Інформаційні технології

УДК 621.396.933 (043.2) **doi: 10.26906/SUNZ.2019.6.038**

О. В. Барабаш, Є. М. Галахов

Державний університет телекомунікацій, Київ, Україна

ВИЗНАЧЕННЯ ОПТИМАЛЬНОГО ЧАСУ ПРОВЕДЕННЯ СПЕЦІАЛЬНОГО АУДИТУ ЗА УМОВИ ЕЛАСТИЧНОСТІ ТА ЧУТЛИВОСТІ ФУНКЦІЇ ІНТЕНСИВНОСТІ КІБЕРАТАК

Анотація. В статті представлено дослідження, що направлені на встановлення оптимального часу проведення спеціального аудиту для покращення рівня кіберзахисту і надання пріоритетних та перевірених заходів для зменшення ризику виникнення кібер-інциденту. Проаналізовано часові ряди інтенсивності кібератак підприємства з проведенням аналітичного вирівнювання часового ряду функції інтенсивності кібератак за допомогою логістичної кривої. За знайденим інтервалом еластичності аналітичної функції інтенсивності кібератак на підприємство, що задовольняє нелінійному диференціальному рівнянню Бернуллі, проведено аналіз часових рядів кібератак на систему підприємства за однакові часові періоди, що попадають у часовий проміжок від кінця планового аудиту до початку наступного. За допомогою *p*–перетворення до функції інтенсивності кібератак на підприємство та, враховуючи без розмірність змінних, обчислено чутливість безрозмірної функції інтенсивності кібератак від параметра *p* за встановлений часовий період за умови проведення попередньої фільтрації часового ряду за трьома точками. Визначено оптимальний час проведення спеціального аудиту після проведення планового аудиту.

Ключові слова: часовий ряд, інтенсивність кібератак, еластичність, рівняння Бернуллі, *p*–перетворення, фільтрація, спеціальний аудит.

Вступ

На сьогоднішній день інформаційно-телекомунікаційні системи розглядаються як мережі із змінюваною структурою, мережі, які можуть самоналаштовуватись, реструктуруватись та самостійно відновлювати функціонування при впливі внутрішніх і зовнішніх дестабілізуючих факторів. Зміна структури здійснюється при підключенні (або відключенні) кожного абонентського пристрою до мережі. Кожного разу, коли новий пристрій підключається до мережі і виходить в Інтернет або з'єднується з іншими пристроями, зростає інтенсивність кібератак. Швидке зростання за останнє десятиліття Інтернету речей, хмарних технологій, великих даних та оцифрування промисловості супроводжується зростанням інтенсивності кібератак. Різноманітність кібератак ускладнює захист підприємства у контексті його інформаційної безпеки. Небезпечне програмне забезпечення, що призначено для нанесення шкоди пристроям або мережам включає віруси, трояни, черв'яки, рекламне та шпигунське програмне забезпечення. Найбільш розповсюдженими стали розподілені атаки відмови в обслуговуванні (DDoS), які роблять ресурси недоступними, переповнюючи їх більшою кількістю запитів, ніж вони можуть впоратися. Також у контексті соціальної інженерії користувачі (фрілансери) мимоволі розголошують конфіденційну інформацію. Найбільш небезпечні типи загроз – це вдосконалені постійні загрози (APT0, що займаються тривалим моніторингом та руйнівними цілями. За умови зростання фінансового впливу кібератак на функціонування підприємств, загострюється невідповідність між витратами на кібернапад та витратами на попередження, аудит та відшкодування. Наприклад, DDoS-атака може коштувати незначну вартість. Але втрати, що понесені цільовим бізнесом, у тому числі пошкодження репутації, значно вищі. Управління кібербезпекою можна покращити, якщо підвищити здатність підприємства реагувати на кібератаки та інциденти. В той же час запобігти всім атакам неможливо. Тому швидке виявлення й реагування та захист критичної інфраструктури і функцій разом з потужним обміном інформацією є ключовими проблемами, які потрібно вирішувати. Одним із аспектів вирішення цієї проблеми є вчасне проведення аудитів, які не обмежуються лише плановою перевіркою, а і дають розуміння й прийняття відповідних заходів щодо запобігання кібератакам. Після завершення аудитів надається вичерпний звіт про результати досліджень, який визначає сфери, які потрібно виправити для підвищення рівня безпеки. Звіт аудиту підприємства використовується для виявлення областей у корпоративному середовищі, які можуть бути поліпшені шляхом здійснення контролю кібербезпеки. Результати цього звіту містять корисні приклади, рекомендації та додаток посилань. Загалом у звіті є базовий рівень, за допомогою якого можна покращити рівень безпеки, використовуючи відчутні кроки та унеможливлюючи подальший ризик.

Постановка завдання. Зі збільшенням швидкості та точності обробки даних, багаторазовим підключенням, швидкою передачею даних на великі відстані, розробка та узагальнення автоматичної обробки принесла багато нових вразливостей, що обумовлює нові категорії ризиків інформаційної безпеки підприємства. Ризики кібератак при аудиті пов'язані з управлінням ризиками небезпеки інформаційних систем. Аудит та контроль інформаційних систем підприємства має на меті повідомляти, які дії потрібно вжити, щоб покращити рівень кіберзахис-

ту, а також надає пріоритетні та перевірені заходи, щоб зменшити ризик виникнення кібер-інциденту. Тому необхідно проаналізували основні типи кібератак та провести дослідження часових рядів їх інтенсивності для встановлення оптимального часу проведення спеціального аудиту між плановими аудитом і контролем. Плановий аудит безпеки підприємства – це аудит IT-операцій з точки зору кібербезпеки. Однак, інформаційна система підприємства може відповідати всім вимогам нормативних документів і все-таки не бути захищеною.

Багато підприємств зосереджуються на технічних аспектах кібербезпеки та ігнорують політику, процеси та процедури. Зауважимо, що спеціальні аудити також є важливими елементами кібернавчання, які пропонуючи можливості підвищити готовність шляхом тестування, дають відповіді на реальні сценарії та побудову відносин суб'єктів. Отже, підвищення обізнаності має важливе значення для створення ефективної кіберстійкості. Таким чином, комплексний аудит кібербезпеки, що включає не тільки планові, а і спеціальні аудити, допоможе підприємству заздалегідь шукати потенційні недоліки безпеки у системі та уникнути великих бізнес-збитків, що забезпечить максимальне зниження ризику та дозволить своєчасно реагувати на загрози безпеці.

Аналіз останніх публікацій і досліджень

Процес аудиту та перевірки кібербезпеки сприяє підвищенню рівня кібербезпеки [1]. Внутрішні аудитори та фахівці управління ризиками відіграють ключову роль в управлінні підприємством. Менеджмент забезпечує існування та ефективне функціонування системи контролю за рівнем кібербезпеки [2]. Оцінки ризику та їх складові (IT-інфраструктура, включаючи апаратне програмне забезпечення, центри обробки даних, мережі, сервери) постійно змінюються, що вимагає впровадження ефективних заходів забезпечення рівня кібербезпеки. Аудит допомагає підприємствам вирішувати проблеми управління кіберзагрозами, забезпечуючи об'єктивну оцінку контролю та надання рекомендацій щодо їх вдосконалення, а також надання допомоги вищому керівництву з точки зору розуміння та реагування на кіберризики [3]. Аудит інформаційної безпеки – це повна оцінка безпеки компанії, яка є невід'ємною частиною послуг інформаційної безпеки. Аудит інформаційної безпеки включає: аудит бізнес-структури, процесів, аудит технічної безпеки (оцінка вразливості та тестування на проникнення) [2, 3].

Процесу прогнозування часових рядів присвячені наукові праці [4, 5, 6, 7]. При цьому, застовуються методи, засновані на авторегресивних моделях, що використовують зовнішні часові ряди в задачі прогнозування [6, 8]. Аналіз авторегресивних моделей перед застосуванням полягає у перегляді спостережень за часовими рядами, особливо за їх властивостями стаціонарності та періодичності. Ілюстрація прогнозування кібератак представлена на рис. 1 [8]. Тут припускається, що основні дані емпіричних кібератак, подаються для налагоджування моделей прогнозування разом із зовнішніми сигналами. Прогнози робляться для подій, що відбудуться протягом майбутнього періоду часу.

Метод оцінювання прогнозування часових рядів, що засновано на нейронних мережах, представлено у роботі [9].

Метод, що ідентифікує сигнали з Інтернет-джерел даних, які послідовно покращують прогнози кібератак, розглянуто у [10]. Огляд класичних підходів, заснованих на авторегресивних моделях та новітні підходи, які використовують нейронні мережі для прогнозування, беруть за основу дослідники в роботі [11] з метою прогнозування кібератак за допомогою машинного навчання. Таким чином дослідження часових рядів інтенсивності кібератак з метою аналізу та визначення ефективного часового інтервалу проведення спеціальних аудитів потребують нових методичних підходів.

Основна частина

Аналітична функція інтенсивність кібератак $I_K(t)$ на підприємство задовольняє нелінійному диференціальному рівнянню Бернуллі:

$$\begin{gathered}\dot{I}_K(t)-\zeta\cdot I_K(t)=-\zeta\cdot\left(I_K(t)_{Max}\right)^{-1}\cdot {I_K}^2(t),\\ I_K(0)=I_{K_0},\end{gathered} \quad (1)$$

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; ζ – рівень корегування загроз кібератак завдяки звичайного аудиту.

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

Інтервал еластичності функції інтенсивності кібератак знаходимо за формулою $El_t=\dfrac{t\cdot\dot{I}_K(t)}{I_K(t)}$ у вигляді нерівності, що розв'язується чисельно:

$$\zeta\cdot\frac{I_K(t)_{Max}-I_{K_0}}{I_{K_0}}\cdot t-\frac{I_K(t)_{Max}-I_{K_0}}{I_{K_0}}>e^{\zeta\cdot t}. \quad (3)$$

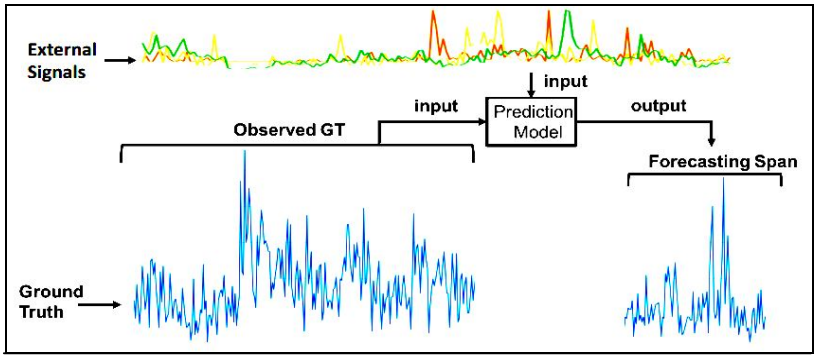


Рис. 1. Ілюстрація прогнозування кібератак

Для зручності викладок введемо заміни:

$$\begin{aligned} &I_K(t) = y(t), \quad I_K(t)_{Max} = k, \\ &-\zeta = a, \quad \left(I_K(t)_{Max} - I_{K_0}\right)\Big/ I_{K_0} = b. \end{aligned}, \tag{4}$$

Тоді функцію (2) перепишемо у вигляді:

$$y(t) = \frac{k}{1 + b \cdot e^{at}} \quad \Rightarrow \quad \frac{k}{y(t)} - 1 = b \cdot e^{at}, \tag{5}$$

Прологарифмуємо (5), маємо:

$$\ln\left(k/y(t) - 1\right) = \ln b + at.$$

Введемо нове позначення:

$$B(t) = \ln\left(k/y(t) - 1\right).$$

Тоді запишемо систему нормальних рівнянь:

$$\begin{cases} \sum B(t) = n \ln b + a \sum t; \\ \sum B(t) \cdot t = \ln b \sum t + a \sum t^2. \end{cases} \tag{6}$$

Нехай статистична регресійна апроксимація, як розв'язок системи (5) має вигляд:

$$\hat{y}(t) = \frac{k}{1 + b \cdot e^{at}}. \tag{7}$$

Знаходимо різницю обернених сусідніх значень

$$\frac{1}{\hat{y}(t+1)} = \frac{(e^a - 1)}{k} + e^a \cdot \frac{1}{\hat{y}(t)},$$

Оцінимо параметри $(e^a - 1)/k$ та e^a. Знаходимо мінімум функції:

$$\min\left\{\sum\left(1/y(t) - 1/\hat{y}(t)\right)^2\right\}, \tag{8}$$

Запишемо систему нормальних рівнянь у такому вигляді:

$$\begin{cases} \sum_{t=1}^{n-1} \frac{1}{y(t+1)} = (n-1) \cdot \frac{(1-e^a)}{k} + e^a \cdot \sum_{t=1}^{n-1} \frac{1}{y(t)}; \\ \sum_{t=1}^{n-1} \frac{1}{y(t+1)} \cdot \frac{1}{y(t)} = \\ \quad = \frac{(1-e^a)}{k} \cdot \sum_{t=1}^{n-1} \frac{1}{y(t+1)} + e^a \cdot \sum_{t=1}^{n-1} \frac{1}{y(t)^2}, \end{cases} \tag{9}$$

Розв'язок цієї системи має вигляд:

$$e^a = \frac{(n-2)}{(n-1) \cdot \sum_{t=1}^{n-1} \frac{1}{y(t)^2} - \left(\sum_{t=1}^{n-1} \frac{1}{y(t)}\right)^2},$$

$$\frac{(1-e^a)}{k} = \frac{\sum_{t=1}^{n-1} \frac{1}{y(t+1)} \cdot \sum_{t=1}^{n-1} \frac{1}{y(t)} - \sum_{t=1}^{n-1} \frac{1}{y(t)} \cdot \sum_{t=1}^{n-1} \frac{1}{y(t+1)} \cdot \frac{1}{y(t)}}{(n-1) \cdot \sum_{t=1}^{n-1} \frac{1}{y(t)^2} - \left(\sum_{t=1}^{n-1} \frac{1}{y(t)}\right)^2} = A,$$

звідки

$$k = \left(1 - e^a\right)\Big/ A. \tag{10}$$

Таким чином, після оцінки параметрів k і a рівняння (7), перейдемо до оцінки параметра b. Для цього перетворимо рівняння (7):

$$k/\hat{y}(t) - 1 = b \cdot e^{at},$$

після логарифмування, дістанемо:

$$\frac{\sum_{t=1}^{n} \ln b}{n} = \frac{-a \cdot \sum_{t=1}^{n} \frac{n(n+1)}{2}}{n} + \frac{\sum_{t=1}^{n} \ln\left(\frac{k}{\hat{y}(t)} - 1\right)}{n}.$$

Зробимо припущення, що

$$\sum_{t=1}^{n} \ln\left(\frac{k}{\hat{y}(t)} - 1\right) = \sum_{t=1}^{n} \ln\left(\frac{k}{y(t)} - 1\right), \tag{11}$$

Тоді маємо:

$$\ln b = \frac{-a \cdot (n+1)}{2} + \frac{1}{n} \cdot \sum_{t=1}^{n} \ln\left(\frac{k}{y(t)} - 1\right). \tag{12}$$

Таким чином, керуючись формулами (8) – (12) можна провести аналітичне вирівнювання часового ряду для функції інтенсивності кібератак за допомогою логістичної кривої. Розглянемо часові ряди кібератак на систему підприємства за однакові часові періоди з липня по листопад (1.07-30.09) 2017-2019 років, що попадає у часовий проміжок від кінця третього аудиту до початку четвертого (рис. 2). Проведемо фільтрацію часових рядів за трьома точками (пунктирні лінії на рис. 2).

Отже, для системи (9) знаходимо значення параметрів за наступним алгоритмом:

1. Обчислення:

$$\sum_{t=1}^{n-1} \frac{1}{y(t)}; \ \sum_{t=1}^{n-1} \frac{1}{y(t)^2}; \ \sum_{t=1}^{n-1} \frac{1}{y(t+1)}; \ \sum_{t=1}^{n-1} \frac{1}{y(t+1)} \cdot \frac{1}{y(t)}.$$

2. Знаходження значення:

$$e^a = \frac{(n-2)}{(n-1) \cdot \sum_{t=1}^{n-1} \frac{1}{y(t)^2} - \left(\sum_{t=1}^{n-1} \frac{1}{y(t)}\right)^2}.$$

3. Логарифмування:

$$A = \frac{\sum_{t=1}^{n-1} \frac{1}{y(t+1)} \cdot \sum_{t=1}^{n-1} \frac{1}{y(t)} - \sum_{t=1}^{n-1} \frac{1}{y(t)} \cdot \sum_{t=1}^{n-1} \frac{1}{y(t+1)} \cdot \frac{1}{y(t)}}{(n-1) \cdot \sum_{t=1}^{n-1} \frac{1}{y(t)^2} - \left(\sum_{t=1}^{n-1} \frac{1}{y(t)}\right)^2}.$$

4. Знаходження значення:

$$k = \left(1 - e^a\right)\Big/ A.$$

5. Знаходження значення:

$$\ln b = \frac{-a \cdot (n+1)}{2} + \frac{1}{n} \cdot \sum_{t=1}^{n} \ln\left(\frac{k}{y(t)} - 1\right).$$

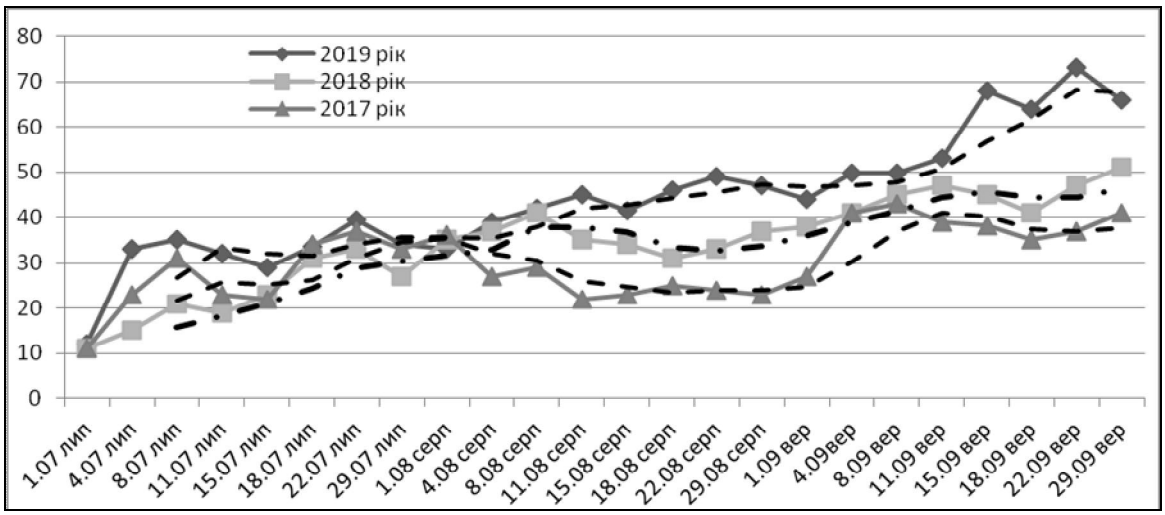


Рис. 2. Часові ряди кібератак на систему підприємства 1.07-30.09 2017-2019 року з проведеною фільтрацією за трьома точками

6. Піднесення до степеня числа *e:*

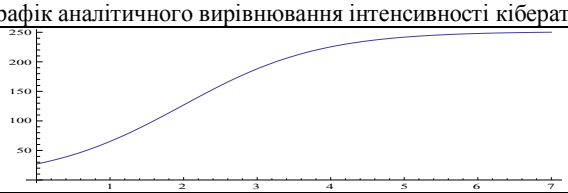
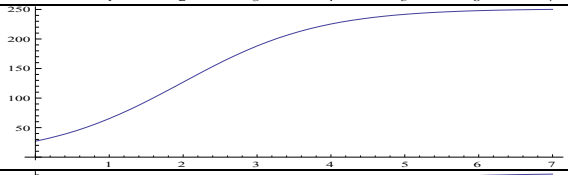
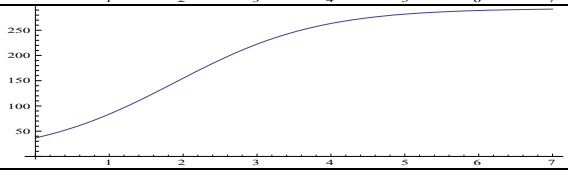
$$b = Exp\left[\frac{-a\cdot(n+1)}{2} + \frac{1}{n}\cdot\sum_{t=1}^{n}\ln\left(\frac{k}{y(t)} - 1\right)\right].$$

7. Аналітичне вирівнювання часового ряду логістичної регресії:

$$\hat{y}(t) = k\Big/\left(1 + b\cdot e^{at}\right).$$

У табл. 1 представлено аналітичне вирівнювання часових рядів кібератак на систему підприємства у період 1.07-30.09 2017-2019 року за умови попередньої фільтрації за трьома точками.

Таблиця 1. **Аналітичне вирівнювання часових періодів кібератак на систему підприємства у період 1.07-30.09 2017-2019 року**

Часовий період	Логістична модель	Графік аналітичного вирівнювання інтенсивності кібератак
1.07-30.09 2017 р.	$I_K(t) = \dfrac{253,47}{1+9,41\cdot e^{-1.02t}}$	
1.07-30.09 2018 р.	$I_K(t) = \dfrac{241,35}{1+8,07\cdot e^{-1.31t}}$	
1.07-30.09 2019 р.	$I_K(t) = \dfrac{261,23}{1+8,77e^{-1,19t}}$	

Застосовуючи *p*–перетворення до функції інтенсивності кібератак $I_K(t)$ на підприємство, для розв'язку рівняння (1) у вигляді:

$$I_K(t) \to i_K(t)^{p-1},\ p \in (0,1)\cup(1,\infty),$$

розв'язок рівняння (1) перетворюється до безрозмірного вигляду:

$$i_K{}^*(t) = \left(1 + \left(\left(1 - i_K{}^*(0)\right)\Big/ i_K{}^*(0)\right)\cdot e^{-\zeta t^*}\right)^{-1/(p-1)},$$

$$i_K{}^*(t) = \frac{i_K(t)}{i_K(t)_{Max}}, \qquad t^* = \frac{t}{T} \qquad (13)$$

де T – період між плановими аудитами.

Це дає можливість знаходити чутливість безрозмірної функції інтенсивності кібератак від параметра *p*.

На рис. 3 представлено чутливість функції інтенсивності кібератак від параметра $p \in [1,9; 2,15]$ за період 1.07-30.09 2019 року за умови проведення фільтрації часового ряду за трьома точками. Мітками на кривих (пунктирні лінії) позначено точки перегину.

На графіку вертикальними лініями окреслено часовий інтервал еластичності функції інтенсивності кібератак, що визначає ефективний час проведення спеціального аудиту (0,64; 0,93) або, починаючи з 57-го дня після проведення планового аудиту по 83-й день необхідно проводити спеціальний аудит.

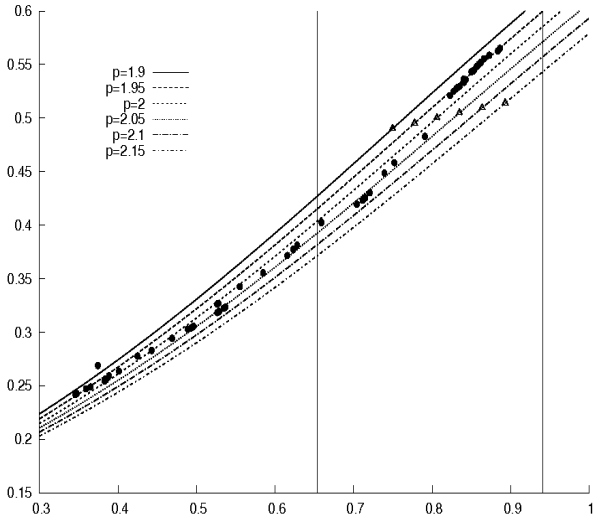


Рис. 3. Чутливість безрозмірної функції інтенсивності кібератак від параметра за період 1.07-30.09 2019 року за умови проведення фільтрації часового ряду за трьома точками

Висновки

За знайденим інтервалом еластичності аналітичної функції інтенсивності кібератак на підприємство, що задовольняє нелінійному диференціальному рівнянню Бернуллі, і проведеним аналітичним вирівнюванням часового ряду функції інтенсивності кібератак за допомогою логістичної кривої (за умови попередньої фільтрації часових рядів за трьома точками), проведено аналіз часових рядів кібератак на систему підприємства за однакові часові періоди 2017-2019 років, що попадають у часовий проміжок від кінця планового аудиту до початку наступного. Застосовуючи *p*–перетворення до функції інтенсивності кібератак на підприємство, враховуючи безрозмірність змінних, представлено чутливість безрозмірної функції інтенсивності кібератак від параметра *p* за встановлений часовий період року за умови проведення попередньої фільтрації часового ряду за трьома точками. Визначено оптимальний час проведення спеціального аудиту, починаючи з 57-го дня після проведення планового аудиту.

СПИСОК ЛІТЕРАТУРИ

1. Шуклін Г. В., Барабаш О. В. Метод побудови стабілізаційної функції керування кібербезпекою на основі математичної моделі коливань. *Телекомунікаційні та інформаційні технології*. Київ. 2018. № 2 (59). С. 110–116.
2. S. Zhang, X. Ou and D. Caragea (2015), "Predicting cyber risks through national vulnerability database". *Information Security Journal: A Global Perspective*, Vol. 24, No. 4-6, pp. 194 – 206.
3. H. Park, S.-O. D. Jung, H. Lee and H. P. In (2012) "Cyber Weather Forecasting: Forecasting Unknown Internet Worms Using Randomness Analysis", *IFIP International Information Security Conference. Springer*, 2012, pp. 376 – 387.
4. C. M. Cheung, P. Goyal, V. K. Prasanna and A. S. Tehrani (2017) "Oreonet: Deep convolutional network for oil reservoir optimization". *Big Data (Big Data)*, 2017 IEEE International Conference on. IEEE, pp. 1277 – 1282.
5. G. E. Box, G. M. Jenkins, G. C. Reinsel and G. M. Ljung (2015), *Time series analysis: forecasting and control*, Published by John Wiley and Sons Inc., Hoboken, New Jersey, 712 p.
6. J. Viinikka, H. Debar, L. Me, A. Lehikoinen and M. Tarvainen (2009) "Processing intrusion detection alert aggregates with time series modeling", *Information Fusion*, Vol. 10, No. 4, pp. 312 – 324.
7. D. Neil, M. Pfeiffer and S.-C. Liu (2016) "Phased lstm: Accelerating recurrent network training for long or event-based sequences". *Neural Information Processing Systems*, pp. 3882 – 3890.
8. Z. Wang, P. Chakraborty, S. R. Mekaru, J. S. Brownstein, J. Ye and N. Ramakrishnan (2015), "Dynamic poisson autoregression for influenza-like-illness case count prediction", *KDD'15*. New York, NY, USA: ACM, pp. 1285 – 1294.
9. S. Yang, H. Du, J. Holsopple and M. Sudit (2014) "Attack Projection". In Cyber Defense and Situational Awareness, A. Kott, C. Wang, and R.F. Erbacher (Eds.). Springer International Publishing, Cham, pp. 239 – 261.
10. E. Gandotra, D. Bansal and S. Sofat (2015) "Computational Techniques for Predicting Cyber Threats". Proceedings Intelligent Computing, Communication and Devices (AISC, Vol. 308) ed J. Kacprzyk (New Delhi: Springer) pp. 247 – 253.
11. B. Munkhdorj and S. Yuji (2017) "Cyber attack prediction using social data analysis". Journal of High Speed Networks, No. 23 (2), pp. 109 – 135.

Received (Надійшла) 29.10.2019
Accepted for publication (Прийнята до друку) 28.11.2019

Attitude optimal hours performed by the special audit for the mind of elasticity and flexibility function intensity cyberattacks

O. Barabash, Ye. Halakhov

Abstract. Cybersecurity management can be improved by enhancing the enterprise's ability to respond to cyberattacks and incidents. At the same time, it is impossible to prevent all attacks. Therefore, the rapid identification and response and protection of critical infrastructure and functions together with powerful information sharing are key issues that need to be addressed. One aspect of addressing this is to conduct timely audits, which are not only limited to scheduled scrutiny, but also provide insight into and take appropriate steps to prevent cyberattacks. The article presents studies aimed at determining the optimal time for conducting a special audit to improve the level of cyber defense and providing priority verified measures to reduce the risk of a cyber-incident. The time series of the cyber-attack intensity of the enterprise are analyzed with analytical alignment of the time series of the cyber-attack intensity function using a logistic curve. Based on the found elasticity intervals of the analytic function of the intensity of cyber-attacks on the enterprise that satisfy the non-linear Bernoulli differential equation, the analysis of the time series of cyber-attacks on the enterprise system for the same time periods that fall in the time period from the end of the planned audit to the beginning of the next. Using the p-transformation to the function of the intensity of cyber-attacks at the enterprise, and taking into account the dimensionlessness of the variables, the sensitivity of the dimensionless function of the intensity of cyber-attacks from the parameter p for a specified time period is calculated under the condition of preliminary filtering of the time series by three points. The optimal time for a special audit after a scheduled audit has been determined.

Keywords: time series, cyber-attack intensity, elasticity, Bernoulli equation, *p*-transformation, filtering, special audit.