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.

О выявленных в ходе научных исследований по вопросам автоматизации управления защитой информации в ИССН некоторых проблемных вопросах и предлагаемых путях их решения ведется речь в докладе.

Литература

1. Интеллектуальные системы управления организационно-техническими системами / А.Н. Антамошин и [др.]; под ред. проф. А.А.Большакова. – М.: Горячая линия – Телеком, 2006. – 160 с.: ил.

ЗАЩИТА ИТКС ОТ УГРОЗ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

А.С. Мешков, В.П. Ширинский, И.Г. Некрашевич

Для современного этапа развития общества характерен непрерывный процесс информатизации. Сфера внедрения телекоммуникаций и вычислительных систем постоянно расширяется. В связи с этим важной задачей является обеспечение достаточной защищенности таких систем. При рассмотрении вопроса безопасности функционирования информационно-телекоммуникационной системы (ИТКС) определяющую роль играют угрозы, реализуемые посредством удаленного воздействия с объектом взаимодействия, или так называемые сетевые атаки. Большинство распределенных систем функционируют и проектируются с учетом использования в них технологии межсетевого взаимодействия, реализованной в Интернет. При этом ИТКС базируется на применении протоколов межсетевого воздействия TCP/IP. Поэтому в РТКС могут реализовываться большинство атак, характерных для Интернет.

Для оценки систем защищенности ИТКС в условиях воздействия на ее компоненты некоторого набора угроз необходимо перейти к категории риска. Риск – это сочетание величины ущерба и возможности реализации исхода, влекущего за собой такой ущерб.

Угрозы информационной безопасности имеют вероятный характер. Анализ возможных угроз и анализ рисков служит основой для выбора мер по защите ИТКС, которые должны быть осуществлены для снижения риска до приемлемого уровня.

Предполагаемая работа заключается в исследовании и разработке методики анализа информационных рисков и управления защищенностью ИТКС от угроз несанкционированного доступа к ее компонентам.

Литература

1. Бобов, М.Н. Протоколы аутентификации в сетях телекоммуникаций / М.Н. Бобов. – Мн.: БГУИР, 2004. – 26 с.

2. Мельников, Д.А. Информационные процессы в компьютерных сетях: протоколы, стандарты, интерфейсы, модели / Д.А. Мельников. – М.: Кудиц-образ, 1999. – 256 с.

3. Щербаков, А.Ю. Современная компьютерная безопасность: теоретические основы, практические аспекты / А.Ю. Щербаков. – М.: Книжный мир, 2009. – 351 с.

4. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах / В.Ф. Шаньгин. – М.: Форум, 2016. – 591 с.

ОБРАБОТКА ДАННЫХ ИДЕНТИФИКАЦИИ ПО СЕТЧАТКЕ ГЛАЗА

А.И. Митюхин, Р.П. Гришель

Изображение кровеносных сосудов глазного дна является биометрическим параметром индивидуального организма человека и может использоваться для решения задачи идентификации человека с помощью технической системы с особыми требованиями по надежности или в криминалистике. В сравнении с другими биометрическими параметрами, используемыми для идентификации личности (например, отпечатки пальцев – качество отпечатков зависит от возраста; распознавания по лицу – систему распознавания можно обмануть с помощью маскировки и пр.), достоинством распознавания по сетчатке глаза является постоянство биометрического параметра. Уникальное изображение отдельных фрагментов сосудистой сети глазного дна описывается совокупностью элементов (пикселями), представляющими эту сеть.