3.2. ПІДСЕКЦІЯ - ПРОГРАМНА ІНЖЕНЕРІЯ

УДК 681.14

ОЦІНЮВАННЯ РІВНЯ ЗАХИЩЕНОСТІ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

Філон А.А., студ. гр. ПІ-161
Науковий керівник: **Трунова О.В.**, к.пед.н., доцент
Національний університет «Чернігівська політехніка»

У сучасному світі корпоративна мережа (КМ) представляє собою досить складну систему технологій та програмного забезпечення [1]. Подібні мережі зберігають і обробляють безліч критичних ресурсів, що потребують високого рівня безпеки даних. Проблема забезпечення якісного захисту КМ є актуальною, оскільки кількість загроз постійно зростає, а такі показники як обсяг інформаційних ресурсів та рівень розвитку інформаційної інфраструктури постійно ускладнюються.

Водночас збільшується вразливість КМ і якщо не забезпечити достатній рівень надійності мережі, то дані можуть бути втрачені внаслідок неправильного проектування мережі або викрадені зловмисниками. У багатьох країнах світу постійно ведуться розробки для мінімізації таких ризиків і як результат збільшення рівня інформаційної захищеності.

Підвищений рівень захищеності мережі потребує значних як апаратних, так і програмних затрат. Проте критичні дані обробляються в мережі не постійно, залишається велика частка операцій, які виконуються з некритичними ресурсами і які не потребують такого надмірного захисту. Тут виникає потреба оптимізувати підхід щодо встановлення затребуваного в даний момент рівня захищеності КМ.

Метою роботи є дослідження адаптивного алгоритму для зменшення навантаження на апаратне та програмне забезпечення КМ та підтримки необхідного рівня безпеки інформації у довільний момент часу на базі нечіткої логіки.

Фактично алгоритм адаптивного управління безпекою полягає у динамічному порівнянні профілів захисту (ПЗ) комп'ютерної мережі – набору параметрів системи захисту КМ, на основі якого оцінюється необхідний рівень безпеки КМ з урахуванням критеріїв оцінювання захищеності інформації. ПЗ вносяться в базу знань і на основі нечіткого виводу приймається рішення по управлінню безпекою КМ. Передбачається використання ПЗ, створених за методологією і на основі каталогу вимог міжнародного стандарту ISO/IEC 15408 «Загальні критерії оцінки інформаційної безпеки», що визнаний одним із найдосконаліших стандартів у галузі безпеки [2]. Сюди відносяться такі функціональні критерії оцінки рівня захищеності: аудит безпеки, зв'язок, криптографічна підтримка, захист даних користувача, ідентифікація та автентифікація, управління безпекою, секретність. Крім функціональних також виділені такі критерії гарантії безпеки, що дозволяють оцінити коректність послуг із забезпечення безпеки: управління конфігурацією, поставка і функціонування, розробка, життєвий цикл, оцінювання вразливих місць. Можна сказати, стандарт ISO/IEC 15408 має практично необмежені можливості до розвитку та представляє собою базовий стандарт, який містить методологію опису вимог безпеки ІТ, а також систематизований перелік вимог безпеки. У ПЗ можуть бути включені й інші вимоги, які є необхідними для забезпечення безпеки конкретного типу мережі.

Застосування теорії нечітких множин дозволяє формалізувати процес прийняття рішень в багатомірному нечіткому середовищі. Пропонується застосувати апарат лінгвістичних змінних для формалізації функціональних критеріїв оцінки рівня захищеності КМ та представити ці критерії у вигляді полінома:

$$Y = \beta_0 + \sum_{i=1}^{n} \beta_i x_i + \sum_{u,j=1}^{n} \beta_{ju} x_j x_u , j \neq u, \quad (1)$$

де Y – залежна лінгвістична змінна (критерій), β_j – правий нечіткий коефіцієнт,

x_j – ім'я лінгвістичної змінної.

Набір продукційних правил представляє собою ортогональну матрицю типу 2^n, де n – розмірність факторного простору.

Для оцінювання рівня захищеності КМ на основі адаптивного алгоритму вводиться поняття помилки регулювання $\Delta = y_m - y_p$, де y_m – затребувані параметри безпеки, а y_p – урегульовані параметри безпеки. Звідси помилка регулювання $\Delta = 0$, якщо параметри безпеки КМ постійні і не виникає потреба «вмикати» засоби адаптації. Але у випадку коли параметри безпеки КМ змінюються (як наслідок зміни рівня захищеності оброблюваної інформації), уже виникає потреба ініціалізувати засоби адаптації системи захищеності КМ, для того щоб привести функціонування системи захисту інформації до необхідних параметрів. Таким чином з'являється помилка регулювання $\Delta \neq 0$, і задача засобів адаптації полягає в тому, щоб мінімізувати помилку регулювання ($\Delta \to 0$).

Пропонується наступний алгоритм побудови прогнозованої моделі управління захищеністю КМ з формалізацією функціональних критеріїв в багатомірному просторі:

1. Визначення факторного простору задачі управління захищеністю безпеки КМ.
2. Визначення меж опозиційної шкали та термів по кожному фактору.
3. Формування матриці функціональних критеріїв оцінки рівня захищеності КМ.
4. Генерація лінгвістичних змінних для формалізації інформації щодо подій безпеки КМ.
5. Розрахунок коефіцієнтів полінома формалізації функціональних критеріїв безпеки КМ за (1).
6. Оцінка помилки кількісного експерименту з управління безпекою КМ.
7. Оцінка адекватності отриманого полінома (1) для системи управління безпекою КМ.
8. Оцінка точності моделі управління безпекою за критерієм Фішера як [4]:

$$F_{\text{критФ}} = \frac{S^2_{\text{зал}}}{S^2_{\text{осн}}} < F_{\text{табл}}. \quad (2)$$

Таким чином пропонуються засоби управління захищеністю КМ на основі формалізації функціональних вимог щодо забезпечення захищеності КМ у вигляді прогнозованих моделей в багатовимірному просторі. Рішення по управлінню безпекою КМ приймаються шляхом точних розв'язань нечітких рівнянь.

Аналіз функціональних засобів захисту інформації КМ двох різних типів: першого – що підтримують фіксований рівень захищеності та другого – що використовують механізм адаптивного управління безпекою КМ, показує, що обчислювальні витрати на реалізацію засобів захисту інформації постійно змінюються незалежно від типу, проте середнє значення витрат для систем другого типу є нижчим, ніж для систем першого типу [3].

Механізм адаптивного управління безпекою на основі нечіткої логіки дозволяє оцінювати необхідний в даний момент часу рівень захищеності корпоративних мереж. Це забезпечує зменшення технічних затрат на обробку даних та підвищення ефективності функціонування засобів захисту інформації. За рахунок застосування адаптивного апарата нечіткої логіки стає можливою формалізація функціональних критеріїв рівня захищеності комп'ютерних мереж.

Продуктивність обробки даних в корпоративних мережах, де застосовуються системи захисту з механізмом адаптивного управління безпекою, виявляється вищою, ніж у випадках використання звичайних засобів захисту інформації з фіксованим рівнем захищеності за рахунок зниження обчислювальних затрат на реалізацію функцій захисту інформації, що підтверджує ефективність запропонованого підходу для побудови засобів захисту інформації.

Список використаних джерел

1. Нагиев, А.Ф. Корпоративные сети и проблемы безопасности // Международный научный журнал «Молодой учёный». – № 29 (133) / 2016, часть I. – С. 34–36.

2. Standard ISO 15408: "The common criteria for information technology security evaluation". – ISO Standards Bookshop.

3. Мухин В.Е., Стретович Е.Н. Адаптивное управление безопасностью компьютерных сетей на основе нечеткой логики // Науково-технічний журнал «Захист інформації» №3, 2007. – С. 48–55.

4. Моделювання та аналіз безпеки розподілених інформаційних систем: навч. посіб. для студ. спец. 121 – Інженерія програмного забезпечення / Литвинов В.В., Казимир В.В., Стеценко І.В., Трунова О.В., Скітер І.С., Ткач Ю.М., Гребенник А.Г., Нехай В.В.. – Чернігів: ЧНТУ, 2016. – 220 с.

УДК 004:631

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ОБРОБКИ ІСТОРИЧНИХ ДАНИХ ДЛЯ ФОРМУВАННЯ ЕФЕКТИВНОГО ПОШУКОВОГО ЯДРА

Ткачук Н. О., студ. гр. МПІн-181
Науковий керівник: **Трунова О. В.**, к.пед.н, доцент
Національний університет «Чернігівська політехніка»

Маркетинг став невід'ємною складовою для існування та розвитку підприємництва. Швидка глобалізація та інформатизація змушують пришвидшувати темпи розвитку малого та великого бізнесу незалежно від сфери його діяльності. Для того, щоб залишатися конкурентоспроможними, компанії інвестують не лише в підбір найкращого персоналу, а й в новітнє програмне забезпечення для пришвидшення процесів виробництва та збільшення ринків збуту продукту.

Саме тому зараз є нагальна потреба в використанні наукового підходу та побудові моделей для створення маркетингових стратегій. Вони призначені аналізувати наявні історичні дані та прогнозувати поведінку цільової аудиторії для мінімізації витрат.

Головна мета даної роботи – розробити інформаційну технологію, що дозволить формувати ефективне пошукове ядро для контекстної реклами завдяки обробці історичних даних.

Контекстна реклама – це текстові оголошення, які показуються користувачам за запитами, якщо ці запити рекламодавець додав в налаштування рекламної кампанії. Оголошення показуються користувачеві саме в той момент, коли він сам проявив інтерес до товару чи послуги і, можливо, готовий до покупки. Контекстна реклама буває пошуковою і тематичною.

Пошукова контекстна реклама показується в результатах пошуку в найбільших пошукових системах (Google, Yandex) або по сайту (так звані вертикальні пошуки) в тому випадку, якщо запит користувача збігається з ключовими словами контекстного оголошення.

Аукціонне ціноутворення, яке застосовується в контекстній рекламі, передбачає участь рекламодавців в торгах по кожному ключовому слову, відповідно до яких показується їх реклама. В результаті оголошення різних рекламодавців показуються користувачеві в певній послідовності. На першому місці виявляється рекламодавець, готовий платити за перехід зацікавленого відвідувача максимальну ставку. Але на розподіл місць у контекстної видачу важливий вплив також надає коефіцієнт ефективності самого оголошення, його конверсія з показу в клік (тобто показник CTR), який демонструє рівень інтересу, проявленого до нього з боку потенційних покупців [1].

Це дозволяє збалансувати рекламну видачу і транслювати оголошення різних рекламодавців не тільки за принципом найбільшої ціни, але і за ступенем корисності для користувачів. Для налаштування контекстної реклами необхідно зібрати початкове пошукове ядро, на елементи якого будуть відбуватися покази. Пошукове ядро – це набір текстових рядків (ключових слів) довжиною від 1 до 7 слів. Пошукове ядро можна розділити за сенсом та сформувати групи оголошень для реклами.

Статистика контекстної реклами дозволяє відстежувати такі показники: кількість показів, кліків, конверсія з показу в клік, середня вартість кліку, кількість виконаних цільових дій на сайті (наприклад, оплата товару), конверсія з кліку в цільову дію, вартість реклами.