



Разработка предложений по повышению защищенности сетей WiMax

<http://diplom-it.ru/product/razrabotka-predlozhenij-po-povysheniju-zashishennosti-setej-wimax/>

Содержание

Введение 3

1. Обзор угроз сети на основе стандарта IEEE 802.16x 4

1.1 Общие теоретические сведения 4

1.2 Безопасность сетей WiMax 10

1.3 Современное положение сетей WiMAX и прогнозы развития 13

1.4 Принципы построения сетей WiMAX 17

2. Описание сети «Орбита» 21

3. Обеспечение безопасности в протоколе IEEE 802.16 27

3.1 Стандарт IEEE 802.16. Краткая характеристика 27

3.1.1 Характеристики стандарта 802.16 28

3.1.2 Подуровень конвергенции 31

3.2 Сетевой уровень безопасности 36

3.2.1 Архитектура. 37

3.2.2 Шифрование пакетов данных 37

3.2.3 Протокол управления ключами. 38

3.2.4 Security Associations 39

3.2.5 Передача Ключей Шифрования пакетов с Данными. Обзор 43

3.3 Используемые алгоритмы шифрования. Общая характеристика 45

3.3.1 Симметричные алгоритмы 46

3.3.2 Алгоритмы с открытым ключом 49

3.3.3 Хэш-функции и дайджесты 51

3.4 Протокол DES 51

3.4.1 Описание DES 51

3.4.2 Надежное использование DES 54

3.4.3 Стойкость ключа DES 55

3.4.4 Надежность ключей DES 56

3.4.5 Triple DES 57

3.4.6 Алгоритм DESX 58

3.4.7 Разновидности DES 58

3.5 Формат сертификата открытого ключа 59

3.6 Протокол AES 66

3.7 SHA 71



3.8 Алгоритм криптографических преобразований в соответствии с ГОСТ 28147-89	75
3.8.1 Структурная схема алгоритма криптографического преобразования	75
3.8.2 Шифрование в режиме простой замены	79
3.8.3 Режим гаммирования	83
3.8.4 Режим гаммирования с обратной связью	86
3.8.5 Режим выработки имитовставки	89
4. Юридические аспекты использования средств защиты информации	91
5. Выработка предложений по защите информации, передаваемой в сети	96
5.1 Общие моменты	96
5.2 Внедрение PKI	102
5.2.1 Удостоверяющий центр	103
5.2.2 Регистрационный центр	106
5.2.3 Репозиторий сертификатов	106
5.2.4 Архив сертификатов	107
5.2.5 Конечные субъекты	108
5.2.6 Физическая топология	108
5.2.7 Проектирование и внедрение	109
5.3 Использование виртуальных сетей	112
Заключение	122
Список использованных источников	123