функціонування ТМЗК потребує випереджувального розроблення нормативних документів, щоб отримати необхідну якість надання телекомунікаційних послуг споживачам.

Література.

1. ДСТУ 2624-94 Системи сигналізації. Терміни та визначення;

2. Про межі та порядок впровадження сигналізації № 7 на мережі телефонного зв'язку загального користування України // КНД 45-109-98**.**

3. Спільноканальна сигналізація № 7. Національна версія України. Правила використання у телефонній мережі загального користування. Версія 3.0 (з чинними змінами), затверджено наказом Міністерства транспорту та зв'язку України від 13.12.2007 № 1164.

УДК 621.391.2

Ружинський В.Г., к.т.н. *(ПАТ «Укртелеком»)*

ДЕЯКІ АСПЕКТИ ВПРОВАДЖЕННЯ СИСТЕМ ЗАХИСТУ ПРОТИ ПОРУШЕНЬ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ ОПЕРАТОРІВ

Ружинський В.Г. Деякі аспекти впровадження систем захисту проти порушень в телекомунікаційних мережах операторів. Проведено аналіз видів шахрайств в телекомунікаційних мережах, пов'язаних з трафіком. Надано рекомендації щодо створення систем захисту проти порушень Fraud Managment System (FMS).

Ключові слова: ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА, СИСТЕМА ЗАХИСТУ, FMS, АСОЦІАЦІЯ ПО КОНТРОЛЮ ЗА ПОРУШЕННЯМИ, ТРАФІК

Ружинский В.Г. Некоторые аспекты внедрения систем защиты против нарушений в телекоммуникационных сетях операторов. Проведен анализ видов мошенничеств в телекоммуникационных сетях, связанных с траффиком. Предоставлены рекомендации относительно создания систем защиты против нарушений Fraud Managment System (FMS).

Ключевые слова: ТЕЛЕКОММУНИКАЦИОННАЯ СЕТЬ, СИСТЕМА ЗАЩИТЫ, FMS, АССОЦИАЦИЯ ПО КОНТРОЛЮ ЗА НАРУШЕНИЯМИ, ТРАФФИК

Ruzhynskyi V.H. Some aspects of creation fraud management systems in the telecommunication networks of operators. Analysis of frauds was provided on telecommunication networks. Practical recommendations of creation fraud management systems (FMS) were introduced.

Keywords: TELECOMMUNICATION NETWORK, FRAUD MANAGMENT SYSTEM, FMS, COMMUNICATIONS FRAUD CONTROL ASSOCIATION, TRAFFIC

Вступ. Оператори телекомунікацій вирішують проблему, яка безпосередньо пов'язана з фінансовим станом компаній, а саме: впровадження систем щодо протидії шахрайств пов'язаних з трафіком.

Згідно з останніми дослідженнями всесвітньої Асоціації по контролю за порушеннями в телекомунікаційних мережах (Communications Fraud Control Association, CFCA), в 2005 році втрати від порушень в телекомунікаційній сфері склали 54,4-60 млдр. дол. Це приблизно на 52% більше цифри, одержаної в дослідженнях CFCA трьохрічної давності. Порушення в телекомунікаційних мережах – це дії абонентів, операторів телекомунікацій чи сторонніх осіб. Експерти CFCA нараховують близько 200 видів порушень в телекомунікаційних мережах. Найбільш поширеними є: *зі сторони операторів* – несанкціоноване, без відповідних договорів, завершення вхідного міжміського та міжнародного трафіку в мережу загального користування під виглядом місцевого; *зі сторони абонентів* – стороннє підключення до абонентської лінії з метою безоплатного одержання телематичних послуг служби «900», здійснення довготривалих міжнародних розмов, організація несанкціонованих переговорних пунктів; *від сторонніх осіб* – використання апаратно-програмного

забезпечення для отримання міжнародного трафіку з мережі Інтернет та завершення його в ТМЗК під виглядом місцевого, що призводить до втручання в роботу засобів зв'язку, підміни інформації про виклик.

Система захисту FMS. Боротьба із зловживаннями в телекомунікаційних мережах значною мірою опирається на аналіз інформації 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, аналіз інцидентів та наявність стандартизованих інтерфейсів для інтеграції з платформами білінгу.

Як правило, робота механізмів виявлення порушень заснована на обробці детальних записів про здійснені виклики CDR (Call Detail Record). Система протидії шахрайству вишукує в них невідповідності певним умовам або не відповідності заданому шаблону, характеристики поведінки абонента. Коли модуль виявлення знаходить одну з аномалій, він генерує повідомлення з попередженням.

До типових перевірок по умові систем FMS можна віднести 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 із закордону; *можливість* організації додаткових перевірок, з легкою зміною правил, які використовуються при аналізі за допомогою редактора правил.

На рис. 1 наведено варіант структури FMS, основою якої є генерація та корекція профілів об'єктів контролю в автоматичному режимі.

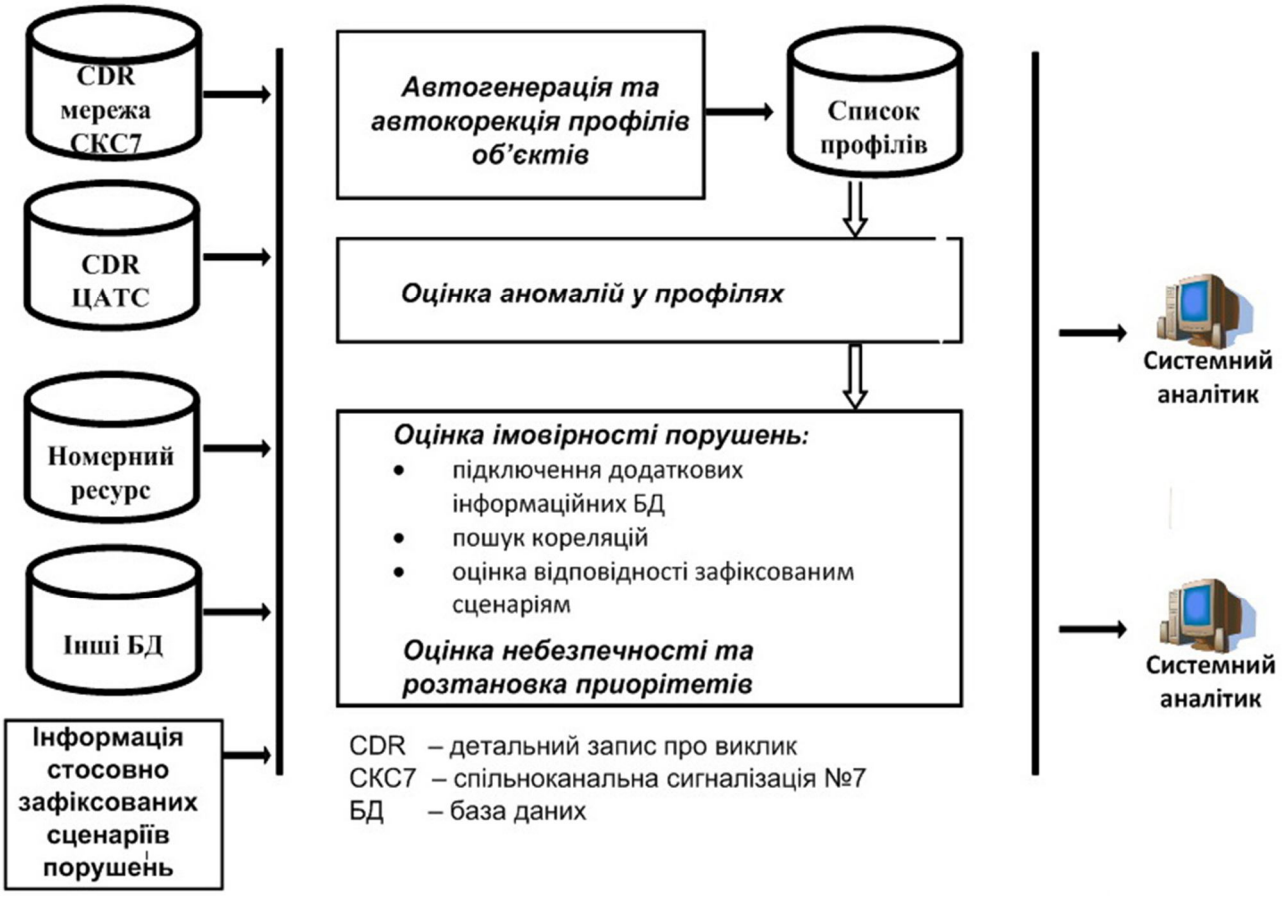

Рис. 1. Структура підсистеми захисту проти порушень (FMS)

Основними функціональними завданнями підсистеми є: *автоматичне* налагодження профілю елементів телекомунікаційної мережі; *створення* алгоритму виявлення, який ґрунтується на особливостях порушень, що створюють динамічний у часі вплив на мережу, викликаючи аномальні явища; *забезпечення* автоматичного аналізу, класифікації даних, пошуку відхилень поведінки елементів телекомунікаційної мережі від звичайного профілю; *оцінка* відповідності параметрів аномалій (неіснуючий номер, велика тривалість виклику тощо) до характерних для даного типу значень; *оцінка* аномалій на ступінь імовірності порушення для визначення пріоритету реагування; *забезпечення* формування звітів про виявленні відхилення та події.

Формування профілю об'єкта. Для формування профілю об'єкта оцінку кількісних характеристик об'єкта та динаміки змін у часі пропонується використовувати методом експонентних середніх значень з різними коефіцієнтами згладжування [1, 2]**:**

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

де: Q – експонентне середнє значення; q – новий вимір; k – коефіцієнт згладжування; Δt – інтервал між вимірами.

Використовується постійний інтервал вимірів. Корекція профілю при кожному виклику складна, оскільки в цьому випадку коефіцієнт згладжування є складною експонентною функцією від інтервалу виміру. Оптимальна кількість середніх значень і величин коефіцієнтів згладжування для кожного параметра можуть бути отримані дослідним шляхом.

Основні параметри профілю об'єкта:

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

$$Q_t = (1-k\frac{\Delta t}{86400})Q_{t-\Delta t} + kT, \text{ якщо } \Delta t < 86400; \text{ і}$$

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

де T – тривалість з'єднань у секундах; Δt – час між закінченнями (початками) попереднього і нового виклику в секундах.

Для аналізу передбачаються такі типи трафіку: вихідний *місцевий*; вихідний *міжміський*; вихідний *міжнародний*.

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

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

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

де T – тривалість з'єднань у секундах; Δt – час закінченнями(початками) попереднього й нового виклику в секундах.

Передбачається також оцінка інтенсивності потоку викликів: вхідних, вихідних, ефективних.

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

- робочий час – 1-й…5-й день тижня з 8 год. 30 хв. до 17 год. 30 хв.;
- неробочий час – 1-й…5-й день тижня з 00 год. до 8 год. 30 хв. та з 17 год. 30 хв. до 24 год.;
- 6-й і 7-й день тижня з 00 год. до 24 год.

4. ***Сигнальний трафік*** – оцінюється як середня кількість байт сигнальних одиниць на один виклик: $Q_t = (1-k)Q_{t-\Delta t} + kB$, де B – кількість байт сигнальної інформації у виклику.

Висновки. Таким чином, є доцільним впровадження інформаційної підсистеми FMS, яка буде спиратись на дані отримані з систем контролю мережі СКС7, цифрових АТС

тощо [2, 3]. Призначення такої інформаційної підсистеми – здійснювати аналіз трафіку, інформувати про ситуації, що є підозрілими та потребують подальшого детального вивчення відповідними програмними засобами.

Література

1. Ружинский В.Г. Організація контролю, вимірів та управління мережі спільноканальної сигналізації №7 ВАТ «Укртелеком» / В.Г. Ружинский , В.М. Аношков // 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 / В. Г. Ружинський // Зв'язок. – 2006. – №4(64). – С. 20-22.

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

УДК 621.39

Максимов В.В., к.т.н.; **Самойлюк А.О.,** магістрант
(Інститут телекомунікаційних систем Національного технічного унів-ту України «КПІ»)

ДОСЛІДЖЕННЯ ЧАСУ УВІМКНЕННЯ IP ІНТЕРФЕЙСА

Максимов В.В., Самойлюк А.О. Дослідження часу увімкнення IP інтерфейса. В роботі досліджено процеси, що відбуваються під час увімкнення IP інтерфейса. Визначено та досліджено компоненти, з яких складається час включення IP інтерфейса.

Ключові слова: IP ІНТЕРФЕЙС, ПРОТОКОЛ ARP, ЗАТРИМКА В КАНАЛІ, СЛУЖБОВА ІНФОРМАЦІЯ, GNS3

Максимов В.В., Самойлюк А.А. Исследование времени включения IP интерфейса. В работе исследованы процессы, происходящие при включении IP интерфейса. Определены и исследованы компоненты, из которых состоит время включения IP интерфейса.

Ключевые слова: IP ИНТЕРФЕЙС, ПРОТОКОЛ ARP, ЗАДЕРЖКА В КАНАЛЕ, СЛУЖЕБНАЯ ИНФОРМАЦИЯ, GNS3

Maksymov V.V., Samoiliuk A.O. Investigate of enabling time of IP interface. The processes, which occur during IP interface enabling, are investigated in the article. Components of IP interface enabling time are dedicated and investigated.

Keywords: IP INTERFACE, ARP PROTOCOL, CHANNEL DELAY, SERVICE INFORMATION, GNS3

Постановка задачі. Під час проведення різноманітних досліджень в галузі IP-мереж виникає необхідність проведення вимірів часу спрацювання того чи іншого процесу, наприклад, часу встановлення TCP-з'єднання або оновлення таблиць маршрутизації будь-якого іншого протоколу. В [1], наприклад, пропонується аналітичний вираз часу збіжності протоколу маршрутизації OSPF, в [2] детально описані процеси, що впливають на час збіжності даного протоколу, в [3] досліджується час збіжності протоколу OSPF при обриві лінії зв'язку. Проте при дослідженні часу збіжності протоколу OSPF у випадку включення нового маршрутизатора, слід врахувати час увімкнення його IP інтерфейса, значення якого не відоме і потребує виміру.

Розглянемо процеси, які відбуваються під час увімкнення IP інтерфейса.

Під часом включення IP інтерфейса будемо розуміти час від подачі живлення на IP інтерфейс до моменту його дієздатності. Ознакою дієздатності IP інтерфейса можна вважати початок надходження ICMP луна-відповідей на луна-запити [4].