

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

СОВРЕМЕННЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АТОМНОЙ ЭНЕРГЕТИКЕ



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

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

СОВРЕМЕННЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АТОМНОЙ ЭНЕРГЕТИКЕ

Монография

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

Саров
2014

УДК 621.039:004.056

ББК 32.973

С56

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

Рецензенты: ректор НГТУ им. Р. Е. Алексеева, д-р техн. наук *С. М. Дмитриев*; декан радиофизического факультета ННГУ им. Н. И. Лобачевского профессор, д-р физ.-мат. наук *А. В. Якимов*; главный научный сотрудник РФЯЦ-ВНИИЭФ д-р. физ.-мат. наук *В. А. Терехин*

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

С56 Современные методы обеспечения безопасности информации в атомной энергетике: Монография / Под ред. А. И. Астайкина. – Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2014. – 636 с. – ил.

ISBN 978-5-9515-0265-0

Рассмотрены аспекты информационной безопасности применительно к системам защиты, управления и контроля объектов атомной энергетики. Рассмотрены возможные модели несанкционированных действий и современные алгоритмы криптографического преобразования информации, используемые для обеспечения безопасности, целостности и подлинности данных в контурах защиты, управления и контроля устройств и объектов атомной энергетики.

Книга предполагает известную математическую подготовку читателей, особенно в области криптографической защиты информации, теории вероятностей и математической статистики.

УДК 621.039:004.056

ББК 32.973

ISBN 978-5-9515-0265-0

© ФГУП «РФЯЦ-ВНИИЭФ», 2014

СОДЕРЖАНИЕ

Предисловие	5
Введение	7
Глава 1. Введение в концептуальные основы построения систем управления и контроля. Особенности построения данных систем в атомной энергетике	9
Глава 2. Информационная составляющая ядерной безопасности систем управления и контроля	16
Глава 3. Криптографические системы и их модели	21
Глава 4. Источники исходного сообщения и их алфавиты	35
Глава 5. Анализ языков ассемблера распространенных процессоров	80
Глава 6. Количество информации и энтропия	114
Глава 7. Теоретическая стойкость криптографических систем	130
Глава 8. Практическая стойкость криптографических систем	143
Глава 9. Криптоалгоритм ЛЮЦИФЕР фирмы <i>IBM</i>	156
Глава 10. Анализ американского стандарта криптографического преобразования информации <i>DES</i>	165
Глава 11. Алгоритм криптографического преобразования систем расчета и обработки информации по ГОСТ 28147-89 и его программная реализация	180
Глава 12. Симметричные криптографические системы	199
Глава 13. Асимметричные криптографические системы	224
Глава 14. Анализ основных принципов организации криптографических протоколов	239
Глава 15. Протоколы аутентификации и шифрования в информационно-вычислительных сетях	294
Глава 16. Защита на канальном уровне	298
Глава 17. Защита на сетевом уровне	310
Глава 18. Защита на транспортном уровне	331
Глава 19. Защита на сеансовом уровне	342

Глава 20. Защита на прикладном уровне	380
Глава 21. Другие прикладные протоколы аутентификации	428
Глава 22. Инфраструктура открытых ключей	448
Глава 23. Структура и основные элементы архитектуры инфраструктуры открытых ключей	456
Глава 24. Структуры данных и политика инфраструктуры открытых ключей	479
Глава 25. Особенности построения инфраструктуры открытых ключей	508
Глава 26. Безопасные системы управления и контроля на базе виртуальных частных сетей	522
Заключение	562
Список терминов, условных обозначений и сокращений	563
Список литературы	566
Приложение 1. Статистические данные по темам «Вычислительная техника», «Политика» и «Художественная литература»	571
Приложение 2. Исходный текст программы STAT	590
Приложение 3. Основы математической теории связи	606
Приложение 4. Сравнительные характеристики средств криптографической защиты информации, межсетевых экранов и VPN-технологий	629

№ 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
	Поддержка TCP/IP						
16	Функции IP-сервера доступа (Dialup.X.25)	Нет	Есть	Нет	Есть (до 34 Dialup)	Нет	Только IP, Средствами ОС
17	Функции IP- маршрутизатора	Есть	Есть		Есть	Есть	Средствами ОС
18	Функции IP- криптомаршрутизатора	Нет	Нет	Нет	Есть	Есть	Средствами ОС
19	Статическая/динамическая ip-маршрутизация/ поддержка RIP	Есть/Есть/Есть	Есть/Есть/Есть	Нет	Есть/Есть/Есть	Средствами ОС	Средствами ОС
	Защита на транспортном уровне (IP)						
20	IP-фильтрация на транспортном уровне	TCP, UDP	TCP, UDP	TCP, UDP	TCP, UDP	TCP, UDP	TCP, UDP
21	IP-фильтрация служебных протоколов	Есть	Есть	Есть	Есть	Есть	Есть
22	IP-фильтрация с учетом вх/вых интерф.	Есть	Есть	Есть	Есть	Есть	Есть
23	Возможность сокрытия наличия МЭ	Частично	Нет	Обеспечивается	Есть	Есть	Частичная
24	Фильтрация ip-port	Есть	Есть	Есть	Есть	Есть	Есть
25	Фильтрация URL	Есть	Есть		HTTP-Proxy	Есть	Есть
26	Трансляция IP-адресов/портов NAT/PAT	Есть/Есть (RFC 1631)	Есть/- (RFC 1631)	Средствами VPN	Есть/- (RFC 1631)	Есть (RFC 1631)	Есть (RFC 1631)
27	Динамический/статический	Есть/Есть	Есть		Есть/Есть		Есть

№ 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
28	Поддержка NAT дина- мического IP-адреса		Нет		Есть, PPP (Dialup, X.25)		
29	IP-фильтрация по гра- фику (Дата, время)	Есть	Нет	Есть	Есть	Есть	Есть/Н.Д.
	Защита на прикладном уровне (IP)						
30	Фильтрация на приклад- ном уровне посредством сервис-посредников	Smtp, http, ftp, telnet, java, snmp	Smtp, http	Telnet, snmp	ftp, telnet, smtp/pop3, http, ftp	Нет	Smtp, http, ftp, telnet, java, snmp
31	Фильтрация почты	Smtp только по 25 port с ограничением команд	smtp	Нет	SMTP-сервер-посредник, Черные-белые списки, Расписание, альтернатив- ные маршруты,	Нет	Smtp
32	Архивация и резервиро- вание почтового графиче- ска (SMTP, Межхост ...)	Нет	Нет	Нет	Есть	Нет	Нет
33	Шифрование почты	Нет	Нет	Нет	Есть, на межузловом уровне	Нет	Нет
34	Контролируемая тран- закция файлов (Клиент- сервер)	Нет	Нет	Нет	Есть	Нет	Нет
35	Возможность доставки почты по альтернатив- ным не IP-каналам (X.25,...)	Нет	Нет	Нет	Есть, Z-modem (X.25, IPX, Dialup)	Нет	Нет
36	Возможность антиви- русной проверки почты	Нет	Нет	Нет	Есть (Диалог-наука)	Нет	Есть

№ 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>
	Аутентификация						
37	Аутентификация	Есть. <i>RAP/CHAP</i> (необходим внешний сервер <i>RADIUS</i> , <i>TACACS+</i>), <i>SecurID</i> , <i>AXENT</i> , <i>CryptoCard</i> , <i>NDS</i> , <i>NT</i> до- мен, <i>UNIX</i> домен	Нет, но есть в со- ставе маршрути- затора и с внеш- ним сервером <i>RADIUS</i> , <i>TACACS+</i>	Х.509 (АМИКОН)	Есть Межузловая и клиент- ская (<i>RAP/CHAP</i> /ГОСТ28147- 89)	Есть ГОСТ28147-89, Х.509	<i>RADIUS</i> , <i>TACACS+</i> , Х.509, <i>MD5</i>
	Туннелирование, шифрование						
38	Туннелирование <i>IP</i> тра- фика	<i>IPSec</i> , <i>IETF</i>	<i>IPSec</i> , <i>IETF</i> , <i>L2TP</i> ..	Есть	<i>IPSec</i>	<i>IPSec</i>	<i>IKE</i> , <i>FWZ</i> , <i>IPSec</i> , <i>SKIP</i>
39	<i>VPN over X.25 (IP VPN over X.25)</i>	Нет	Есть	Нет	Есть	Нет	Нет
40	Метод шифрования, маскирования <i>IP</i> - трафика	<i>DES</i> 56, 112, 186 <i>bit</i> (аппа- ратно или программно) <i>CISCO PIX</i> <i>Ravlin encr.</i> <i>card</i>	<i>DES</i> 40, 56, <i>bit</i> (аппаратно или программно) <i>CISCO PIX Ravlin encr. card</i>	Свой, ГОСТ28147-89	ГОСТ28147-89 (аппарат- но или программно)	ГОСТ28147-89 (программно)	<i>DES</i> 40, 56, 168 <i>RSA</i> 512/1024
41	Компрессия <i>IP</i> -трафика	Нет	Нет	Есть	Есть	Есть	Сторонних фирм
42	Число <i>VPN</i> направлений	256	Нет данных	1024	256 стат., 4000 динам.	Нет данных	Нет
43	Абонентское шифрова- ние	Нет	Нет	Нет данных	Есть, <i>DisSec</i>	Есть, АП Континент	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>
	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, разраб. Анкей)	Нет	При старте, хэш-функция	В динамике, при старте, хэш-функция по госту	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, <i>SMTP</i>	Нет данных	Есть
50	Защита целостности ПО, Данных и системы (НСД)	Пароль	Пароль	TM, Floppy disk key (Аккорд)	TM, Floppy disk key (Криптон, Аккорд и др.)	Есть	Пароль
51	Используемые средства НСД	Собственные	Собственные	Аккорд	Криптон, Аккорд, <i>Secret Net</i>	<i>SecretNet</i> , Соболь	Аккорд + средствами 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 (+ <i>RAID HDD</i>)	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 защищенного 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+Filter</i>	~ 50-90 Мбит/с	> 10 Мбит/с	Без <i>NAT</i> 55 Мбит/с	~ 90 Мбит/с (PII 500)	Нет	15-18 Мбит/с
59	Производительность с <i>Ftr+NAT+шифр</i>	Нет данных	500 кбит/с	~10 Мбит/с	~ 90 Мбит/с	30-80 Мбит/с	4-18 Мбит/с
60	Увеличение производительности при включенной 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-Filter</i> – Не ограничено <i>NAT</i> – 2048, <i>SMTP</i> – 32	Нет данных	25, 50

Научное издание

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

***Современные методы обеспечения безопасности информации
в атомной энергетике***

Монография

Редактор *Н. П. Мишкина*
Компьютерная подготовка оригинала-макета
С. В. Макеева, Н. В. Мишкина

Подписано в печать 04.08.2014. Формат 70×100/16
Усл. печ. л. 51,27 Уч.-изд. л. 49,67 Тираж 500 экз. Зак. тип. 1587-2013

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