

УДК 004.056
ББК 32.973.26-018.2
Ч55

- Ч55** Система защиты информации ViPNet: учеб. пособие. / Сост. Н. В. Грициенко, А. О. Чефранова, А. В. Уривский, Ю. Ф. Алабина и др.; под ред. д. п. н., профессора А. О. Чефрановой. – М.: ДМК Пресс, 2013. – 384 с.: ил.

ISBN 5-94074-878-6

Пособие представляет собой краткий обзор продуктов торговой марки ViPNet, разработанных компанией ОАО «ИнфоТеКС» для решения задач организации защищенных виртуальных частных сетей (VPN), развертывания инфраструктуры открытых ключей (PKI), а также защиты персональных мобильных и домашних компьютеров. Рассмотрены практические сценарии использования технологии ViPNet.

Пособие предназначено для слушателей учебных курсов по технологии ViPNet, а также для авторизованных центров ОАО «ИнфоТеКС», на базе которых проходит обучение по программам подготовки специалистов ViPNet. Также оно может быть рекомендовано специалистам служб компьютерной безопасности по вопросам построения комплексных систем защиты информации и применения средств защиты в автоматизированных системах.

УДК 004.056
ББК 32.973.26-018.2

Все права защищены. Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ОАО «ИнфоТеКС».

ViPNet является зарегистрированной торговой маркой ОАО «ИнфоТеКС».

Все торговые марки и названия программ являются собственностью их владельцев.

Материал, изложенный в данной книге, многократно проверен. Но, поскольку вероятность технических ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. По этой причине издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 5-94074-878-6

© Коллектив авторов, 2013
 © Оформление, ДМК Пресс, 2013



Используемые аббревиатуры	12
Введение	14
История компании ОАО «ИнфоТеКС»	18

Глава 1

Продукты ViPNet для построения виртуальных защищенных сетей	23
1.1. Продуктовая линейка ViPNet CUSTOM	23
1.2. Программный пакет ViPNet OFFICE	26
1.3. ViPNet Administrator 3.x	28
1.3.1. ViPNet Центр управления сетью (ЦУС)	28
Основные функциональные возможности	28
Типовой порядок первичной конфигурации сети ViPNet	43
Подсистема адресной администрации сети	44
Подсистема прикладной администрации сети	45
Управление сетью	46
1.3.2. ViPNet Удостоверяющий и ключевой центр (УКЦ)	46
Основные функции программы ViPNet Удостоверяющий и ключевой центр	46
Лицензионное ограничение	48
Системные требования	48
Варианты развертывания	49

Выбор необходимого дополнительного программного обеспечения ViPNet	50
Ключевая структура ViPNet	51
Формирование ключевой информации в ViPNet.....	61
Обновление мастер-ключей в сети ViPNet.....	69
1.4. ViPNet Client.....	72
1.4.1. Назначение ПО ViPNet Client	72
1.4.2. Функции ПО ViPNet Client	73
1.4.3. Состав ПО ViPNet Client.....	76
ViPNet Монитор.....	76
Модули: ViPNet MFTP (Client).....	85
ViPNet Контроль приложений	90
Модули: ViPNet Деловая почта.....	92
1.5. ViPNet Coordinator (Windows).....	96
1.5.1. Назначение ПО ViPNet Coordinator.....	96
1.5.2. Состав ПО ViPNet Coordinator.....	98
ViPNet-драйвер	98
Принцип работы ViPNet-драйвера.....	99
ViPNet Монитор.....	101
ViPNet MFTP	102
ViPNet Контроль приложений	103
1.5.3. Функции координатора в защищенной сети ViPNet.....	103
Сервер-маршрутизатор	104
Маршрутизатор VPN-пакетов	105
Сервер IP-адресов.....	106
Межсетевой экран	112
Туннелирование.....	123
NAT-сервер.....	125
Сервер Открытого Интернета	129
1.5.4. Принципы осуществления соединений в сети ViPNet	132
1.5.5. Виртуальные IP-адреса.....	134
Назначение технологии виртуальных IP-адресов	134

1.5.6. Практические сценарии использования координатора	137
Использование DHCP-сервера в сети ViPNet	137
Организация DMZ	138
1.6. ViPNet Coordinator (Linux)	139
1.6.1. Система защиты от сбоев	141
1.7. Программный модуль ViPNet Cluster (Windows)	143
1.7.1. Назначение ViPNet-кластера	144
1.7.2. Сетевая структура кластера	145
1.7.3. Ролевая структура кластера	147
1.7.4. Отказоустойчивость кластера	148
1.7.5. Логическая архитектура кластера	151
1.7.6. Производительность кластера	152
1.7.7. Модуль управления кластером ViPNet Cluster Монитор	156
1.7.8. Система горячего резервирования	158
1.8. ViPNet StateWatcher	159
1.8.1. Назначение системы мониторинга	159
1.8.2. Архитектура и общая топология системы мониторинга	161
1.8.3. Сервер мониторинга	164
1.8.4. АРМ мониторинга	166
1.8.5. Архитектура каскадирования Серверов мониторинга	168
1.9. ViPNet Policy Manager	170
1.9.1. Принципы централизованного управления политиками безопасности сетевых узлов	170
1.9.2. Основные возможности ViPNet Policy Manager	172
1.9.3. Интерфейс программы	174
1.9.4. Разграничение полномочий на основе ролей пользователей	176
1.9.5. Общие сведения о шаблонах политики безопасности	177
1.9.6. Правила формирования результирующей политики безопасности	178
Отправка и получение политик безопасности	180
Применение политик безопасности на сетевых узлах	180
1.10. ViPNet SafeDisk-V	181

1.10.1. Назначение программы.....	181
1.10.2. Основные возможности программы.....	182
1.10.3. Принципы защиты информации в ViPNet SafeDisk-V.....	184
Интеграция с программой ViPNet Client	185
1.11. Сценарии использования технологии ViPNet CUSTOM.....	186
1.11.1. Организация соединений Client-Client и Remote Client-Office.....	186
1.11.2. Организация соединений Office-Office	188
1.11.3. Защищенное соединение Mobile Client.....	190
1.11.4. Организация туннеля и полутуннеля	192
1.11.5. Защита IP-телефонии на примере решения Cisco.....	194
1.11.6. Использование ViPNet SafeDisk.....	196
1.11.7. Сценарий использования виртуальных адресов при работе со службами WINS И DNS.....	197
1.12. ViPNet Manager	199
1.12.1. Встроенные функции ViPNet OFFICE	201
1.12.2. Сценарий развертывания сети ViPNet.....	202
1.12.3. Интерфейс программы.....	204
1.12.4. Создание сети ViPNet: порядок действий.....	206
1.13. Схемы развертывания сети ViPNet OFFICE.....	212
1.13.1. Соединение между удаленным пользователем и офисом.....	212
1.13.2. Соединение между двумя удаленными пользователями.....	215
1.13.3. Соединение между двумя офисами.....	216
1.13.4. Соединение между двумя офисами с использованием туннелирования	219

Глава 2

Программно-аппаратный комплекс

УЦКУ ViPNet..... 224

2.1. Назначение программно-аппаратного комплекса УЦКУ ViPNet	224
--	-----

Услуги безопасности, предоставляемые криптографией с открытым ключом	224
--	-----

2.2. Состав ПАК УЦКУ ViPNet	226
2.2.1. Стандартизация и совместимость.....	228
2.3. Услуги, предоставляемые удостоверяющим центром	229
2.4. Архитектура PKI	230
Иерархическая модель установления доверительных отношений.....	230
Сетевая (распределенная) модель установления доверительных отношений.....	231
«Мостовая» модель установления доверительных отношений.....	232
Браузерная модель установления доверительных отношений.....	233
2.5. ViPNet Registration Point	234
2.5.1. Основные возможности программы ViPNet Registration Point.....	236
2.5.2. Принципы работы программы ViPNet Registration Point	238
Регистрация пользователей.....	238
Создание запросов в Центре регистрации	241
Передача данных пользователю.....	242
2.5.3. Основные схемы установки программы.....	245
2.5.4. Форматы экспорта сертификатов в программе ViPNet Registration Point	246
2.6. ViPNet Publication Service	247
2.6.1. Основные функции программы	249
2.6.2. Назначение публикаций.....	250
Публикация сертификатов и СОС.....	250
Импорт СОС из доверенных сетей ViPNet и сторонних УЦ.....	254
2.7. ViPNet CryptoService	254
2.7.1. Состав и назначение ViPNet CryptoService	255
Компоненты ViPNet CryptoService.....	256
Схемы использования ViPNet CryptoService.....	258
Схема работы в качестве сервера-маршрутизатора	258
Схема использования совместно с ViPNet CryptoFile.....	260
2.7.2. ViPNet CryptoFile	262

Глава 3

Программно-аппаратные комплексы ViPNet..... 264

3.1. Программно-аппаратный комплекс ViPNet Coordinator HW	265
3.1.1. Состав программного обеспечения ПАК ViPNet Coordinator HW	265
3.1.2. Назначение ПАК ViPNet Coordinator HW.....	266
3.1.3. Аппаратная архитектура	266
ViPNet Coordinator HW	266
ViPNet Coordinator NME-RVPN.....	277
3.1.4. Применение ПАК ViPNet Coordinator HW	279
3.1.5. Сертификация	279
3.1.6. Функциональные возможности.....	280
Сервер-маршрутизатор	280
Сервер IP-адресов.....	281
Межсетевой экран	282
Антиспуфинг.....	283
Сервер NAT – принципы трансляции адресов.....	284
3.1.7. Система защиты от сбоев на базе ПАК Coordinator HW ...	289
Режимы работы системы защиты от сбоев	291
Схемы кластера горячего резервирования.....	294
3.2. Программно-аппаратный комплекс ViPNet Terminal	296
Варианты исполнения ViPNet Terminal	297
Сценарии применения	298
Преимущества ViPNet Terminal	299

Глава 4

Межсетевые экраны..... 301

4.1. ViPNet Office Firewall	301
4.1.1 Назначение программы ViPNet Office Firewall	301
4.1.2. Основные возможности программы	302
4.1.3. Состав программного обеспечения.....	306

4.1.4. Основные преимущества программы.....	306
4.1.5. Типовые варианты использования ViPNet Office Firewall	307
4.2. ViPNet Personal Firewall.....	308
4.2.1. Назначение программы ViPNet Personal Firewall	308
4.2.2. Основные возможности программы	308
4.2.3. Состав программного обеспечения.....	310
4.2.4. Основные преимущества программы.....	311
4.2.5. Настройка сетевых фильтров в программе ViPNet Personal Firewall	313
Действие фильтров.....	314

Глава 5

Шифраторы логических дисков316

5.1. ViPNet SafeDisk.....	316
5.1.1. Принципы защиты информации в ViPNet SafeDisk	317
5.1.2. Уничтожение следов работы с информацией.....	318

Глава 6

Криптопровайдеры и защищенный документооборот321

6.1. Прикладные криптографические интерфейсы в ПО ViPNet.....	321
6.1.1. Стандартные интерфейсы.....	321
6.1.2. Интерфейсы разработки компании «ИнфоТеКС»	322
ViPNet SDK	323
Схема использования компонента ViPNet SDK в системе электронного документооборота	324
6.2. ViPNet CSP.....	325
6.2.1. Функции программы.....	325
6.2.2. Практическое применение ViPNet CSP.....	326
Схема использования в составе ViPNet CryptoService.....	326
Шифрование и подпись документов	327

Шифрование и подпись сообщений в Microsoft Outlook	330
Создание запроса на сертификат и формирование контейнера ключей электронной подписи.....	331
Аутентичность и конфиденциальность соединений TLS/SSL	333

Глава 7

Продукты ViPNet для мобильных устройств	334
7.1. Преимущества технологии ViPNet	336
7.2. Мобильные приложения ViPNet	337
7.3. Поддерживаемые мобильные устройства	338
7.3.1. Устройства Apple	338
7.3.2. Устройства Android	339
7.4. Практические сценарии использования мобильных приложений ViPNet	339
7.4.1. Защищенная IP-телефония	339
7.4.2. Терминальный доступ к корпоративным ресурсам и интернет-ресурсам	340
7.4.3. Удаленный доступ к корпоративному серверу Microsoft Exchange	341

Глава 8

Защита межведомственных взаимодействий с использованием технологии ViPNet	343
8.1. Система межведомственного электронного взаимодействия	343
8.2. Организация защиты межведомственного электронного взаимодействия на основе технологии ViPNet	344
8.2.1. Компоненты системы ViPNet ЭДО	344
8.2.2. ПАК ViPNet ЭДО Шлюз безопасности	347
Аппаратная архитектура ПАК ViPNet ЭДО Шлюз безопасности первой модификации	348

Аппаратная архитектура ПАК ViPNet ЭДО Шлюз безопасности второй модификации.....	349
Принцип работы программного обеспечения ViPNet ЭДО Шлюз безопасности	350

Приложение 1

Информация о внешних устройствах хранения данных.....	354
--	------------

Глоссарий.....	359
-----------------------	------------

Указатель	382
------------------------	------------