

УДК 681.326  
ББК 67.408  
Б81

Издание доступно в электронном виде по адресу  
<https://bmstu.press/catalog/item/7085/>

Факультет «Информатика и системы управления»  
Кафедра «Информационная безопасность»

*Рекомендовано Научно-методическим советом  
МГТУ им. Н.Э. Баумана в качестве учебного пособия*

*Рецензент*  
д-р техн. наук *Б.Н. Коробец*

**Бондарев, В. В.**

Б81 Введение в информационную безопасность автоматизированных систем : учебное пособие / В. В. Бондарев. — 3-е изд. — Москва : Издательство МГТУ им. Н. Э. Баумана, 2021. — 250, [2] с. : ил.

ISBN 978-5-7038-5541-6

Рассмотрена законодательная база информационной безопасности, приведен перечень возможных угроз, отражены основные подходы к созданию систем защиты информации, представлена классификация предупредительных мер, изучены вопросы, связанные с программно-аппаратными механизмами обеспечения информационной безопасности.

Для студентов, обучающихся по направлению подготовки «Информационная безопасность», по специальности «Информационная безопасность автоматизированных систем» и слушателей факультета повышения квалификации. Может быть полезно студентам и аспирантам других специальностей, интересующимся современными средствами и методами обеспечения информационной безопасности.

УДК 681.326  
ББК 67.408

ISBN 978-5-7038-5541-6

© МГТУ им. Н.Э. Баумана, 2016  
© Оформление. Издательство  
МГТУ им. Н.Э. Баумана, 2021

## ОГЛАВЛЕНИЕ

Предисловие .....	3
<b>Р а з д е л I. Основы безопасности автоматизированных систем</b> .....	5
<b>Глава 1.</b> Актуальность проблемы обеспечения безопасности автоматизированных систем .....	5
1.1. Место и роль автоматизированных систем в управлении бизнес-процессами .....	5
1.2. Обострение проблемы обеспечения безопасности автоматизированных систем на современном этапе .....	6
1.3. Защита автоматизированных систем как процесс управления рисками .....	9
1.4. Методы оценки целесообразности затрат на обеспечение безопасности .....	10
1.5. Особенности современных автоматизированных систем как объектов защиты .....	13
<b>Глава 2.</b> Основные понятия в области безопасности автоматизированных систем .....	15
2.1. Определение безопасности автоматизированных систем .....	15
2.2. Информация и информационные ресурсы .....	16
2.3. Субъекты информационных отношений, их безопасность .....	17
2.4. Цель защиты автоматизированной системы и циркулирующей в ней информации .....	19
<b>Глава 3.</b> Угрозы безопасности автоматизированных систем .....	20
3.1. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем .....	20
3.2. Угрозы безопасности информации, автоматизированных систем и субъектов информационных отношений .....	22
3.3. Классификация угроз безопасности .....	24
3.4. Классификация каналов проникновения в автоматизированную систему и утечки информации .....	27
3.5. Неформальная модель нарушителя .....	28
<b>Глава 4.</b> Меры и основные принципы обеспечения безопасности автоматизированных систем .....	33
4.1. Виды мер противодействия угрозам безопасности .....	33
4.2. Принципы построения системы обеспечения безопасности информации в автоматизированной системе .....	35

<b>Глава 5. Правовые основы обеспечения безопасности автоматизированных систем</b> .....	39
5.1. Защищаемая информация .....	41
5.2. Лицензирование .....	52
5.3. Сертификация средств защиты информации и аттестация объектов информатизации .....	57
5.4. Специальные требования и рекомендации по технической защите конфиденциальной информации .....	68
5.5. Юридическая значимость электронных документов с электронной подписью .....	69
5.6. Ответственность за нарушения в сфере защиты информации .....	71
<b>Глава 6. Государственная система защиты информации</b> .....	77
6.1. Главные направления работ по защите информации .....	77
6.2. Структура государственной системы защиты информации .....	78
6.3. Организация защиты информации в системах и средствах информатизации и связи .....	81
6.4. Контроль состояния защиты информации .....	83
6.5. Финансирование мероприятий по защите информации .....	84
<b>Р а з д е л II. Обеспечение безопасности автоматизированных систем</b> .....	85
<b>Глава 7. Организационная структура системы обеспечения безопасности автоматизированных систем</b> .....	85
7.1. Технология управления безопасностью информации и ресурсов в автоматизированной системе .....	85
7.2. Институт ответственных за обеспечение информационной безопасности .....	87
7.3. Регламентация действий пользователей и обслуживающего персонала автоматизированной системы .....	90
7.4. Политика безопасности организации .....	91
7.5. Мероприятия по созданию и обеспечению функционирования комплексной системы защиты .....	93
7.6. Распределение функций по обеспечению безопасности автоматизированных систем .....	95
7.7. Организационно-распорядительные документы по обеспечению безопасности автоматизированных систем .....	96
<b>Глава 8. Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях</b> .....	98
8.1. Проблема человеческого фактора .....	99
8.2. Общие правила обеспечения безопасности .....	99
8.3. Обязанности ответственного за обеспечение безопасности информации в подразделении .....	100
8.4. Ответственность за нарушения требований обеспечения безопасности .....	101
8.5. Порядок работы с носителями ключевой информации .....	102

<b>Глава 9. Регламентация работ по обеспечению безопасности автоматизированных систем .....</b>	<b>106</b>
9.1. Регламентация правил парольной и антивирусной защиты .....	107
9.2. Регламентация порядка допуска к работе и изменения полномочий пользователей автоматизированной системы .....	110
9.3. Регламентация порядка изменения конфигурации аппаратно-программных средств автоматизированной системы ....	112
9.4. Регламентация процессов разработки, испытания, опытной эксплуатации, внедрения и сопровождения задач .....	117
<b>Глава 10. Категорирование и документирование защищаемых ресурсов ....</b>	<b>121</b>
10.1. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов .....	121
10.2. Категорирование защищаемых ресурсов .....	123
10.3. Проведение информационных обследований и документирование защищаемых ресурсов .....	126
<b>Глава 11. Концепция информационной безопасности. Планы защиты и обеспечения непрерывной работы и восстановления подсистем автоматизированной системы .....</b>	<b>128</b>
11.1. Концепция информационной безопасности организации .....	129
11.2. План защиты информации .....	130
11.3. План обеспечения непрерывной работы и восстановления подсистем автоматизированной системы .....	131
 <b>Р а з д е л III. Средства защиты информации от несанкционированного доступа .....</b>	 <b>138</b>
<b>Глава 12. Назначение и возможности средств защиты информации от несанкционированного доступа .....</b>	<b>138</b>
12.1. Основные механизмы защиты автоматизированных систем .....	138
12.2. Защита периметра компьютерных сетей и управление механизмами защиты .....	151
12.3. Страхование информационных рисков .....	153
<b>Глава 13. Аппаратно-программные средства защиты информации от несанкционированного доступа .....</b>	<b>156</b>
13.1. Рекомендации по выбору средств защиты информации от несанкционированного доступа .....	156
13.2. Обзор существующих на рынке средств защиты информации от несанкционированного доступа .....	159
13.3. Средства аппаратной поддержки .....	166
13.4. Способы аутентификации .....	167
<b>Глава 14. Применение штатных и дополнительных средств защиты информации от несанкционированного доступа .....</b>	<b>176</b>
14.1. Стратегия безопасности Microsoft .....	177
14.2. Защита от вмешательства в процесс нормального функционирования автоматизированной системы .....	177

14.3. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы .....	179
14.4. Оперативное оповещение о зарегистрированных попытках несанкционированного доступа .....	185
14.5. Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования .....	187
<b>Р а з д е л IV. Обеспечение безопасности компьютерных сетей.....</b>	<b>189</b>
<b>Глава 15. Проблемы обеспечения безопасности в компьютерных сетях .....</b>	<b>189</b>
15.1. Типовая корпоративная сеть .....	189
15.2. Уровни информационной инфраструктуры корпоративной сети .....	190
15.3. Уязвимости и их классификация .....	190
15.4. Классификация атак .....	198
15.5. Средства защиты сетей .....	203
<b>Глава 16. Защита периметра корпоративной сети .....</b>	<b>204</b>
16.1. Угрозы, связанные с периметром корпоративной сети .....	205
16.2. Составляющие защиты периметра .....	206
16.3. Межсетевые экраны .....	207
16.4. Анализ содержимого почтового и веб-трафика .....	215
16.5. Виртуальные частные сети .....	216
<b>Глава 17. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности .....</b>	<b>219</b>
17.1. Управление уязвимостями .....	219
17.2. Архитектура систем управления уязвимостями .....	220
17.3. Особенности сетевых агентов сканирования .....	221
17.4. Средства анализа защищенности системного уровня .....	223
<b>Глава 18. Мониторинг событий безопасности .....</b>	<b>224</b>
18.1. Введение в управление журналами событий .....	224
18.2. Категории журналов событий .....	225
18.3. Инфраструктура управления журналами событий .....	225
18.4. Введение в технологию обнаружения атак .....	227
18.5. Классификация систем обнаружения атак .....	228
Глоссарий .....	230
Литература .....	237
Приложение. Нормативно-правовое обеспечение информационной безопасности .....	239