



Инженерные и математические модели борьбы с мошенничеством

УДК 621.395:004.8

Б.С. ГОЛЬДШТЕЙН, старший научный сотрудник ООО “НТЦ СевенТест” доктор технических наук, **В.Н. КОРОЛЕВ**, директор по развитию, **Б.Я. РОЗЕНЦВАЙГ**, генеральный директор

Инженерные и математические модели борьбы с мошенничеством *Engineering and mathematical models of fraud management*

В данной статье представлен обзор современных инженерных и математических подходов к проектированию и реализации систем борьбы с мошенничеством в современных телекоммуникационных сетях. Описывается эволюция методов обнаружения “фрода” от ранних систем ТфОП до эпохи Beyond 5G, учитывая растущую сложность и разнообразие сценариев “фрода”, таких как подмена CLI, мошенничество с SIM-боксом, контроль ложных ответов, схемы несанкционированной маршрутизации и другие.

Приводится архитектура типичных решений системы и их интеграции с компонентами OSS/BSS. Рассматриваются различные математические модели, включая статистические методы, вероятностные модели и контролируемые методы машинного обучения, такие как логистическая регрессия, деревья решений и нейронные сети. Обсуждаются подходы к обнаружению аномалий и кластеризации в неуправляемых средах. Приводится сравнительный анализ нескольких ведущих платформ системы и рассматриваются будущие направления в борьбе с “фродом”.

This article offers an overview of modern engineering and mathematical methods used in designing and implementing Fraud Management Systems in today's telecommunication networks. It details the evolution of fraud-detection techniques from early PSTN-era methods to the Beyond 5G environment, marked by increased complexity and variety of fraud cases, including CLI spoofing, SIM-box fraud, False Answer Supervision, unauthorized routing schemes, and more.

The structure of typical Systems solutions and how they integrate with OSS/BSS components are explored. Several mathematical models are discussed, such as statistical methods, probabilistic models, and supervised machine learning techniques like logistic regression, decision trees, and neural networks. Approaches for anomaly detection and clustering in unsupervised settings are also covered. The article compares major Systems platforms and suggests future directions for fraud mitigation technology.

Ключевые слова: обнаружение мошенничества, гарантирование доходов, система борьбы с мошенничеством, xDR, OSS/BSS, обеспечение доходов, машинное обучение, анализ аномалий, 5G/6G.

Keywords: fraud detection, revenue assurance, fraud management systems, xDR, OSS/BSS, revenue protection, machine learning, anomaly detection, Beyond 5G.

Эволюция управления мошенничеством

Финансовые и репутационные потери, которые несут операторы связи и телекоммуникационная отрасль в целом из-за мошенничества, имеют долгую историю, восходящую к периоду телеграфных сетей еще до изобретения Александром Беллом телефона. В литературе самый известный случай телекоммуникационного мошенничества описан в знаменитом романе Александра Дюма середины XIX века, в котором граф Монте-Кристо смог отомстить барону Данглару, подменив на тран-

зитном участке передаваемую телеграмму. С тех пор прошло много лет, и за это время было придумано и использовано множество различных тактик мошенничества абонентами, операторами связи, недобросовестными конкурентами, похитителями данных кредитных карт, нелегальными распространителями спама и другими.

Важной подгруппой глобального отраслевого мошенничества являлось межоператорское мошенничество, примером которого может служить подмена идентификатора абонента. В этом случае оператор, генерирующий трафик, меняет пре-

фиксы ABC, выдавая междугородний (международный) трафик за местный, оператор, терминирующий трафик, теряет значительную часть доходов из-за разницы в тарифах на терминацию междугороднего (международного) и местного трафика.

Другим примером может служить незаконное завершение вызова по технологии FAS (False Answer Supervision), когда транзитный оператор, принимающий вызов, имитирует ответ абонента и получает деньги за якобы заверченный вызов, хотя на самом деле вызывающий абонент в этой ситуации не получает никаких услуг.

**Статью целиком читайте
в бумажной версии журнала**