

УДК 004.732.056(075.8)

ББК 32.973.2-018.2я73

К26

Рецензенты: кафедра «Информационная безопасность» Государственного бюджетного образовательного учреждения высшего образования Московской области Технологический университет (МГОТУ); доктор техн. наук, профессор, начальник отделения АО «Российские космические системы»
В. М. Ватулин

Карпухин Е. О.

К26 Технологии и методы защиты инфокоммуникационных систем и сетей. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2021. – 120 с.: ил.

ISBN 978-5-9912-0896-3.

Приведены проблемы безопасности локальной беспроводной сети стандартов IEEE 802.11 и пример ее защиты на основе технологии WPA3. Рассмотрены задачи аудита безопасности в инфокоммуникационных системах с использованием SIEM-систем. Представлены методы аутентификации пользователя как на основе парольных, так и биометрических систем. Отдельное внимание уделено технологиям единой аутентификации на нескольких Интернет-ресурсах. Показаны методы и средства выявления уязвимостей и защиты локальных сетей, а также предотвращение утечек информации в телекоммуникационных системах. Сделан акцент на защиту инфокоммуникационных систем от атак класса «отказ в обслуживании». Для знакомства читателей с методами и средствами надежного и безопасного хранения данных рассмотрена технология резервного копирования путем децентрализованного распределения файлов по устройствам. Особое место в пособии уделено проблемам обеспечения безопасности защищенного соединения с использованием протокола HTTPS и мобильных устройств в открытых сетях. Приведены методы, технологии и средства защиты веб-ресурсов от актуальных угроз.

Для студентов, обучающихся по направлениям подготовки 10.03.01 – «Информационная безопасность», 10.05.02 – «Информационная безопасность телекоммуникационных систем», 11.03.02 и 11.04.02 – «Инфокоммуникационные технологии и системы связи».

ББК 32.973.2-018.2я73

Учебное издание

Карпухин Евгений Олегович

Технологии и методы защиты инфокоммуникационных систем и сетей

Учебное пособие для вузов

Тиражирование книги начато в 2020 г.

Все права защищены.

Любая часть этого издания не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения правообладателя

© ООО «Научно-техническое издательство «Горячая линия – Телеком»

www.techbook.ru

© Е.О. Карпухин

Оглавление

Введение	3
1. Защита локальной беспроводной сети стандартов IEEE 802.11	5
2. Аудит безопасности в инфокоммуникационных системах	13
3. Методы аутентификации пользователя ИКС	18
3.1. Парольные системы аутентификации	18
3.2. Технологии единой аутентификации на нескольких Интернет-ресурсах	20
3.3. Биометрические методы аутентификации	22
4. Проблемы обеспечения безопасности защищенного соединения с использованием протокола HTTPS в открытых сетях	30
4.1. Варианты реализации атаки «человек посередине» при использовании протокола HTTPS с последующим анализом трафика	31
4.1.1. Атака «человек посередине» с понижением протокола HTTPS до HTTP	31
4.1.2. Атака «человек посередине» на HTTPS-соединение с использованием доверенного (скомпрометированного) цифрового сертификата	33
4.1.3. Атака «человек посередине» на HTTPS-соединение с использованием самоподписанного сертификата	34
4.2. Технологии и методы повышения защищенности соединений по протоколу HTTPS	35
4.2.1. HTTP Strict Transport Security	36
4.2.2. HTTP Public Key Pinning	37
4.2.3. Online Certificate Status Protocol и Certificate Revocation List	39
4.2.4. Применение дополнительных модулей в браузере	40
4.3. Пример реализации атаки на протокол HTTPS и проверка работоспособности методов защиты	41
5. Обеспечение информационной безопасности мобильных устройств	46
5.1. Модели использования мобильных устройств сотрудниками организации	47

5.2. Угрозы информационной безопасности мобильных устройств при их интеграции в сеть предприятия	50
5.2.1. Угрозы со стороны ПО	51
5.2.2. Интернет-угрозы	53
5.2.3. Сетевые угрозы	54
5.2.4. Ненадежные источники	55
5.2.5. Угрозы физического доступа к устройству	55
5.2.6. Угрозы со стороны пользователей	56
5.3. Технологии управления и обеспечения безопасности мобильных устройств	57
5.3.1. Управление мобильными устройствами	57
5.3.2. Управление мобильными приложениями	58
5.3.3. Обеспечение безопасности мобильных устройств	60
6. Использование сканеров уязвимостей и межсетевых экранов для защиты локальной сети	65
7. Предотвращение утечек информации в телекоммуникационных системах	74
8. Защита от атак класса «отказ в обслуживании» ...	77
9. Обеспечение надежного и безопасного хранения данных в ИКС	84
9.1. Проблемы безопасности систем хранения данных	85
9.2. Требования к системам хранения данных	86
9.3. Технологии резервного копирования	87
10. Защита веб-ресурсов и их пользователей от распространенных атак и уязвимостей	94
10.1. Распространенные атаки на веб-ресурсы	94
10.1.1. SQL-инъекция	94
10.1.2. Межсайтовый скриптинг	97
10.2. Уязвимости веб-приложений	100
10.2.1. Cross-Origin Resource Sharing (CORS)	100
10.2.2. Веб-сокеты	101
10.2.3. Технология обмена данными между доменами	102
10.2.4. Кеш веб-приложения	104
10.2.5. Веб-хранилище	106
10.2.6. Геолокация	108
10.3. Методы и средства защиты веб-ресурсов	109
10.3.1. Принцип работы web application firewall	109
10.3.2. ModSecurity	110
10.3.3. Функция htmlspecialchars	111
Литература	114