ИНСАЙДЕР

INSIDERS: SIDES OF INTERACTION

© ХАРЬКОВСКИЙ ИНСТИТУТ ГВУЗ УБД

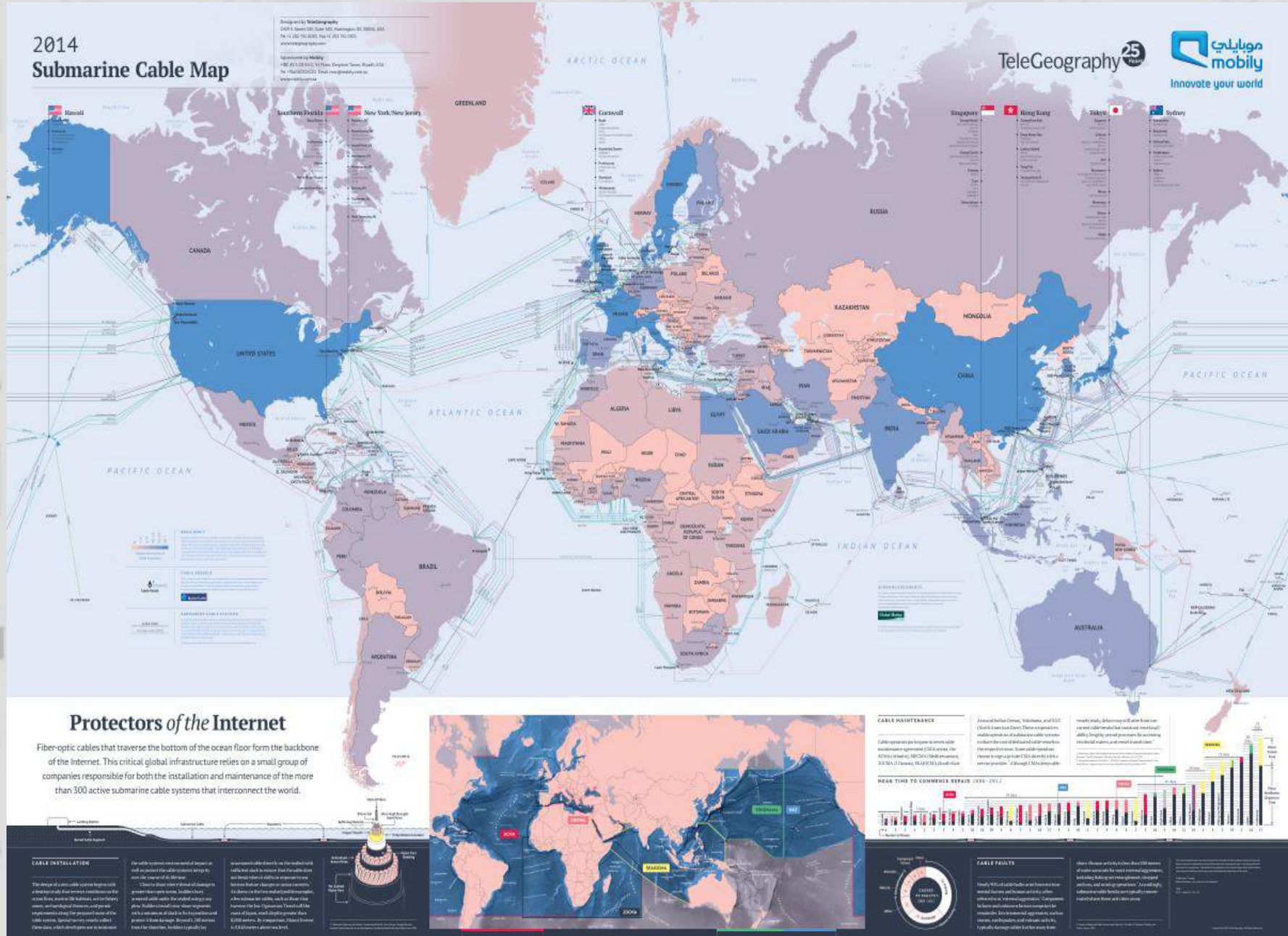
кафедра ИТ, д.э.н., к.т.н., Ph.D. Кавун С.В.

Email: kavserg@gmail.com Skype: serg_kavun

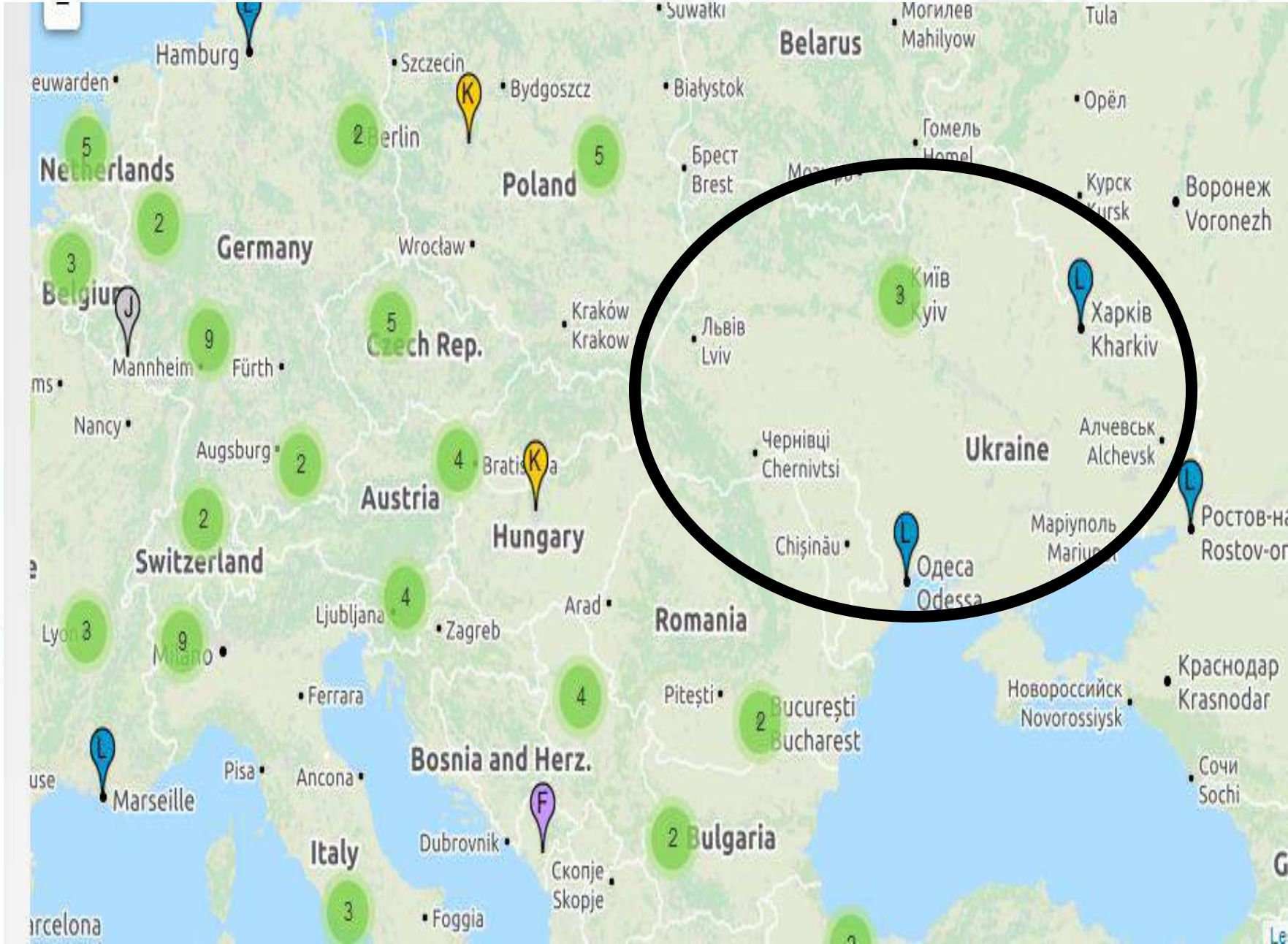
Немного данных ☺

Немного данных ☺

Немного данных ☺



Немного данных ☺



ИНСАЙДЕР

Немного данных ☺

Paul Kane, chief executive officer of CommunityDN in England

Norm Ritchie of Canada

Jiankang Yao of China

Dan Kaminsky, chief scientist at Recursion Ventures in New York City

Bevil Wooding from Trinidad and Tobago

Moussa Guebre of Burkina Faso

Ondrej Sury of the Czech Republic

ICANN

DNS SEC

Overload of the INTERNET

ОпределениЯ

лицо, благодаря своему служебному положению или родственным связям имеет доступ к конфиденциальной информации о деятельности банка, недоступна широкой общественности, и может использовать ее в собственных целях с целью обогащения, получения неконкурентных преимуществ, привилегий и т.п.

служащие компании, директора и акционеры, владеющие более 10 % акционерного капитала компании

лицо, имеющее в силу своего служебного или семейного положения доступ к конфиденциальной информации в организации ©

лица с существенной и публично нераскрытой служебной информацией компании, которая в случае ее раскрытия способна негативно повлиять на ее развитие ©

ИНСАЙДЕР

Что нам от них? ☺

		Секунды	Минуты	Часы	Дни	Недели	Месяцы	Годы
Действия за МИНУТЫ !!	Дискретизация бренда	10%	75%	12%	2%	0%	1,5%	1,5%
	Утечки информации	8%	38%	14%	25%	7,5%	7,5%	0%
Локализация и ликвидация за НЕДЕЛИ и МЕСЯЦЫ !!!	Детектирование утечки	0%	0%	2%	13%	29%	54%	2%
	Обнаружение, локализация и ликвидация	0%	1%	9%	32%	38%	16,5%	3,5%

Как происходят утечки?

80% менеджеров готовы продать коммерческую информацию конкурентам

75% менеджеров держат ценную информацию на собственных съемных устройствах

47% персонала провоцирует утечки ценной информации из-за халатности

37% персонала копируют и крадут собственные разработки компании

Как происходят утечки?

19% персонала уже забрали уникальные разработки, которые были созданы в команде

11% персонала скопировали клиентские базы и контакты партнеров

3% уволенных сотрудников забрали конфиденциальную информацию о своем предприятии

ИНСАЙДЕР

еще немного статистики ☺

50% персонала не уверены в выявлении утечки данных

49% внутренние инциденты с инсайдерами за год

37% случаев, когда инсайдеры скомпрометировали корпоративную сеть

80% крупнейших кредитно-финансовых организаций мира используют мониторинг действий инсайдеров

ИНСАЙДЕР

Классификация

умышленно совершающие противоправные действия

неумышленно совершающие противоправные действия

сочувствующие совершаемым противоправным действиям

имеющий необоснованные привилегии к ресурсам

желающие получить легальный доступ к ресурсам

желающие получить НЕ легальный доступ к ресурсам

имеющие легальный доступ к ресурсам

Методы обнаружения

Аналитический: комплексный мониторинг data-at-rest (данные в местах хранения), data-in-motion (каналы передачи данных) и data-in-use (данные во время обработки)

Дезинформация: формирование ложных сведений и анализ результатов – «ловля на живца»

Эвристический: прогнозирование (на основе шаблонов, элементов искусственного интеллекта)

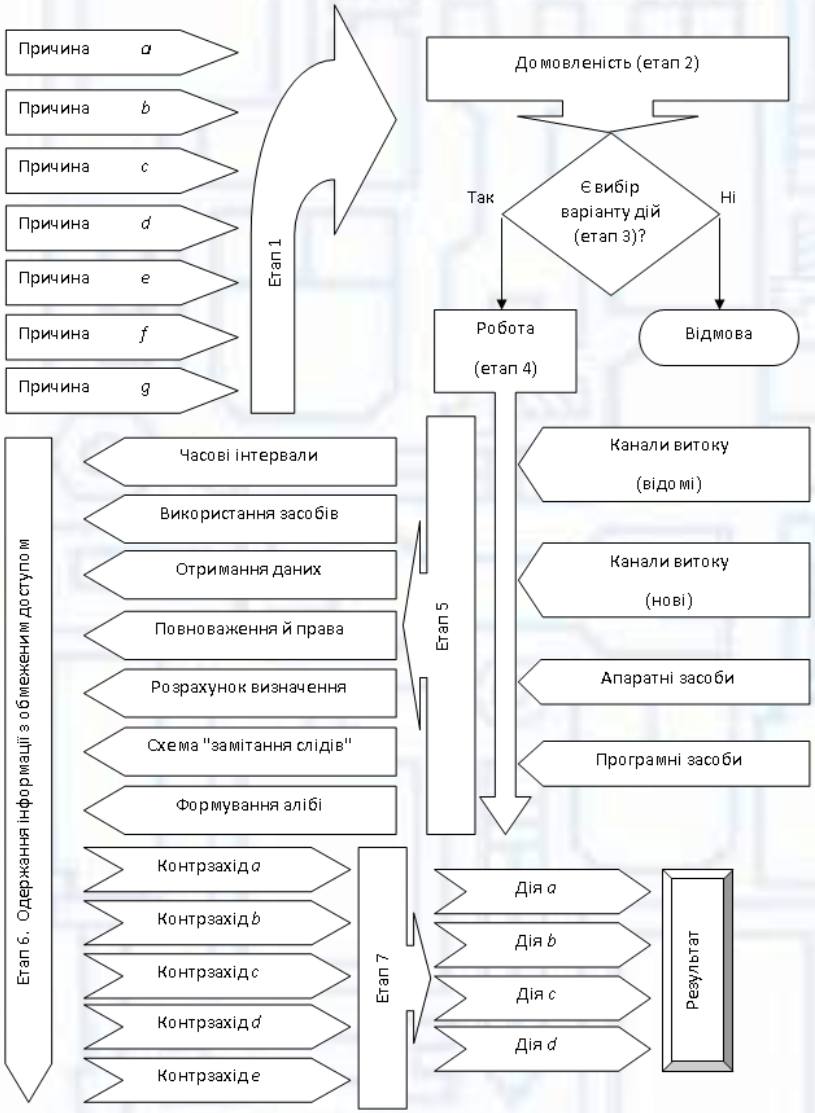
Математический: разрабатывается учеными – нами ☺

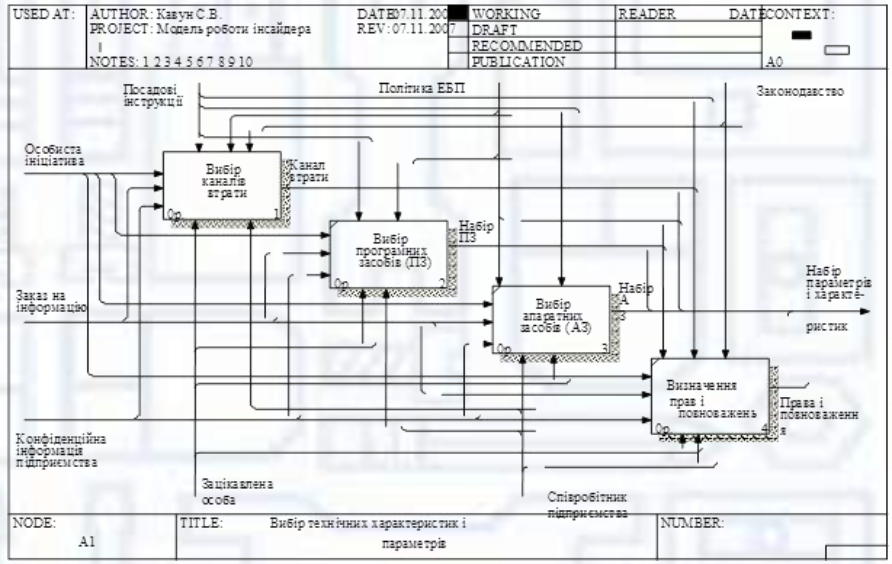
Психологический: использование полиграфа или тест-системы (на основании ст. 26 КЗОТ Украины)

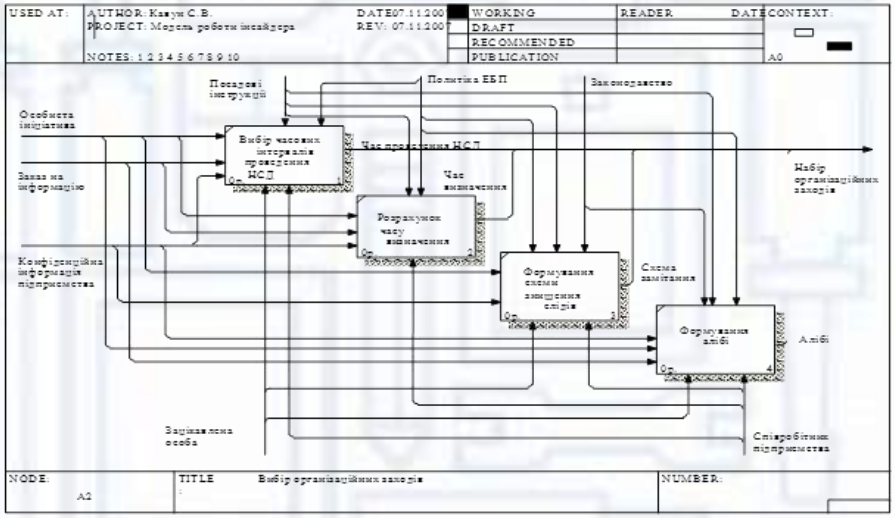
Методы борьбы

- Системы физического доступа (технические)
- Тренинги сотрудников (организационные)
- Математические, алгоритмические, моделирование, предсказание (научные)
- Стимулирование сотрудников (финансовые)
- Теория незаконного присвоения (США) !!
- НИКАКИЕ ☺ …и это 63% случаев

А что у нас? ☺







...научные исследования...

А что у нас? ☺

For any further possible accounting, the coefficient $^{i}K_{CW}$ must be normalized. Then one comes to the expression

$$^{N}K_{CW}^{i} = \frac{K_{CW}^{i}}{\sum_{j=1}^{n-1} K_{CW}^{j}} \qquad (4)$$

Therefore, using formula (4) yields the following values (base on the data from the example in Table 2) $^{N}K_{CW} = \{^{N}K^{i}_{CW}\} = \{0,2; 0,2; 0,1; 0,15; 0,25; 0,05; 0,05\}$.

For the further use of the factor of importance of different indicators of physical nature, expression (1) will be transformed into the following form

$$CW^{ij}_{IRA} = V^{ij} \times {}^{N}K^{i}_{S} \times {}^{i}K_{CW}, \qquad (5)$$

where $^{N}K^{i}_{S}$ is the normalized importance factor of the information with restricted access, calculated by the following expression

$$^{N}K_{S}^{i} = \frac{\sum_{j=1}^{n-1} K_{S}^{ij}}{\sum_{i=1}^{n}\sum_{j=1}^{n-1} K_{S}^{ij}}. \qquad (6)$$

Thus, based on formulas (4) and (6), what can be considered is the possibility of using the dynamic coefficients obtained from the experts.

Proof. Assume that inequalities $m > n$ and $m \neq 2n$ are valid, or else $K^{i}_{CW} \geq 3$ for the i^{th} node on the graph **G**. Let **a** and **b** be the nodes of the graph **G**, which are adjacent to the i^{th} node on this graph. Consider the set $V = \{v_i\}$, then $^{N}K^{i}_{S} = f(V^{ib} + V^{ia} + V^{bi} + V^{ai})$ is a function depending on time. Further, consider a node for which nodes **c** and **d** are adjacent, while $c, d \in V = \{v_i\}$. Then the right side of that the dependence $V^{a} = g(V^{ac} + V^{ad} + V^{ca} + V^{da})$, is also a function depending on time. Since $f \neq g$, then their dependence is not linear and not direct and has several variations of the distribution. ■

So, the problem of insider detecting on the enterprise can be represented as an integer programming problem:

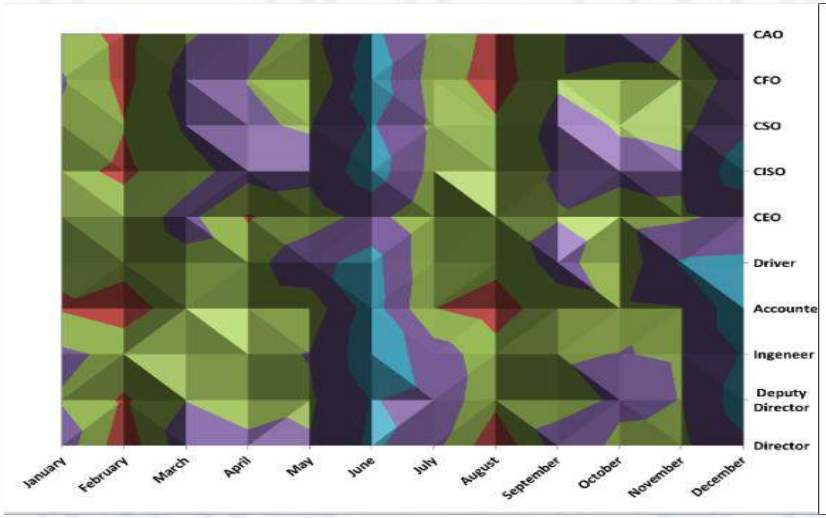
$$CW_{IRA} = min \sum_{i=1}^{n}\sum_{j=1}^{m}\left(V^{ij} \times {}^{N}K_{S}^{i} \times {}^{N}K_{CW}^{i} \times x_{ij}\right) \qquad (7)$$

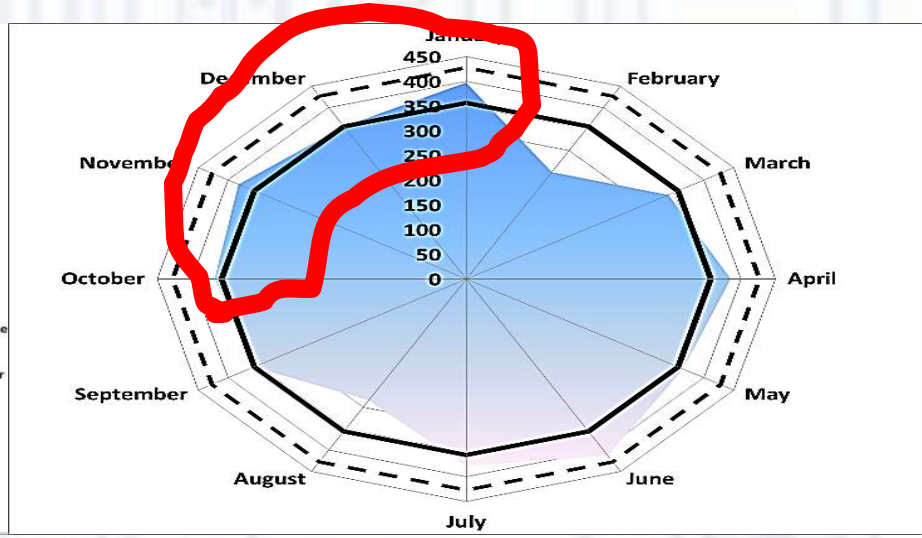
where x_{ij} is the corresponding element of matrix M_c.

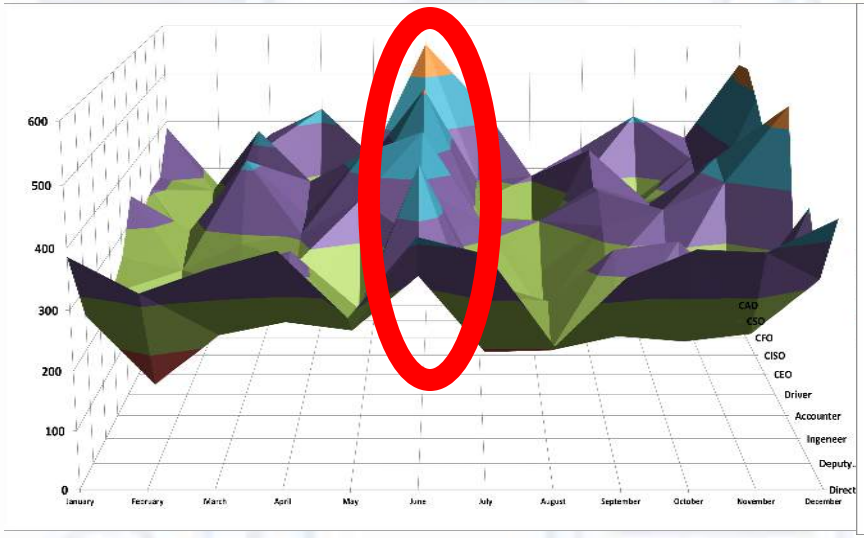
Based on the further mathematical interpretation of the use of a known mathematical method for solving this task and, on base of these methods, an optimal solution can be found.

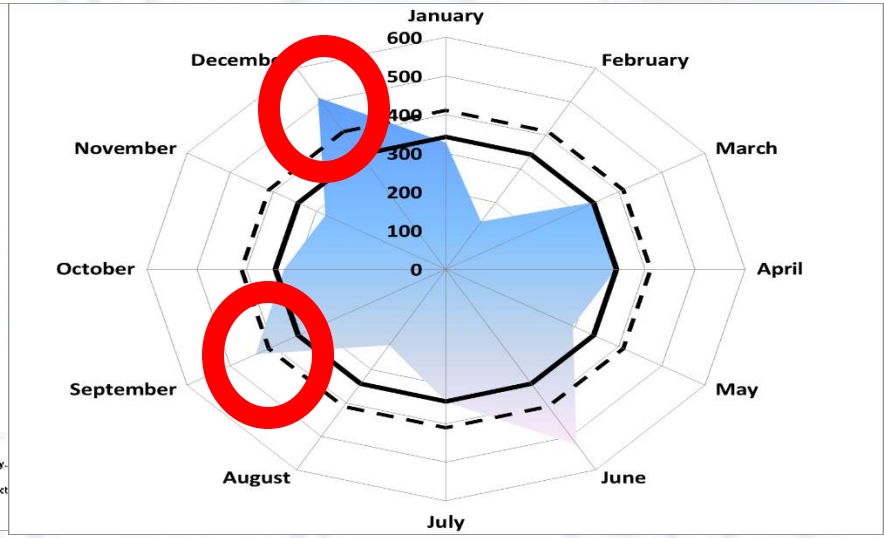
...научные исследования...

А что у нас? ☺









...научные исследования...

И как же оно работает

...да вот как-то так ☺ ...

Спасибо за внимание

Буду рад общению

д.э.н., к.т.н., Ph.D.
Кавун С.В.
Email: kavserg@gmail.com
Skype: serg_kavun