



Программные средства защиты информации от преднамеренных угроз в ЛВС под управлением WINDOWS

<http://diplom-it.ru/product/programmnye-sredstva-zashity-informacii-ot-prednamerennyh-ugroz-v-lvs-pod-upravleniem-windows/>

Оглавление

ВВЕДЕНИЕ 2

1 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. АНАЛИЗ ВОЗМОЖНЫХ АТАК И УЯЗВИМЫХ МЕСТ 4

1.1 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ОПРЕДЕЛЕНИЕ, ОСНОВНЫЕ ПОНЯТИЯ 4

1.2 СОВРЕМЕННЫЕ ПОЛОЖЕНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЛВС 8

1.3 ОБЩИЕ КРИТЕРИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ГОСТ Р ИСО/МЭК 15408-2008 16

1.4 УЯЗВИМЫЕ МЕСТА ЛВС 19

1.4.1 Основные понятия 19

1.4.2 Несоответствующий доступ к ресурсам ЛВС 21

1.4.3 Раскрытие данных 22

1.4.4 Неавторизованная модификация данных и программ 23

1.4.5 Раскрытие трафика ЛВС 24

1.4.6 Подмена трафика ЛВС 25

1.4.7 Разрушение функций ЛВС 26

1.5 ВЫВОДЫ ПО РАЗДЕЛУ 27

2 МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ 29

2.1 АНАЛИЗ ВОЗМОЖНЫХ ТИПОВ АТАК И МОДЕЛИ НАРУШИТЕЛЯ ОСУЩЕСТВЛЯЮЩЕГО АТАКИ НА ЛОКАЛЬНУЮ СЕТЬ 29

2.2 АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ, ПРИМЕНЯЕМЫХ В ЛОКАЛЬНЫХ СЕТЯХ 41

1.1.1.1 Идентификация и аутентификация 43

1.1.1.2 Управление доступом 46

1.1.1.3 Конфиденциальность данных и сообщений 48

1.1.1.4 Целостность данных и сообщений 49

1.1.1.5 Контроль участников взаимодействия 51

1.1.1.6 Регистрация и наблюдение 51

2.3 ОБЗОР СРЕДСТВ ЗАЩИТЫ СЕТЕЙ ПОД УПРАВЛЕНИЕМ ОС СЕМЕЙСТВА WINDOWS 53

2.3.1 Dallas Lock 53



2.3.2	Secret Net 5.0	53
2.3.3	Страж NT	54
2.3.4	Электронный замок «Соболь»	56
2.3.5	Security Studio	58
2.3.6	Аккорд-NT/2000 V3.0	59
2.4	РАЗРАБОТКА ПРЕДЛОЖЕНИЙ ПО СОЗДАНИЮ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ	60
3	ОЦЕНКА СОСТОЯНИЯ БЕЗОПАСНОСТИ ЛВС С ПОМОЩЬЮ РЕКОМЕНДУЕМЫХ СРЕДСТВ	74
3.1	ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ	74
3.2	ОЦЕНКА СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	85
3.3	ВЫВОДЫ ПО РАЗДЕЛУ	98
	ЗАКЛЮЧЕНИЕ	99
	СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ	101