УДК 007:351.778.542

О.О. ІЛЬЇН, С.О. СЄРИХ

КОГНІТИВНА МОДЕЛЬ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ВИЩОГО НАВЧАЛЬНОГО ЗАКЛАДУ

З метою синтезу моделі управління інформаційною безпекою вищого навчального закладу проведено аналіз уразливості інформаційних ресурсів навчальних закладів в Україні. Для вирішення проблеми управління ризиками інформаційної безпеки пропонується використовувати математичний апарат нечіткої логіки. Розглянути можливі загрози, причини їх виникнення, напрямки вдосконалення управління інформаційними ризиками навчальних закладів на основі розробки нечітких когнітивних карт. Проведено синтез моделі, адекватної впливу потенційним загрозам захищеності інформаційного ресурсу, оцінки їх наслідків при наявності неповної вхідної інформації. Отримані вирази, що складають математичну модель інформаційної безпеки вищого навчального закладу.

Ключові слова: інформаційна, безпека, когнітивна, модель, загрози, управління, ризиками.

Вступ

В умовах стрімкої глобалізації сучасного світу механізми поширення, накопичення та обробки даних ускладнюються і стають громіздкими для аналітичних можливостей людини. Людина спостерігає, накопичує знання, аналізує отриману інформацію і приймає рішення. З часом цей когнітивний процес дозволяє сформувати професійну експертизу. Однак, можливості людей перероблювати інформацію обмежені і це стає проблемою. В умовах збільшення об'єму даних від різноманітних датчиків та пристроїв, записів в соціальних мережах можливі збої і прийняття неоптимального чи помилкового рішення, а у найкращому випадку значного збільшення терміну виконання управлінських дій.

Ефективним рішенням даної проблеми є впровадження когнітивної системи, як засобу ініціалізації неструктурованих даних, особливо для центрів зосередження інформаційних потоків, таких як вищі навчальні заклади (ВНЗ).

Неконтрольований доступ до інформаційного ресурсу ВНЗ, стан інформаційної безпеки (ІБ), низька захищеність від зовнішніх та внутрішніх загроз мають негативні наслідки – ризик порушення цілісності, доступності та конфіденційності інформації. Тому актуальність теми статті, що присвячена складанню (синтезу) когнітивної моделі управління ризиками в ВНЗ на основі дослідження моделі [1] порушника ІБ є очевидною.

Аналіз останніх досліджень і публікацій

Питання пов’язані з тематикою дослідження і синтезу моделі управління ІБ різних структур і закладів зустрічаються в працях: І.М. Ажмухамедова, А.В. Тімошенко. В.Козко. Е. Хрустальова, А.Ю. Берко, В.М. Лопатіна, Ю.Є. Максименко, А.І. Марущака та інших. Проте, не зважаючи на значний рівень наукового осмислення проблем інформаційної безпеки, питання адекватності моделі управління, побудованої на основі когнітивних карт продовжують мати актуальність, яка з часом стає все більшою.

Мета статті

Головною метою роботи є теоретичне обґрунтування інформаційної безпеки ВНЗ, напрямків вдосконалення управління інформаційними ризиками навчальних закладів на основі розробки нечітких когнітивних карт (НКК) при когнітивному моделювання, що поєднує теорію пізнання, когнітивну психологію, нейрофізіологію, когнітивну лінгвістику та теорію штучного інтелекту. А це в свою чергу забезпечить розв’язання проблем пошуку, розробки і оптимізації засобів для систем надійного управління і стійкого захисту інформації ВНЗ.

Виклад основного матеріалу дослідження.

Аналіз уразливості інформаційного ресурсу ВНЗ та наслідки цього, відповідають негативним проявам для ВНЗ таким як збільшення фактів протизаконного перехоплення і використання інформації, що проявляються у блокуванні доступу до відкритої інформації,

введенні хибних теоретичних і оціночних даних, а при несанкціонованому доступі і незаконному копіюванні у викраденні інформації з бібліотек, архівів і баз даних, появі та активізації програм-вірусів, знищення або модифікації даних ВНЗ.

У Державному стандарті України ДСТУ 3396.0-96 передбачено загальні шляхи реалізації інформаційної безпеки закладів держави [2], що дозволяє визначити ймовірні загрози, провести їх класифікацію і оцінити ступень проявів і наслідків для ВНЗ і на їх основі синтезувати модель порушника.

Але для підвищення ІБ синтезу навіть системної моделі порушника ІБ і локалізації місця доступу до інформаційного ресурсу недостатньо. Потрібна оцінка інформаційних ризиков, їх ваги і впливовостей один на інший для здійснення в подальшому оптимізації управління ними.

Управління інформаційними ресурсами вищого навчального закладу в сучасних умовах неможливо без наукового обґрунтування та практичної реалізації збалансованої політики інформаційної безпеки.

Вищі навчальні заклади мають ряд особливостей, які необхідно врахувати при побудові системи інформаційної безпеки. Специфіка захисту інформації в освітній установі полягає в тому, що це - публічні заклади з непостійною аудиторією, а також місце підвищеної активності "Початківців кібер-злочинців". Крім того, в сучасному ВНЗ зберігається і обробляється величезна кількість різних даних, пов'язаних не тільки із забезпеченням навчального процесу, а й з науково-дослідними і проектно-конструкторськими розробками. В базах ВНЗ зосереджені персональні дані студентів і співробітників, службова, комерційна і інша конфіденційна інформація. Особливості ВНЗ, як об'єкта інформатизації, пов'язані також з багатопрофільним характером діяльності, великою кількістю форм і методів навчальної роботи, просторової розподіленості інфраструктури (філії, представництва) і т.і.

Для оцінки рівня інформаційної безпеки ВНЗ необхідно отримати дані по складу загроз, вразливостям ресурсів закладу, зв’язків засобів захисту між собою і розглянути вплив потенційно можливих атак на основні сервіси безпеки інформаційних активів навчального закладу.

Побудована динамічна нечітка когнітивна модель дає можливість послідовно простежити всі рівні її ієрархії, оцінити рівень безпеки інформаційних активів ВНЗ і виробити рекомендації по його підвищенню. Така модель будується на основі оцінки ризиків, що супроводжуються терміном – інформаційні і розуміються як ймовірність реалізації загрози ІБ. Тому у загальному поданні оцінка ризиків включає в себе оцінку загроз, вразливостей і шкоди, що завдається при їх реалізації, а їх аналіз полягає в моделюванні процесу настання подій, що обумовлені ризиком у наслідок несприятливих умов на основі врахування усіх можливих факторів, що апріорно визначають ризик.

Тоді першочерговим завданням для підвищення ІБ навчального закладу стає реалізація можливості управління інформаційними ризиками завдяки виконанню їх детальної оцінки і застосуванню ймовірністно-раціонального підходу. При цьому процедури оцінювання інформаційних ризиків ВНЗ доцільно поділити на частини, які в подальшому слід вважати вхідними параметрами моделі побудованої на основі НКК. Вони такі:

- ідентифікація та кількісна оцінка інформаційних ресурсів ВНЗ, значно впливових на ефективність функціонування останнього;
- оцінювання ймовірних загроз ІБ навчального закладу і рівня шкоди, що вони завдають;
- оцінювання вразливостей, терміну їх дії і місць ймовірного [1] застосування в інформаційному ресурсі (ІР) ВНЗ;

- оцінювання ефективності засобів забезпечення ІБ навчального закладу і розробка стратегій протидії загрозам.

При цьому ймовірність того, що загроза реалізується, значно залежіть від персоналізації показників ІБ навчального закладу і є наслідком:

- привабливості ІР для порушника [1];
- обмежено захищеного і відкритого доступу із можливістю використання ІР для одержання порушником доходу;
- зростаючих технічних можливостях порушників у реалізації загрози;
- слабкої підготовленості персоналу ВНЗ до протидії загрозі у разі її настання.

У загальному вигляді і відповідно до міжнародних стандартів управління ризиками ІБ навчального закладу передбачає:

- визначення основних цілей і завдань захисту інформаційних активів закладів;
- створення ефективної системи оцінки та управління ризиками ІБ;
- розрахунок сукупності деталізованих якісно, а при можливості і кількісно оцінок ризиків;
- застосування спеціального інструментарію оцінки та управління ризиками із використанням для моделювання причинних взаємозв'язків, виявлених між концептами деякої області інформаційних і технічних аспектів ВНЗ [4].

Для вирішення проблеми управління ризиками ІБ пропонується використовувати математичний апарат нечіткої логіки, зокрема НКК. На відміну від простих когнітивних карт, НКК являють собою нечіткий орієнтований граф, вузли якого як концепти є нечіткими множинами. Спрямовані ребра графа не тільки відображають причинно-наслідкові зв'язки між концептами, але і визначають ступінь прямого і опосередкованого впливу одних концептів на інші. Активне використання НКК як засобу моделювання систем управління ризиками обумовлено можливістю подання наочно проаналізованої заздалегідь системи і простотою подання причинно-наслідкових зв'язків між концептами, які мають відносну, більш якісну оцінку – «сильно», «середньо», «слабко» і не мають чисельної, ймовірнісної оцінки.

Використання теорії графів зазвичай використовується для подальшої оптимізації систем [5], але не у випадку побудови НКК, коли процес не піддається формалізації, а тим більш обмеженням чи частковим виключенням. Це не дозволяє застосовувати алгоритми автоматичної побудови НКК на основі вибірки даних в повному обсязі для всіх ВНЗ, а при їх використанні потребує уточнення і додаткового відпрацювання до етапу отримання НКК адекватної реальної моделі системі ІБ з урахуванням індивідуальних можливостей і потреб навчального закладу.

Разом з тим їх застосування має суттєві переваги, пов’язані із використання штучних нейронних мереж для більш швидкої і точної класифікації активів ВНЗ за рівнем ризику, а також можливістю формалізації кількісно невизначених факторів при використанні нечіткої, неповної і суперечливої інформації [4]. Особливостей додає той факт, що структура любої установи, як і ВНЗ, має ієрархічну побудову управління і як наслідок - різні вимоги до ІБ, що потребує розподілу знакового орієнтованого графа НКК на низкорівневі графи, наприклад, взаємопов'язаних вузлів в комп’ютерній мережі відділу, враховуючи присутні уразливості в програмному забезпеченні їх обладнання, і карти верхнього рівня, які показують вплив відділів на підрозділи, враховуючи всі присутні їм уразливості. Таким чином, можлива оцінка ризику організації в цілому тільки на основі поєднання різнорівневих [4] НКК і поглибленої оцінки концептів ВНЗ.

Тоді, оскільки ключовими об'єктами дослідження визначаються концепти, що в НКК розташовуються у вершинах графа, то їх множину доцільно визначити як $\{C_n\}$, де C – *concept*. Безліч причинно-наслідкових зв'язків між концептами, тобто гілок графу - як $\{L_{ci}\}$, де L - *linkage causati*; різноманітність знаковості зв'язків (+,-), як $\{S_j\}$, де S - *signification*; перелік ваги зв'язків (середньо, слабо, сильно), як $\{W_g\}$, де W - *weight*.

Таким чином множину НКК можливо представити так:

$$\text{НКК} = \{C_n, L_{ci}, S_j, W_g\}. \quad (1)$$

Разом з тим безліч концептів представляє собою кінцевий набір окремих підмножин, що визначаються індивідуалізацією системи ІБ вищого навчального закладу:

$$\{C_n\} = \{C_n^{к}, C_n^{д}, C_n^{у}, C_n^{б}\}, \quad (2)$$

де $\{C_n^{к}\}$ - підмножина ключових, цільових факторів, стан яких є критично важливим для власника ІР чи персоналу, що використовує елемент активу ВНЗ у своїй професійній діяльності;

$\{C_n^{д}\}$ - підмножина дестабілізуючих факторів впливових на ІБ, що є наслідком дії конкретної загрози, які наносять значної шкоди і потребують фінансових або часових затрат на ліквідацію;

$\{C_n^{у}\}$- підмножина концептів, за допомогою яких вирішується завдання управління ризиками;

$\{C_n^{б}\}$ - підмножина базових факторів, до яких відносять проміжні концепти на які впливають попередні і що приймають участь безпосередньо або опосередковано на наступні концепти.

У разі коли виконується оцінка впливовості концептів пов’язаних безпосередньо, наприклад, ($C_1 \rightarrow C_2$), розв’язання і прогнозування є нескладним завданням. Але аналіз НКК і зв’язків навіть безпосередніх, наприклад, ($C_{n-1} \rightarrow C_n$), ускладняються тим, що з’являються декілька додаткових шляхів графу, наприклад, , ($C_{n-1} \rightarrow C_k \rightarrow C_n$), що може змінити оцінку кардинально і вимагає участі експертів високої кваліфікації. Поява в НКК непрямих шляхів графу потребує аналізу і оцінки усіх впливовостей і причинних ефектів, які в теорії НКК визначені як повні причинні ефекти [3], що додатково до прямих додають непрямі ефекти, а їх впливовість значно залежіть від кількості проміжних концептів, кількості вхідних гілок до концепту, що підлягає аналізу, від ваги кожної складової шляху або в загальному випадку шляхів.

Якщо розглядається шлях НКК - ($C_k \rightarrow C_{k+1} \ldots \rightarrow C_{l-1} \rightarrow C_l$) для концепту C_l, коли кількість проміжних концептів складає l-k при $k<l$, а причинно-наслідкові зв'язки між усіма вершинами відомі і задані, то можливо вирахувати значення непрямого ефекту однієї гілки. Він визначається у спрощеному випадку так:

$$N_1(C_k \rightarrow C_{k+1} \ldots \rightarrow C_{l-1} \rightarrow C_l) = \min(W_{g\,k+1}, \ldots, W_{g\,l-1}, W_{g\,l}), \quad (3)$$

де $W_{g\,i}$ вага причинно-наслідкових зв'язків між вершинами графу шляху ($C_k \rightarrow C_{k+1} \ldots \rightarrow C_{l-1} \rightarrow C_l$).

При наявності декількох шляхів - більше одного від C_k до C_l, загальний ефект від непрямих ефектів *indirect effect* - N шляхів доцільно представити як:

$$E(C_k \rightarrow C_l) = \max(I_1, I_2, \ldots I_{N-1}, I_N), \quad (4)$$

де I_i непрямий ефект шляхів від C_k до C_l, а N їх загальна кількість.

Практичне використання (4) дозволяє простежити шлях від k -*ї* загрози до l - го елементу активу і визначити значення повного ефекту впливу загрози на ресурс ($C_k^{д} \rightarrow C_l^{к}$).

Аналогічним чином, можливо відстежити всі можливі шляхи впливу загроз на активи та виявити найбільш небезпечні. В подальшому дотримуючись однієї із стратегії управління ризиками, таким як зменшення ризику, прийняття ризику, зміна його характеру, ухилення від ризику або застосовуючи їх комбінації забезпечити покращення управління інформаційної безпеки ВНЗ.

При побудові НКК слід враховувати, що у ВНЗ певна кількість інформаційного ресурсу обґрунтовано має відкритий доступ для слухачів і працівників закладу. Це обумовлює необхідність розподілу ризиків на два класи:

- ризики, оцінка яких проводиться без урахування цінності інформації – відкрита для доступу;

- ризики, оцінка яких потребує урахування цінності яку несе в собі інформація – конфіденційна, закрита чи обмежена в доступі інформація.

Отримати вирази для оцінки ризиків обох класів можливо спираючись на приведений в [4] розподіл на системозалежні і системонезалежні ризики. Адаптуючи їх для проведеного дослідження отримуємо наступне.

Для ризиків, що не враховують цінність інформації:

$$R_y=\sum_{y=1}^{M}\sum_{g=1}^{n} D_g * R_g)_y, \quad (5)$$

де D_g - наявність уразливості; R_g - ступінь критичності вразливості; n - число вразливостей;

y - індекс активу; M - кількість активів; g - індекс уразливості.

Тоді загальний ризик ІР навчального закладу можливо розрахувати через ризики окремих підрозділів, відділів, кафедр – r_y за формулою:

$$R_y = \sum_{y=1}^{k} r_y, \quad (6)$$

де k - число відділів, кафедр, підрозділів; y - індекс ієрархії підрозділу.

Значення ризику r_y який оцінюється з урахуванням цінності інформації обчислюється на основі НКК за виразом:

$$r_y = S(C_n^{\partial} \rightarrow C_n^{\kappa})*A_g, \quad (7)$$

де A_g - цінність елемента активу.

Разом з тим слід врахувати той факт, що навіть активи, які не несуть в собі цінну інформацію, можуть бути використані для отримання доступу, спотворення чи модифікації інформації або інших дій зловмисника. Тому виникає необхідність класифікувати елементи активу за рівнем ризику з урахуванням цінності і значущості даного елемента для ВНЗ, що в свою чергу удосконалює (1) і ускладнює НКК. Але використання (5) – (7) продовжує залишатись актуальним.

Висновки

Таким чином застосування підходу до аналізу ризиків на базі нечіткої логіки і побудові НКК надає можливість синтезу моделі адекватної впливу загроз на захищеність ІР, а оцінка наслідків при наявності неповної або навіть суперечливої вхідної інформації отримати

достовірні розрахунки за (5), (6), (7) значення прогнозованих ризиків, що і складають когнітивну модель інформаційної безпеки ВНЗ.

Визначення повного ефекту впливу загрози на ресурс закладу та характера зміни цільових факторів дозволяють обрати раціональну стратегію управління ризиками і застосовувати адекватні заходи захисту для протидії інформаційним загрозам.

Напрямки подальших досліджень

Проведені дослідження уразливості інформаційних ресурсів ВНЗ і синтез моделі управління інформаційними ризиками навчальних закладів з метою підвищення їх інформаційної безпеки дозволяють перейти до оцінки ефективності стратегії управління ризиками. Зменшення ризику, прийняття ризику, зміна його характеру, ухилення від ризику або застосування їх комбінацій, що є базисною основою розв'язання проблем ефективного управління інформаційною безпекою навчального закладу.

Список використаної літератури

1. Ільїн О.О. Аналіз уразливості інформаційного ресурсу вищого навчального закладу та класифікація загроз інформаційної безпеки // Ільїн О.О., Сєрих С.О., Вишнівський В.В. Сучасний захист інформації.- №1, 2017, с.66-72.

2. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 8 липня 2009 року № 514/2009 [Електронний ресурс]. – Режим доступу : Офіційне Інтернет-представництво Президента України http: // www.president.gov.ua

3. Ажмухамедов И.М. Нечеткая когнитивная модель оценки компетенций специалиста // Вестник АГТУ. Серия: "Управление, вычислительная техника и информатика" №2/2011, С.186-190.

4. Волобуев Б. Управление рисками информационной безопасности с использованием нечётких когнитивных карт // Б. Волобуев, В. Черныш. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 1(23) вип., 2012, С. 44-49.

5. Стеклов В.К., Беркман Л.Н. Проектування телекомунікаційних мереж. Київ, "Техніка", 2003 – 923 с.

Надійшла 19.04.2017 р. Рецензент: д.т.н., проф. Карпінський М.П.