УДК 621.396.933 (043.2)
DOI: 10.31673/2409-7292.2019.033035

Є.М. Галахов, О.В. Барабаш

СТРАТЕГІЧНІ ПРІОРИТЕТИ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА, ЩО ЗАЛУЧАЄ ФРІЛАНС-РЕСУРС

Дослідницька увага орієнтована на стратегічні пріоритети системи інформаційної безпеки підприємства, що залучає фріланс-ресурс та на вивчення системи кібербезпеки підприємства у контексті аналізу ризик-менеджменту підприємства з детермінацією його послідовних етапів. Запропоновано модель визначення рекомендованої частоти для процесу управління кібер-ризиками на підприємстві, визначено основні принципи, ключові питання, підходи щодо ефективної реалізації даної моделі в сучасних умовах діяльності підприємства. Математична модель базується на розкладі кусково-неперервної аналітичної апроксимуючої функції в ряд Фур'є, що дає можливість перейти системі аудиту кібер-загроз підприємства від дискретного до неперервного автоматизованого процесу аудиту.

Ключові слова: фріланс-ресурс, бізнес-процеси, комунікаційні канали, соціальна інженерія, експрес-аудит, ряд Фур'є.

Вступ

В умовах сучасних ринкових трансформацій набуває актуальності формування і реалізація ефективного стратегічного вектору бізнес-діяльності підприємства, що пов'язано з системою інформаційної безпеки підприємства. У цьому контексті кібер-безпека підприємства, як складова інформаційної безпеки визначається як захист локальної та хмарної інфраструктури бізнесу, а також перевірка сторонніх постачальників та забезпечення захисту зростаючої кількості кінцевих точок підключення до інформаційної системи підприємства через мережу Інтернет [1]. Зі зростанням загрози та вартості кіберзлочинності зростає і потреба у тактичних діях (експрес-аудитах та ін.) та комплексній стратегії інформаційної безпеки підприємства [3].

Постановка завдання

Необхідно дослідити стратегічні пріоритети системи інформаційної безпеки підприємства, що залучає фріланс-ресурс. Дослідницьку увагу необхідно сконцентрувати на ключових елементах системи інформаційної безпеки підприємства, що залучає фріланс-ресурс.

Основна частина

У табл. 1 структурно представлено 3 ключові блоки бізнес-процесів підприємства, що пов'язані з інформаційною безпекою підприємства, а саме:

1. Бізнес-процеси підприємства, які включають он-лайн канали комунікації.

1.1. Електронна пошта. Шифрування електронної пошти забезпечує захист критичної інформації щодо електронної документації (наприклад корпоративної документації, що стосується реквізитів фінансових рахунків, податкових форм та ін.). Зауважимо, що шифрування електронної пошти використовує складні алгоритми та ключі шифрування, щоб зробити повідомлення та вкладені файли недоступними для тих, хто не має наміру бути одержувачем. Варто зазначити, що на сьогодні багато інструментів шифрування реалізуються на безкоштовній основі і можуть бути розширенням поточного веб-браузера. Згідно статистичних даних за 2017-2019 рр. [5] 91 % усіх кібератак починається з електронної пошти.

1.2. Електронний канал комунікацій замовників і фрілансерів на базі інших програм (наприклад, таких як SLUCK, Skype, Google Hangout та ряду інших альтернативних програм). Можна скористатися низкою програм для експертної роботи. Деякі програми і додатки можуть зберігати інформацію в Інтернеті або, навіть, продавати її третім сторонам. Важливо зрозуміти політику конфіденційності кожної програми, яку розглядає підприємство, що залучає фріланс-ресурс.

2. Бізнес-процеси підприємства, які включають оф-лайн канали комунікації.

2.1. Соціальна інженерія (оф-лайн канали комунікації). У сучасних бізнес-відносинах суттєву роль відіграють не тільки он-лайн канали комунікації, а і оф-лайн відносини, які відзначаються високим рівнем інформаційних ризиків, що впливає не тільки на комерційний, але й на репутаційний базис підприємства.

Таблиця 1.

Стратегічні пріоритети системи інформаційної безпеки підприємства, що залучає фріланс-ресурс

Сфери ризиків	*Фріланс-ресурс*	*Заходи по мінімізації ризиків*	*Стратегічні пріоритети системи інформаційної безпеки підприємства*
Бізнес-процеси підприємства, які включають он-лайн канали комунікації			
Електронна пошта	Високий ризик втрати комерційно значимої інформації	Використання сучасних інструментів шифрування електронної пошти	Імператив аналізу попередніх методів шифрування і постійний аудит імплементації новітніх методів і підходів
Електронний канал комунікацій замовників і фрілансерів на базі інших програм (наприклад, таких як SLUCK, Skype, Google Hangout та інші)	Порушення конфіденційності інформації	Обізнаність у функціональних можливостях програмного продукту	Ознайомлення з політикою конфіденційності програмного продукту, відслідковування поточних змін, що орієнтовані на вдосконалення програмного продукту через реалізацію нових версій
Бізнес-процеси підприємства, які включають оф-лайн канали комунікації			
Соціальна інженерія (оф-лайн канали комунікації)	Небезпека розповсюдження конфіденційної інформації через оф-лайн канали комунікацій	Залучення фрілансерів до тренінгів у сфері соціальної інженерії	Створення високого рівня корпоративної культури підприємства з актуалізацією питання соціальної інженерії (одним із напрямків може бути проведення тренінгів для фрілансерів)
Бізнес-процеси підприємства, що стосуються внутрішньої діяльності			
Введення фінансової звітності і реалізація фінансової політики	Ризик неправильної інтерпретації представленої фінансової інформації	Надання розширеного тлумачення фінансових показників, передання фрілансерам фінансової інформації індивідуалізовано через захищені канали комунікації	Надання фінансової звітності та окремих фінансових показників підприємства в рамках детермінованої фінансової стратегії
Реалізація антивірусного програмного забезпечення	Ризик деструкції бізнес-процесів підприємства	Встановлення сучасного антивірусного програмного забезпечення	Дослідження ринку антивірусного програмного забезпечення, вибір і вчасне встановлення відповідних антивірусних програм високого рівня надійності і в той же час збалансовані за рівнем витрат підприємства

3. Бізнес-процеси підприємства, що стосуються внутрішньої діяльності

3.1. Ведення фінансової звітності і реалізація фінансової політики. Вірне тлумачення показників фінансової звітності підприємства надає можливість зрозуміти не тільки ключові аспекти бізнес-діяльності підприємства, але і зробити певні стратегічні прогнозні оцінки. Тому неправильна інтерпретація вищезазначених показників несе в собі ризики нерозуміння стратегічних пріоритетів компанії і знижує рівень мотивації фрілансерів до довгострокового співробітництва.

3.2. Реалізація антивірусного програмного забезпечення. Висока ефективність реалізації ключових бізнес-процесів значною мірою залежить від використання сучасних

високонадійних антивірусних програм. Тому ефективна мінімізація ризику деструкції бізнес-процесів підприємства передбачає постійне дослідження ринку антивірусного програмного забезпечення, як один із орієнтирів стратегічної політики інформаційної безпеки.

Щоденні кібер-загрози в мережі Інтернет створюють все більш нові кібер-ризики підприємства, які обумовлюються більшою складністю, повнотою і трансформаційним впливом на діяльність підприємства.

Сучасний підхід ризик-менеджменту підприємства складається з наступних послідовних етапів: передбачення кількості можливих кібератак, проведення їх статистично-аналітичної оцінки кібератак, вчасної ідентифікації, розробки плану дій та превентивних заходів щодо усунення ідентичних кібератак, реалізації системи контролю та внесення модернізованих підходів аудиту кібератак на підприємстві [4].

Основою вищезазначеного підходу ризик-менеджменту може виступати запропонована математична модель зв'язку між рівнем кібер-ризику та частотою аудиту, що дає можливість забезпечити ефективну автоматизацію процесів кібер-безпеки підприємства.

Разом з тим, існуючі роботи у напрямку забезпечення кібербезпеки підприємства недостатньо розкривають проблемне питання ефективного інтервального аналізу проведення аудитів орієнтованих на попередження кібератак.

У цьому контексті модель спирається на те, що визначення часу між оцінками має вирішальне значення для загального рівня ризику. Тобто, чим довший часовий період між оцінками ризику, тим вищий рівень ризику. На практиці підприємства використовують різні інтервальні підходи оцінки кібер-ризиків.

Розглянемо більш деталізовано сутність зазначеної математичної моделі.

Дослідницький інтерес даної моделі полягає у визначенні рекомендованної частоти для процесу управління кібер-ризиками на підприємстві.

Модель орієнтується на наступні ключові базиси дослідження:

1. Ретроспективний статистичний аналіз часових рядів ідентифікації кібер-ризику:

1.1. Визначених часових проміжків аудиту та апроксимування статистичних зрізів аналітичними функціями (рис. 1).

1.2. Графічна візуалізація проведеного реалізованого статистичного аналізу часових рядів ідентифікації кібер-ризику (знаходиться за результатами моделювання).

2. Аналіз існуючої стратегії кібер-ризиків підприємства на основі вище проведеного ретроспективного статистичного аналізу часових рядів ідентифікації кібер-ризику з виокремленням: слабких сторін існуючої стратегії, можливих кібер-загроз, ідентифікації потенційних сильних сторін і знаходження можливостей подальшої модернізації.

3. Розробка прогнозно-аналітичної моделі проведення аудитів.

4. Внесення модернізованих підходів у існуючу систему аудиту підприємства.

На рис.1 зображено 4 часових періоди проведення аудиту в рамках запропонованої моделі. Впровадження послідовних аудиторських заходів забезпечує мінімізацію кібер-загроз у кожному часовому періоді, що ілюструє рис. 1.

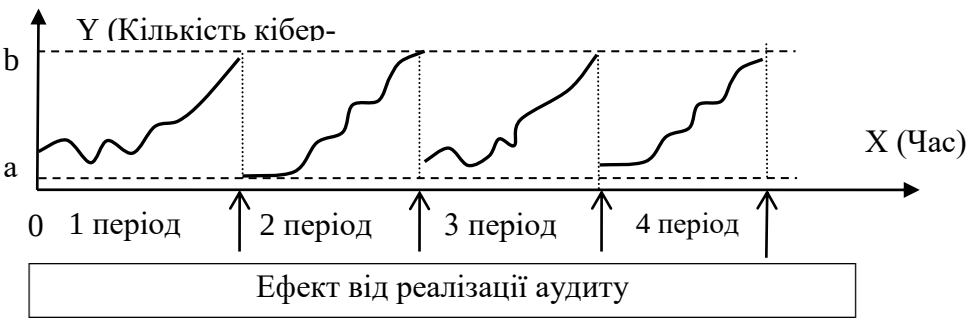

Рис. 1. Залежність кількості кібер-загроз від частоти проведення аудиту за 4 часових проміжки

Згідно п.1.1. вищезазначених ключових базисів дослідження моделі, проведена апроксимація статистичних зрізів аналітичними функціями (табл. 2).

Таблиця 2.

Апроксимація часових рядів кібер-загроз аналітичними функціями

Часовий період	Нелінійне рівняння апроксимуючої функції на інтервалі (0; 1)	Коефіцієнт детермінації
1 період	$y = 1,0643e^{0,064x}$	0,9032
2 період	$y = 1,0534e^{0,053x}$	0,904
3 період	$y = 1,0626e^{0,065x}$	0,9012
4 період	$y = 1,0596e^{0,059x}$	0,8933

На рис. 2 представлена графічна інтерпретація апроксимації часових рядів кібер-загроз аналітичними функціями з усередненими значеннями для кожного часового періоду.

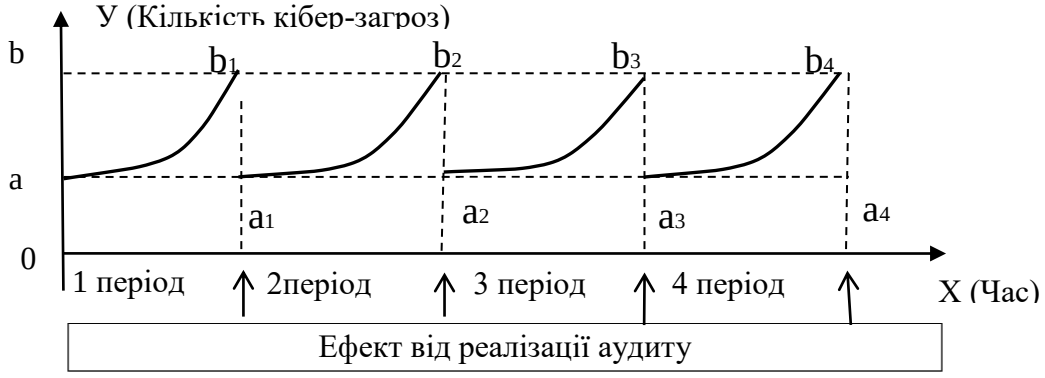

Рис. 2. Апроксимація статистичних зрізів аналітичними функціями

З рис. 2 встановлюємо, що функція періодична з періодом T=1 ($2l$=1, l=1/2), тоді задану функцію розкладаємо в ряд Фур'є на відрізку [0, 2l] =[0, 1]. Запишемо рівняння заданої функції, що представлена на рис. 2 з невідомими коефіцієнтами: $y = Ae^{Bx}$. Визначимо розрахункові координати точок із пучка нелінійних кривих, апроксимуючих статистичний ряд, які знаходяться в довірчому інтервалі з найменшими дисперсіями у вигляді: $y = 1,0595e^{0,060205x}$. Зауважимо, що 0,52975 – статистичне середнє значення функції кібер-загроз в її точках розриву 1-го роду. Отже, маємо:

$$y = \begin{cases} 1,0595e^{0,060205x}; & k < x < k+1, \\ 0,52975; & x = k, \quad k \in Z. \end{cases} \tag{1}$$

Знаходимо коефіцієнти ряду Фур'є за формулами (3.3):

$$a_0 = \frac{1}{1}\int_0^1 \left(1,0595e^{0,060205x}\right)dx = \frac{1,0595}{0,060205}\left(e^{0,060205x}\right)\Big|_0^1 = 17,5982(e^{0,060205} - 1) = 1,09351. \tag{2}$$

Позначивши шуканий інтеграл через I та, застосовуючи подвійне інтегрування частинами, знаходимо:

$$a_n = \frac{1}{1/2}\int_0^1 1{,}0595e^{0{,}060205x}\cdot\cos\left(\frac{n\pi x}{1/2}\right)dx = 2\cdot 1{,}0595\cdot I = 2{,}119\cdot I = \left|\begin{matrix}\left(e^{0{,}060205x}\right)=U, & 0{,}060205\cdot e^{0{,}060205x}dx = dU\\ \cos\left(\frac{n\pi x}{1/2}\right)dx = dV, & V=\frac{1}{2n\pi}\sin\left(\frac{n\pi x}{1/2}\right)\end{matrix}\right| =$$

$$= 2{,}119\left(e^{0{,}060205x}\cdot\frac{1}{2n\pi}\sin\left(\frac{n\pi x}{1/2}\right)\Big|_0^1 - \frac{0{,}060205}{2n\pi}\int_0^1\left(e^{0{,}060205x}\right)\sin(2n\pi x)dx\right) =$$

$$= \left|\begin{matrix}e^{0{,}060205x}=U, & 0{,}060205\cdot e^{0{,}060205x}dx = dU\\ \sin\left(2n\pi x\right)dx = dV, & V=-\frac{1}{2n\pi}\cos\left(2n\pi x\right)\end{matrix}\right| =$$

$$= -2{,}119\cdot\frac{0{,}060205}{2n\pi}\left(\left(-\frac{e^{0{,}060205x}}{2n\pi}\cos\left(2n\pi x\right)\right)\Big|_0^1 + \frac{0{,}060205}{2n\pi}\int_0^1 e^{0{,}060205x}\cdot\cos\left(2n\pi x\right)dx\right) =$$

$$= \frac{0{,}127574}{2n\pi}\left(-\frac{\left(e^{0{,}060205}-1\right)}{2n\pi} + \frac{0{,}060205}{2n\pi}\cdot I\right).$$

Для знаходження інтегралу I розв'яжемо рівняння:

$$2{,}119\cdot I = \frac{0{,}127574}{2n\pi}\left(-\frac{\left(e^{0{,}060205}-1\right)}{2n\pi} + \frac{0{,}060205}{2n\pi}\cdot I\right) \Rightarrow I\left(2{,}119 - \frac{0{,}127574}{2n\pi}\cdot\frac{0{,}060205}{2n\pi}\right) = -\frac{0{,}127574}{2n\pi}\cdot\frac{\left(e^{0{,}060205}-1\right)}{2n\pi}.$$

Таким чином, маємо: $I = \dfrac{0{,}127574\left(e^{0{,}060205}-1\right)}{0{,}00678 - 2{,}119\cdot\left(2n\pi\right)^2}$. Тоді коефіцієнт a_n одержимо у вигляді:

$$a_n = \frac{1}{1/2}\int_0^1\left(1.06^{1-x}\right)\cdot\cos\left(\frac{n\pi x}{1/2}\right)dx = 2{,}119\cdot I = \frac{2{,}119\cdot 0{,}127574\left(e^{0{,}060205}-1\right)}{0{,}00678 - 2{,}119\cdot\left(2n\pi\right)^2} = \frac{0{,}27033\left(e^{0{,}060205}-1\right)}{0{,}00678 - 2{,}119\cdot\left(2n\pi\right)^2}. \quad (3)$$

Аналогічно знаходимо коефіцієнти b_n:

$$b_n = \frac{1}{1/2}\int_0^1 1{,}0595e^{0{,}060205x}\cdot\sin\left(\frac{n\pi x}{1/2}\right)dx = 2{,}119\cdot I = \left|\begin{matrix}\left(e^{0{,}060205x}\right)=U, & 0{,}060205\cdot e^{0{,}060205x}dx = dU\\ \sin\left(\frac{n\pi x}{1/2}\right)dx = dV, & V=-\frac{1}{2n\pi}\cos\left(\frac{n\pi x}{1/2}\right)\end{matrix}\right| =$$

$$= 2{,}119\left(-\left(e^{0{,}060205x}\right)\cdot\frac{1}{2n\pi}\cos\left(\frac{n\pi x}{1/2}\right)\Big|_0^1 + \frac{0{,}060205}{2n\pi}\int_0^1 e^{0{,}060205x}\cos(2n\pi x)dx\right) =$$

$$= \left|\begin{matrix}e^{0{,}060205x}=U, & 0{,}060205\cdot e^{0{,}060205x}dx = dU\\ \cos\left(2n\pi x\right)dx = dV, & V=\frac{1}{2n\pi}\sin\left(2n\pi x\right)\end{matrix}\right| =$$

$$= 2{,}119\left(-\left(e^{0{,}060205}-1\right)\cdot\frac{1}{2n\pi} + \frac{0{,}060205}{2n\pi}\left(\frac{e^{0{,}060205x}}{2n\pi}\sin\left(2n\pi x\right)\Big|_0^1 - \frac{0{,}060205}{2n\pi}\int_0^1 e^{0{,}060205x}\sin(2n\pi x)dx\right)\right) =$$

$$= \frac{2{,}119\left(1-e^{0{,}060205}\right)}{2n\pi} - \frac{0{,}0076806}{\left(2n\pi\right)^2}\cdot I.$$

Для знаходження інтегралу I розв'яжемо рівняння:

$$2,119\cdot I=\frac{2,119\left(1-e^{0,060205}\right)}{2n\pi}-\frac{0,0076806}{\left(2n\pi\right)^2}\cdot I.\Rightarrow I\left(2,119+\frac{0,0076806}{\left(2n\pi\right)^2}\right)=\frac{2,119\left(1-e^{0,060205}\right)}{2n\pi}.$$

Отже, одержимо:

$$I=\frac{2,119\left(1-e^{0,060205}\right)}{2n\pi\left(2,119+\frac{0,0076806}{\left(2n\pi\right)^2}\right)}.$$

Тоді коефіцієнти b_n, будуть мати наступний вигляд:

$$b_n=\frac{4,49020\left(1-e^{0,060205}\right)}{2n\pi\left(2,119+\frac{0,0076806}{\left(2n\pi\right)^2}\right)} \quad (4)$$

Отже, запишемо розклад функції (1) в ряд Фур'є:

$$f(x)=1,09351+\sum_{n=1}^{\infty}\left(\left\{\frac{0,27033\left(e^{0,060205}-1\right)}{0,00678-2,119\cdot\left(2n\pi\right)^2}\right\}\cos\left(2n\pi x\right)+\left\{\frac{4,49020\left(1-e^{0,060205}\right)}{2n\pi\left(2,119+\frac{0,0076806}{\left(2n\pi\right)^2}\right)}\right\}\cdot\sin\left(2n\pi x\right)\right). \quad (5)$$

Таким чином, функція (5) є неперервною функцією, яка моделює кусково-неперервну функцію з точками розриву 1-го роду неусувного характеру. Математична модель базується на розкладі кусково-неперервної аналітичної апроксимуючої функції (рис. 2) в ряд Фур'є, що дає можливість перейти системі аудиту кібер-загроз підприємства від дискретного до неперервного автоматизованого процесу аудиту.

Висновки

Таким чином, постійний неперервний моніторинг та аудит кібер-загроз підприємства надає керівництву ключову інформацію у режимі реального часу щодо ефективності кібербезпеки підприємства, дозволяючи не тільки краще розуміти проблеми під час їх виникнення, але і передбачати їх виникнення, що покращує здатність керувати ризиками та можливостями.

У висновку зауважимо, що комплексна система інформаційної безпеки підприємства має включати в себе як тактичні аспекти інформаційного захисту (експрес-аудит інформаційних загроз підприємства), так і стратегічні пріоритети, що відображає інформаційна політика та інформаційна стратегія підприємства.

Перелік посилань

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

2. Lange M., Kuhr F. and Möller R. "Using a Deep Understanding of Network Activities for Network Vulnerability Assessment," in Proceedings of the 1st International Workshop on AI for Privacy and Security, 2016.

3. Котенко И.В., Саенко И.Б., Коцыняк М.А., Лаута О.С. Оценка киберустойчивости компьютерных сетей на основе моделирования кибератак методом преобразования стохастических сетей. Тр. СПИИРАН, 2017, выпуск 55, 160 – 184.

4. Авсентьев О.С., Дровникова И.Г., Застрожнов И.И., Попов А.Д., Рогозин Е.А. Методика управления защитой информационного ресурса системы электронного документооборота, Тр. СПИИРАН, 2018, выпуск 57, 188 – 210.

5. How to perform a cyber risk assessment. [Електронний ресурс] // Режим доступу: https://www.thesslstore.com/blog/cyber-risk-assessment/ (Дата звернення 12.06.2019).

Надійшла: 5.08.2019 Рецензент: д.т.н., проф. Кожухівський А.Д.