

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное
образовательное учреждение высшего образования
«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Инженерно-технологическая академия

Ю. А. БРЮХОМИЦКИЙ

**БЕЗОПАСНОСТЬ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

*Учебное пособие
в двух частях*

Часть 1

Ростов-на-Дону – Таганрог
Издательство Южного федерального университета
2020

УДК 004.056.5(075.8)

ББК 32.97я73

Б898

*Печатается по решению кафедры информационной безопасности
Института компьютерных технологий и информационной безопасности
Южного федерального университета
(протокол № 6 от 6 марта 2020 г.)*

Рецензенты:

заведующий кафедрой системного анализа и телекоммуникаций
Института компьютерных технологий и информационной безопасности
ЮФУ, доктор технических наук, профессор *Ю. И. Rogozov*

директор ООО «Инженерный центр «Интегра», г. Таганрог,
кандидат технических наук *А. С. Басан*

Брюхомицкий, Ю. А.

Б898 Безопасность информационных технологий. Часть 1. : учебное
пособие : в 2 ч. / Ю. А. Брюхомицкий ; Южный федеральный универ-
ситет. – Ростов-на-Дону ; Таганрог : Издательство Южного федераль-
ного университета, 2020.

ISBN 978-5-9275-3526-2

Часть 1. – 171 с.

ISBN 978-5-9275-3571-2 (Ч. 1)

Пособие содержит описание основных понятий информационной безо-
пасности; угроз и уязвимостей информационных систем; стандартов защиты
данных; методов и средств аутентификации, контроля доступом; политик и
моделей безопасности; технической защиты информации; организационно-
правового обеспечения информационной безопасности.

УДК 004.056.5(075.8)

ББК 32.97я73

ISBN 978-5-9275-3571-2 (Ч. 1)

ISBN 978-5-9275-3526-2

© Южный федеральный университет, 2020

© Брюхомицкий Ю. А., 2020

© Оформление. Макет. Издательство

Южного федерального университета, 2020

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
1. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ	6
2. УГРОЗЫ И УЯЗВИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ	13
2.1. Классификация источников угроз информационной безопасности	14
2.2. Классификация угроз информационной безопасности ИС ...	19
2.3. Обеспечение безопасности инфраструктуры ИС	23
2.4. Методы оценивания угроз безопасности ИС	24
2.5. Классификация злоумышленников	26
2.6. Каналы проникновения в ИС и каналы утечки информации	28
Выводы	29
3. КРИТЕРИИ И СТАНДАРТЫ ЗАЩИТЫ ДАННЫХ	31
3.1. Введение и общая модель (часть 1 ОК)	35
3.2. Функциональные требования безопасности (часть 2 ОК)	38
3.3. Требования доверия безопасности (часть 3 ОК)	39
3.4. Другие отечественные стандарты	40
4. МЕТОДЫ И СРЕДСТВА АУТЕНТИФИКАЦИИ	43
4.1. Основные понятия	43
4.2. Парольная аутентификация	49
4.3. Одноразовые пароли	51
4.4. Функциональные методы аутентификации	53
4.5. Персональные средства аутентификации	55
4.6. Биометрические средства аутентификации	57
4.7. Аутентификация по информации, ассоциированной с субъектом	61
4.8. Многоканальная аутентификация	61
5. МЕТОДЫ И СРЕДСТВА АВТОРИЗАЦИИ	62
5.1. Контроль доступа	62
5.2. Политики и модели безопасности	66
5.3. Дискреционная модель безопасности	67
5.4. Мандатная модель безопасности	70

5.5. Ролевая модель разграничения доступа	75
5.6. Модель безопасности информационных потоков	78
5.7. Модель изолированной программной среды	78
5.8. Модель тематического доступа	79
Выводы	79
6. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ	80
6.1. Использование ТКУИ для ведения технической разведки	82
6.1.1. Классификация технических каналов утечки информации ..	87
6.2. Технические каналы утечки информации с ОТСС	88
6.2.1. Электромагнитные каналы утечки в ОТСС	89
6.2.2. Электрические каналы утечки информации в ОТСС	92
6.2.3. Параметрические каналы утечки информации в ОТСС ...	94
6.3. Технические каналы утечки информации при передаче данных	96
6.3.1. Подвижная радиосвязь	97
6.3.2. Радиорелейные и космические системы связи	99
6.3.3. Электрические каналы утечки информации в проводных линиях связи	102
6.3.4. Перехват информации с проводных электрических линий связи	106
6.3.5. Перехват информации с телефонных линий связи	107
6.3.6. Перехват информации с радиотелефонных линий связи ...	111
6.3.7. Каналы утечки информации с волоконно-оптических линий связи	113
6.4. Технические каналы утечки речевой информации	115
6.4.1. Речевая информация	115
6.4.2. Акустические каналы утечки речевой информации	117
6.4.3. Виброакустические каналы утечки речевой информации ...	121
6.4.4. Акустоэлектрические каналы утечки речевой информации	123
6.4.5. Акусто-оптоволоконные каналы утечки речевой инфор- мации	124
6.4.6. Оптико-электронные каналы утечки речевой информации	126
6.4.7. Параметрические каналы утечки речевой информации	128
6.5. Технические каналы утечки видовой информации	130
6.5.1. Скрытое наблюдение за объектами	132

Содержание

6.5.2. Оптико-механические приборы	132
6.5.3. Тепловизоры и приборы ночного видения	134
6.5.4. Скрытная фотосъемка	135
6.5.5. Скрытная фотосъемка объектов наблюдения	135
6.5.6. Скрытная фотосъемка документов	136
6.5.7. Скрытное видеонаблюдение	137
6.6. Материально-вещественные каналы утечки информации	138
6.7. Комплексирование каналов утечки информации	139
7. ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	142
7.1. Классификация методов защиты информации	142
7.2. Классификация и виды информационных ресурсов	143
7.3. Информация ограниченного доступа. Государственная тайна ..	145
7.4. Информация конфиденциального характера	148
7.5. Коммерческая тайна	151
7.6. Грифы конфиденциальности	151
7.7. Правовая основа системы лицензирования и сертификации ...	153
7.8. Лицензирование деятельности, связанной с государственной тайной и защитой информации	154
7.9. Сертификации средств защиты информации	156
7.10. Лицензирование деятельности по технической защите конфиденциальной информации	157
7.11. Сертификация деятельности по технической защите конфиденциальной информации	158
ЗАКЛЮЧЕНИЕ	161
СПИСОК ЛИТЕРАТУРЫ	162