезпеченні. Це зумовлено високою ефективністю використання вразливостей, що, у свою чергу, пов’язано з двома фактами – високим поширенням уразливого ПЗ (саме таке програмне забезпечення, як правило, атакують) і деяким часовим проміжком між виявленням уразливості компанією-розробником програмного забезпечення і випуском відповідного оновлення для виправлення помилки.

Загроза відмичка (глобальний пріоритет – 0,025) покликана перебрати контроль над комп’ютером жертви або мережею комп’ютерів за допомогою реєстру або файлу у спосіб застосування замаскованого програмного продукту, з наперед заданими шкідливими кодами.

Порівнюючи з DDoS-атакою DoS-атака (глобальний пріоритет – 0,019) не дуже страшні, оскільки відбувається з одного комп’ютера, і приносять лише короткочасну шкоду, поки відбувається атака.

Щодо сніфферів: з одного боку це – потужна зброя (глобальний пріоритет – 0,015), за допомогою якого можна здійснити пасивну мережеву атаку. З іншого боку сніффери допомагають системним адміністраторам здійснювати діагностику мережі і відслідковувати атаки комп’ютерних хуліганів. Крім того, вони служать для перевірки і детального аналізу правильності конфігурації мережевого програмного забезпечення. Ці програми можуть являти собою серйозну загрозу, оскільки можуть перехоплювати і розшифровувати імена і паролі користувачів, конфіденційну інформацію, порушувати роботу комп’ютерів і мережі в цілому.

Особливої шкоди воєнне катання (глобальний пріоритет – 0,011) нанести саме по собі не здатне. Але при атаці на бездротову мережу з подальшим її зломом можливі втрати особистих даних користувачів, втрата дієздатності мережі тощо.

Оцінимо вплив елементів найнижчого ієрархічного рівня на найвищий. Складемо матрицю, елементи якої описують вплив третього рівня, що репрезентує ризики об’єктів захисту системи кібернетичної безпеки, на елемент першого рівня – кібернетичну безпеку. Перемножимо цю матрицю на вектор-стовпець глобальних пріоритетів загроз щодо мети.

$$\begin{pmatrix} 0{,}65 & 0{,}62 & 0{,}45 & 0{,}65 & 0{,}67 & 0{,}19 & 0{,}65 & 0{,}65 & 0{,}68 & 0{,}68 & 0{,}67 & 0{,}53 \\ 0{,}28 & 0{,}28 & 0{,}45 & 0{,}28 & 0{,}27 & 0{,}73 & 0{,}28 & 0{,}28 & 0{,}25 & 0{,}25 & 0{,}27 & 0{,}33 \\ 0{,}07 & 0{,}09 & 0{,}1 & 0{,}07 & 0{,}06 & 0{,}08 & 0{,}07 & 0{,}07 & 0{,}07 & 0{,}07 & 0{,}06 & 0{,}14 \end{pmatrix} X \begin{pmatrix} 0{,}25 \\ 0{,}20 \\ 0{,}15 \\ 0{,}12 \\ 0{,}08 \\ 0{,}06 \\ 0{,}04 \\ 0{,}03 \\ 0{,}025 \\ 0{,}019 \\ 0{,}015 \\ 0{,}011 \end{pmatrix} = \begin{pmatrix} 0{,}59 \\ 0{,}33 \\ 0{,}08 \end{pmatrix}$$

Отриманий вектор стовпець презентує глобальні пріоритети ризиків об’єктів захисту щодо головної мети, оцінки яких наведені на Рис. 15.

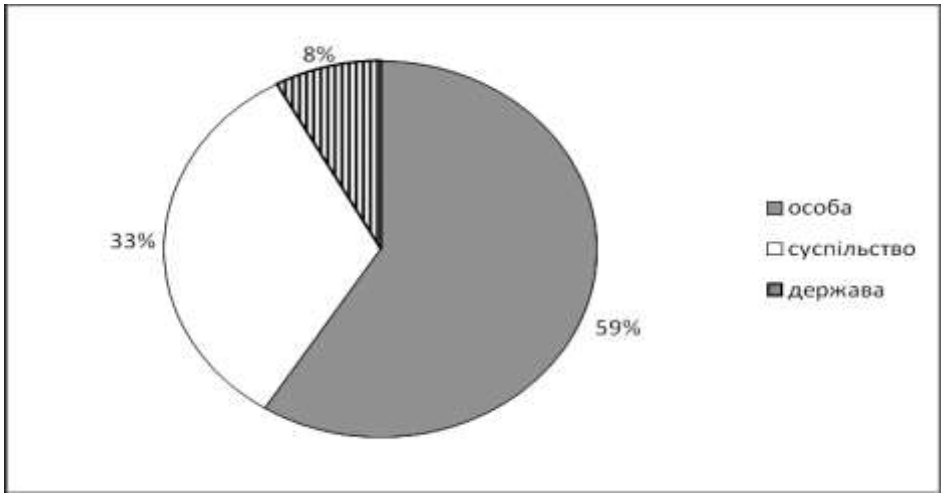

Рис. 15. Глобальні пріоритети ризиків об’єктів захисту.

Зазначимо, що для третього рівня таких загроз як: троян, віруси, вішинг, логічні бомби, DDoS-атаки, атака 0 дня, відмички, DoS, сніфферу, воєнного катання пріоритетом є особа.

Висновки.

Головною ознакою системи кібернетичної безпеки, як будь-якої соціальної системи, є ієрархічність. При цьому система будується у вигляді трьохрівневої структури, де функції управління розподілені між субпідрядними рівнями, і організація всієї системи кібернетичної безпеки підпорядкована головній меті. Тому пріоритети можна розглядати як формалізовані значення величин, що визначаються за допомогою певної системи правил і надають різної ваги різними рішенням.

Локальні пріоритети – це вид ієрархії, коли деяким елементам або цілям надають перевагу у порівнянні з іншими. При цьому індекс узгодженості можна розглядати як показник порушення числової та транзитивної узгодженості матриці парних порівнянь.

Надання різним елементам систем кібернетичної безпеки різної ваги зумовлено їх політичною доцільністю, суспільною необхідністю, результатами формального математичного аналізу. Тому глобальні пріоритети є важливими елементами при формуванні стратегії прийняття рішень у системі кібернетичної безпеки. Вони визначають комплексний характер заходів щодо її забезпечення.

Використана література.

1. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков. – К. : Видавнича група BHV, 2009. – 608 с.

2. Казиев В.М. Введение в анализ, синтез и моделирование систем / В.М. Казиев. – М. : Интернет-университет информационных технологий “БИНОМ”. Лаборатория знаний, 2006. – 244 с.

3. Качинський А.Б. Безпека, загрози та ризик / А.Б. Качинський. – К. : ІПНБ РНБО; НА СБ України, 2004. – 472 с.

4. Кемени Дж. Кибернетическое моделирование / Дж. Кемени, Дж. Снелл. – М. : Советское радио, 1972 – 192 с.

5. Кларк Р. Третья мировая война : какой она будет? Высокие технологии на службе милитаризма / Р. Кларк, Р. Найк. – С-Пб. : Питер, 2011. – 396 с.

6. Роговский Е.А. Глобальные информационные технологии – фактор международной безопасности / Е.А. Роговский / США и Канада : экономика – политика – культура. – 2011. – № 6. – С. 3 - 26.

7. Саати Т. Принятие решений. Метод анализа иерархий / Т. Саати. – М : Радио и связь, 1993. – 278 с.

8. Саати Т. Принятие решений при зависимостях и обратных связях. Аналитические сети / Т. Саати. – М : ЛКИ, 2008. – 360 с.

9. Харрис Ш. Кибервойн@ : Пятый театр военных действий / Ш. Харрис. – М : Альпина нон-фикшн, 2016. – 390с.

10. Lehtinen R. Computer Security Basics O’Reilly/ R. Lehtinen, D. Russell, G. T. Gantemi. – O'Reilly Media, 2006. – 312 с.

11. – Режим доступу : http://www.kaspersky.ru

~~~~~~~~~~~~ * * * ~~~~~~~~~~~~
~~~~~~~~~~~~