

**А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов**

# **Программно-аппаратные средства обеспечения информационной безопасности**

*Под редакцией А. В. Душкина*

*Рекомендовано УМО по образованию в области  
Инфокоммуникационных технологий и систем связи в  
качестве учебного пособия для студентов высших учебных  
заведений, обучающихся по направлению подготовки 11.03.02,  
11.04.02 – «Инфокоммуникационные технологии и системы  
связи» квалификации (степени) «бакалавр», «магистр» и  
11.05.04 – «Инфо-коммуникационные технологии и системы  
специальной связи» квалификации «специалист»*

**Москва  
Горячая линия – Телеком  
2016**

УДК 681.3.067

ББК 32.81

П78

Рецензенты: нач. кафедры Воронежского института МВД России, доктор физ.-мат. наук, профессор *В. В. Меньших*; нач. кафедры Военного учебно-научного центра «Военно-воздушная академия им. профессора Н. Е. Жуковского и Ю. А. Гагарина» доктор техн. наук, профессор *П. А. Федюнин*

Авторы: А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов

**П78 Программно-аппаратные средства обеспечения информационной безопасности. Учебное пособие для вузов / А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов. Под редакцией А. В. Душкина. – М.: Горячая линия – Телеком, 2016. – 248 с: ил. ISBN 978-5-9912-0470-5.**

Изложены теоретические основы создания и практического применения программно-аппаратных средств обеспечения информационной безопасности. Рассмотрены основные принципы создания программно-аппаратных средств обеспечения информационной безопасности; методы и средства реализации отдельных функциональных требований по защите информации и данных; программно-аппаратные средства защиты программ; программно-аппаратные средства защиты от несанкционированного доступа к информации, хранимой в ПЭВМ; программно-аппаратные средства защиты информации в сетях передачи данных; вопросы сертификации программно-аппаратных средств обеспечения информационной безопасности. Значительное внимание уделено нормативно-правовой базе в области создания, применения и сертификации программно-аппаратных средств обеспечения защиты информации. Подробно описана технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.

Предназначено для студентов, курсантов, слушателей, аспирантов, адъюнктов, преподавателей, научных и практических работников, занимающихся вопросами информационной безопасности.

**ББК 32.81**

Адрес издательства в Интернет [www.techbook.ru](http://www.techbook.ru)

*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](http://www.techbook.ru)

© А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов

# Оглавление

Введение .....	3
1. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности .....	6
1.1. Основные понятия и определения в области создания ПАСОИБ .....	6
1.2. Нормативно-правовая база создания ПАСОИБ .....	9
1.3. Анализ угроз информационной безопасности .....	12
1.4. Анализ сетевых угроз информационной безопасности .	19
1.5. Классификация ПАСОИБ .....	25
1.6. Функциональные возможности ПАСОИБ .....	30
1.7. Принципы разработки ПАСОИБ .....	34
1.8. Концепция диспетчера доступа .....	36
1.9. Основные этапы проектирования ПАСОИБ .....	41
2. Основные методы и средства реализации отдельных функциональных требований по защите информации и данных .....	44
2.1. Классификация функциональных требований по защите информации и данных .....	44
2.2. Принципы действия и технологические особенности программно-аппаратных средств, реализующих отдельные функциональные требования по защите информации и данных и их взаимодействие с общесистемными компонентами вычислительных систем .....	46
2.3. Методы обеспечения идентификации и аутентификации	50
2.4. Методы криптографической защиты .....	62
2.5. Методы и средства хранения ключевой информации...	70
2.6. Методы и средства ограничения доступа к компонентам вычислительных систем .....	73
2.7. Характеристика методов и средства привязки программного обеспечения к аппаратному окружению и физическим носителям .....	78
2.8. Методы аудита безопасности .....	81
2.9. Методы обеспечения доступа к системе защиты и управления безопасностью .....	84
2.10. Методы обеспечения целостности системы защиты....	86

<b>3. Программно-аппаратные средства защиты программ</b>	<b>92</b>
3.1. Классификация аппаратных компонентов средств защиты программ	92
3.2. Классификация программных компонентов средств защиты программ	94
3.3. Структура программного обеспечения	96
3.4. Способы встраивания средств защиты в программное обеспечение	98
3.5. Способы определения факта незаконного использования программ	100
3.6. Способы защиты программ от незаконного использования	102
3.7. Способы изучения кода программ	107
3.8. Способы защиты программ от изучения кода	110
3.9. Основные принципы обеспечения безопасности программ	112
3.10. Понятие изолированной программной среды	114
<b>4. Программно-аппаратные средства защиты от несанкционированного доступа к информации, хранимой в ПЭВМ</b>	<b>120</b>
4.1. Классификация программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ	120
4.2. Характеристики программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ	120
4.3. Понятие электронного замка	132
4.4. Принципы построения и функционирования электронных замков	135
4.5. Механизмы контроля аппаратной конфигурации ПЭВМ	137
4.6. Общие принципы разграничения доступа пользователей к устройствам ПЭВМ	138
4.7. Основные принципы криптографической защиты информации	141
<b>5. Программно-аппаратные средства защиты информации в сетях передачи данных</b>	<b>143</b>
5.1. Классификация программно-аппаратных средств защиты информации в сетях передачи данных	143
5.2. Принципы построения и функционирования межсетевых экранов в сетях передачи данных	146
5.3. Программно-аппаратные средства межсетевого экранирования	148

5.4. Основные принципы защиты информации при передаче по каналам связи .....	151
5.5. Программно-аппаратные средства защиты информации при передаче по каналам связи .....	152
5.6. Основные принципы разграничения доступа к сетевым ресурсам.....	155
5.7. Основные принципы обнаружения сетевых атак.....	157
5.8. Программно-аппаратные средства обнаружения сетевых атак .....	161
5.9. Основные принципы защиты от сетевых атак.....	162
5.10. Программно-аппаратные средства защиты от сетевых атак .....	164
5.11. Основные принципы управления безопасностью сети ..	170
5.12. Программно-аппаратные средства управления безопасностью сети .....	174
5.13. Обзор штатных средств сетевого оборудования, предназначенных для защиты информации при передаче по каналам связи .....	176
5.14. Способы применения штатных средств сетевого оборудования, предназначенных для защиты информации при передаче по каналам связи.....	179
<b>6. Сертификация программно-аппаратных средств обеспечения информационной безопасности .....</b>	<b>180</b>
6.1. Основные требования к информационной безопасности	182
6.2. Задачи сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности .....	184
6.3. Технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности .....	186
6.4. Классификация требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.....	189
6.5. Проверка ОИ на базе вычислительной техники .....	196
<b>Литература .....</b>	<b>234</b>
<b>Приложение. Руководящие документы в области сертификации программно-аппаратных средств обеспечения информационной безопасности .....</b>	<b>236</b>
<b>Список сокращений .....</b>	<b>243</b>