

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



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

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

© ФГУП «РФЯЦ-ВНИИЭФ», 2011

СОДЕРЖАНИЕ

Список условных обозначений, сокращений и терминов	9
Введение	11
Часть первая. ШИФРОВАНИЕ, ЦЕЛОСТНОСТЬ, АУТЕНТИФИКАЦИЯ.	14
1. Алгоритмы шифрования	14
1.1. Блочные симметричные алгоритмы шифрования	14
1.1.1. Принципы построения блочных алгоритмов	14
1.1.2. Режимы работы блочных шифров	17
1.1.3. Алгоритм <i>AES</i>	19
1.1.4. Статистическое тестирование блочных криптоалгоритмов	25
1.2. Асимметричные алгоритмы шифрования	29
1.2.1. Общие принципы построения асимметричных алгоритмов	29
1.2.2. <i>RSA</i>	31
1.2.3. Протокол согласования ключей Диффи – Хеллмана	34
1.2.4. Сравнение асимметричных и симметричных криптосистем	35
1.3. Поточные шифры	36
1.3.1. Общие принципы построения поточных шифров	36
1.3.2. Самосинхронизирующиеся поточные шифры	38
1.3.3. Российский шифр – <i>ABC</i>	40
1.3.4. Конкурс <i>eSTREAM</i>	42
1.3.5. Построение псевдослучайных генераторов случайных чисел	45
1.3.6. Методы тестирования поточных шифров и генераторов случайных чисел	48
1.3.7. Аппаратные генераторы случайных чисел	51
2. Методы защиты целостности данных	53
2.1. Криптографические методы контроля целостности	53
2.2. Защита целостности данных на основе <i>CRC</i> -кодов	56
2.3. Имитозащита на основе криптографических бесключевых хэш-функций	58
2.3.1. Свойства хэш-функций	58
2.3.2. Хэш-функция <i>MD5</i>	60
2.3.3. Хэш-функция <i>SHA</i>	63
2.3.4. Хэш-функция ГОСТ 34.11-94	65
2.4. Функции хэширования с ключом	66

2.4.1. Функции хэширования на основе блочных алгоритмов шифрования	66
2.4.2. Алгоритм <i>НМАС</i>	68
2.5. Защита целостности и аутентификация отправителя на основе ЭЦП	69
2.5.1. Понятие об ЭЦП	69
2.5.2. Схема подписи <i>RSA</i>	72
2.5.3. Схема подписи Эль-Гамала	74
2.5.4. ГОСТ 34.10-2001	76
2.5.5. О стойкости ЭЦП	79
3. Аутентификация	81
3.1. Основные понятия аутентификации	81
3.2. Основные типы механизмов аутентификации	83
3.3. Парольная аутентификация	85
3.3.1. Многоразовые пароли	85
3.3.2. Атаки на парольную систему защиты и методы защиты	89
3.3.3. Одноразовые пароли	90
3.4. Механизмы типа запрос-ответ	96
3.4.1. Запрос-ответ с использованием симметричных алгоритмов шифрования	97
3.4.2. Запрос-ответ с использованием асимметричных алгоритмов шифрования	99
3.5. Идентификация и механизмы подтверждения подлинности пользователя	101
3.6. Взаимная проверка подлинности пользователей	103

Часть вторая. ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ И ШИФРОВАНИЯ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ ..

4. Защита на канальном уровне	111
4.1. Протокол канального уровня <i>L2F</i>	111
4.1.1. Формат протокола	113
4.2. Протокол канального уровня <i>L2TP</i>	114
4.2.1. Формат протокола	115
4.2.2. Протокольные операции	116
4.2.3. Соображения безопасности	120
5. Защита на сетевом уровне	122
5.1. Протокол сетевого уровня <i>IPSec</i>	122
5.1.1. Архитектура защиты	123
5.1.2. Аутентифицирующий заголовок <i>AH</i>	128
5.1.3. Инкапсуляция зашифрованных данных <i>ESP</i>	129
5.1.4. Алгоритмы аутентификации и шифрования <i>IPSec</i>	131
5.1.5. Установление безопасных ассоциаций	133

5.1.6. База данных политики безопасности (<i>SPD</i>)	135
5.1.7. База данных безопасных ассоциаций (<i>SAD</i>)	136
5.1.8. Атаки на <i>AH</i> , <i>ESP</i> и <i>IKE</i>	138
5.2. Протокол сетевого уровня <i>SKIP</i>	139
5.2.1. Принципы функционирования и формат протокола	140
6. Защита на транспортном уровне	143
6.1. Протокол транспортного уровня <i>PPTP</i>	143
6.1.1. Принципы функционирования и формат протокола	144
6.1.2. Аспекты безопасности	146
6.2. Криптоанализ туннельного протокола типа точка-точка (<i>PPTP</i>)	147
6.2.1. Криптоанализ <i>MS-CHAP</i>	148
6.2.2. Криптоанализ <i>MPPE</i>	149
6.2.3. Другие атаки на <i>MS-PPTP</i>	152
7. Защита на сеансовом уровне	153
7.1. Протокол сеансового уровня <i>SSL</i>	154
7.1.1. Описание взаимодействий	157
7.1.2. Формат протокола	161
7.1.3. Атаки на протокол <i>SSL</i>	162
7.2. Протокол сеансового уровня <i>TLS</i>	164
7.2.1. Краткое описание протокола	166
7.2.2. Протокол записей <i>TLS</i>	168
7.2.3. Протокол диалога <i>TLS</i>	173
7.2.4. Особенности реализации	177
7.2.5. Аспекты безопасности	179
7.3. Протокол сеансового уровня <i>SOCKS 5</i>	181
7.3.1. Функционирование протокола <i>SOCKS 5</i>	183
7.3.2. Аспекты безопасности	189
8. Защита на прикладном уровне	189
8.1. Управление идентификацией и доступом	192
8.2. Защищенный удаленный доступ	196
8.3. Протокол <i>S/Key</i>	199
8.4. Протокол <i>PPP PAP</i>	200
8.5. Протокол <i>PPP CHAP</i>	201
8.6. Протокол <i>RADIUS</i>	202
8.6.1. Порядок работы протокола	203
8.6.2. Режим <i>Challenge/Response</i>	205
8.6.3. Взаимодействие с <i>PAP</i> и <i>CHAP</i>	205
8.6.4. Сервер-посредник (<i>Proxy</i>)	206
8.6.5. Формат заголовков протокола <i>RADIUS</i>	208
8.6.6. Вопросы безопасности	208
8.7. Протокол управления доступом <i>TACACS</i>	209

8.7.1. Описание соединений	210
8.7.2. Форматы запросов	210
8.7.3. Формат заголовков протокола <i>TACACS</i>	213
8.7.4. Вопросы безопасности	214
8.8. Доступ по схеме однократного входа с авторизацией <i>Single Sign-On (SSO)</i>	215
8.8.1. Серверные системы однократного входа	217
8.8.2. Клиентские системы однократного входа	218
8.8.3. Аутентификация на основе маркера	219
8.8.4. Системы однократного входа <i>Web-SSO</i>	220
8.8.5. <i>SSSSO</i> системы однократного входа	223
8.9. <i>Pretty Good Privacy (PGP)</i>	223
8.9.1. Краткое описание <i>PGP</i>	224
8.9.2. Шифрование файлов и сообщений	225
8.9.3. Симметричные алгоритмы <i>PGP</i>	226
8.9.4. Сжатие данных	227
8.9.5. О случайных числах, используемых в качестве сеансовых ключей	228
8.9.6. Расшифрование файлов и сообщений	228
8.9.7. Электронная цифровая подпись	229
8.10. Протокол <i>S/MIME</i>	230
8.10.1. Спецификация <i>MIME (Multipurpose Internet Mail Extension)</i>	230
8.10.2. Функциональные возможности <i>S/MIME</i>	231
8.10.3. Формирование объекта <i>envelopedData</i> (упакованные данные)	232
8.10.4. Формирование объекта <i>signedData</i> (подписанные данные)	233
8.10.5. Расширенные сервисы обеспечения безопасности	235
9. Другие прикладные протоколы аутентификации	236
9.1. Протокол обмена ключами <i>IKE</i>	236
9.1.1. Основной режим	236
9.1.2. Активный режим	237
9.1.3. Ускоренный режим	238
9.2. Протокол <i>SSH</i>	239
9.2.1. Ключ хоста	240
9.2.2. Транспортный уровень <i>SSH</i>	241
9.2.3. Протокол аутентификации <i>SSH-USERAUTH</i>	242
9.2.4. Протокол соединения <i>SSH-CONNECT</i>	243
9.3. <i>Kerberos</i>	244
9.3.1. Концепции функционирования <i>Kerberos</i>	246
9.3.2. Управление ключами	248
9.3.3. Сеансовые мандаты	249

17.1. VPN-решения ОАО «Элвис-Плюс»	360
17.2. Структура решений	363
17.3. Выбор продуктов	364
17.4. Описание решений	367
17.5. Использование ПЗИП в сетях <i>Cisco</i>	370
17.6. Поддержка VPN в маршрутизаторах компании <i>Cisco Systems</i>	371
17.7. Поддержка VPN в маршрутизаторах компании <i>3Com</i>	374
17.8. VPN-решения и продукты компании <i>Check Point</i>	375
17.8.1. Программные решения	377
17.8.2. Программно-аппаратные комплексы	379
17.9. VPN-решения ФГУП НТЦ «Атлас»	382
17.9.1. Ключевая система	382
17.10. Программные продукты <i>RAS</i> и <i>RRAS</i> от компании <i>Microsoft</i>	384
17.11. VPN-решения компании <i>Nortel</i>	385
17.12. VPN-решения ОАО «Инфотекс»	386
17.13. VPN-решения ЗАО «Сигнал-КОМ»	389
17.13.1. Программно-аппаратный комплекс <i>CSP VPN</i>	389
17.13.2. IP-шифратор для организации VPN с функциями межсетевого экрана (<i>IPSafe-PRO</i>)	392
Список литературы	395
Приложение 1	400
Приложение 2	404

№ 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 <i>tcp/ip</i>)	Есть (по <i>tcp/ip</i>)	Нет	Есть. Интерактивное (по <i>tcp/ip</i> , x.25, rs232), <i>SNMP</i>	Есть. В пакетном режиме	Есть (по <i>tcp/ip</i>)
45	Проверка целостности ПО	При старте (необходим отдельный модуль, разрабатки 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., трасировка 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, <i>SMTP</i>	Нет данных	Есть
50	Защита целостности ПО, Данных и системы (НСД)	Пароль	Пароль	TM, Florry disk key (Аккорд)	TM, Florry 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	<i>DHCP-Server</i>	Нет	Нет	Нет	Есть	Нет	Средствами ОС
53	<i>DNS Server</i> (разделяемый)	Нет	Нет	Нет	Есть	Нет	Средствами ОС
54	Интеллектуальное взаимодействие с <i>UPS</i>	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 <i>DioNIS</i> ООО «ФАКТОР-ТС»	«КОНТИНЕНТ-К» «Информзащита»	<i>FireWall-1</i> <i>Check Point</i>
56	Функции защищенно- го сервера доступа	Нет	Есть	Нет	Есть	Есть	Нет
57	Обеспечение <i>QoS</i>	Есть	Есть	Нет	Есть	Нет	Нет
	Производительность комплекса						
58	Производительность с <i>NAT+Filtr</i>	~ 50-90 Мбит/с	> 10 Мбит/с	Без <i>NAT</i> 55 Мбит/с	~ 90 Мбит/с (РПШ 500)	Нет	15-18 Мбит/с
59	Производительность с <i>Ftr+NAT</i> +шифр	Нет данных	500 кбит/с	~10 Мбит/с	~ 90 Мбит/с	30-80 Мбит/с	4-18 Мбит/с
60	Увеличение производи- тельности при включен- ной компрессии	Нет	Нет	Нет	В 5 раз при скоростях до 1 Мбит/с и трафике <i>FTP</i> , <i>HTTP</i>	Нет данных	Нет
61	Число одновременных виртуальных соединений через <i>Firewall</i>	Лицензии на 128, 1024, 65536	Лицензии на 25, 50, 250, 65536	2048	<i>IP-Filtr</i> – Не ограничено <i>NAT</i> – 2048, <i>SMTP</i> – 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



9 785951 501660