УДК 004.056

Проценко Я. А., Ломонос Я. Г., Білоусов В. В.

АДАПТИВНА НЕЧІТКА МОДЕЛЬ ІДЕНТИФІКАЦІЇ ШАХРАЙСЬКИХ СИТУАЦІЙ У ТРАНЗАКЦІЙНИХ СИСТЕМАХ

Представлена адаптивна нечітка модель ідентифікації шахрайських ситуацій дозволяє зменшити кількість повернень платежів за рахунок раннього виявлення шахрайських дій користувача і тим самим зменшити грошові втрати, які несе продавець внаслідок санкцій із боку таких платіжних систем, як VISA і MasterCard.

Ключові слова: *нечітка модель, ризики, безпека транзакційних систем.*

Представлена адаптивная нечеткая модель идентификации мошеннических ситуаций, позволяющая уменьшить количество возвратов платежей за счет раннего обнаружения мошеннических действий пользователя и тем самым уменьшить денежные потери, которые несет продавец в следствие санкций со стороны таких платежных систем, как VISA и MasterCard.

Ключевые слова: *нечеткая модель, риски, безопасность транзакционных систем.*

The presented adaptive unclear model of authentication of knavish situations allowing to decrease the amount of returns of payments due to the early discovery of knavish actions of user and to decrease money losses that is carried by a salesman in investigation of approvals from the side of such payment systems the same, as VISA and MasterCard.

Key words: *unclear model, risks, safety of the transaction systems.*

Вступ. Управління ризиками, пов'язаними зі шахрайською діяльністю (fraud risk management), і запобігання шахрайським ситуаціям (anti-fraud management) є одними з основних напрямів діяльності таких структур комерційних підприємств, як аналітичний відділ та відділ безпеки (у тому числі інформаційної безпеки). У сфері fraud risk management вироблено безліч правил, стратегій і алгоритмів, таких як, наприклад, гібридний підхід до запобігання шахрайським діям [1], який дозволяє запобігати шахрайству в багатьох ситуаціях.

У статті розглядаються випадки шахрайства з боку користувачів комп'ютерних систем із метою отримання особистої незаконної вигоди за рахунок комп'ютерної системи або третіх осіб. У ролі комп'ютерної системи може виступати платіжний сервіс, інформаційна система з платним контентом або будь-яка інша комп'ютерна система, яка надає платні сервіси.

Основним видом шахрайства в таких комп'ютерних системах є CNP-шахрайство (Card-not-present fraud) [2], яке включає в себе:

– незаконне замовлення дорогих товарів у мережі інтернет;

– перехоплення товарів, замовлених в інтернеті;

– незаконні угоди (купівля послуг від туристичних компаній / авіакомпаній);

– фізичні операції з підробленими кредитними картками (або краденими даними віртуальних карток);

– спонсорування ОЗУ країн Балтії та Південно-Східної Європи;

За даними Europol, у 2011 р. близько 60 % випадків шахрайства, пов'язаних із платежами, були CNP, які склали 900 млн євро.

Існує два основних підходи до відсіювання шахрайських операцій:

1. База правил безпеки конкретного ресурсу.
2. Використання сторонніх спеціалізованих джерел.

Внутрішня база правил ресурсу може включати в себе аналіз суми та мети платежу, історії платежів клієнта, історії параметрів аутентифікації клієнта, персональної інформації про клієнта (вік, місце проживання тощо) [3]. Цей підхід дозволяє врахувати досвід, накопичений компанією за період роботи, і дає гнучкість у налаштуванні anti-fraud модуля.

Використання сторонніх спеціалізованих ресурсів, таких як minFraud [4] компанії MaxMind, дозволяє отримати доступ до бази знань fraud ситуацій множини сервісів і запобігати багатьом випадкам шахрайства на ранньому етапі.

Тим не менш, зловмисники постійно вдосконалюють методи шахрайства та,

незважаючи на всі вжиті заходи, в інформаційних системах періодично відбуваються випадки «вдалого» шахрайства. Ці випадки можна описати такою послідовністю подій:

1) пошук зловмисником нових схем або комбінування старих підходів для обходу захисту нового або існуючого ресурсу;

2) виконання успішної шахрайської дії на ряді однотипних ресурсів;

3) ідентифікація шахрайської дії і, в разі успішної ідентифікації, аналіз критичності шахрайства (на жаль, багато електронних ресурсів запобігають тільки тим шахрайським операціям, які тягнуть за собою втрати компанії, пропускаючи або заохочуючи ситуації, у яких несуть потенційні втрати актуальні клієнти);

4) вироблення правил ідентифікації схеми шахрайства;

5) доробка anti-fraud модуля й оновлення ресурсу.

І дуже часто fraud-ситуація не може бути розпізнана тільки за набором якісних або кількісних параметрів окремого запиту або навіть з урахуванням історії запитів. Не завжди можлива верифікація користувача (наприклад, за паспортом), а там, де вона можлива, все одно не виключається ймовірність шахрайства. Як правило, для ідентифікації шахрая доводиться проводити аналіз поведінки користувача від створення профілю (ідентифікації) до відомого випадку шахрайства. І, як правило, після визначення поведінкової схеми, її легко застосовувати для ідентифікації нових випадків і розбору спірних доконаних ситуацій.

Метою статті є представлення адаптивної нечіткої моделі ідентифікації шахрайських ситуацій, яка дозволить ідентифікувати fraud-поведінку користувача не тільки на основі значень параметрів запиту, але й врахувати схему поведінки користувача.

Виклад основних результатів досліджень. Адаптивна нечітка модель ідентифікації шахрайських ситуацій.

Платіжна ситуація – запит на виконання платіжних дій із боку користувача електронної платіжної системи.

Легальна платіжна ситуація – платіжна ситуація, яка призводить до очікуваного результату: користувач витрачає легальні грошові кошти (власні або довірені) та отримує товар або послугу.

Шахрайська платіжна ситуація – платіжна ситуація, яка призводить до спірного або негативного результату: витрата користувачем нелегальних коштів (за рахунок інших користувачів або продавця), замовлення неіснуючих товарів або послуг, перерахування коштів завідомо шахраєві, перехоплення товарів або послуг.

Параметри платіжної ситуації – платіжна і неплатіжна інформація, яку можна отримати від користувача в період виконання платежу:

$$S = \{S^p, S^n\}, \qquad (1)$$

де $S^p = \{s_i^p\}$ – множина платіжних параметрів ситуації, $S^n = \{s_i^n\}$ – множина неплатіжних параметрів ситуації.

До множини S^p належать такі параметри, як номер кредитної картки, термін закінчення кредитної картки, CVC/CVV код, наявність захисту 3dsecure, правильність пароля 3dsecure (за умови наявності), банк кредитної картки, сума платежу, призначення платежу, IP адреса користувача, одержувач.

До множини S^n входять такі параметри, як дані профілю користувача (email, телефон, ПІБ, вік, KYC рівень), країна банку кредитної картки, країна/адреса користувача відповідно до IP-адреси, країна/адреса користувача згідно з профілем.

Як правило, платіжні параметри ситуації є визначальними при формуванні висновку, а неплатіжні параметри змінюються слабко від ситуації до ситуації.

Історія платіжних ситуацій – множина попередніх платіжних ситуацій з ознакою легальності:

$$H = \{S_k | f(S_k)\}, f(S_k) \in \{legal, fraud\}, \qquad (2)$$

де S_k – платіжна ситуація, $f(S_k)$ – ознака легальності платіжної ситуації.

Схема поведінки користувача – послідовність ключових подій профілю, які передують або закінчуються платіжною ситуацією з характеристиками події:

$$P = (< p_1, X(p_1) >, < p_2, X(p_2) >, \ldots, < p_T, X(p_T) >), \qquad (3)$$

де $p_t, t \in 1 \ldots T$ – ключова дія, як то: реєстрація, авторизація, редагування профілю, виконання платежу, запит на зміну/зміна KYC рівня, отримання платежу та ін. залежно від специфіки системи, $X(p_t)$ – характеристики події, специфічні для кожного типу подій.

Кожна схема поведінки може характеризувати певний вид шахрайської операції, наприклад ситуація, описана як: (<авторизація, успішно>, <редагування профілю, зміна країни та/або зміна паролю>, <платіж, кругла сума або вся доступна сума та/або новий одержувач і/або одержувач-шахрай>), може свідчити про крадіжку реєстраційних даних.

Вхідними даними для адаптивної нечіткої моделі ідентифікації шахрайських ситуацій слугує така множина:

$$IN = \{S, H, P\}. \qquad (4)$$

Висновок будується на основі вхідних даних і бази знань, що дозволяє припустити легальність вхідної операції і визначити $f^*(S)$ – попередню ознаку легальності для вхідної ситуації S ($f^*(S) \in \{legal, cond-legal, cond-fraud, fraud\}$ – може приймати такі значення: легальна, умовно легальна, умовно шахрайська, шахрайська ситуація). У подальшому, залежно від налаштувань

платіжної системи, може виконуватися блокування користувача або просто повідомлення оператора.

Концептуальна схема роботи адаптивної нечіткої моделі ідентифікації шахрайських ситуацій.

Система оцінки ситуації складається з п'яти блоків: блоку оцінки параметрів платіжної ситуації PE (фазифікатор), блоку прийняття нечіткого рішення FD (нечіткий логічний висновок), бази знань KB, блоку аналізу поведінки TA (адаптаційний блок), блоку ухвалення чіткого рішення CD (дефазифікатор). Також із метою збереження контролю людини над системою реалізація цієї моделі повинна містити оболонку, за допомогою якої адміністратор може в будь-який момент змінити налаштування системи. Схему системи представлено на рис. 1.

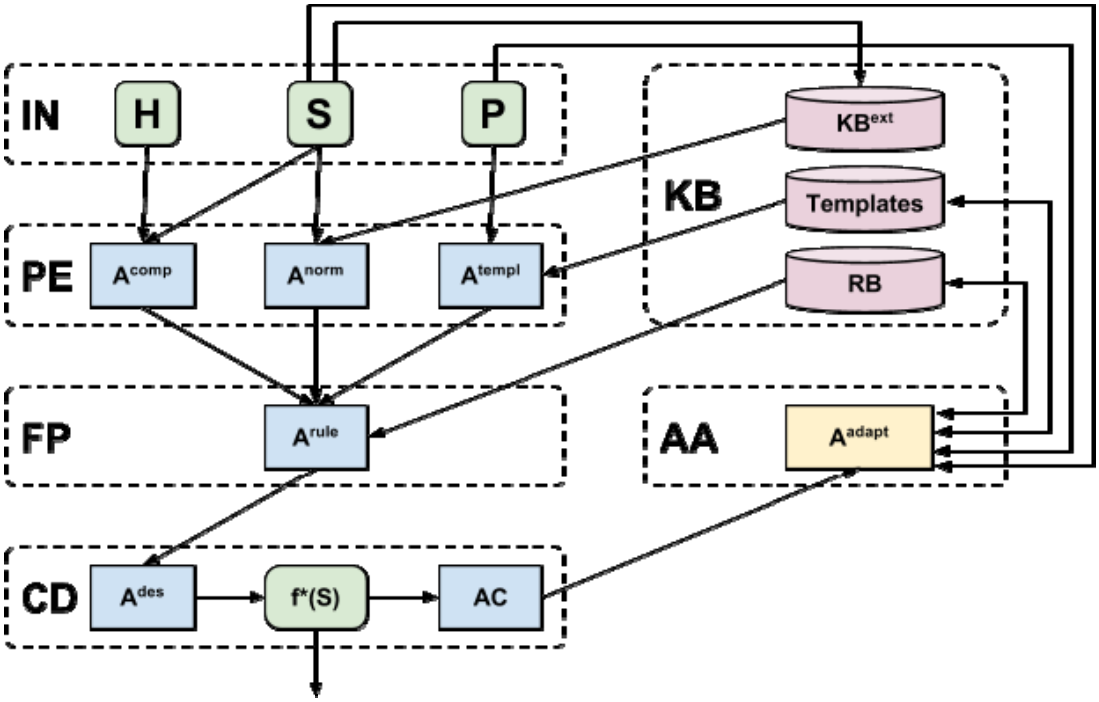

Рис. 1. Схема обробки платіжної ситуації

На схемі представлено такі блоки та модулі:

Блок оцінки параметрів платіжної ситуації PE (попередній аналіз і збір інформації про поточну платіжну ситуацію):

– Acomp – модуль нечіткого порівняння ситуацій;

– Anorm – модуль оцінки нормальності параметрів ситуації;

– Atempl – модуль нечіткого співставлення з шаблоном.

Адаптаційний блок TA (налаштування бази шаблонів поведінки шахраїв і пост-аналіз бази історії ситуацій):

– Aadapt – модуль адаптації шаблонів поведінки шахраїв.

База знань KB (зберігання даних про систему та її користувачів, а також зберігання всіляких чітких і нечітких правил та критеріїв, згідно з якими виконується аналіз ситуації й ухвалення рішення):

– RB – база правил комплексного аналізу параметрів платіжної ситуації;

– Templates – база шаблонів поведінки шахраїв;

– KBext – зовнішня база даних, яка зберігає дані про профілі користувачів системи та їх історії платежів (а також, можливо, іншу інформацію, необхідну для зовнішнього щодо описуваної системи середовища).

Блок прийняття нечіткого рішення FD (глибокий аналіз попередніх оцінок вхідних даних і визначення ступеня відповідності платіжної ситуації кожній з ознак легальності):

– Arule – модуль нечіткого аналізу з допомогою правил.

Блок ухвалення чіткого рішення CD (ухвалення остаточного рішення щодо відповіді системи на ситуацію):

– Ades – модуль ухвалення рішення;

– AC – консоль оператора, за допомогою якої він може змінити остаточне рішення щодо легальності ситуації, а також проводити пост-аналіз ситуації з метою поповнення чи коригування бази шаблонів (Templates) і бази правил (RB).

Модуль нечіткого порівняння ситуацій. Модуль отримує на вхід поточну ситуацію та історію ситуацій. Результат – нечітка множина, що характеризує «типовість» ситуації порівняно з усіма іншими ситуаціями цього користувача на основі дисперсії параметрів з урахуванням важливості кожного параметру:

$$A^{comp}(S, II) = \widetilde{X^{comp}} = \{s_i | \mu(s_i)\}, \quad (5)$$

де $\mu(s_i)$ визначається ступенем атиповості параметру s_i, обчисленого на основі статистичних функцій.

Цей модуль зберігає таблицю, у якій для кожного типу параметру платіжної ситуації вказано ступінь зв'язаності (наскільки сильно впливає дисперсія іншого параметру на нетиповість поточного параметру) із кожним із решти параметрів і його рівень важливості (наскільки сильно свідчить про нетиповість дисперсія цього та інших зв'язкових параметрів), а також правило обчислення дисперсії параметру у вигляді числа (наприклад, якщо обчислюється дисперсія призначення платежу, то необхідне правило, згідно з яким дисперсію буде визначено як число). Тоді для кожного параметру рівень типовості обчислюється за формулою:

$$\mu(s_i) = 1 - \gamma_i \frac{\sum_k \alpha_k \cdot \sigma(s_k)}{\sum_k \alpha_k \cdot \sigma_{max}(s_k)}, \quad (6)$$

де γ_i – рівень важливості k-того параметру, α_k – рівень зв'язаності k-того параметру з i-тим, $\sigma(s_k)$ – дисперсія k-того параметру, $\sigma_{max}(s_k)$ – найбільша за всю історію дисперсія цього параметру при обліку тільки платежів, що мають остаточну оцінку legal. Вихідний результат – нечітка множина виду (5).

Модуль оцінки нормальності параметрів ситуації.

Вхідні дані: множина S.

Вихідні дані: нечітка множина виду:

$$A^{norm}(S) = \widetilde{X^{norm}} = \{s_i | \mu(s_i)\}, \quad (7)$$

де $\mu(s_i)$ є ступенем «нормальності» параметру s_i.

Під «нормальністю» вважається відсутність відхилень параметру від значення, яке вказує на повну довіру, іншими словами, ступінь належності відображає ступінь близькості цього параметру до «ідеального». Такими значеннями найчастіше є дані, зазначені в профілі, або значення, які зустрічаються в переважній більшості платіжних ситуацій даного користувача. Наприклад, якщо місто вихідного платежу збігається з містом, зазначеним у профілі, то параметр «Місто» вважається нормальним, якщо це місто знаходиться недалеко, то значення нормальності трохи падає, якщо ж це місто знаходиться взагалі в іншій країні, то система вважає, що це незвично і присвоює низьку ступінь нормальності.

Модуль нечіткого зіставлення з шаблоном. Цей модуль працює з моменту авторизації користувача та до моменту запиту на платіж. Результат – нечітка множина, що визначає належність ситуації до всіх шаблонів шахрайської поведінки:

$$A^{templ}(P) = \widetilde{X^{templ}} = \{P_i | \mu(P_i)\}, P_i \in \{P\}, \quad (8)$$

де $\mu(P_i)$ визначає ступінь подібності поведінки користувача в рамках поточної сесії до шаблону шахрайської поведінки P_i.

Модуль нечіткого аналізу за допомогою правил. Цей модуль становить нечітка думка про те, чи є цей запит легальним. Вхідні дані: вихідні дані всіх модулів, що входять у блок РЕ.

Вихідні дані: нечітка множина, що описує думку системи про легальність ситуації:

$$A^{rule}(\widetilde{X^{templ}}, \widetilde{X^{norm}}, \widetilde{X^{comp}}) = \widetilde{f^*(S)}, \quad (9)$$

де $\widetilde{f^*(S)}$ – нечітка множина на базі множин $\{legal, cond-legal, cond-fraud, fraud\}$ і ступеня приналежності його елементів, які виражають ступінь істинності кожної відповідної ситуації.

Аналіз здійснюється за допомогою правил, узятих з бази правил **(RB)**, які мають такий вигляд:

$$\text{ЕСЛИ } x_1 \oplus A_1 \ \dots \text{ И } \dots x_n \otimes A_n \text{ ТО } y = y + E, \quad (10)$$

де x_i – значення функції належності елементів вхідних нечітких множин (мають різний зміст у кожному з цих множин), A_i – якесь термінальне значення, з яким порівнюється значення x_i за допомогою деякого оператора порівняння $\oplus$, y – значення функції приналежності елемента вихідної множини блоку ухвалення нечіткого рішення, має сенс ступеня істинності відповідної ознаки легальності. B-приріст, позитивний чи негативний, який отримає y, якщо умову правила буде виконано. Значення A і B зберігаються в базі правил RD. Початкові значення y визначаються параметрами системи.

Цей модуль проводить глибокий усебічний комплексний аналіз усіх отриманих на попередніх етапах даних. Наприклад, якщо має місце нетипова ситуація і поведінка близько до якого-небудь із шаблонів поведінки шахраїв, це свідчить про можливу атаку шахрая, якщо в поточній сесії проведені деякі такі зміни, що нормальність параметрів стала дуже високою, і при цьому ситуація сильно нетипова, а близького збігу з якимось шаблоном поведінки немає, то це може свідчити про нову шахрайську тактику.

Модуль ухвалення рішення дефазифіковує значення, отримане на попередньому кроці:

$$A^{def}(\widetilde{f^*(S)}) = f^*(S), \quad (11)$$

де $f^*(S)$ є результатом дефазифікації нечіткої множини $\widetilde{f^*(S)}$, визначеної на базовій множині $\{legal, cond-legal, cond-fraud, fraud\}$.

Залежно від значення, система може визначати своє подальшу поведінку, наприклад при значенні *legal* або *cond-legal* виконувати платіж, при значенні *cond-fraud* або *fraud* платіж блокувати, при значенні *cond-legal* або *cond-fraud* сповіщати оператора для перевірки ситуації й ухвалення остаточного рішення.

Далі ситуація додається до історії платіжних ситуацій з ознакою legal, якщо ситуації відповідає *legal* або *cond-legal, fraud-cond-fraud* або *fraud*, і значення ознаки може бути змінено оператором.

Визначення оператором ситуації як шахрайської супроводжується описом типу шахрайства і на підставі цього опису додається новий шаблон шахрайської поведінки або коректується / доповнюється вже існуючий.

Модуль адаптації шаблонів поведінки шахраїв. Призначення цього модуля полягає в адаптації системи до нової поведінки шахраїв. При кожній нелегальній платіжній ситуації або просто підозрілій ситуації модуль пропонує оператору додати новий шаблон, який відповідає поточній схемі поведінки користувача. Якщо оператор вважає за потрібне, він може додати цей шаблон на базі шаблонів (можливо, відредагувавши запропоноване системою) або відхилити пропозицію модуля. Також оператор може редагувати, видаляти і створювати нові шаблони. Адаптаційний модуль може, якщо, наприклад, оператор зауважив небезпечну схему поведінки, не помічену системою, запускати сканування всієї бази платіжних історій за заданими оператором правилами нечіткого аналізу історії з метою знаходження ситуацій і схем поведінки, які відповідають поміченій схемою, щоб у разі знаходження множини підозрілих ситуацій додати новий шаблон шахрайської поведінки.

Висновки

Представлена адаптивна нечітка модель ідентифікації шахрайських ситуацій дозволить зменшити кількість повернень платежів за рахунок раннього виявлення шахрайських дій користувача і тим самим зменшити грошові втрати, які несе продавець унаслідок санкцій із боку таких платіжних систем, як VISA і MasterCard. Адаптованість системи дозволить вчасно відстежувати виникнення нових стратегій обходу системи захисту і тим самим виключити значну кількість помилок через неповноту бази перевірок. Крім того, ця модель необов'язково застосовувати саме для безпеки транзакційних систем: її можна легко модифікувати для практично будь-якої системи, що вимагає аутентифікації та авторизації.

ЛІТЕРАТУРА

1. How a Hybrid Anti-Fraud Approach Could Have Saved Government Benefit Programs More than $100 Million – Whitepaper – SAS Institute Inc. World Headquarters [Електронний ресурс]. – Режим доступу : http://www.sas.com/resources/whitepaper/wp_41905.pdf.
2. Payment Card Fraud in the European Union. Perspective of Law Enforcement Agencies. Situation Report. Public Version. Europol[Електронний ресурс]. – Режим доступу : – https://www.europol.europa.eu/sites/default/files/publications/1public_full_20_sept.pdf.
3. Raul Moreno, David Rios. Transactional Data Analysis for Antifraud decision support. JSM, Denver, 07.08.2008 [Електронний ресурс]. – Режим доступу : http://www.slideshare.net/raulmoreno/transactional-data-analysis-for-antifraud-decision-support.
4. Reduce Online Fraud with the minFraud Service. Описання продукту [Електронний ресурс]. – Режим доступу : http://www.maxmind.com/en/ccv_overview.
5. Richard E. Smith(2002). Authentication: From Passwords to Public Keys.
6. Defuzzification methods [Електронний ресурс]. – Режим доступу : http://www.mathworks.com/products/demos/shipping/ fuzzy/defuzzdm.html.
7. Mamdani Fuzzy Systems [Електронний ресурс]. – Режим доступу : http://www.bindichen.co.uk/post/AI/mamdani-fuzzy-model.html.
8. Fuzzy Identity Authentication [Електронний ресурс]. – Режим доступу : http://www.wseas.us/e- library/conferences/2010/Corfu/COMPUTERS/COMPUTERS1-24.pdf.

Дата надходження статті до редколегії 08.10.2013 р.

ПРОЦЕНКО Ярослав Андрійович – студент 2 курсу спеціальності «Безпека інформаційних і комунікаційних систем» Донецького національного університету, м. Донецьк.

Коло наукових інтересів: програмні методи захисту інформації.

ЛОМОНОС Ярослав Геннадійович – кандидат технічних наук, доцент кафедри комп'ютерних технологій Донецького національного університету, м. Донецьк.

Коло наукових интересів: програмні методи захисту інформації.

БІЛОУСОВ В'ячеслав Володимирович – доктор технічних наук, професор, в. о. завідувача кафедри фізики нерівноважних процесів, метрології та екології Донецького національного університету, м. Донецьк.

Коло наукових інтересів: математичне моделювання гідродинамічних і теплофізичних процесів, криптографічні та програмні методи захисту інформації.