

УДК 004.3:004.056(075.8)  
П 784

Коллектив авторов:

*С. А. Зырянов, М. А. Кувишинов, И. А. Огнев, И. В. Никрошкин*

Рецензенты:

*А. В. Иванов*, канд. техн. наук, зав. кафедры ЗИ НГТУ

*А. Н. Фионов*, д-р техн. наук, проф. кафедры ПМИК СибГУТИ

Работа подготовлена на кафедре защиты информации

П 784

**Программно-аппаратные средства защиты информации** : учебное пособие / С. А. Зырянов, М. А. Кувишинов, И. А. Огнев, И. В. Никрошкин. – Новосибирск : Изд-во НГТУ, 2023. – 80 с.

ISBN 978-5-7782-4905-9

В учебном пособии приведены базовые понятия информационной безопасности и теоретические сведения о средствах защиты информации. Практическая часть включает в себя примеры заданий по изучаемым темам.

Учебное пособие предназначено для студентов направлений 10.00.00 «Информационная безопасность», может быть полезно преподавателям и слушателям курсов по направлению «Информационная безопасность», а также специалистам-практикам в области защиты компьютерной информации.

УДК 004.3:004.056(075.8)

**Зырянов Сергей Алексеевич  
Кувишинов Максим Алексеевич  
Огнев Игорь Александрович  
Никрошкин Иван Владимирович**

## **ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ**

**Учебное пособие**

Редактор *Е.Е. Татарникова*  
Выпускающий редактор *И.П. Брованова*  
Редактор *И.Е. Семенова*  
Дизайн обложки *А.В. Ладыжская*  
Компьютерная верстка *Л.А. Веселовская*

Налоговая льгота – Общероссийский классификатор продукции  
Издание соответствует коду 95 3000 ОК 005-93 (ОКП)

---

Подписано в печать 21.03.2023. Формат 60 × 84 1/16. Бумага офсетная. Тираж 50 экз.  
Уч.-изд. л. 4,65. Печ. л. 5,0. Изд. № 238/22. Заказ № 111. Цена договорная

---

Отпечатано в типографии  
Новосибирского государственного технического университета  
630073, г. Новосибирск, пр. К. Маркса, 20

**ISBN 978-5-7782-4905-9**

© Коллектив авторов, 2023  
© Новосибирский государственный  
технический университет, 2023

## ОГЛАВЛЕНИЕ

Введение .....	6
<b>1. Задача защиты информации.....</b>	<b>7</b>
<b>2. Требования законодательства РФ в сфере применения средств защиты информации.....</b>	<b>10</b>
2.1. Основные нормативные акты по применению средств защиты информации.....	10
2.2. СТР-К и РД АС.....	13
2.3. Приказы ФСТЭК России и ФСБ России.....	15
2.4. Сертификация средств защиты информации ФСТЭК и ФСБ.....	16
2.4.1. Общие требования законодательства.....	16
2.4.2. Общие требования к безопасности СЗИ .....	18
<b>3. Программно-аппаратные средства защиты информации .....</b>	<b>21</b>
3.1. Средства защиты от несанкционированного доступа .....	22
3.1.1. Система идентификации и аутентификации .....	22
3.1.2. Системы разграничения доступа .....	23
3.1.3. Средства доверенной загрузки.....	25
3.1.4. Аппаратные средства аутентификации и хранения ключевой информации.....	27
3.1.5. Замкнутые программные среды.....	28
3.1.6. Подсистема регистрации и учета.....	29
3.1.7. Средства контроля съемных машинных носителей информации .....	31
Контрольные вопросы .....	31

3.2. Межсетевые экраны.....	32
3.2.1. Классические межсетевые экраны .....	32
3.2.2. Межсетевые экраны уровня веб-приложений .....	35
3.2.3. Универсальный шлюз безопасности .....	36
3.2.4. Межсетевые экраны нового поколения .....	37
Контрольные вопросы .....	38
3.3. Системы обнаружения вторжений .....	39
Контрольные вопросы .....	41
3.4. Средства антивирусной защиты информации.....	42
Контрольные вопросы .....	45
3.5. Операционные системы.....	46
Контрольные вопросы .....	46
3.6. Средства криптографической защиты информации и защиты электронной подписи.....	47
3.6.1. Средства криптографической защиты информации .....	47
3.6.2. Электронные подписи .....	47
3.6.3. Инфраструктура открытых ключей.....	50
Контрольные вопросы .....	53
3.7. Системы сбора, корреляции и обработки событий ИБ.....	53
Контрольные вопросы .....	57
3.8. Системы предотвращения утечек информации .....	57
Контрольные вопросы .....	58
3.9. Системы защиты сред виртуализации .....	59
3.9.1. Основы виртуализации.....	59
3.9.2. Защита средств виртуализации.....	61
Контрольные вопросы .....	62
3.10. Песочницы и honeypot.....	63
3.10.1. Песочницы .....	63
3.10.2. Noreupot.....	67
Контрольные вопросы .....	69
<b>4. Практическая часть .....</b>	<b>70</b>
4.1. Настройка СЗИ от несанкционированного доступа Dallas Lock .....	70

4.2. Работа с операционной системой Astra Linux и средством антивирусной защиты Kaspersky Endpoint Security .....	71
4.3. Настройка МСЭ в СЗИ от несанкционированного доступа Secret Net Studio, работа со сканером уязвимостей «Сканер-ВС» .....	72
4.4. Создание правил для IDS Snort.....	73
Библиографический список .....	75