УДК 004.056.5:621.395.3:343.53.003.2 DOI: 10.31673/2412-9070.2022.064399

В. Г. РУЖИНСЬКИЙ, доцент кафедри;
В. Ф. ЗАЇКА, доктор техн. наук, професор;
О. М. МАРЧУК, ст. викладач,
Державний університет телекомунікацій, Київ

СИСТЕМИ ЗАХИСТУ ПРОТИ ПОРУШЕНЬ ЯК ЗАПОРУКА ФІНАНСОВОЇ СТАБІЛЬНОСТІ ОПЕРАТОРІВ

Проведено аналіз видів шахрайства, пов'язаного з трафіком, у телекомунікаційних мережах. Порушення на телекомунікаційних мережах — це дії абонентів, операторів телекомунікацій або третіх осіб, спрямовані на отримання телекомунікаційних послуг за заниженим тарифом або без оплати. Фахівці ЦАКУ налічують майже 200 видів порушень на телекомунікаційних мережах. Найпоширенішими порушеннями з боку операторів є несанкціоноване завершення вхідного міжміського або міжнародного трафіку в мережу загального користування під виглядом місцевого, без відповідних договорів. Зловживання призводять до значних втрат прибутку. Найбільш відомими серед абонентів є стороннє підімкнення до абонентської лінії з метою отримання безкоштовних телематичних послуг служби «900», здійснення довгострокових міжнародних дзвінків, організація несанкціонованих місць зустрічі. Порушенням із боку третіх осіб є використання апаратно-програмного забезпечення для отримання міжнародного трафіку з мережі «Інтернет» та його проходження в телекомунікаційній мережі загального користування під виглядом локальної, що призводить до втручання в роботу засобів зв'язку, підміна інформації про виклик. Боротьба з неправомірним використанням телекомунікаційних мереж переважно базується на аналізі даних про послуги та даних, що містяться в системах розрахунків з абонентами та операторами. Виявлення підозрілих дій абонентів та їх аналіз є основним принципом роботи сучасних систем захисту від Fraud Management System (FMS). Ключовими критеріями ефективності FMS є швидкість роботи, гнучкість налаштування алгоритмів, що забезпечують виявлення та аналіз інцидентів, а також наявність стандартизованих інтерфейсів для інтеграції з білінговими платформами. Надано практичні рекомендації щодо створення систем захисту від порушень FMS.

Ключові слова: профіль об'єкта; інтенсивність потоку викликів; трафік; аномалії; ефективність; параметри мережі.

ВСТУП

Постановка проблеми. Сьогодні оператори телекомунікацій вирішують проблему, яка безпосередньо пов'язана з фінансовим станом компаній, а саме: впровадження систем з протидії шахрайствам, пов'язаних із трафіком.

Згідно з останніми дослідженнями всесвітньої Асоціації щодо контролю за порушеннями на телекомунікаційних мережах (*Communications Fraud Control Association*, CFCA), у 2005 році втрати від порушень у телекомунікаційній галузі становили 54,4–60 млдр дол. Це приблизно на 52% більше за цифру, одержану в дослідженнях CFCA трирічної давності. Порушення на телекомунікаційних мережах це дії абонентів, операторів телекомунікацій чи сторонніх осіб, спрямовані на одержання телекомунікаційних послуг за більш низькою ставкою або без оплати. Експерти CFCA налічують майже 200 видів порушень на телекомунікаційних мережах.

Найпоширенішими з боку операторів порушеннями є несанкціоноване, без відповідних договорів, завершення вхідного міжміського та міжнародного трафіку на мережу загального користування під виглядом місцевого. Зловживання призводять до значних втрат доходів.

З боку абонентів найчастіше спостерігається стороннє підімкнення до абонентської лінії з метою безоплатного одержання телематичних послуг служби «900», здійснення довготривалих міжнародних розмов, організація несанкціонованих переговорних пунктів.

Порушенням з боку сторонніх осіб є використання апаратно-програмного забезпечення для отримання міжнародного трафіку з мережі «Інтернет» та завершення його на телекомунікаційній мережі загального користування під виглядом місцевого, призводячи до втручання в роботу засобів зв'язку, а також до підміни інформації про виклик.

Боротьба із зловживаннями на телекомунікаційних мережах переважно ґрунтується на аналізі даних про послуги та даних, що їх містять розрахункові системи з абонентами та операторами. Виявлення підозрілих дій абонентів та їх аналіз є основним принципом дії сучасних систем захисту проти порушень Fraud Managment System (FMS). Ключовими критеріями ефективності FMS є швидкість роботи, гнучкість налагодження алгоритмів, які забезпечують виявлення та аналіз інцидентів та наявність стандартизованих інтерфейсів для інтеграції з платформами білінгу.

Зазвичай роботу механізмів виявлення порушень засновано на обробленні детальних записів про здійснені виклики CDR (Call Detail Record). Система протидії шахрайству вишукує в них невідповідності певним умовам або невідповідності заданому шаблону, характеристики поведінки абонента. Коли модуль виявлення знаходить одну з аномалій, він генерує повідомлення з попередженням.

До типових перевірок за умовою систем FMS належать такі:

- неіснуюча нумерація;
- перевірка авторизації, тимчасового блокування;
- відповідність шаблону;
- перевірка «чорних та білих списків»;
- неіснуючий код міста/області/країни;
- номери абонентів «А» або «Б» що найчастіше повторюються;
- перевірка на тривалість;
- перевірка підозрілих викликів від абонентів «А» на входження до переліку абонентів «Б» яким найчастіше надходять виклики з-за кордону;
- можливість організації додаткових перевірок з легкою зміною правил, застосованих під час аналізу за допомогою редактора правил.

Пошук за заданим шаблоном опирається на шаблони трафіку, який створюється для кожного оператора телекомунікацій. Різниця, що виникає між наявним трафіком та шаблоном, свідчить про можливе порушення. Додаткове застосування шаблонів полягає в складанні профілю абонента (оператора телекомунікацій) зловмисника та пошук відповідності такому профілю серед наявних абонентів (операторів телекомунікацій). Профілі можуть мати в своєму складі такі характеристики:

- активність у денний час;
- активність у вечірній час;
- активність у нічний час;
- обсяги вихідного трафіку на мобільні телефони;
- обсяги вихідного трафіку на фіксовані місцеві номери (включно з часто використовуваними номерами);
- обсяги вихідного трафіку на фіксовані номери в інших містах (включно з часто використовуваними номерами);
- обсяги вихідного трафіку на фіксовані номери в інших країнах (включаючно з часто використовуваними номерами);
- номерний діапазон оператора;
- середня кількість з'єднань за проміжок часу;
- середній обсяг трафіку за проміжок часу;
- середня тривалість з'єднань;
- кількість унікальних номерів;
- характерні напрямки.

Найбільш критичними з погляду зниження втрати доходів є порушення порядку маршрутизації міжміських та міжнародних викликів: виявлення активності абонентських номерів по вихідному місцевому трафіку та активності операторів по вхідному місцевому трафіку, схожу на роботу шлюзів для завершення вхідного міжміського та міжнародного трафіку: виявлення змін в активності абонентських номерів, які можуть бути свідченням стороннього підімкнення до абонентської лінії або дій абонента, що потенційно призводять до скарг, несплат за послуги та списання заборгованості.

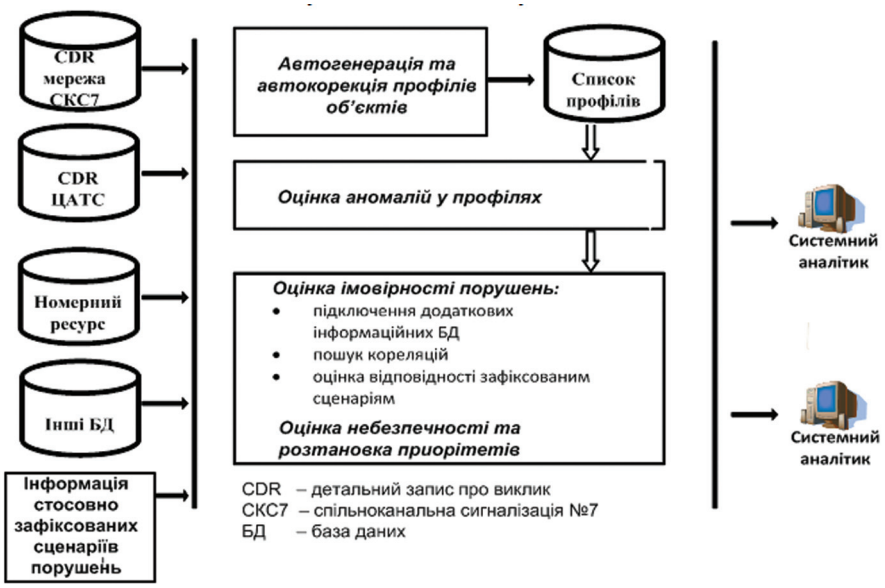
Отже, є доцільним упровадження інформаційної підсистеми в складі системи контролю трафіку (основна складова FMS), яка буде спиратись на дані, отримані із систем контролю мережі спільноканальної сигналізації №7 (СКС7), цифрових АТС тощо та призначена для здійснення аналізу трафіку, інформування про ситуації, що є підозрілими та потребують подальшого детального вивчення відповідними програмними засобами.

ОСНОВНА ЧАСТИНА

До основних функціональних завдань підсистеми FMS належать (рисунок):

- автоматичне або за участю оператора налагодження профілю елементів телекомунікаційної мережі;
- забезпечення автоматичного аналізу, класифікації даних, пошуку відхилень поведінки елементів телекомунікаційної мережі від звичайного профілю;
- створення алгоритму виявлення, який ґрунтується на особливостях порушень, що формують динамічний у часі вплив на мережу, спричинюючи аномальні явища;
- можливість графічного відображення змін кількісних характеристик за певний проміжок часу.

• оцінювання відповідності параметрів аномалій (неіснуючий номер, велика тривалість виклику тощо) до характерних для даного типу значень.
• оцінювання аномалій на ступінь імовірності порушення для визначення пріоритету реагування.
• забезпечення інформування про виявлені відхилення та події.
• забезпечення розроблення зручного інтерфейсу оператора.



Структура підсистеми захисту проти порушень (FMS)

Формування профілю об'єкта

Щоб оцінити кількісні характеристики об'єкта та динаміки змін у часі пропонується використовувати метод експонентних середніх значень із різними коефіцієнтами згладжування:

$$Q_t = (1-k)Q_{t-\Delta t} + kq_{\Delta t}, \quad (1)$$

де Q — експонентне середнє значення; q — новий вимір; k — коефіцієнт згладжування; Δt — інтервал між вимірюваннями;

У формулі (1) використовується постійний інтервал вимірювань. Корекція профілю під час кожного виклику складна, оскільки в цьому разі коефіцієнт згладжування є складною експонентною функцією від інтервалу вимірювання. Однак особливості параметрів дають змогу використовувати більш прості формули.

Оптимальна кількість середніх значень і величин коефіцієнтів згладжування для кожного параметра можуть бути здобуті дослідним шляхом. Для початку передбачається використовувати для кожного параметра три значення з коефіцієнтами k = 0,3; 0,05 і 0,005 з орієнтацією на добовий інтервал вимірювань.

Для всіх використовуваних далі параметрів і коефіцієнтів подано значення, які можна застосовувати в процесі розроблення, але в разі одержання практичних результатів ці значення можуть бути змінені оператором. Крім того, використання деяких параметрів профілю й розрахунків аномальності може виявитися неможливим або недоцільним, а інші потрібно буде додати.

Параметри профілю об'єкта

1. **Трафік** оцінюється як середньодобова кількість секунд з'єднань:

$$Q_t = \left(1 - k\frac{\Delta t}{86400}\right)Q_{t-\Delta t} + kT, \text{ якщо } \Delta t < 86400, \quad (2)$$

і

$$Q_t = (1-k)Q_{t-\Delta t} + kT\frac{86400}{\Delta t}, \text{ якщо } \Delta t \geq 86400, \quad (3)$$

де T — тривалість з'єднань, с; Δt — час між закінченнями (початками) попереднього і нового виклику, с.

Для аналізу передбачаються такі типи трафіку:
• вихідний місцевий
• вихідний міжміський
• вихідний міжнародний
• вхідний.

2. **Інтенсивність потоку викликів** оцінюється як середньодобова кількість спроб з'єднань:

$$Q_t = \left(1 - k\frac{\Delta t}{86400}\right)Q_{t-\Delta t} + kT, \text{ якщо } \Delta t < 86400, \quad (4)$$

і

$$Q_t = (1-k)Q_{t-\Delta t} + kT\frac{86400}{\Delta t}, \text{ якщо } \Delta t \geq 86400, \quad (5)$$

де T — тривалість з'єднань, с; Δt — час закінченнями (початками) попереднього й нового виклику, с.

Передбачається оцінювання інтенсивності потоку таких викликів:

- вхідних
- вихідних
- ефективних.

3. **Розподіл трафіку за типом часу** оцінюється як середньодобова кількість секунд з'єднань для робочого часу:

- робочий час — 1-й–5-й день тижня з 8^{30} до 17^{30};
- не робочий час — 1-й–5-й день тижня з 0^{00} до 8^{30} і з 17^{30} до 24^{00};
- 6-й–7-й день тижня з 0^{00} до 24^{00}.

4. **Розподіл трафіку за часом доби** оцінюється як середньодобова кількість секунд з'єднань у денний період.

- денний час із 7^{00} до 24^{00};
- нічний час із 0^{00} до 7^{00}.

5. **Сигнальний трафік** оцінюється як середня кількість байтів сигнальної інформації на один виклик:

$$Q_t = (1-k)Q_{t-\Delta t} + kB, \quad (6)$$

де B — кількість байтів сигнальної інформації у виклику.

6. **Нестабільність стійких мережних параметрів об'єкта** оцінюється за їхньою зміною від виклику до виклику. Для всіх параметрів можливе використання однієї характеристики.

Для кожного виклику маємо:

$$Q_t = LQ_{n-1} + \Sigma hi, \quad (7)$$

де h_i — рівні інкременту для параметрів, значення яких відрізняються в попередніх і наступних викликах; L — коефіцієнт, що враховує застарілу інформацію, $L = 0{,}9$.

Інші значення параметрів (якщо є в CDR):

- доступ (ISDN, non ISDN) $h = 10$;
- категорія абонента, що викликає $h = 5$;
- наявність або відсутність взаємодії сигналізацій під час встановлення з'єднання $h = 8$;
- неприпустима локалізація абонента, що викликає (відповідність адреси припустимому шаблону) $h = 200$;
- неприпустима категорія абонента, що викликає $h = 100$.

Необхідно передбачити можливість розширення й зміни подібних параметрів у майбутньому, а також використання різних характеристик для різних груп параметрів.

Додаткові коефіцієнти:

- постійний додатковий коефіцієнт, що дозволяє знижувати або підвищувати чутливість до аномалій під час оцінювання. Може змінюватися тільки оператором;
- тимчасовий додатковий коефіцієнт, що дозволяє знижувати або підвищувати чутливість до аномалій при оцінці. Може змінюватися тільки оператором, але згодом автоматично прагнути до нормального значення.

Після кожного виклику тимчасовий додатковий коефіцієнт визначається за формулою

$$K2_t = (1-k)K2_{t-\Delta t} + kK2_{norm}, \quad (8)$$

де Δt — час між закінченнями (початками) попереднього й наступного викликів у секундах; $kK2_{norm}$ — нормальне значення; k — коефіцієнт згладжування, $k = 0{,}05$.

Нормальні значення для додаткових коефіцієнтів: $K1_{norm} = 100$, $K2_{norm} = 100$.

Запис про профіль об'єкта

$Q1(0.3)$ — трафік вихідний місцевий;
$Q1(0.05)$ — трафік вихідний місцевий;
$Q1(0.005)$ — трафік вихідний місцевий;
$Q1(0.3)$ — трафік вихідний міжміський;
$Q1(0.05)$ — трафік вихідний міжміський;
$Q1(0.005)$ — трафік вихідний міжміський;

$Q1(0.3)$ — трафік вихідний міжнародний;
$Q1(0.05)$ — трафік вихідний міжнародний;
$Q1(0.005)$ — трафік вихідний міжнародний;
$Q1(0.3)$ — трафік вихідний;
$Q1(0.05)$ — трафік вихідний;
$Q1(0.005)$ — трафік вихідний;
$Q1(0.3)$ — інтенсивність вихідного потоку викликів;
$Q1(0.05)$ — інтенсивність вихідного потоку викликів;
$Q1(0.005)$ — інтенсивність вихідного потоку викликів;
$Q1(0.3)$ — інтенсивність вхідного потоку викликів;
$Q1(0.05)$ — інтенсивність вхідного потоку викликів;
$Q1(0.005)$ — інтенсивність вхідного потоку викликів;
$Q1(0.3)$ — інтенсивність ефективного потоку викликів;
$Q1(0.05)$ — інтенсивність ефективного потоку викликів;
$Q1(0.005)$ — інтенсивність ефективного потоку викликів;
$Q1(0.3)$ — розподіл трафіку за типом часу;
$Q1(0.05)$ — розподіл трафіку за типом часу;
$Q1(0.005)$ — розподіл трафіку за типом часу;
$Q1(0.3)$ — розподіл трафіку за часом доби;
$Q1(0.05)$ — розподіл трафіку за часом доби;
$Q1(0.005)$ — розподіл трафіку за часом доби;
$Q1(0.3)$ — середній сигнальний трафік;
$Q1(0.05)$ — середній сигнальний трафік;
$Q1(0.005)$ — середній сигнальний трафік;
W — нестабільність параметрів мереж;
P_i — параметри мережі;
T — час останнього виклику;
$K1$ — постійний додатковий коефіцієнт;
$K2$ — тимчасовий додатковий коефіцієнт.

У процесі створення об'єкта у поле T заноситься час початку спостереження, у поле $K2$ — знижене значення для стабілізації характеристик, в інші поля — значення, прийняті за замовчуванням.

Оцінювання аномального поводження об'єкта

Аномальність у поводженні об'єкта оцінюється за загальним рейтингом, як середнє визначеної аномалії з урахуванням додаткових коефіцієнтів:

$$A_{pr} = \frac{\left(\sum A\right) \cdot K1 \cdot K2}{\left(\sum C\right) \cdot K1_{norm} \cdot K2_{norm}}. \tag{9}$$

1. Визначення аномалій.

Під час визначення аномалій використовуються загальні для всіх об'єктів коефіцієнти та параметри:

- C — ваговий коефіцієнт, враховує вплив кожної аномалії на загальний рейтинг (табл. 1);
- m — параметр, що компенсує високу невизначеність у профілях об'єктів із низьким трафіком (табл. 2).

Трафік ($A1$, $A2$, $A3$, $A4$):

$$A(0,3) = C(0,3) \cdot \frac{|Q(0,3) - Q(0,05)}{Q(0,05) + m}, \quad A(0,05) = C(0,05) \frac{Q(0,05) - Q(0,005)}{Q(0,05) + m}. \tag{10}$$

Таблиця 1

Ваговий коефіцієнт, що враховує вплив кожної аномалії на загальний рейтинг

$C1(0.3)$	$C1(0.05)$	$C2(0.3)$	$C2(0.05)$	$CC3(0.3)$	$C3(0.05)$	$C4(0.3)$	$C4(0.05)$
1	3	20	60	100	300	1	3

Таблиця 2

Параметр, що компенсує високу невизначеність у профілях об'єктів із низьким трафіком

$m1$	$m2$	$m3$	$m4$
200	100	80	200

2. Тривалість з'єднання.
Вихідний трафік:

$$Q_{tout} = Q_1 + Q_2 + Q_3; \quad m_{tout} = m_1 + m_2 + m_3 . \tag{11}$$

Вихідні виклики:

$$A5(0,3) = C5(0,3) \cdot \left[\left| \frac{(Q_{tout}(0,3) + m_{tout}) \cdot (Q5(0,05) + m_5)}{(Q5(0,3) + m_5) \cdot (Q_{tout}(0,05) + m_{tout})} - 1 \right| \right]; \tag{12}$$

$$A5(0,05) = C5(0,05) \cdot \left[\left| \frac{(Q_{tout}(0,05) + m_{tout}) \cdot (Q5(0,005) + m_5)}{(Q5(0,05) + m_5) \cdot (Q_{tout}(0,005) + m_{tout})} - 1 \right| \right] \cdot \tag{13}$$

Вхідні виклики:

$$A6(0,3) = C6(0,3) \cdot \left[\left| \frac{(Q4(0,3) + m_4) \cdot (Q6(0,05) + m_6)}{(Q6(0,3) + m_6) \cdot (Q4(0,05) + m_4)} - 1 \right| \right]; \tag{14}$$

$$A6(0,05) = C6(0,05) \cdot \left[\left| \frac{(Q4(0,05) + m_4) \cdot (Q6(0,005) + m_6)}{(Q6(0,05) + m_6) \cdot (Q4(0,005) + m_4)} - 1 \right| \right] \cdot \tag{15}$$

Таблиця 3

Ваговий коефіцієнт та параметр, що компенсує високу невизначеність у профілях об'єктів із низьким трафіком

$C_5(0,3)$	$C_5(0,05)$	$C_6(0,3)$	$C_6(0,05)$	$m_5(0,3)$	$m_6(0,05)$
3	10	3	10	5	5

3. Ефективність.
Загальна кількість викликів:

$$Q_{nall} = Q5 + Q6; \quad m_{nall} = m_5 + m_6 ; \tag{16}$$

$$A7(0,3) = C7(0,3) \cdot \left[\left| \frac{Q7(0,3) + 0,45 \cdot m_{nall}}{Q_{nall}(0,3) + m_{nall}} - \frac{Q7(0,05) + 0,45 \cdot m_{nall}}{Q_{nall}(0,05) + m_{nall}} \right| \right]; \tag{17}$$

$$A7(0,05) = C7(0,05) \cdot \left[\left| \frac{Q7(0,05) + 0,45 \cdot m_{nall}}{Q_{nall}(0,05) + m_{nall}} - \frac{Q7(0,005) + 0,45 \cdot m_{nall}}{Q_{nall}(0,005) + m_{nall}} \right| \right]. \tag{18}$$

Таблиця 4

Ваговий коефіцієнт, що враховує вплив кожної аномалії на загальний рейтинг

$C_7(0,3)$	$C_7(0,05)$
3	10

4. Розподіл за типом часу.
Загальний трафік:

$$Q_{tall} = Q_{tout} + Q4; \quad m_{tall} = m_{tout} + m_4 . \tag{19}$$

$$A8(0,3) = C8(0,3) \cdot \left[\left| \frac{Q_{tall}(0,3) - k_1(d,h) \cdot Q8(0,3)}{Q_{tall}(0,3) + m_{tall}} - \frac{Q_{tall}(0,05) - k_2(d) \cdot Q8(0,05)}{Q_{tall}(0,05) + m_{tall}} \right| \right], \tag{20}$$

де $k_1(d,h)$, $k_2(d)$ — коефіцієнти, які враховують помилку експонентного усереднення (d — день тижня, h — година).

Таблиця 5

Коефіцієнти, які враховують помилку експонентного усереднення

d	1	2	3	4	5	6	7
$k_2(d)$	1,031	1,008	0,988	0,970	0,952	1,003	1,055

$$A8(0,05) = C8(0,05) \cdot \left[\left| \frac{Q_{tall}(0,05) - k_2(d) \cdot Q8(0,05)}{Q_{tall}(0,05) + m_{tall}} - \frac{Q_{tall}(0,005) - Q8(0,005)}{Q_{tall}(0,005) + m_{tall}} \right| \right]. \tag{21}$$

Таблиця 6

Ваговий коефіцієнт, що враховує вплив кожної аномалії на загальний рейтинг

$C8(0,3)$	$C8(0,05)$
5	15

5. Розподіл за часом доби.

$$A9(0,3)=C9(0,3)\cdot\left[\left|\frac{Q_{tall}(0,3)-k_3(h)\cdot Q9(0,3)}{Q_{tall}(0,3)+m_{tall}}-\frac{Q_{tall}(0,05)-Q9(0,05)}{Q_{tall}(0,05)+m_{tall}}\right|\right], \quad (22)$$

$$A9(0,05)=C9(0,05)\cdot\left[\left|\frac{Q_{tall}(0,05)-Q9(0,05)}{Q_{tall}(0,05)+m_{tall}}-\frac{Q_{tall}(0,005)-Q9(0,005)}{Q_{tall}(0,005)+m_{tall}}\right|\right], \quad (23)$$

де $k_3(h)$ — коефіцієнт, що враховує помилку експонентного усереднення (h — година).

Таблиця 7

Коефіцієнт, що враховує помилку експонентного усереднення

h	0	1	2	3	4	5	6	7	8	9	10	11
$k_3(h)$	0,9709	0,9832	0,9956	1,0082	1,0210	1,0339	1,0470	1,0408	1,0347	1,0288	1.,0230	1,0173
h	12	13	14	15	16	17	18	19	20	21	22	23
$k_3(h)$	1,0118	1,0064	1,0012	0,9960	0,9910	0,9861	0,9813	0,9766	0,9720	0,9675	0,9630	0,9587

Таблиця 8

Ваговий коефіцієнт, що враховує вплив кожної аномалії на загальний рейтинг

$C_9(0,3)$	$C_9(0,05)$
8	24

6. Сигнальний трафік.

$$A10(0,3)=C10(0,3)\cdot\left[\left|\frac{Q10(0,3)}{Q_{nall}(0,3)+m_{nall}}-\frac{Q10(0,05)}{Q_{nall}(0,05)+m_{nall}}\right|\right]; \quad (24)$$

$$A10(0,05)=C10(0,05)\cdot\left[\left|\frac{Q10(0,05)}{Q_{nall}(0,05)+m_{nall}}-\frac{Q10(0,005)}{Q_{nall}(0,005)+m_{nall}}\right|\right]. \quad (25)$$

Таблиця 9

Ваговий коефіцієнт, що враховує вплив кожної аномалії на загальний рейтинг

$C10(0,3)$	$C10(0,05)$
20	60

7. Стійкі параметри мережі.

$$A11 = \mathrm{W}. \quad (26)$$

Подальшій обробці можуть піддаватися не всі об'єкти, а тільки об'єкти з найвищим загальним рейтингом аномальності. Достатньо обробляти близько 1% від загальної кількості.

Оцінювання ймовірності порушення

Крім високого рівня аномальності профілю об'єкта, додатковими факторами, що підвищують можливість виявлення шахрайства під час оцінювання є такі:

- кореляція подій аномальних об'єктів — збіг унікальних адрес у записах викликів об'єктів за останній час (2-3 доби);
- відповідність профілю об'єкта відомого випадку порушення, збіг специфічної для цього відомого випадку інформації про виклик (напрямок, адресація) за останній час;
- невідповідність профілю об'єкта типовому профілю абонентського обліку. Категорія користувача: РАВХ, група абонентських ліній, установа, квартира, таксофон, доступ в інтернет, абонентська категорія, абонентський доступ і т.д. (Можливо тільки за наявності доступу до бази абонентського обліку, не обов'язково на перших етапах розроблення, однак необхідно передбачити таку можливість у майбутньому).

Визначення ймовірності порушення:

$$P=\max\left(\frac{A}{A+a}\max(P_{known})P_{subbase}\right), \quad (27)$$

де $\frac{A}{A+a}$ — імовірність порушення, певна за аномальністю поводження; a — аномальність при 50% імовірності. Значення а може бути здобуто дослідним шляхом.

Спочатку можна використовувати a =20.

$$A = A_{pr} + \sum A_{cor\,pr}, \tag{28}$$

де $A_{cor\,pr}$ — аномальність об'єкта, в якого спостерігається кореляція у викликах (у процесі перевірки необхідно виключати збіг по популярних адресах: спецслужби, серійні модемні пули тощо), якщо кореляція не визначена, то $A_{cor\,pr} = 0$; $P_{subbase}$ — імовірність шахрайства, що оцінена за невідповідністю профілю об'єкта типовому профілю у відповідність абонентському обліку; P_{known} — імовірність відомого типу порушення (визначається для кожного відомого типу).

Методика визначення ймовірності відомого типу порушення може бути також побудована на відповідності характерних аномалій у профілі спостережуваного об'єкта і профілю об'єкта, що порушує на момент виявлення, а також кореляції у викликах за адресами або префіксами.

Більш точно методику можна визначити тільки після нагромадження достатньої кількості дослідних результатів.

Оцінювання ступеня небезпеки шахрайства

Оцінювання ступеня небезпеки необхідна для випадків, які потребують першочергового втручання. Його можна розглянути як дію ймовірності порушення на збиток або недоотриманий дохід:

$$\Delta Q(0,3) = |\, Q(0,3) - Q(0,05)\,|; \tag{29}$$

$$\Delta Q(0,05) = |\, Q(0,05) - Q(0,005)\,|; \tag{30}$$

$$D = P\cdot(\Delta Q1(0,3) + k_2\cdot\Delta Q2(0,3) + k_3\cdot\Delta Q3(0,3) + L\cdot\Delta Q1(0,05) + k_2\cdot\Delta Q2(0,05) + k_3\cdot\Delta Q3(0,05)), \tag{31}$$

де k_2, k_3 — коефіцієнти, що враховують середню різницю в тарифах.

Таблиця 10

Коефіцієнти, що враховують середню різницю в тарифах

k_2	k_2	L
15	250	3

Деякі особливості функціонування системи

1. Створення профілів об'єктів.

Для кожної групи з'єднувальних ліній і для кожного напрямку заняття каналу описується перелік припустимих адрес вихідної сторони, перелік неконтрольованих адрес вихідної сторони, списки об'єктів, які мають більш ніж одну адресу у відповідному списку адрес. Якщо під час оброблення виклику запис інформації про профіль об'єкта не знайдено, він має бути згенерований автоматично.

2. Формування профілю.

Якщо відбулася втрата інформації про виклики за будь-який період, для запобігання збоїв у формуванні інформації про профілі об'єктів необхідно перевірити ще раз усі об'єкти, використовуючи нульові значення трафіку на початок періоду й відновити інформацію в профілях на момент закінчення.

ВИСНОВКИ

Таким чином, є доцільним упровадження інформаційної підсистеми FMS, яка буде ґрунтуватись на даних, отриманих із систем контролю мережі СКС7, цифрових АТС тощо, здійснювати аналіз трафіку, інформувати про ситуації, що є підозрілими та потребують подальшого детального вивчення відповідними програмними засобами.

Список використаної літератури

*1. **Ружинский В. Г., Аношков В. М.** Організація контролю, вимірів та управління мережі спільноканальної сигналізації №7 ВАТ «Укртелеком» // 2-а міжнародна конференція «Проблеми управління мережами та послугами телекомунікацій в умовах конкурентного ринку» // Вісник УБЕНТЗ: 2003, №2. С. 44–48.*

*2. **Ружинський В. Г.** Визначення інтенсивності сигнального навантаження мережі спільноканальної сигналізації № 7 при взаємодії різних телекомунікаційних мереж // Зв'язок. 2006. №4(64). С. 20–22.*

*3. **Ружинський В. Г.** Построение центра контроля, измерений и управления сети ОКС-7 Укртелекома // «Телеком-2003» 6-я международная научно-техническая конференция.*

V. G. Ruzhynsky, V. F. Zaika, O. M. Marchuk

IMPLEMENTATION OF SYSTEMS OF PROTECTION AGAINST VIOLATIONS (FRAUD MANAGEMENT SYSTEM) A GUARANTEE OF THE FINANCIAL STABILITY OF OPERATORS

An analysis of the types of traffic-related frauds on telecommunication networks was carried out. Violations on telecommunication networks are the actions of subscribers, telecommunications operators or third parties who are directed to receive telecommunication services at a lower rate or without payment. CFCA experts count about 200 types of violations on telecommunication networks. The most common violations on the part of operators are the unauthorized termination of incoming long-distance and international traffic to the public network under the guise of a local one, without appropriate contracts. Abuses lead to significant loss of income. The most common among subscribers are third-party connection to the subscriber line in order to receive free telematics services of the "900" service, making long-term international calls, and organizing unauthorized meeting points. On the part of third parties, it is a violation to use hardware and software to receive international traffic from the Internet and complete it on a public telecommunications network under the guise of a local one, which leads to interference in the operation of communication means, substitution of call information. The fight against misuse of telecommunication networks relies to a large extent on the analysis of data about services and data contained in settlement systems with subscribers and operators. Detection of suspicious actions of subscribers and their analysis is the main operating principle of modern Fraud Management System (FMS) protection systems. The key criteria for the effectiveness of FMS are the speed of work, the flexibility of setting up algorithms that ensure the detection and analysis of incidents, and the availability of standardized interfaces for integration with billing platforms. Practical recommendations for creating protection systems against Fraud Management System (FMS) violations are provided.

Keywords: object profile; call flow intensity; traffic; anomalies; efficiency; network parameters.