

А. И. Астайкин, А. П. Мартынов,  
Д. Б. Николаев, В. Н. Фомченко

# МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ПРОГРАММНО-АППАРАТНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

ПРЕЗИДЕНТСКАЯ ПРОГРАММА  
ПЕРЕПОДГОТОВКИ  
ИНЖЕНЕРНЫХ КАДРОВ

Защищенная  
локальная  
сеть

SKIP - защищенный  
трафик в публичной сети

Защищенная  
локальная  
сеть

Screen-  
устройство

Screen-  
устройство



ФГУП «Российский федеральный ядерный центр –  
Всероссийский научно-исследовательский институт  
экспериментальной физики»

А. И. Астайкин, А. П. Мартынов,  
Д. Б. Николаев, В. Н. Фомченко

# **Методы и средства обеспечения программно-аппаратной защиты информации**

**Президентская программа  
переподготовки инженерных кадров**

Саров  
2015

УДК 004.056(075.8)  
ББК 32.973я723  
М54

Одобрено научно-методическим советом Саровского физико-технического института Национального исследовательского ядерного университета «МИФИ» и ученым советом ФГМУ «Институт информатизации образования» Российской академии образования

Астайкин А. И., Мартынов А. П., Д. Б. Николаев, В. Н. Фомченко  
М54 Методы и средства обеспечения программно-аппаратной защиты информации: Научно-техническое издание. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2015. – 214 с. : ил.

ISBN 978-5-9515-0305-3

Курс Президентской программы «Методы и средства обеспечения программно-аппаратной защиты информации» на базе СарФТИ НИЯУ МИФИ позволяет оценить современное состояние дел в области защиты данных и получить практические навыки реализуемого информационно-технического обеспечения. Обобщены самые последние результаты исследований отечественных и зарубежных специалистов в области проектирования и построения систем защиты информации. Однако в первую очередь обсуждаются теоретические и практические результаты проведенных исследований и проектирования механизмов защиты несанкционированных действий.

Курс предназначен для студентов, аспирантов, научных работников, изучающих вопросы обеспечения безопасности информации, для инженеров–проектировщиков средств обеспечения безопасности информации, а также будет интересен специалистам в области теории информации и компьютерной безопасности.

УДК 004.056(075.8)  
ББК 32.973я723

ISBN 978-5-9515-0305-3

© ФГУП «РФЯЦ-ВНИИЭФ», 2015

## Содержание

<b>Предисловие</b> .....	5
<b>Введение</b> .....	13
<b>1. Общие положения</b> .....	16
1.1. Технический канал утечки информации .....	19
1.2. Демаскирующие признаки объектов .....	21
1.3. Каналы несанкционированного воздействия .....	23
1.4. Организационно-технические мероприятия и технические способы защиты информации защищаемого помещения .....	24
1.5. Организация защиты информации .....	28
<b>2. Криптографические методы защиты информации</b> .....	32
2.1. Исторические аспекты возникновения криптографии .....	32
2.2. Криптология в наши дни .....	34
2.3. Классификация алгоритмов шифрования .....	35
2.4. Симметричные алгоритмы шифрования .....	36
2.5. Асимметричные алгоритмы шифрования .....	51
<b>3. Технические средства защиты ЛВС</b> .....	59
3.1. Маршрутизаторы .....	59
3.2. Брандмауэр (firewall) .....	60
3.3. Пакетные фильтры .....	61
3.4. Шлюзы сеансового уровня .....	62
3.5. Шлюзы прикладного уровня .....	62
3.6. SPI-брандмауэры .....	63
3.7. Протокол NAT .....	63
3.8. Перенаправление портов (Port mapping) .....	64
3.9. DMZ-зона .....	66
3.10. Методы аутентификации .....	66
3.11. DHCP-сервер .....	67
3.12. Виртуальные сети VPN .....	67
3.13. Режимы функционирования VPN .....	68
3.14. Сетевой мост .....	69
3.15. Назначение мостов .....	69
3.16. Способы соединения ЛВС Ethernet и ЛВС Token Ring .....	71
3.17. Проблема защиты информации в Internet .....	72
3.18. Протокол SKIP .....	73
3.19. Выбор средств для построения системы защиты .....	83

<b>4. Защита информации в базах данных</b> .....	97
4.1. Реализация защиты в некоторых СУБД .....	103
4.2. Юридическая защита авторских прав на базы данных .....	116
<b>5. Практически навыки при работе с программой TrueCrypt</b> .....	118
5.1. Основные понятия .....	118
5.2. Преимущества TrueCrypt .....	120
5.3. Установка portable версии .....	120
5.4. Обычная установка .....	122
5.5. Создание виртуального зашифрованного диска, содержимое которого хранится в файле на физическом диске .....	125
5.6. Подключение зашифрованной флешки .....	131
<b>6. СЗИ «Dallas Lock 7.7»</b> .....	134
<b>7. Аккорд-АМДЗ</b> .....	140
<b>Заключение</b> .....	143
<b>Список литературы</b> .....	144
<b>Приложение А. Указ Президента Российской Федерации</b> .....	146
<b>Приложение Б. Приказ Министерства образования и науки Российской Федерации</b> .....	159
<b>Приложение В. Приказ Госкомвуза РФ от 22.12.1995 N 1687</b> .....	162
<b>Приложение Г. Программа повышения квалификации</b> .....	166
<b>Приложение Д. Программа стажировки (стажировок) на территории России</b> .....	201
<b>Приложение Е. Техническая характеристика примененных средств защиты</b> .....	204

Тема 10. Контроль целостности программного обеспечения и информации	Применяемые методы. Сравнительная оценка методов контрольной суммы и хэш-функций. Контроль с использованием циклических кодов. Методы дублирования. Средства защиты программного обеспечения от несанкционированной загрузки. Предпринимаемые меры обеспечения безопасности.		2
	Лабораторные занятия		2
Тема 11. Защита информации в линиях связи	1	Разработка программ защиты программного обеспечения от несанкционированной загрузки и изменения	2
	Средства обеспечения безопасности. Межсетевые экраны. Схема построения. Основные функции.		2
Тема 12. Средства регистрации доступа к информации	Лабораторные занятия		2
	1	Разработка программного обеспечения защиты от несанкционированного изменения в линиях связи	2
Тема 13. Методы расчета и инструментального контроля показателей защиты информации	Лабораторные занятия		
	1	Регистрируемые события. Способы регистрации. Организационные мероприятия по защите информации в автоматизированной системе.	2
Тема 14. Программно-аппаратная реализация средств обеспечения информационной безопасности	Лабораторные занятия		
	1	Виды контроля эффективности защиты информации. Основные положения методологии инженерно-технической защиты информации. Методы расчета и инструментального контроля показателей защиты информации.	2
	Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности. Программно-аппаратные средства защиты информации в сетях передачи данных.		2
	Лабораторные занятия		2
	1	Программно-аппаратные средства защиты информации в автоматизированных системах и сетях передачи данных	2

### 3. Материально-технические условия реализации программы модуля

Материально-технические условия реализации программы	Обеспеченность реализации программы собственными материально-техническими условиями (указать наименование, год выпуска используемого оборудования)	Наличие договоров/соглашений с предприятиями, учреждениями или организациями об использовании помещений, технологического оборудования, размещенного вне образовательного учреждения, в целях организации обучения
Технические средства	Компьютерный класс (2010 г.в.)	–
Компьютерно-информационные средства	Операционная система: Windows XP SP3 (2012 г.в. дополнений) Microsoft Office Project (v.2007 SP3) (2007 г.в.) Microsoft Office Groove (v.2007) (2007 г.в.) Авторское ПО	–
Наличие внутренних сетей и выхода Интернет	Локальная вычислительная сеть с выходом в Интернет (пропускная способность 10 Мбит/с)	–

Научно-техническое издание

**Астайкин** Анатолий Иванович, **Мартынов** Александр Петрович,  
**Николаев** Дмитрий Борисович, **Фомченко** Виктор Николаевич

***Методы и средства обеспечения  
программно-аппаратной защиты информации***

Президентская программа переподготовки инженерных кадров

Редактор *Н. П. Мишкина*

Компьютерная подготовка оригинала-макета

*Н. В. Мишкина*

Дизайн обложки *Е. Л. Соседко*

---

Подписано в печать 04.11.2015. Формат 70×100/16  
Усл. печ. л. 17,3 Уч.-изд. л. ~16,3 Тираж 300 экз. Зак. тип. 1438-2015

---

Отпечатано в ИПК ФГУП «РФЯЦ-ВНИИЭФ»  
607188, г. Саров Нижегородской обл., ул. Силкина, 23





**Астайкин Анатолий Иванович**

Главный научный сотрудник РЯЦ-ВНИИЭФ, заслуженный деятель науки РФ, доктор технических наук, профессор, действительный член Академии информатизации образования



**Мартынов Александр Петрович**

Начальник научно-исследовательского отдела, доктор технических наук, профессор, действительный член Академии информатизации образования



**Николаев Дмитрий Борисович**

Ведущий научный сотрудник, кандидат технических наук, доцент, член-корреспондент Академии информатизации образования



**Фомченко Виктор Николаевич**

Главный конструктор РЯЦ-ВНИИЭФ, заслуженный конструктор РФ, доктор технических наук, профессор, действительный член Академии информатизации образования

ISBN 978-5-9515-0305-3



9 785951 503053