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.