УДК 621.396.933 (043.2)
DOI: 10.31673/2409-7292.2019.041221

О.В. Барабаш, Є.М. Галахов

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ІНТЕНСИВНОСТІ КІБЕРАТАК ПІДПРИЄМСТВА З УРАХУВАННЯМ ЕЛАСТИЧНОСТІ ЧАСОВОГО ПЕРІОДУ ПРОВЕДЕННЯ АУДИТУ

Дослідницька увага орієнтована на аудит кібербезпеки підприємства для його інформаційної захищеності з огляду на те, що аудит – складний процес, який вимагає не тільки фахових знань, а і визначення стратегічних пріоритетів та орієнтирів інформаційної безпеки підприємства. Виокремлено чинники, які впливають на тривалість часу між аудитами: інвестування підприємства у кібербезпеку, рівень складності систем, конфіденційні дані. Розглянуто плановий автоматизований аудит на підприємстві у розрізі кібер-загроз типу Спаму і розрахувати середнє значення ефекту. Змодельовано функціональну залежність інтенсивності кібератак, що описується нелінійним диференціальним рівнянням Бернуллі, яке згідно з гіпотезою, що інтегральна функція інтенсивності кібератак підлягає логістичному закону, описує процес часового ряду інтенсивності кібератак.

Ключові слова: аудит, куб COSO, кібер безпека, кібер захист, функція інтенсивності кібератак, рівняння Бернуллі, еластичність.

Вступ

Аудит кібербезпеки комерційної мережі та комп'ютерної безпеки може забезпечувати не тільки програмне забезпечення, а і IT-аудитори (аналізі апаратних та програмних програм IT-системи підприємства: підтримка регулярних операцій та мінімізація ризику програмного забезпечення та IT обладнання), які як правило працюють на умовах аутсорсингу разом з внутрішньою командою підприємства і яким притаманні наступні навички: регулярні оцінки ризику:

- досвід внутрішнього аудиту;
- високі міжособистісні та комунікативні навички;
- досвід тестування інформаційної безпеки на підприємствах;
- поглиблені знання IT-безпеки та інфраструктури;
- знання різних платформ операційної системи;
- уміння формувати звіти;
- аналітична здатність з можливістю ефективного використання відповідного програмного забезпечення;
- наявність сертифікації та кваліфікації IT-аудиту (ISO27001).

На сьогодні є необхідність у проведенні регулярних аудитів кібербезпеки для інформаційної захищеності підприємства. Це вимагає дослідження частоти проведення аудитів та виявлення часового інтервалу еластичності їх проведення.

Постановка завдання. В процесі **м**оделювання підготовки до аудиту інформаційної безпеки підприємства необхідно зробити наступні завдання:

1. Обґрунтувати структурну схему проведення аудитів кібербезпеки підприємства. Розглянути плановий автоматизований аудит на підприємстві, яке залучає фріланс-ресурс, у розрізі кібер-загрозу, що представляється Спамом.

2. Представити математичну модель поведінки функції інтенсивності кібератак на підприємство.

5. Дослідити еластичний інтервал проведення аудиту інформаційної безпеки на підприємстві.

6. Надати рекомендації у прогнозованому періоді стосовно часових інтервалів проведення аудиту інформаційної безпеки підприємства.

Основна частина.

На теперішній час постає необхідність у регулярних глибоких аудитів кібербезпеки для інформаційної захищеності підприємства. Взагалі, як правило, для корегування структур

управління інформаційною безпекою на підприємстві та доповнення існуючих ресурсів необхідно виконання наступних дій аудиту [2,3]:

1. Оцінка реєстру активів.
2. Обстеження, аудит та рекомендації щодо безпеки сайту.
3. Впровадження політики, планів та процедур безпеки.
4. Дизайн інформаційної безпеки сайту.
5. Управління командами з інформаційної безпеки.
6. Навчання та розвиток груп інформаційної безпеки.
7. Інформаційна безпека та її забезпечення.
8. Проникнення на сайт та оцінка вразливості (команди тигра / червоні клітини)
9. Введення брокера служби інформаційної безпеки.
10. Введення менеджер подій інформаційної безпеки.

Потрібен, насамперед, базовий рівень кібербезпеки, що забезпечує аудит. Існує плановий аудит (автоматичний метод), який включає контроль та оцінку кібер-ризику підприємства. На рахунок звичайного аудиту (рішення IT-менеджера), то він може проводитися по різному [1,4].

Виокремимо чинники, які впливають на тривалість часу між аудитами: інвестування підприємства у кібербезпеку, рівень складності систем, конфіденційні дані. Розробляючи план внутрішнього аудиту з питань кібербезпеки, використовується куб COSO як основа для підходу до внутрішнього аудиту для визначення загроз інформаційній системі підприємства та рівнів кіберпрофільного ризику [5, 6]. Структура куба COSO для підходу до внутрішнього аудиту підприємства представлена на рис.1.

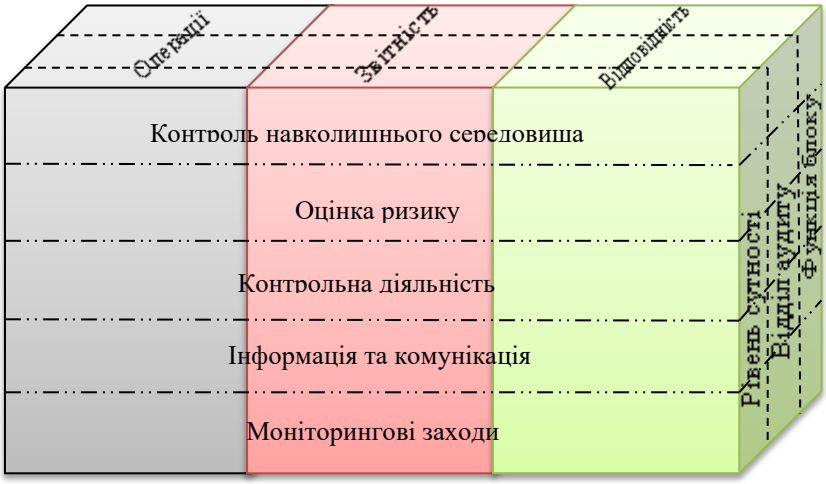


Рис. 1. Структура куба COSO для підходу до внутрішнього аудиту підприємства
Джерело: складено авторами на основі [5,6]

Спеціальний аудит (аналіз ситуації та систем) проводиться після звичайного аудиту для швидкості запровадження запропонованих рішень. Структурна схема проведення аудиту приведена на рис.2.

Розглянемо плановий автоматизований аудит на підприємстві, яке залучає фріланс-ресурс, у розрізі кібер-загрозу, що представляється Спамом [9, 10]. Наприклад, сьогодні найбільш широко визнаною формою спаму є спам електронної пошти. Спам відноситься до надсилання нерелевантних, невідповідних та непотрібних повідомлень. Спам виявився дуже прибутковим ринком, оскільки спам надсилається анонімно, без витрат, пов'язаних із управлінням списками розсилки. Через такий низький бар'єр для входу, спамерів чимало, а обсяг небажаної пошти надзвичайно виріс [11].

Рис.2.Структурна схема проведення аудитів кібербезпеки підприємства
Джерело: складено авторами на основі [7, 8]

Завдяки автоматизованому аудиту на підприємстві, яке залучає фріланс-ресурс, отримано наступний ефект кіберзахисту у розрізі Спаму за трьома часовими періодами в інтервалі січень-листопад 2019 року (табл. 1).

Таблиця 1

Середнє значення ефекту від автоматизованого аудиту у розрізі Спаму за період січень-вересень 2019 року

Ефект від автоматизованого аудиту	***Середнє значення (%)***
Автоматизований аналіз формальних ознак	41,173
Аналіз атрибутів відправника	37,821
Аналіз формальних ознак	6,917
Лінгвістичний аналіз	4,714
Графічний контент-аналіз	3,649
Виявлення хмари	3,287
Аналіз підписів	1,364
Поліпшена послуга оновлення спаму	1,075

Джерело: складено автором на основі даних підприємства

Розглянемо функціональну залежність інтенсивності кібератак (кількість кібератак за 3 дні) $I_K(t)$. Розглянемо нелінійне диференціальне рівняння Бернуллі, яке згідно з гіпотезою, що інтегральна функція інтенсивності кібератак підлягає логістичному закону, описує процес часового ряду інтенсивності кібератак:

$$\frac{I_K(t)}{I_K(t)} = \zeta \cdot \frac{I_K(t)_{Max} - I_K(t)}{I_K(t)_{Max}}, \quad I_K(0) = I_{K_0}, \quad \zeta = \frac{\alpha}{\beta}. \qquad (1)$$

де $I_K(t)_{Max}$ – максимально можливий рівень функції інтенсивності кібератак;

$I_K(0) = I_{K_0}$ – початковий рівень функції інтенсивності кібератак після проведення планового аудиту;

$\frac{I_K(t)}{I_K(t)}$ – відносна зміна швидкості інтенсивності кібератак;

$\frac{I_K(t)_{Max} - I_K(t)}{I_K(t)_{Max}} = 1 - \frac{I_K(t)}{I_K(t)_{Max}}$, $0 < \frac{I_K(t)}{I_K(t)_{Max}} < 1$ – відносне відхилення значення функції інтенсивності кібератак від її максимально можливого рівня, як частка можливих уражень системи підприємства кібератаками за умови вчасного не проведення звичайних і спеціальних аудитів;

$\zeta = \frac{\alpha}{\beta}$ - рівень корегування загроз кібератак завдяки звичайного аудиту;

α – рівень загроз інформаційній безпеці підприємства, яке могло бути ураженим у разі наближення до $I_K(t)_{Max}$ за умови невчасно проведених спеціальних аудитів;

β – коефіцієнт впливу чинників системи інформаційної безпеки на функцію інтенсивності кібератак.

Рівняння (1) запишемо у вигляді:

$$\begin{aligned} &\frac{\dot{I}_K(t)}{I_K(t)} = \zeta \cdot \left(1 - \frac{I_K(t)}{I_K(t)_{Max}}\right), \quad 0 < \frac{I_K(t)}{I_K(t)_{Max}} < 1, \\ &I_K(0) = I_{K_0}, \quad \zeta = \frac{\alpha}{\beta}. \end{aligned} \tag{2}$$

або

$$\dot{I}_K(t) - \zeta \cdot I_K(t) = -\zeta \frac{1}{I_K(t)_{Max}} \cdot {I_K}^2(t), \; I_K(0) = I_{K_0}, \tag{3}$$

Отже, рівняння (3) є нелінійним диференціальним рівнянням 1-го порядку Бернуллі. Поділивши ліву і праву частини рівняння (6) на ${I_K}^2(t) \neq 0$, одержимо:

$$\begin{aligned} &I_K(t)^{-2} \cdot \dot{I}_K(t) - \zeta \cdot I_K(t)^{-1} = -\zeta \cdot \frac{1}{I_K(t)_{Max}}, \\ &-I_K(t)^{-2} \cdot \dot{I}_K(t) + \zeta \cdot I_K(t)^{-1} = \zeta \cdot \frac{1}{I_K(t)_{Max}}. \end{aligned} \tag{4}$$

Після заміни $I_K(t)^{-1} = W, \quad -I_K(t)^{-2} \cdot {I_K}'(t) = W'$, маємо:

$$W' + \zeta \cdot W = \frac{\zeta}{I_K(t)_{Max}}. \tag{5}$$

Формула загального розв'язку лінійного диференціального рівняння 1-го порядку $W' + p(t)W = q(t)$, має вигляд:

$$W = \int \left(p(t) \cdot e^{-\int p(t)dt} \right) dt \cdot \left(\int \left(q(t) \cdot e^{\int p(t)dt} \right) dt + C \right). \tag{6}$$

Знаходимо загальний розв'язок лінійного диференціального рівняння (5), для якого $p(t)=\zeta;\quad q(t)=\dfrac{\zeta}{I_K(t)_{Max}}$. Маємо:

$$W=\int\zeta\cdot e^{-\zeta\cdot t}dt\cdot\left(\int\frac{\zeta}{I_K(t)_{Max}}e^{\zeta\cdot t}dt+C\right)=$$

$$=-e^{-\zeta\cdot t}\cdot\left(-\frac{1}{I_K(t)_{Max}}\cdot e^{\zeta\cdot t}+C\right)=\frac{1}{I_K(t)_{Max}}-C\cdot e^{-\zeta\cdot t},$$

$$W=\frac{1}{I_K(t)}=\frac{1}{I_K(t)_{Max}}-C\cdot e^{-\zeta\cdot t},\quad I_K(0)=I_{K_0}. \tag{7}$$

Використовуючи початкові умови, знаходимо С:

$$C=-\frac{1}{I_{K_0}}+\frac{1}{I_K(t)_{Max}}=-\frac{I_K(t)_{Max}-I_{K_0}}{I_{K_0}\cdot I_K(t)_{Max}}. \tag{8}$$

Підставляючи (8) у (7), отримаємо:

$$\frac{1}{I_K(t)}=\frac{1}{I_K(t)_{Max}}+\frac{I_K(t)_{Max}-I_{K_0}}{I_{K_0}\cdot I_K(t)_{Max}}\cdot e^{-\zeta\cdot t}. \tag{9}$$

Отже, розв'язок диференціального рівняння (5) буде мати вигляд:

$$I_K(t)=\frac{I_K(t)_{Max}}{1+\dfrac{I_K(t)_{Max}-I_{K_0}}{I_{K_0}}\cdot e^{-\zeta\cdot t}}. \tag{10}$$

Знайдемо першу та другу похідні функції інтенсивності кібератак:

$$\dot{I}_K(t)=-I_K(t)_{Max}\cdot\left(1+\left(\frac{I_K(t)_{Max}-I_{K_0}}{I_{K_0}}\right)\cdot e^{-\zeta\cdot t}\right)^{-2}\cdot\left(-\zeta\cdot\left(\frac{I_K(t)_{Max}-I_{K_0}}{I_{K_0}}\right)\cdot e^{-\zeta\cdot t}\right); \tag{11}$$

$$\ddot{I}_K(t)=2I_K(t)_{Max}\cdot\left(1+\frac{I_K(t)_{Max}-I_{K_0}}{I_{K_0}}\cdot e^{-\zeta\cdot t}\right)^{-3}-I_K(t)_{Max}\cdot\left(1+\frac{I_K(t)_{Max}-I_{K_0}}{I_{K_0}}\cdot e^{-\zeta\cdot t}\right)^{-2}\cdot$$

$$\cdot\left(\zeta^2\cdot\left(\frac{I_K(t)_{Max}-I_{K_0}}{I_{K_0}}\right)\cdot e^{-\zeta\cdot t}\right)=$$

$$= I_K(t)_{Max} \cdot \left(1 + \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot e^{-\zeta \cdot t}\right)^{-2} \zeta^2 \cdot \left(\frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}}\right) \cdot e^{-\zeta \cdot t} \cdot$$

$$\cdot \left(2\left(1 + \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot e^{-\zeta \cdot t}\right)^{-1} \cdot \left(\frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}}\right) \cdot e^{-\zeta \cdot t} - 1\right) =$$

$$= \zeta^2 \cdot \left(\frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}}\right) \cdot e^{-\zeta \cdot t} \cdot I_K(t)_{Max} \cdot \frac{1}{\left(1 + \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot e^{-\zeta \cdot t}\right)^2} \cdot$$

$$\cdot \left(\frac{2\frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot e^{-\zeta \cdot t}}{1 + \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot e^{-\zeta \cdot t}} - 1\right) =$$

$$= \zeta^2 \cdot I_K(t)_{Max} \cdot \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot e^{-\zeta \cdot t} \cdot \frac{\left(\frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot e^{-\zeta \cdot t} - 1\right)}{\left(1 + \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot e^{-\zeta \cdot t}\right)^3} \cdot$$

Знаходимо координати точки перегину:

$$I_K(t) = 0 \Rightarrow \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot e^{-\zeta \cdot t} - 1 = 0,$$

$$e^{-\zeta \cdot t} = \frac{I_{K_0}}{I_K(t)_{Max} - I_{K_0}}, \qquad -\zeta \cdot t = -\ln \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}}, \tag{12}$$

$$t = \frac{1}{\zeta} \cdot \ln \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}}.$$

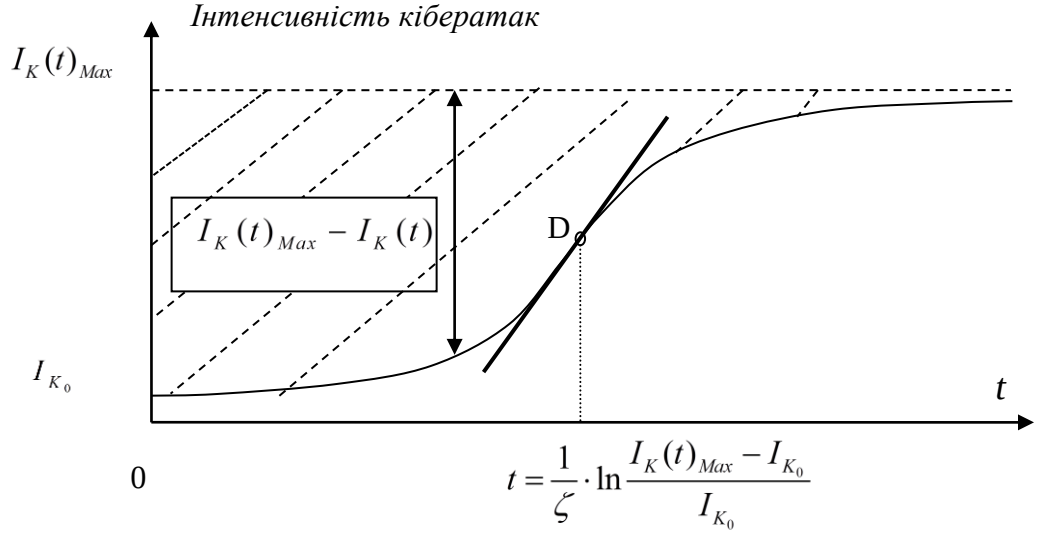
Отже, $A\left(\frac{1}{\zeta} \cdot \ln \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}}, \frac{I_K(t)_{Max}}{2}\right)$ – точка перегину.

Знайдемо границю:

$$\lim_{t\to\infty} I_K(t) = \lim_{t\to\infty} \frac{I_K(t)_{Max}}{1+\frac{I_K(t)_{Max}-I_{K_0}}{I_{K_0}}\cdot e^{-\zeta\cdot t}} = I_K(t)_{Max}. \quad (13)$$

Таким чином, $I_K(t) = I_K(t)_{Max}$ – горизонтальна асимптота *s*-кривої.

На рис. 3 зображена крива інтенсивності кібератак від часу зі знайденою точкою перегину *D*, у якій проведена дотична для візуалізації перегину.



– область невикористаної можливості інтенсивності кібератак

Рис.3. Логістична крива функції інтенсивності кібератак підприємства в залежності від часу

Джерело: авторські розробки

Обчислимо еластичність El_t функції інтенсивності кібератак підприємства в залежності від часу за наступною формулою:

$$El_t = \frac{t\cdot I_K'(t)}{I_K(t)}. \quad (14)$$

Відомо, якщо $|El_t|>1$, то функція інтенсивності кібератак підприємства – еластична. За формулою (14) знаходимо:

$$El_t = \frac{t \cdot I_K{}'(t)}{I_K(t)} = \zeta \cdot \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot I_K(t)_{Max} \cdot$$

$$\cdot \frac{t}{e^{\zeta \cdot t}\left(1 + \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot e^{-\zeta \cdot t}\right)^2} \cdot \frac{\left(1 + \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot e^{-\zeta \cdot t}\right)}{I_K(t)_{Max}} = . \qquad (15)$$

$$= \zeta \cdot \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot \frac{t}{e^{\zeta \cdot t}\left(1 + \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot e^{-\zeta \cdot t}\right)^2}$$

Отже,

$$El_t = \zeta \cdot \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot \frac{t}{e^{\zeta \cdot t} + \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}}} . \qquad (16)$$

За умови еластичності $|El_t| > 1$, знайдемо інтервал еластичності для функції інтенсивності кібератак:

$$\zeta \cdot \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot \frac{t}{e^{\zeta \cdot t} + \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}}} > 1 \quad \Rightarrow$$

$$\frac{\zeta \cdot \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot t - e^{\zeta \cdot t} - \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}}}{e^{\zeta \cdot t} + \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}}} > 0 \quad \Rightarrow \qquad (17)$$

$$\zeta \cdot \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot t - e^{\zeta \cdot t} - \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} > 0 \quad \Rightarrow$$

$$\left(e^{\zeta \cdot t} + \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} > 0\right).$$

Або

$$\zeta \cdot \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot t - \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} > e^{\zeta \cdot t}. \qquad (18)$$

Отже, розв'язком нерівності (19) є інтервал еластичності.

При визначенні параметрів $\frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}}$ і $\frac{1}{\zeta}$ нерівність (19) розв'язується чисельно із візуалізацією на графіку (рис.4). Таким чином, можна визначити інтервал еластичності $\left[t_1^{el}, t_2^{el} \right]$.

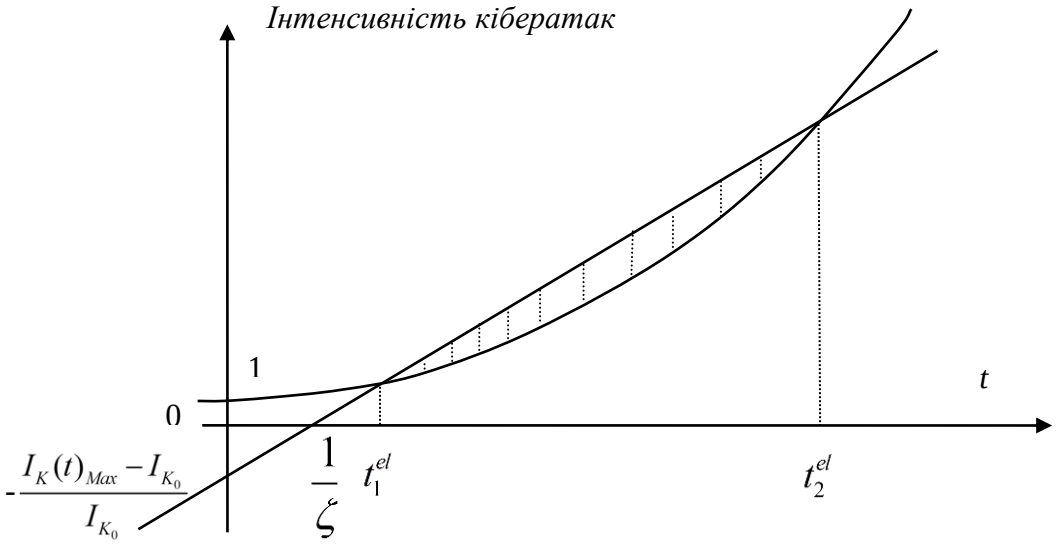


Рис. 4. Знаходження інтервалу еластичності $\left[t_1^{el}, t_2^{el} \right]$

Отже, час проведення спеціального аудиту необхідно вибирати з інтервалу еластичності, який визначається графічно (рис.3) і аналітично формулою (18).

Висновки

Показано, що аудит – складний процес, який вимагає не тільки фахових знань, а і визначення стратегічних пріоритетів та орієнтирів інформаційної безпеки підприємства. Розглянуто плановий автоматизований аудит на підприємстві у розрізі кібер-загроз типу Спаму. Знайдено розв'язок нелінійного диференціального рівнянням Бернуллі, яке описує процес часового ряду інтенсивності кібератак. Доведено, що інтегральна функція інтенсивності кібератак підлягає логістичному закону, що знайдено в аналітичному вигляді. Одержано інтервал еластичності функції інтенсивності кібератак за часом, що дає можливість визначити часовий інтервал проведення спеціального аудиту кібербезпеки підприємства.

Перелік посилань

1. Барабаш О.В. Построение функционально устойчивых распределенных информационных систем: монография. К.: НАОУ, 2004. 224 с.

2. Almukaynizi, Mohammed, et al. "Predicting cyber threats through the dynamics of user connectivity in darkweb and deepweb forums." ACM Computational Social Science. (2017).

3. Almukaynizi, Mohammed, et al. "Proactive identification of exploits in the wild through vulnerability mentions online." IEEE CyCON, 2017.

4. Bilge, Leyla, and Tudor Dumitras. "Before we knew it: an empirical study of zero-day attacks in the real world." Proceedings of the 2012 ACM conference on Computer and communications security.

5. Khandpur, Rupinder Paul, et al. "Crowdsourcing cybersecurity: Cyber attack detection using social media." ACM CIKM 2017.

6. Liu, Yang, et al. "Cloudy with a Chance of Breach: Forecasting Cyber Security Incidents." USENIX Security Symposium. 2015.

7. Liu, Yang, et al. "Predicting cyber security incidents using featurebased characterization of network-level malicious activities." 2015 ACM International Workshop Security and Privacy Analytics.

8. Meier, Lukas, Sara Van De Geer, and Peter Bühlmann. "The group lasso for logistic regression." Journal of the Royal Statistical Society: Series B (Statistical Methodology) 70.1 (2008): 53-71.

9. A.P. Moore, R.J. Ellison, R.C. Linger. Attack Modeling for Information Security and Survivability. Technical Note CMU/SEI-2001-TN-001. Survivable Systems, 2001.

10. Nunes, Eric, et al. "Darknet and deepnet mining for proactive cybersecurity threat intelligence." IEEE ISI (2016).

11. Sabottke, Carl, Octavian Suciu, and Tudor Dumitras. "Vulnerability Disclosure in the Age of Social Media: Exploiting Twitter for Predicting Real-World Exploits." USENIX Security Symposium. 2015.

Надійшла: 24.09.2019 Рецензент: д.т.н., професор Кожухівський А.Д.