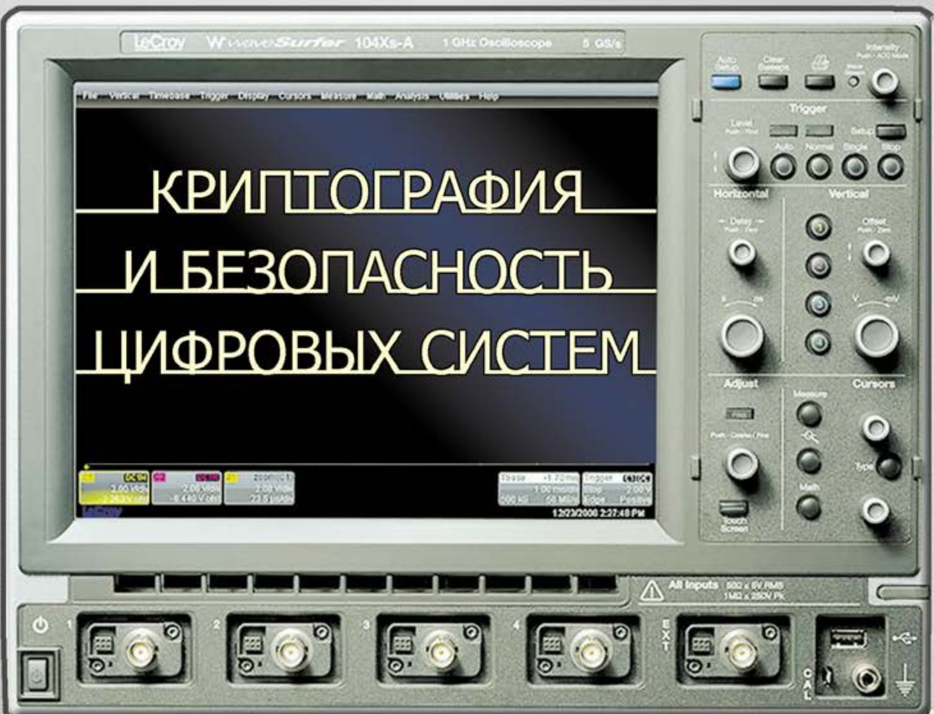
В. Г. Грибунин, А. П. Мартынов,
Д. Б. Николаев, В. Н. Фомченко

КРИПТОГРАФИЯ И БЕЗОПАСНОСТЬ ЦИФРОВЫХ СИСТЕМ



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

В. Г. Грибунин, А. П. Мартынов,
Д. Б. Николаев, В. Н. Фомченко

КРИПТОГРАФИЯ И БЕЗОПАСНОСТЬ ЦИФРОВЫХ СИСТЕМ

Учебное пособие

Под редакцией доктора технических наук, профессора,
заслуженного деятеля науки РФ А. И. Астайкина

Саров
2011

ŋqddɐǝɎ bɆ dǝdɆbɎзǝ d ɛɑɑbɔɐ ɟqddɎqɐè

УДК 004.056
ББК 32.973
К82

Грибунин В. Г., Мартынов А. П., Николаев Д. Б., Фомченко В. Н. Криптография и безопасность цифровых систем: Учебное пособие / Под ред. А. И. Астайкина. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2011, 411 с.

ISBN 978-5-9515-0166-0

В книге рассмотрены вопросы построения блочных и поточных алгоритмов преобразования информации, методы защиты ее целостности и подлинности, а также протоколы и методики, обеспечивающие безопасность данных в вычислительных сетях различного назначения. Особое место уделено проблемной области развития безопасных сетей – распространению ключевых параметров. Подробно рассмотрены практические подходы к построению инфраструктуры открытых ключей *PKI*. В настоящее время *PKI* активно развертываются не только на уровне крупных компаний, но и на общегосударственном уровне. Рассмотренные вопросы в совокупности представляют собой новое направление в сетевой криптографии, получившее название – виртуальные частные сети *VPN*. Применение этой основанной на криптографии технологии позволяет строить механизмы, обеспечивающие конфиденциальность и целостность передаваемой информации в корпоративных сетях и при соединении нескольких сетей через *Internet*.

В основу книги положены материалы лекций, прочитанных авторами в НИЯУ МИФИ, и учебно-методические пособия, разработанные авторами или при их непосредственном участии на кафедре «Радиофизика и электроника» по курсам «Основы криптографии» и «Криптография и специальные исследования». Изложение вопросов предполагает математическую подготовку читателей. Книга предназначена для студентов, аспирантов и преподавателей соответствующих специальностей. Она может быть использована инженерно-техническими и научными работниками, занимающимися разработкой и применением вычислительных и радиоэлектронных систем и систем их защиты, а также специалистами в области защиты информации.

ISBN 978-5-9515-0166-0

СОДЕРЖАНИЕ

№ п/п	Функции	*Cisco PIX* 520 *Firewall* v4.2 *CISCO LTD*	*IOS Cisco Firewall Feature Set CISCO LTD*	ФПСУ-*IP* ООО «АМИКОН»	Технология *DioNIS* ООО «ФАКТОР-ТС»	«КОНТИНЕНТ-К» «Информзащита»	*FireWall*-1 *Check Point*
	Другие функции						
44	Удаленное управление	Есть (по *tcp/ip*)	Есть (по *tcp/ip*)	Нет	Есть. Интерактивное (по *tcp/ip*,x.25, rs232), *SNMP*	Есть. В пакетном режиме	Есть (по *tcp/ip*)
45	Проверка целостности ПО	При старте (необходим отдельный модуль, разработки Анкей)	Нет	При старте, хэш-функция	В динамике, при старте, хэш-функция по госту	В динамике, при старте	В динамике, при старте
46	Резервирование своего состояния	Нет	Нет	Есть (администратором)	Есть	Есть	Есть
47	Мониторинг в р.в., трассировка каналов	Нет	Нет	Нет	Есть	Нет	Мониторинг
48	Фиксация событий, протоколирование	Есть	На внешнем сервере	Встроенная	Встроенная	Есть	Есть
49	Сигнализация	На ЦУС	На внешнем сервере	Встроенная, ЦУС	Консоль, ЦУС, *SMTP*	Нет данных	Есть
50	Защита целостности ПО, Данных и системы (НСД)	Пароль	Пароль	ТМ, Floppy disk key (Аккорд)	*ТМ, Floppy disk key* (Криптон, Аккорд и др.)	Есть	Пароль
51	Используемые средства НСД	Собственные	Собственные	Аккорд	Криптон, Аккорд , *Secret N*	*SecretNet*, Соболь	Аккорд + средства ОС
52	*DHCP-Server*	Нет	Нет	Нет	Есть	Нет	Средствами ОС
53	*DNS Server* (разделяемый)	Нет	Нет	Нет	Есть	Нет	Средствами ОС
54	Интеллектуальное взаимодействие с *UPS*	Нет	Нет	Нет	Есть (корректное закрытие)	Нет данных	Есть
55	Отказоустойчивое исполнение с горячим резервом	Есть	Нет	Нет данных	Есть (+*RAID HDD*)	Есть	Нет

№ п/п	Функции	*Cisco PIX* 520 *Firewall* v4.2 *CISCO LTD*	*IOS Cisco Firewall Feature Set CISCO LTD*	ФПСУ-*IP* ООО «АМИКОН»	Технология *DioNIS* ООО «ФАКТОР-ТС»	«КОНТИНЕНТ-К» «Информзащита»	*FireWall*-1 *Check Point*
56	Функции защищенного сервера доступа	Нет	Есть	Нет	Есть	Есть	Нет
57	Обеспечение *QoS*	Есть	Есть	Нет	Есть	Нет	Нет
	Производительность комплекса						
58	Производительность с *NAT+Filtr*	~ 50-90 Мбит/с	> 10 Мбит/с	Без *NAT* 55 Мбит/с	~ 90 Мбит/с (PIII 500)	Нет	15-18 Мбит/с
59	Производительность с *Ftr+NAT*+шифр	Нет данных	500 кбит/с	~10 Мбит/с	~ 90 Мбит/с	30-80 Мбит/с	4-18 Мбит/с
60	Увеличение производительности при включенной компресссии	Нет	Нет	Нет	В 5 раз при скоростях до 1 Мбит/с и трафике *FTP, HTTP*	Нет данных	Нет
61	Число одновременных виртуальных соединений через *Firewall*	Лицензии на 128, 1024, 65536	Лицензии на 25, 50, 250, 65536	2048	*IP-Filtr* – Не ограниченно *NAT* – 2048, *SMTP* – 32	Нет данных	25, 50 …..

Грибунин Вадим Геннадьевич**, Мартынов** Александр Петрович**,**
Николаев Дмитрий Борисович**, Фомченко** Виктор Николаевич

Криптография и безопасность цифровых систем

Учебное пособие

Редактор *Н. П. Мишкина*
Компьютерная подготовка оригинала-макета
Н. В. Мишкина
Художник *Т. В. Андреева*

Подписано в печать 17.06.2011. Формат 70×100/16
Усл. печ. л. 33,14 Уч. изд. л. 33,3 Тираж 300 экз. Зак. тип. 2008-2010

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

Грибунин Вадим Геннадьевич
Заместитель начальника инженерно-криптографического отдела Восьмого Управления ГШ ВС РФ, кандидат технических наук

Мартынов Александр Петрович
Начальник научно-исследовательского отдела РФЯЦ-ВНИИЭФ, доктор технических наук, профессор, действительный член Академии информатизации образования

Николаев Дмитрий Борисович
Начальник научно-исследовательской группы РФЯЦ-ВНИИЭФ, кандидат технических наук, доцент, член-корреспондент Академии информатизации образования

Фомченко Виктор Николаевич
Главный конструктор РФЯЦ-ВНИИЭФ, заслуженный конструктор РФ, доктор технических наук, профессор, действительный член Академии информатизации образования

ISBN 978-5-9515-0166-0