

УДК 621.37
ББК 32.843
С56

Авторы:

В. А. Майстренко, А. А. Соловьев, М. Ю. Пляскин, А. И. Тихонов

Рецензенты:

*В. С. Кукис, доктор технических наук, профессор,
действительный член (академик) Академии военных наук;*

В. М. Лебедев, доктор технических наук, профессор Академии военных наук;

*П. С. Ложников, кандидат технических наук, доцент,
заведующий кафедрой «Комплексная защита информации» ОмГТУ*

Современные радиоэлектронные средства и технологии информационной безопасности : монография / [В. А. Майстренко и др.] ; М-во образования и науки РФ, ОмГТУ, СибАДИ; Акад. воен. наук РФ. – Омск : Изд-во ОмГТУ, 2017. – 356 с. : ил.

ISBN 978-5-8149-2554-1

Монография посвящена современным радиоэлектронным каналам и системам связи сверхвысокочастотного диапазона волн, используемым в качестве оружия информационных технологий. Важное внимание уделено актуальным вопросам криптографии и информационно-коммуникационным технологиям безопасности и защиты информации современных радиоэлектронных средств.

Рассмотрены особенности приема и обработки информационных спутниковых сигналов и применение навигационных технологий с помощью современных глобальных спутниковых радионавигационных систем GPS, ГЛОНАСС, GNSS и GALILEO.

Издание адресовано научным сотрудникам и специалистам отраслевых и военных вузов, а также магистрантам, аспирантам и адъюнктам при изучении соответствующих курсов.

УДК 621.37
ББК 32.843

*Печатается по решению научно-технического совета
Омского государственного технического университета.
Протокол № 11 от 24.10.2017 года.*

ISBN 978-5-8149-2554-1

© ОмГТУ, 2017

ОГЛАВЛЕНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ	6
ВВЕДЕНИЕ	10
Глава 1. РАДИОЭЛЕКТРОННЫЕ КАНАЛЫ И СИСТЕМЫ СВЯЗИ СВЕРХВЫСОКОЧАСТОТНОГО ДИАПАЗОНА ВОЛН	11
1.1. Современная шкала электромагнитных волн.....	11
1.2. Особенности использования СВЧ диапазона волн в каналах связи	13
1.3. Радио и лазерные оптико-локационные устройства и системы	18
1.3.1. Радиолокационные и оптико-локационные системы.....	19
1.3.2. Лазерный (квантовый) дальномер	26
1.3.3. Лазерные излучатели непрерывного и импульсного действия.....	28
1.4. Оптико-электронные и тепलोкационные приборы	34
1.4.1. Приборы ночного видения и тепловизоры	34
1.5. Основы волоконно-оптической, радиорелейной связи и голографии	41
1.5.1. Оптоволоконный и беспроводный оптические каналы связи.....	41
1.5.2. Отечественные волоконно-оптические и радиорелейные линии связи	51
1.5.3. Космическая оптическая связь	68
Глава 2. ИНФОРМАЦИОННЫЕ МИКРОВОЛНОВЫЕ КАНАЛЫ ВООРУЖЕНИЯ И БЕЗОПАСНОСТИ	77
2.1. Общие предпосылки и принципы использования СВЧ в системах вооружения	77
2.2. Глобальные навигационные системы GPS, ГЛОНАСС, GNSS и GALILEO.....	84
2.3. Оружие информационных технологий и информационная безопасность ...	115
2.3.1. Понятия «информационное оружие» и информационная безопасность	115
2.3.2. Виды и типы информационного оружия и их краткая характеристика.....	119
2.3.3. Информационное оружие на основе программного кода.....	121
2.3.4. Информационное оружие на основе средств воздействия на психику	123
2.3.5. Информационное оружие на основе информационных технологий...	124
2.3.6. Главные принципы применения информационного оружия	131
2.3.7. Информационная безопасность.....	142
2.4. Информационные каналы микроволнового излучения – вид современного оружия.....	151
2.4.1. Особенности использования лазерного оружия.....	151
2.4.2. Рентгеновские лазеры.....	155
2.4.3. Пучковое оружие	160
2.5. Основные положения математических методов криптографии.....	166
2.5.1. Определения и краткие этапы истории криптографии.....	166
2.5.2. Из истории криптографии.....	168
2.5.3. Математическая формализация.....	174
2.5.4. Алгоритм шифрования RSA	179
2.5.5. Открытый и закрытый ключи.....	184

2.5.6. Криптография и «трудные» математические задачи.....	185
2.5.7. Криптографические протоколы.....	187
2.5.8. Протокол аутентификации.....	188
2.5.9. Доказательство с нулевым разглашением.....	190
2.5.10. Электронная подпись.....	190
2.5.11. Электронные торги.....	192
2.5.12. Протокол электронного голосования.....	194
2.5.13. Закрытый информационный обмен между двумя партнерами.....	201
2.5.14. Криптографические протоколы и «честное слово».....	202
2.5.15. Криптография и массовые информационные коммуникации.....	204
2.5.16. Инфраструктура открытых ключей и удостоверяющие центры.....	205
2.5.17. Обеспечивающие алгоритмы.....	207
2.5.18. Обмен между клиентами одного удостоверяющего центра.....	208
2.5.19. Система взаимодействующих удостоверяющих центров.....	210
2.5.20. Общий случай.....	214
2.5.21. Промежуточные итоги.....	216

ГЛАВА 3. ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНОЙ СЕТИ

3.1. Определение и основные функции корпоративной сети.....	217
3.2. Архитектура корпоративных сетей на основе VPN и вопросы безопасности.....	219
3.2.1. Архитектура VPN.....	219
3.2.2. Вопросы безопасности.....	219
3.3. Пример использования информационной безопасности в локальной вычислительной сети (ЛВС).....	220
3.3.1. Топология ЛВС.....	220
3.3.2. Мониторинг и анализ ЛВС.....	226
3.3.3. Анализ трафика сегментов сети.....	240

Глава 4 ВОПРОСЫ И ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МОБИЛЬНОЙ ПЕРСОНАЛЬНОЙ РАДИОСВЯЗИ

4.1. Персональная сотовая связь и актуальность информационной безопасности.....	252
4.2. Наиболее важные вопросы и проблемы безопасности мобильного общения.....	253
4.2.1. Как прослушивают разговоры по мобильному телефону.....	253
4.2.2. Почему при смене SIM-карты надо менять и мобильный телефон....	256
4.2.3. Как определяют местоположение человека по его мобильному телефону.....	257
4.2.4. Почему коммуникаторы не стоит использовать в качестве навигаторов.....	260
4.2.5. Чем опасен SMS-спам.....	262
4.2.6. Как подделывают имя отправителя SMS-сообщения.....	267
4.2.7. Как вымогают деньги с помощью SMS-сообщений.....	270
4.2.8. Как расплачиваются за покупки деньгами с чужого счета мобильного телефона.....	272
4.2.9. Какие SMS-сообщения выводят телефон из строя.....	277

4.2.10. Почему включенный мобильный телефон может не получать SMS-сообщения и звонки	280
4.2.11. Как используют Bluetooth для поиска дорогих мобильных телефонов	284
4.2.12. Как с помощью Bluetooth выводят из строя мобильный телефон	286
4.2.13. Как с помощью мобильного телефон прослушивают нетелефонные разговоры	290
4.2.14. Как выводят из строя мобильные телефоны во время синхронизации с компьютером	296
4.2.15. Как Bluetooth-гарнитуру превращают в подслушивающее устройство	298
4.2.16. Почему SMS-сообщения приходят с пустым номером отправителя	303
4.2.17. Почему опасно принимать файлы от незнакомцев	303
4.2.18. Почему неожиданно сел аккумулятор вашего мобильного телефона.....	304
4.2.19. Как узнают состояние вашего банковского счета, зная только ваш телефонный номер	305
4.2.20. Как используют уязвимости мобильного телефона для снятия денег с банковского счета.....	308
4.2.21. Как блокируется доступ в Интернет с мобильного телефона.....	312
4.2.22. Почему злоумышленник знает сайты, на которые вы заходили с мобильного телефона.....	313
4.2.23. Почему опасно выходить в Интернет через Wi-Fi точку	316
4.2.24. Как вирус попадает на телефон при использовании конфигурационных сообщений.....	318
4.2.25. Как телефон заражают вирусами с помощью MMS-сообщений.....	321
4.2.26. Как заражают мобильный телефон E-MAIL-сообщениями	327
4.2.27. Почему опасно выходить с мобильного телефона в Интернет по Bluetooth.....	328
4.2.28. Как вирусы заражают телефон в кинотеатрах, кафе и на стадионах	329
4.2.29. Как функционируют вирусы для MacOS телефона iPhone	334
4.2.30. Как к вашему телефонному разговору может подключиться злоумышленник	340
4.2.31. Чем опасны мобильные телефоны со встроенными видеокамерами	341
4.2.32. Почему опасны мобильные телефоны нового поколения	342
4.2.33. Почему опасно оплачивать проезд на метро с помощью мобильного телефона	346
4.2.34. Почему мобильные телефоны нового поколения могут оплачивать чужие покупки без вашего ведома	347
4.3. Основные выводы и пожелания.....	348
ЗАКЛЮЧЕНИЕ.....	350
БИБЛИОГРАФИЧЕСКИЙ СПИСОК.....	351