**Сычев Владимир Михайлович Оценка возможностей предотвращения несанкционированного доступа к информационным системам розничных сетей**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

кандидат наук Сычев Владимир Михайлович

ВВЕДЕНИЕ

Глава 1. КОНЦЕПЦИЯ ОЦЕНКИ ВОЗМОЖНОСТЕЙ

ПРЕДОТВРАЩЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИОННЫМ СИСТЕМАМ

РОЗНИЧНЫХ СЕТЕЙ

1.1. Базовые понятия в проблематике оценки возможностей предотвращения несанкционированного доступа к информационным системам розничных сетей

1.2. Особенности оценки защищенности объектов информатизации при помощи существующего методического аппарата

1.3. Обоснование показателей для оценки возможностей предотвращения несанкционированного доступа к информационным системам розничных сетей

1.4. Задача оценки возможностей предотвращения

несанкционированного доступа к информационным системам 39 розничных сетей

Выводы по первой главе

Глава 2. ФУНКЦИОНАЛЬНЫЕ МОДЕЛИ УГРОЗ

НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИОННЫМ СИСТЕМАМ РОЗНИЧНЫХ СЕТЕЙ И ПРОЦЕССОВ ПРЕДОТВРАЩЕНИЯ ТАКОГО РОДА УГРОЗ .... 43 2.1. Методика построения функциональных моделей угроз несанкционированного доступа к информационным системам розничных сетей и процессов предотвращения такого рода угроз

2.2. Функциональная модель угроз несанкционированного доступа к

информационным системам розничных сетей

2.3. Особенности функционального представления процессов предотвращения угроз несанкционированного доступа к информационным системам розничных сетей

Выводы по второй главе

Глава 3. МАТЕМАТИЧЕСКИЕ МОДЕЛИ ПОКАЗАТЕЛЕЙ ДЛЯ ОЦЕНКИ ВОЗМОЖНОСТЕЙ ПРЕДОТВРАЩЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К

ИНФОРМАЦИОННЫМ СИСТЕМАМ РОЗНИЧНЫХ СЕТЕЙ

3.1. Структура математических моделей показателей для оценки возможностей предотвращения несанкционированного доступа к информационным системам розничных сетей

3.2. Математические модели временных характеристик угроз

Стр

20

несанкционированного доступа к информационным системам розничных сетей

3.3. Математические модели временных характеристик процессов предотвращения угроз несанкционированного доступа к информационным системам розничных сетей

3.4. Аналитическая модель показателя своевременности реализации процессов предотвращения несанкционированного доступа к информационным системам розничных сетей

3.5. Аналитическая модель показателя своевременности реализации информационных процессов в информационных системах розничных сетей

3.6. Аналитическая модель показателя технологической устойчивости информационных систем розничных сетей

Выводы по третьей главе

Глава 4. ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ПРЕДОТВРАЩЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИОННЫМ СИСТЕМАМ РОЗНИЧНЫХ СЕТЕЙ (НА ПРИМЕРЕ РОЗНИЧНОЙ СЕТИ ЛЕРУА МЕРЛЕН)

4.1. План проведения исследования возможностей предотвращения несанкционированного доступа к информационной системе розничной сети

4.2. Результаты вычислительного эксперимента по оценке возможностей предотвращения несанкционированного доступа к информационной системе розничной сети

Выводы по четвертой главе

Общие выводы и заключение

Список использованных источников

ПРИЛОЖЕНИЕ

Словарь используемых терминов, сокращений и обозначений

АП - абонентский пункт;

ИС - информационная система;

Маршрутизатор - (проф. жарг. роутер, от англ. router), устройство, специализирующееся на пересылке пакетов между сегментами компьютерной сети. В основу работы маршрутизатора положены правила маршрутизации, задаваемые соответствующими таблицами;

НСД - несанкционированный доступ;

ПО - программное обеспечение;

РС - розничная сеть;

Субъект доступа к ИС РС - лицо, обладающее полномочиями доступа на территорию расположения ИС РС;

Субъект доступа к информации ИС РС - лицо, обладающее полномочиями доступа к информации ИС РС;

Хост (host) - сервер, уникально определённый на интерфейсах сервиса «клиент-сервер»;

ARP (Address Resolution Protocol) - протокол определения MAC-адреса по IP-адресу другого СВТ;

DNS (Domain Name System) - сервис получения информации о доменах компьютерной сети. Используется для получения IP-адреса на основании известного имени хоста, данных об обслуживающих узлах при формировании протоколов обмена информации в домене, а также для маршрутизации электронной почты;

ICMP (Internet Control Message Protocol) - протокол межсетевых сообщений, обеспечивающий функции управления обменом данными между отдельными сегментами компьютерной сети;

IP-адрес (Internet Protocol) - идентификатор СВТ, обеспечивающий его работу в компьютерной сети в соответствии с протоколом TCP/IP;

MAC-адрес (Media Access Control) - идентификатор, присваиваемый каждому активному СВТ или его интерфейсам в компьютерных сетях типа Ethernet;

TCP/IP (Transmission Control Protocol/Internet Protocol) - модель, описывающая способ передачи данных в компьютерной сети от источника информации к получателю.