**Литература**

1. Криптология / Ю.С. Харин [и др.]. – Минск: БГУ, 2013. – 512 с.

2. Палуха, В.Ю. Статистические тесты на основе оценок энтропии для проверки гипотез о равномерном распределении случайной последовательности // Вес. Нац. акад. навук Беларуси. Сер. фіз.-мат. навук. – 2017. – №1. – С. 79–88.

3. Мальцев, М.В. Малопараметрические марковские модели в задачах защиты информации / М.В. Мальцев, Ю.С. Харин // Электроника ИНФО. – 2013.– С. 202–207.

## СРЕДСТВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОЛОСОВОГО ТРАКТА

М.Г. Матуть, В.А. Вишняков

Контроль телефонных переговоров остается одним из наиболее распространенных видов промышленного шпионажа и действий злоумышленников. Причины – низкий уровень затрат и риск реализации угроз, необязательность захода в контролируемое помещение, разнообразие способов и мест съема информации. В широком смысле можно выделить средства противодействия: физическая защита информации, включающие в себя постановщики заградительных помех, нейтрализаторы, фильтры и средства физического поиска каналов утечки информации; криптографическая защита информации.

Криптофон представляет собой смартфон с установленным специальным программным обеспечением. Современные криптофоны используют, в основном, алгоритмы шифрования AES и Twofish. В сфере IP-телефонии можно рассматривать варианты использования IPsec (Internet Protocol Security) на сетевом уровне, либо протоколы TLS (Transport Layer Security) и SRTP (Secure RTP) на транспортном уровне.

В качестве основы разрабатываемого программного средства был выбран проект с открытым исходным кодом – CSipSimple, который является бесплатным SIP-клиентом, работающим под ОС Android и распространяющимся по лицензии GNU GPL. Выбор CSipSimple обусловлен наличием в нем открытых реализаций протоколов SIP over TLS, SRTP и ZRTP; поддержка различных кодеков (Speex, G.711, GSM-FR, G.729, G.722 и другие) и возможность добавления новых, при помощи плагинов; наличие плагина для осуществления видеозвонков, одновременно может быть активно до 10 аккаунтов.

## АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СЕТЯХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

А.Р. Мацылевич

Автоматизация управления защитой информации в информационных сетях специального назначения (ИССН) позволит максимально исключить влияние так называемого «человеческого фактора», который является не только фактором, снижающим эффективность системы защиты информации в ИССН, но, в некоторых условиях, становится угрозой безопасности информации высокого потенциала.

Основными вопросами автоматизации управления защитой информации являются:

представление защиты информации как объекта управления (определение входных и выходных переменных, метрик пространства состояний, описание поведения защиты информации в пространстве ее состояний и другие);

постановка целей, определение методов их достижения, а также критериев управления защитой информации адекватных целям, задачам и условиям функционирования ИССН;

разработка порядка применения средств и систем автоматизированного управления защитой информации в ИССН;

разработка методов контроля эффективности и оптимизации управления защитой информации в ИССН с учетом специфики их функционирования.

В настоящее время уже существуют подходы для создания систем управления организационно-техническими процессами, к которым относится защита информации [1]. Одним из подходов в автоматизации управления защитой информации в ИССН является применение научно-методологического аппарата теории автоматического управления.