***R. Sokolov**, Saint-Petersburg State University of Economics,*
Saint-Petersburg, Russia, rsok7@rambler.ru

Models of information risk management in conditional access systems

The paper describes principles of information risk management in conditional access systems (CAS). The purpose of models is to justify the economical choice of options for an information system to counter attacks, which in turn is a set of measures to counter attacks. Proposed three models of constrained optimization and one of unconstrained optimization system of protection against information attacks, which are a model of linear programming with binary variables.

Keywords: management models, communication channels, information risk management, conditional access systems, information risks, models for selecting information security, information attacks, risk events.

I. Introduction

The article reviews the principles of construction and development of economic and mathematical models of information risk management using the example of conditional access systems.

The Conditional Access System of the communications enterprise is a software and hardware complex designed to restrict access to paid encoded digital satellite, cable, terrestrial television and radio channels.

The principle structural scheme [1] of conditional access systems (CAS) is presented in fig. 1.

As it follows from the presented figure (see Figure 1), the information flow of the content owner before reaching the subscribers passes through the CAS, the task of which is to provide information to subscribers only if the conditions specified in the contracts for functionality are complied with in accordance with the payment.

There is an ESS (Encryption and Scrambling System) in the path of the information stream that uses the scrambling keys generated by the KMS (Key Management System) module. For the encrypted information flow enters the Subscriber Authorization System (SAS), which provides subscriber authentication and protection of decoders and smart cards from unauthorized access.

Directly at subscribers there is a security module for the hardware — software decoder SRS (Secured Receiver System) which provides decoding of an information stream arriving in receiving equipment of the subscriber.

Currently, there are dozens of variants of CAS, each of them serves tens and hundreds of thousands of subscribers. CAS's are divided into closed systems which used corporate encryption standards and systems with a single scrambling algorithm, based on the DVB (Digital Video Broadcasting) standard. The most popular CAS's used in Russia are the following:

- DRECrypt (developed by LLC «Tsifra», Russia). The conditional access system has been used in Russia since 2004. It is one of the leaders on the CAS market and has more than 15 million subscribers. Implemented by more than 50 pay-TV operators in Russia and CIS countries. Supports DVB standard.