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 образоваия» 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

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*
	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
26	Трансляция *IP*-адресов/портов *NAT/PAT*	Есть/Есть (*RFC* 1631)	Есть/– (*RFC* 1631)	Средствами *VPN*	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* динамического *IP*-адреса		Нет		Есть ,*PPP* (*Dialup*, X.25)		
29	*IP*-фильтрация по графику (Дата, время)	Есть	Нет	Есть	Есть	Есть	Есть/Н.Д.
	Защита на прикладном уровне *(IP)*						
30	Фильтрация на прикладном 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, альтернативные маршруты,	Нет	*Smtp*
32	Архивация и резервирование почтового трафика (*SMTP*, Межхост …)	Нет	Нет	Нет	Есть	Нет	Нет
33	Шифрование почты	Нет	Нет	Нет	Есть, на межузловом уровне	Нет	Нет
34	Контролируемая транзакция файлов (Клиент-сервер)	Нет	Нет	Нет	Есть	Нет	Нет
35	Возможность доставки почты по альтернативным не *IP*-каналам (X.25,..)	Нет	Нет	Нет	Есть , *Z-modem* (X.25, *IPX, Dialup*)	Нет	Нет
36	Возможность антивирусной 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 *DioNIS* ООО «ФАКТОР-ТС»	«КОНТИНЕНТ-К» «Информзащита»	*FireWall-1 Check Point*
	Аутентификация						
37	Аутентификация	Есть. *PAP/CHAP* (необходим внешний сервер *RADIUS, TACACS*+), *SecurID, AXENT, CryptoCard, NDS, NT* домен, *UNIX* домен	Нет, но есть в составе маршрутизатора и с внешним сервером *RADIUS, TACACS*+	X.509 (АМИКОН)	Есть Межузловая и клиентская (*PAP/CHAP*/ГОСТ28147-89)	Есть ГОСТ28147-89, X.509	*RADIUS, TACACS*+, X.509, *MD*5
	Туннелирование, шифрование						
38	Туннелирование *IP* трафика	*IPSec, IETF*	*IPSec*, *IETF, L2TP*..	Есть	*IPSec*	*IPSec*	*IKE, FWZ, IPSec, SKIP*
39	*VPN over* X.25 (*IP VPN over* X.25)	Нет	Есть	Нет	Есть	Нет	Нет
40	Метод шифрования, маскирования *IP*-трафика	*DES* 56, 112, 186 *bit* (аппаратно или программно) *CISCO PIX Ravlin encr. card*	*DES* 40, 56, *bit* (аппаратно или программно) *CISCO PIX Ravlin encr. card*	Свой, ГОСТ28147-89	ГОСТ28147-89 (аппаратно или программно)	ГОСТ28147-89 (программно)	*DES* 40, 56, 168 *RSA* 512/1024
41	Компрессия *IP*-трафика	Нет	Нет	Есть	Есть	Есть	Сторонних фирм
42	Число *VPN* направлений	256	Нет данных	1024	256 стат., 4000 динам.	Нет данных	Нет
43	Абонентское шифрование	Нет	Нет	Нет данных	Есть. *DiSec*	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 *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	TM, Floppy disk key (Аккорд)	*TM, 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 …..

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.