УДК 658:0005.922.1:33(082) DOI 10.36910/6775.24153966.2019.68.16

І.О. Семенова

РОЗРОБКА МЕТОДИКИ ПЛАНУВАННЯ БЮДЖЕТУ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В статті представлено, що кібератаки здатні привезти організації до різного типу втрат: втрата інформації, прибутку, здатності функціонувати. Оцінка окупності інвестицій завжди була ключовим моментом для технологічних інвестицій. Розроблено метод обробки екстремальних значень, який відрізняється незначними обчислювальними витратами і забезпечує отримання однорідних вибірок даних та можливість їх використання для побудови моделей. Практичне значення отриманих результатів полягає у тому, що використання створеної в роботі інформаційної технології аналізу та прогнозування бюджету моделювання дозволило підвищити точність прогнозу в галузі інформаційної безпеки у реальному часі.

Ключові слова: *кібератака, планування, бюджет, інформаційні технології, технологічні інвестиції, обчислення витрат.*

И.А. Семенова

РАЗРАБОТКА МЕТОДИКИ ПЛАНИРОВАНИЯ БЮДЖЕТА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье представлено, что кибератаки способны привезти организации к различного типа потерь: потеря информации, прибыли, способности функционировать. Оценка окупаемости инвестиций всегда была ключевым моментом для технологических инвестиций. Разработан метод обработки экстремальных значений, который отличается незначительными вычислительными затратами и обеспечивает получение однородных выборок данных и возможность их использования для построения моделей. Практическое значение полученных результатов заключается в том, что использование созданной в работе информационной технологии анализа и прогнозирования бюджета моделирование позволило повысить точность прогноза в области информационной безопасности в реальном времени.

Ключевые слова: *кибератака, планирование, бюджет, информационные технологии, технологические инвестиции, вычисления расходов.*

I.O. Semenova

DEVELOPMENT OF BUDGET PLANNING METHODS IN THE INFORMATION SECURITY

The research paper presents that cyber-attacks can cause different types of losses of the organization: loss of information, profit, ability to operate. Estimating return on investment has always been a key point in technological investment. The method of processing of extreme values is developed, which is characterized by low computational costs and provides for obtaining homogeneous samples of data and the possibility of their use for building models. The practical significance of the obtained results is that the use of information technology of analysis and forecasting the budget created in the work allowed improving the accuracy of forecasting in the field of information security in real time.

Keywords: *cyberattack, planning, budget, information technology, technological investment, cost calculation.*

Постановка проблеми. Кібератаки здатні привезти організації до різного типу втрат: втрата інформації, прибутку, здатності функціонувати. Також сліж пам’ятати про витрати на відновлення системи після атаки. Оцінка окупності інвестицій завжди була ключовим моментом для технологічних інвестицій. Незважаючи на достатній рівень розвитку математичного апарату для аналізу та прогнозування відповідних процесів, існують очевидні проблеми узгодження цих методів. На жаль, фахівці з прогнозування економічних показників не прогнозують екологічні і навпаки, фахівці з прогнозування екологічних процесів не прогнозують економічні. Не в останню чергу це залежить від несхожого математичного апарату прогнозування відповідних процесів.

Аналогічно парадоксу продуктивності IT [6], Returns of Investents in Security Investments окупність інвестицій в забезпечення безпеки (ROSI) стала спірною темою в зв'язку з величезним зростанням електронного бізнесу. При розрахунку ROSI здається занадто обтяжливим, збільшення можливостей і масштабів IT-безпеки порушення в зв'язку з ростом міжмережевої взаємодії робить це за необхідним. Організації визначили та пріоритезували найбільш важливі загрози для їх організації, використовуючи здебільшого кращі практики та методики галузі, за якими слідують дані про минулі кібератаки на організацію. Кількісні заходи, наприклад рентабельність інвестицій та чиста теперішня вартість, посіла четверте місце, і лише кілька CISO згадували, використовуючи числові показники при визначенні пріоритетності інвестицій

Тим не менше наука моделювання ризику все ще на початкових стадіях розвитку. Було підраховано, що компрометуючі фірми, в середньому, втратили приблизно 2,1% від їх ринкової вартості протягом двох днів оточуючих порушень безпеки [7].

Таким чином, проблема в даному дослідженні, полягає у відсутності ефективного використання інструментів оцінки InfoSec в процесі прийняття інвестиційних рішень InfoSec для визначення того, "в що" інвестувати. Це призводить до наступного головного питання дослідження: "Що повинен включати оптимальний інструмент самооцінки InfoSec, щоб допомогти InfoSec в прийнятті інвестиційних рішень?"

Однією з цілей методик та стандартів Інформаційної Безпеки, що часто використовуються на даний час, змусити керівників організацій замислюватися над своєю перспективою щодо ризику організації, а їх використання вказує на зрілість управління InfoSec. Однак залишається занепокоєння тим, що навіть якщо CISO використовують правильні інструменти, вони можуть не використовувати їх ефективно, тобто вони використовують їх як списки «для галочки».

Аналіз досліджень та публікацій. Усі організації заявляли про різні потреби в нових інструментах, які вони потребували б для керування витратами та визначення бюджету. Література показує, що більшість організацій визначає бюджет просто за рахунок копіювання витрат минулих років. Існує низка публікацій, що присвячені проблемам інформаційної безпеки в інформаційних системах і мережах передачі й обробки інформації. Завдання створення, організації й дослідження процесів функціонування, удосконалювання й розвитку систем забезпечення безпеки інформації тою чи іншою мірою знайшли відбиття в працях ряду вітчизняних і закордонних учених [1 – 4].

Метою цієї роботи є структурувати та спростити процес оцінювання інвестицій в галузі Інформаційної Безпеки. План, який допоможе організаціям зрозуміти, що необхідно розглянути, щоб ефективно визначити, в яку область Інформаційної Безпеки інвестувати.

Предмет дослідження - методи та підходи щодо вдосконалення процесу прийняття рішень щодо бюджетування проектів за напрямом Інформаційна Безпека в організаціях.

Виклад матеріалу дослідження. В ході дослідження було стверджено, що на даний час класичні моделі не є придатними рішеннями для охоплення потреби організацій в прийнятті інвестиційних рішень в InfoSec. Ранні дослідження InfoSec були зосереджені в основному на технологічній стороні, але в той же час то, як вчені відзначають, що недостатньо вивчати тільки технологію InfoSec. Для ефективної оцінки організаційної структури InfoSec необхідно враховувати людей, процеси і технології. Багато проектів в області інформаційних систем, як правило, зазнають невдачі. мають бути враховані при інвестуванні в InfoSec.

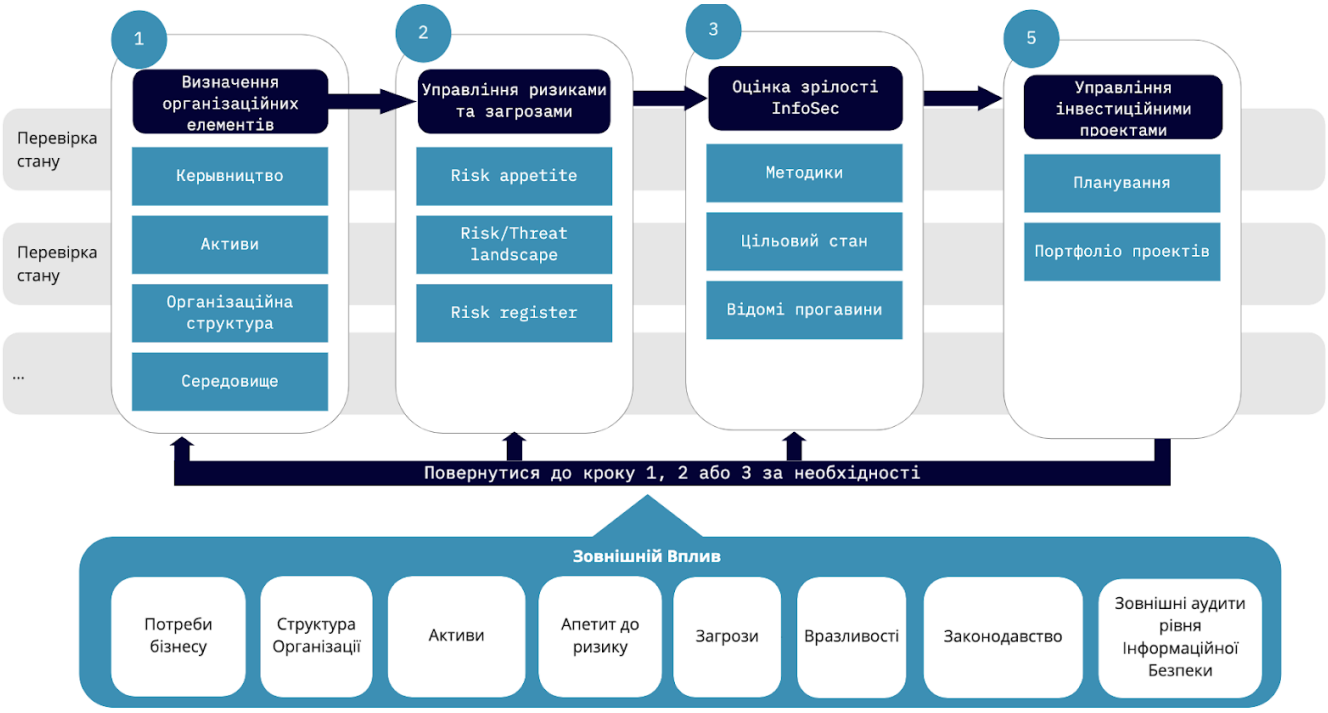
Проведені дослідження ґрунтуються на комплексі взаємопов'язаних методів дослідження – дедукція та індукція, синтез та порівняння, моделювання та аналіз, систематизація та узагальнення, використання яких у комплексі, передбачало теоретико-методологічний підхід у вивченні наукової літератури з теми дослідження, що мало на меті осмислення фактичного матеріалу, формування підгрунття для подальшого дослідження, аналіз концепцій, відомих методик та пропонованих теорій для встановлення шляхів розв'язання досліджуваної проблеми; методах експертного оцінювання, опитування, спостереження, тестування; аналізу та прогнозування бюджету в галузі інформаційної безпеки з метою розробки досконалої моделі прогнозу, експертне оцінювання існуючих методів прогнозування часових рядів – з метою визначення рівня розробленості теми дослідження [1]. При статистичних методах аналізу отриманих даних прогнозування з метою встановлення кількісних та якісних характеристик прогнозного фінансового часового ряду, виявлення їх розбіжності за різними методиками.

У ході дослідження запропоновано рекомендувати завжди робити огляд наступних концепцій:

- Зовнішнє середовище бізнесу (усвідомлення інформаційної безпеки, потреба у дотриманні інформаційної безпеки)
- Організаційна структура бізнесу
- Розуміння ландшафту кіберзагроз
- Поточний стан зрілості InfoSec в організації
- Аналіз прогавин інформаційної безпеки
- Побудови організаційної стратегії
- Визначення відповідних альтернатив
- Прийняття Рішення
- Змінні Рішення
- Ініціювання, планування та дотримання проекту

Наведені концепції пропонують брати до уваги усі зазначені фактори, але не показують структуру впливу та процесу прийняття рішення щодо бюджету. Після проведених опитувань

було виявлено внутрішні та зовнішні фактори, що впливають на рішення. Також було запропоновано структуру огляду та підготування даних.



Легенда

1. Визначення організаційних елементів та зовнішні фактори (не вичерпний перелік)
2. Створення специфічного для організації реєстру ризиків та плани їх лікування
3. Оцінка поточної зрілості (суб'єкти господарювання), встановлення цільового стану та визначення прогалин / результати (наприклад, ризики зареєструвати план лікування)
4. Визначення інвестиційних цілей та приймаймання інвестиційного рішення (проекти)
5. Створення плану розвитку, що містить інвестиційні проекти та їх інформацію (наприклад, ресурси, графік, сфера застосування)
6. Контроль та вимірювання ходу плану/ проекту та, у разі необхідності, повернення до кроків 1, 2 або 3

Організації повинні знати їх організацію (структуру) та активи в межах, які мають важливе значення для нормальної безперервності діяльності. У режимі інструментів InfoSec функціональна структура організаційної структури описує структуру, на яку організація може орієнтуватися на оцінки методології InfoSec та розподіляти активи. Ці функції допоможуть організації вдосконалити оцінку InfoSec з огляду на (ділову) операцію.

Організації роблять оцінки InfoSec, які зазвичай мають деяку шкалу зрілості для оцінки постави InfoSec. Крім того, зазвичай застосовується підхід на основі ризику. Сприйняте зниження ризику вважається одним із найбільших рушійних факторів для інвестицій в InfoSec [4], і, таким чином, функція управління ризиками повинна мати можливість забезпечувати добре загальне розуміння ситуації з ризиком в InfoSec, щоб організація могла максимально орієнтувати інвестиції. необхідні області InfoSec.

Функціонал управління ризиками повинен мати можливість орієнтуватися на виявлені ризики для організаційної структури та активів, щоб визначити пріоритетність критичності інвестицій InfoSec між підрозділами та активами організації.

Функціонал управління загрозами забезпечить реєстр ідентифікованих для організації загроз, які стосуються організації (структури) та активів. Загрози можуть випливати з операційного середовища, оцінок ризику та зрілості InfoSec, а також рамки InfoSec [4]. Загрози можна визначити також із загальних списків уразливості, таких як OWASP (OWASP, 2017), і організація може краще оцінити загрози, спрямовані на поширені вразливості, наприклад. у своїх інформаційних системах, і, таким чином, краще оцінити, у що інвестувати.

Нарешті, слід визначити сфери інвестицій InfoSec для ефективного розподілу ресурсів. Там InfoSec є останньою, але, мабуть, найбільш критичною областю в інструменті. По-перше, методики використовуються в оцінках зрілості InfoSec, і ці оцінки проводяться в організації та в конкретних підрозділах, якщо це необхідно. Ризики, що виникають в результаті цих оцінок, повинні керуватися ними відповідно. Методики використовуються для ідентифікації загроз і можуть розглядатися також як “найкращі практики в галузі", що також є основним джерелом ідентифікації загрози.

Висновки. Розроблено метод обробки екстремальних значень, який відрізняється незначними обчислювальними витратами і забезпечує отримання однорідних вибірок даних та можливість їх використання для побудови моделей. Таким чином, задача створення інформаційної технології для підтримки прийняття рішень щодо прогнозування економічних процесів, що є складовою парадигми якості життя, на основі спільного математичного апарату.

Практичне значення отриманих результатів полягає у тому, що використання створеної в роботі інформаційної технології аналізу та прогнозування бюджету моделювання дозволило підвищити точність прогнозу в галузі інформаційної безпеки у реальному часі. У комплексі застосовані розроблені методи автоматизованого прогнозування наведено моделі аналізу використовувані при рішенні завдань вибору планування бюджету в галузі інформаційної безпеки

1. Баклан І.В. Математичні моделі прогнозування часових рядів різної природи / Баклан І.В., Селін Ю.М., Шулькевич Т.В. // Вестн. Херсонського національного техн. ун-та. - Херсон: ХНТУ, 2014. - Вып. 3 (50).– С.213-218.

2. Гарбарчук В. Кибернетический подход к проектированию систем защиты информации; Украинская академия информатики; Волынский гос. ун-т им. Леси Украинки; Люблинский политехнический ун-т / В. Гарбарчук, З. Зинович, А. Свиц. – К., Луцк, Люблин, 2003. – 658 с.

3. Киселев В.Д. Современные проблемы защиты в системах ее передачи и обработки / В.Д. Киселев, О.В. Есиков, А.С. Кислицын. – М.: Солид, 2000. – 200 с.

4. Маслова Н.А. Построение модели защиты информации с заданными характеристиками качества / Н.А. Маслова // Штучний інтелект. – Донецьк: ІШІ, 2007. – № 1. – С. 51-57.

5. Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах / В.Ф. Шаньгин, А.В. Соколов. – М. : ДМК, 2002. – 134 с.

6. Berinato, S. Finally, a real return on security spending. CIO Magazine 2002, Feb. 15.

7. Denning, D. Reflections on cyberweapons controls. Computer Security J. 2000.- Vol.16(4). - P. 43–53.

8. Dor, D. & Elovici, Y. A model for the information security investment decision-making process. Computers & security. 2016. - Vol. 63. - P. 1-13.

9. Shulkevych T.V. Data Mining Mathematical Apparatus for Forecasting of Nonlinear Nonstationary Processes of Various Nature / T.V. Shulkevych, I.V. Baklan, Yu.M. Selin // Системні тезнології. Регіональний міжвузівський збірник наукових праць.– Дніпро, 2016. – Вип. 6 (107). – С. 151-158.

Стаття надійшла до редакції 15.12.2019