

О ГЛАВЛЕНИЕ

ВВЕДЕНИЕ	3
1. ОБЩИЕ СВЕДЕНИЯ ОБ ИНФОРМАЦИИ КАК ОБЪЕКТЕ ЗАЩИТЫ.....	4
2. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ ПРИ ЭКСПЛУАТАЦИИ КОМПЬЮТЕРОВ.....	7
3. ОСНОВНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ СЕТЕЙ	9
4. ВОЗМОЖНЫЕ АТАКИ НА ОС, ИХ КЛАССИФИКАЦИЯ.....	12
5. ПАРОЛЬНАЯ ЗАЩИТА ПК. ВЗЛОМ ПАРОЛЕЙ WINDOWS NT И UNIX. ЗАЩИТА ОТ ВЗЛОМА.....	14
6. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ.....	16
6.1. Аутентификация в системах Windows	16
Локальная аутентификация.	16
<i>LAN Manager (LM)</i>	17
<i>NT LAN Manager (NTLM)</i>	17
<i>NTLMv2. NTLMv2 (NTLM версии 2)</i>	18
<i>Kerberos</i>	19
6.2. Аутентификация клиента	22
<i>Авторизация клиента на TGS. Для запроса сервиса клиент формирует сообщение TGS-REQ</i>	22
<i>Запрос сервиса клиентом. После получения TGS-REP у клиента</i>	23
6.3. Аутентификация пользователей ОС Unix	23
7. МЕТОДЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В СЕТИ ИНТЕРНЕТ.....	26
7.1. Аутентификация по паролю	26
<i>HTTP authentication</i>	26
<i>Forms authentication</i>	28
7.2. Аутентификация по сертификату	31
7.3. Аутентификация по одноразовым паролям	31
7.4. Аутентификация по ключам доступа	32
7.4. Аутентификация по токенам	35
8. СРЕДСТВА ЗАЩИТЫ СЕТЕВОЙ ИНФОРМАЦИИ	40
8.1. Межсетевые экраны	40
8.2. Демилитаризованная зона	46
8.3. Виртуальная частная сеть	47
8.4. Системы обнаружения сетевого вторжения.....	49
9. ВРЕДОНОСНЫЕ ПРОГРАММЫ И СПОСОБЫ БОРЬБЫ С НИМИ.....	50
9.1. Разновидности вирусных программ	50
9.2. Программная защита от вредоносного программного обеспечения	53
10. ОСНОВЫ КРИПТОГРАФИИ	56
10.1. Классификация криптографических алгоритмов	63
10.2. Модели шифров и открытых текстов	67
Алгебраические модели.	67
Вероятностные модели шифров.	70
Математические модели открытых сообщений.	72
10.3. Криптографическая стойкость шифра.....	75
Теоретическая стойкость шифров.....	78
Практическая стойкость шифров.	78

10.4. Имитостойкость и помехоустойчивость шифров.....	79
Способы обеспечения имитостойкости.....	81
Помехоустойчивость шифров.....	82
10.5. Криптографические хеш-функции.....	83
Радужные таблицы.....	85
Хеш-функция MD5.....	87
Хеш-функция SHA-1.....	90
Сравнение SHA-1 и MD5. Безопасность.....	92
Электронно-цифровая подпись.....	93
Цифровой сертификат.....	97
11. Протоколы Web-защиты.....	99
11.1. Архитектура SSL	100
11.2. Протокол извещения	102
11.3. Протокол квтирования SSL	102
11.4. Протокол SET	104
11.5. Сравнительные характеристики протоколов SSL и SET.....	108
Библиографический список.....	111

*Бондарев Евгений Сергеевич, Васюков Василий Михайлович,
Грушевский Павел Ришардович, Скулябина Ольга Владимировна*

Защита компьютерной информации

Редактор Г.М. Звягина

Корректор Л.А. Петрова

Компьютерная верстка: Н.А. Андреева

Подписано в печать 11.12.2019. Формат 60×84^{1/16}. Г.-1600. полиграфия

Печать трафаретная. Усл. печ. л. 6,575. Тир.

Балтийский государственный технический

Типография БГТУ

190005, С.-Петербург, 1-я Красноар

БИБЛИОТЕКА БГТУ "ВОЕНМЕХ"



00503117