УТВЕРЖДЕН

ИСКП.00022-01 32 01-ЛУ

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	2373
Подп. и дата	
Инв. № подл.	

ПРОГРАММНЫЙ КОМПЛЕКС МЕЖСЕТЕВОГО ЭКРАНА

С ФУНКЦИЯМИ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Руководство системного программиста

ИСКП.00022-01 32 01

Листов 45

2018

Литера $О_1$

АННОТАЦИЯ

Данный документ является руководством системного программиста для программного комплекса межсетевого экрана с функциями системы обнаружения вторжений (далее по тексту – МЭ или программа), предназначенного для организации и предоставления услуг телекоммуникационного взаимодействия по протоколу IPv4.

Документ описывает назначение, структуру МЭ, последовательность установки и настройки программы.

Настоящее описание входит в состав эксплуатационной документации и рассчитано на системного программиста, имеющего навыки работы на персональной электронно-вычислительной машине (ПЭВМ) в операционной системе (ОС) Linux.

СОДЕРЖАНИЕ

Лист

1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1. Назначение программы

1.1.1. Программа предназначена для реализации следующих телекоммуникационных услуг:

– маршрутизации/коммутации сетевого трафика;

– балансировки трафика;

– туннелирования трафика;

– организации защищенных соединений;

– динамического конфигурирования настроек сетевых узлов;

– синхронизации часов сетевых узлов;

– групповой маршрутизации;

– зеркалирования трафика;

– фильтрации трафика;

– преобразования сетевых адресов;

– защищенной передачи трафика;

– приоритизации IP-трафика;

– обеспечения заданного качества обслуживания;

– обеспечения увеличения доступности шлюза;

– локального и удаленного управления.

1.1.2. МЭ обеспечивает производительность не менее 1000000 пакетов/с при размере пакета 64 байта (таблицы фильтрации пустые, настройки приоритизации отсутствуют).

1.1.3. МЭ обеспечивает производительность не менее 500000 пакетов/с (размер пакета 64 байта) при заполненной таблице маршрутизации (1000 маршрутов), заполненной таблице фильтрации (1000 записей) и настроенной приоритизацией (1000 классов).

1.1.4. МЭ обеспечивает пропускную способность в режиме межсетевого экранирования не менее 400 Мбит/с при минимально допустимой заполненной таблице маршрутизации, заполненной таблице фильтрации (1000 записей), отсутствующих настройках приоритизации и длине пакета 1500 байт.

1.1.5. МЭ поддерживает следующие интерфейсы:

– Ethernet 10BASE-T/100BASE-T/1000BASE-T, SFP;

– G.703 (2048 кбит/с, framed/unframed);

– RS-232.

Примечания:

1. Для интерфейсов Ethernet МЭ обеспечивает программное определение позиций интерфейсов.

2. Для локального управления МЭ используется выделенный порт RS-232 или Ethernet.

1.1.6. МЭ обеспечивает:

– функционирование PPP;

– функционирование MLPPP;

– функционирование протокола LLDP;

– функционирование в роли сервера и клиента PPPoE;

– функционирование в роли сервера и клиента PPTP.

1.1.7. МЭ обеспечивает:

– функционирование по протоколу IPv4;

– прием и передачу IP-пакетов по протоколам семейства TCP/IP;

– явное задание скорости интерфейса для Ethernet (10/100/1000), режим работы (half duplex, full duplex), автосогласование;

– явную настройку MTU на сетевых интерфейсах, в том числе и туннельных;

– вывод в интерфейс управления статистики по сетевым интерфейсам (тип/количество ошибок, тип/количество переданных/принятых пакетов);

– возможность снятия бита DF на сетевых интерфейсах;

– возможность объединения сетевых интерфейсов в группу IEEE 802.3ad;

– возможность мониторинга состояния каналов Ethernet по протоколам TCP, ICMP;

– функционирование протокола NetFlow v9;

– возможность работы под управлением гипервизора системы виртуализации.

1.1.8. Программа в части маршрутизации (коммутации) сетевого трафика обеспечивает предоставление пользователям следующих услуг:

– маршрутизацию IP-трафика;

– статическую маршрутизацию;

– динамическую маршрутизацию;

– маршрутизацию на основе политик;

– объединение портов Ethernet по технологии switch;

– организацию взаимодействия телекоммуникационных устройств на канальном уровне VLAN (Virtual Local Area Network);

– поддержку технологии VXLAN;

– распределение трафика в соответствии с классом трафика между каналами.

Примечание. Порты Ethernet, объединенные по технологии switch, имеют общий IP-адрес.

1.1.9. Динамическая маршрутизация осуществляется по следующим протоколам:

– RIPv2 (Routing Information Protocol);

– OSPFv2 (Open Shortest Path First);

– BGPv4 (Border Gateway Protocol).

Примечания:

1. Существует возможность отключения (блокирования) протоколов динамической маршрутизации.

2. МЭ обеспечивает вывод в интерфейс управления информации об источниках маршрутов в таблице маршрутизации.

1.1.10. Программа позволяет осуществлять маршрутизацию в зависимости от значения поля ToS (DSCP), длины IP-пакета, входного интерфейса. Существует возможность настройки маршрутизации выделенных абонентов (подсетей) через определенный шлюз.

1.1.11. МЭ обеспечивает:

– настройку таймеров OSPFv2;

– возможность просмотра через интерфейс управления таблицы принятых и анонсируемых маршрутов BGPv4.

1.1.12. Программа поддерживает правила фильтрации при перераспределении маршрутной информации.

1.1.13. МЭ обеспечивает:

– балансировку нагрузки при наличии нескольких маршрутов с одинаковой метрикой;

– объединение сетевых интерфейсов для отказоустойчивости и увеличения пропускной способности – Bonding;

– распространение трафика через несколько физических каналов, имея одно логическое соединение – MLPPP.

1.1.14. Программа в части туннелирования трафика обеспечивает предоставление пользователям следующих услуг:

– туннелирование PPTP;

– туннелирование PPPoE;

– туннелирование IPIP;

– туннелирование GRE.

Программа обеспечивает защиту данных, передаваемых по межсетевому протоколу IP (IPSec).

Программа поддерживает протокол туннелирования второго уровня L2TP.

1.1.15. МЭ обеспечивает настройку маршрутизации выделенных IP-потоков в туннели PPPoE и PPTP как с клиентской стороны, так и с серверной стороны туннеля.

1.1.16. Программа обеспечивает:

– возможность изменения значения MSS в TCP-пакетах для предотвращения Path MTU Discovery Black Hole;

– функционирование DNS-клиента и DNS-proxy;

– средства расширенной сетевой диагностики (расширенный ping, traceroute, arp-ping);

– возможность разделения одного физического сетевого интерфейса на несколько логических подинтерфейсов (subinterface);

– поддержку loopback-интерфейсов;

– возможность назначения (изменения) MAC-адреса на своих интерфейсах и подинтерфейсах;

– возможность назначения нескольких IP-адресов на своих интерфейсах и подинтерфейсах;

– статическое и динамическое заполнение таблицы MAC-адресов (ARP);

– возможность функционирования как ARP-proxy.

1.1.17. В части организации взаимодействия телекоммуникационных устройств на канальном уровне VLAN МЭ обеспечивает:

– добавление и снятие тегов VLAN IEEE 802.1Q, VLAN QinQ IEEE 802.1ad на интерфейсах, работающих в режиме коммутатора;

– выборочное добавление верхнего тега VLAN QinQ в зависимости от нижнего VLAN 802.1Q (Selective QinQ);

– создание логических подинтерфейсов сетевого уровня для каждого тега VLAN 802.1Q или совокупности верхнего и нижнего тегов VLAN QinQ, с возможностью привязки их к физическим портам.

1.1.18. Программа в части организации защищенных соединений обеспечивает предоставление пользователям услуги аутентификации в PPP посредством CHAP.

1.1.19. Программа в части динамического конфигурирования настроек сетевых узлов обеспечивает предоставление пользователям следующих услуг:

– обеспечение запрашивающих хостов IP-адресами и другими конфигурационными параметрами посредством DHCPv4;

– настройку интерфейса автоконфигурированием средствами DHCPv4;

– распределение IP-адресов на определенный срок;

– ретрансляцию сообщений DHCP между клиентами и серверами в разных подсетях.

Распределение IP-адресов посредством DHCP осуществляется тремя способами:

– ручное распределение;

– автоматическое распределение;

– динамическое распределение.

1.1.20. Программа в части синхронизации часов сетевых узлов обеспечивает предоставление пользователям услуги функционирования NTPv4–клиента (сервера) с возможностью явно задать часовой пояс.

1.1.21. Программа в части групповой маршрутизации обеспечивает предоставление пользователям следующих услуг:

– функционирование IGMPv2;

– механизм доставки дейтаграмм для групп хостов без организации соединений – PIM SM.

1.1.22. Программа обеспечивает фильтрацию на всех интерфейсах (реальных и виртуальных) и предоставляет пользователям следующие услуги:

– фильтрацию трафика по порту (TCP/UDP) отправителя;

– фильтрацию трафика по порту (TCP/UDP) получателя;

– фильтрацию трафика по IP-адресу отправителя;

– фильтрацию трафика по IP-адресу получателя;

– фильтрацию трафика по MAC-адресу отправителя;

– фильтрацию трафика по флагам заголовка сегмента TCP;

– фильтрацию трафика по значению поля «Протокол» заголовка IP;

– фильтрацию трафика по значению поля «ToS» (TOS/DSCP) заголовка IP;

– фильтрацию трафика по флагам заголовка IP;

– фильтрацию трафика по времени;

– фильтрацию трафика по состоянию соединения;

– фильтрацию трафика по регулярным выражениям;

– фильтрацию трафика по сетевым интерфейсам;

– фильтрацию трафика по мандатным меткам.

Примечания:

1. МЭ обеспечивает фильтрацию входящего, исходящего и пересылаемого трафика.

2. МЭ обеспечивает фильтрацию фрагментированных пакетов.

3. МЭ имеет возможность тестирования (вручную) реализации правил фильтрации и прохождения сетевых пакетов.

4. Существует возможность добавления (удаления) мандатных меток безопасности в поле опций IP-заголовка.

1.1.23. Программа обеспечивает маркировку IP-пакетов, предусматривающую обработку поля DSCP в заголовке IP-пакета со следующими возможностями:

– сохранение имеющегося значения;

– маркировку DSCP;

– перемаркировку DSCP.

1.1.24. В МЭ существует возможность просмотра средствами локального управления таблицы состояний TCP-соединений.

МЭ поддерживает не менее 1000000 конкурирующих TCP-сессий.

1.1.25. Программа обеспечивает три базовые концепции трансляции адресов:

– статическую (Static Network Address Translation);

– динамическую (Dynamic Address Translation);

– маскарадную (NAPT, NAT Overload, PAT).

1.1.26. МЭ поддерживает настройку демилитаризованной зоны (DMZ) в сочетании с маршрутизацией и трансляцией адресов (NAT) или трансляцией портов (PAT).

1.1.27. Программа в части защищенной передачи трафика обеспечивает предоставление пользователям следующих услуг:

– шифрованный IP-туннель IPSec;

– защищенный канал VPN на основе OpenVPN.

В МЭ реализована поддержка групповой передачи данных multicast routing (сетевой пакет одновременно направляется определенной группе адресатов) для VPN-соединений.

1.1.28. МЭ обеспечивает классификацию и приоритетную обработку пакетов по следующим критериям:

– порту (TCP/UDP) отправителя;

– порту (TCP/UDP) получателя;

– IP-адресу отправителя;

– IP-адресу получателя;

– MAC-адресу отправителя;

– значению поля «Протокол» заголовка IP;

– значению поля «ToS» (TOS/DSCP) заголовка IP;

– длине пакетов;

– значению трех битов в теге 802.1Q Ethernet-кадра;

– совокупности указанных критериев.

1.1.29. МЭ обеспечивает маркировку и перемаркировку кадров/пакетов в трех битах в теге 802.1Q Ethernet-кадра и поле «ToS» (TOS/DSCP) заголовка IP по следующим критериям:

– порту (TCP/UDP) отправителя;

– порту (TCP/UDP) получателя;

– IP-адресу отправителя;

– IP-адресу получателя;

– MAC-адресу отправителя;

– значению поля «Протокол» заголовка IP;

– значению поля «ToS» (TOS/DSCP) заголовка IP;

– длине пакетов;

– значению трех битов в теге 802.1Q Ethernet-кадра;

– совокупности указанных критериев.

1.1.30. Программа в части обеспечения заданного качества обслуживания обеспечивает предоставление пользователям следующих услуг:

– организацию и обработку очередей методами FIFO, PQ, CBQ, SFQ, TBF, HTB, HFSC;

– функционирование механизма явного уведомления о перегрузке ECN;

– функционирование алгоритма раннего обнаружения переполнения очередей маршрутизатора RED (Random Early Detection – отброс очередей недопустимой длины в произвольном порядке);

– функционирование алгоритма раннего обнаружения переполнения очередей маршрутизатора GRED (Generic Random Early Detection).

1.1.31. МЭ позволяет задать полосу пропускания в процентах для определенного администратором типа трафика.

1.1.32. Программа в части обеспечения увеличения доступности шлюза обеспечивает автоматическое назначение функций шлюза на резервный маршрутизатор в случае отказа основного – VRRP (Virtual Router Redundancy Protocol).

1.1.33. Программа в части локального и удаленного управления обеспечивает предоставление пользователям следующих услуг:

– возможность конфигурирования себя посредством CLI (command-line interface) локально (путем ввода с клавиатуры текстовых команд) и удаленно (при подключении по протоколу SSHv2 или Telnet);

– возможность удаленного управления по протоколам NETCONF и SNMP.

Примечания:

1. МЭ обеспечивает возможность отключения (блокирования) любого из способов управления, кроме локального.

2. МЭ обеспечивает возможность ограничения доступа к управлению только с доверенных IP-адресов либо подсетей.

3. Первоначально доступно только локальное управление через консольный порт управления.

4. Максимальное число одновременных подключений для управления МЭ через Telnet, SSH или локально равно пяти.

1.1.34. Программа обеспечивает передачу данных о событиях на удаленный сервер (syslog, SNMP trap).

1.1.35. МЭ обеспечивает:

– проверку корректности основных задаваемых параметров функционирования;

– вывод текстового предупреждения в CLI при некорректно задаваемом параметре;

– сохранение сконфигурированных профилей;

– возможность вывода в текстовом виде имеющихся в системе профилей через интерфейс управления, а также их копирование на внешний носитель информации;

– применение сохраненных профилей;

– возможность вывода информации о текущей загруженности центрального процессора и оперативного запоминающего устройства;

– возможность поддерживать работу сервиса сторожевого таймера («watchdog») для отслеживания состояния демона «mprd» и выполнения автоматической перезагрузки устройства в случае прекращения нормального функционирования демона (зависания).

1.1.36. В МЭ реализована функция отказоустойчивого кластера в конфигурации «Активный/Пассивный».

1.1.37. МЭ обеспечивает:

– возможность одновременной работы с несколькими внешними сетями;

– возможность переключения на резервный канал;

– возможность ограничения числа соединений с одного IP-адреса;

– возможность поддержки модели ролевого доступа.

1.1.38. В МЭ реализованы системы ролевого доступа со следующими пользователями:

– администратор сети (с функцией настройки сетевых интерфейсов и служб);

– администратор безопасности (с функцией настройки туннелей и правил межсетевого экранирования);

– администратор аудита (с функцией доступа на чтение).

1.1.39. Программа обеспечивает ведение журналов, в которых регистрирует следующие события:

– загрузка и инициализация системы и её остановки;

– вход (выход) пользователей в систему (из системы), с фиксацией ошибок авторизации;

– пользовательские команды;

– работа правил списка доступа;

– результат фильтрации входящих (исходящих) пакетов.

При регистрации событий фиксируется:

– дата и время регистрируемого события;

– IP-адрес источника и IP-адрес получателя (при фильтрации), включая порты протоколов TCP, UDP.

Программа позволяет сортировать, архивировать, просматривать и печатать журналы.

МЭ обеспечивает передачу данных о событиях на удаленный сервер.

1.1.40. В МЭ осуществляется автоматический контроль целостности программного обеспечения.

1.1.41. Программа обеспечивает возможность обновления программного обеспечения.

1.1.42. Программа имеет возможность отключения неиспользуемых портов и сервисов.

1.1.43. МЭ обладает функциями самотестирования (проверки работоспособности).

При обнаружении нарушения функций МЭ с помощью системы самотестирования, МЭ выводит на консоль управления и в журналы сообщение о возникшей проблеме и полностью блокирует передачу всех видов транзитного трафика.

МЭ сохраняет штатный режим функционирования или автоматически к нему возвращается при следующих типах сбоев:

– нарушение целостности контролируемых файлов с последующей успешной попыткой восстановления этих файлов из резервной копии;

– нарушение работы МЭ (снижение доступности) в результате DDOS-атаки при условии, что вмешательство оператора позволило нейтрализовать атаку с помощью настроек фильтрации МЭ либо если атака прекратилась по другим причинам.

При невозможности восстановления файлов с нарушенной целостностью, МЭ завершает работу всех процессов и отключается.

Примечание. Сбой – это самоустраняющийся отказ или однократный отказ, устраняемый незначительным вмешательством оператора.

1.1.44. В МЭ предусмотрена система обнаружения вторжений (СОВ), соответствующая следующим требованиям и обладающая возможностями:

– обнаружение попыток несанкционированного доступа;

– работа в режиме предотвращения компьютерных атак;

– поддержка статистического метода выявления аномалий сетевого трафика типа DoS-flooding;

– эвристический метод выявления сетевых атак;

– контроль нескольких сетей с разными скоростями;

– добавление, редактирование и удаленное обновление баз сигнатур атак;

– централизованное управление и мониторинг посредством CLI, используя удаленное подключение по протоколу SSHv2;

– гибкость системы генерации отчетов;

– обеспечение интеграции с подсистемой мониторинга, управления и корреляции событий информационной безопасности по протоколу Syslog.

1.1.45. Существует следующее ограничение при использовании МЭ – для защиты информации, составляющей государственную тайну, подключенные к МЭ каналы связи, подверженные пассивному и (или) активному прослушиванию, должны быть защищены с помощью средств защиты информации (СЗИ), использующих методы, устойчивые к таким воздействиям, а сам МЭ, СЗИ и связывающие их интерфейсы должны находиться в пределах контролируемой зоны.

1.1.46. Ограничением на применение является также то, что программа не поддерживает телекоммуникационные взаимодействия по протоколу IPv6 и не осуществляет защиту от изменения кадров и пакетов средствами перехватчиков трафика.

1.2. Требования к техническим и программным средствам

1.2.1. МЭ функционирует на аппаратной платформе с характеристиками не хуже:

– процессор с архитектурой x86;

– оперативная память 4 Гбайта;

– постоянное запоминающее устройство 16 Гбайт;

– порт RS-232;

– интерфейс USB;

– две сетевых карты Fast Ethernet.

Примечание. Порт RS-232 необходим для работы по протоколу PPP. На некоторых аппаратных платформах он может отсутствовать.

1.2.2. В ходе эксплуатации МЭ допускается замена Ethernet-карт без изменения мест установки в слотах системной шины. При этом перед вводом имени пользователя и пароля будет выводиться сообщение вида «Autocheck: ERRORS: …. hardware_check=ERROR ……», сигнализирующее об изменении состава аппаратного обеспечения. Для утверждения текущего состава аппаратного обеспечения требуется выполнить команду «system update hardware».

В случае необходимости увеличения или уменьшения количества Ethernet-карт требуется переустановить программное обеспечение.

1.2.3. В зависимости от версии программного обеспечения и комплектации оборудования функциональные возможности программы могут отличаться.

2. СТРУКТУРА ПРОГРАММЫ

2.1. В МЭ реализован принцип модульного построения программного обеспечения, когда каждый отдельный модуль отвечает за решение узкоспециализированной задачи. Все программное обеспечение разделяется на несколько подсистем. Каждая подсистема в свою очередь разделяется на набор модулей, которые реализуют определенную специализированную задачу.

2.2. Взаимодействие между модулями организовано на базе прямой адресации объектов в пределах одной подсистемы, или же с использованием буферизированных средств взаимодействия (файлы, сокеты и сигналы).

2.3. Структурная схема программы представлена на рис. 1.

2.4. МЭ функционально подразделяется на следующие составные части:

– сетевая подсистема;

– файловая подсистема;

– подсистема управления (агент управления);

– подсистема межсетевого экрана и обнаружения вторжений;

– подсистема кластеризации;

– подсистема обмена управляющими взаимодействиями;

– подсистема аутентификации;

– подсистема контроля целостности;

– подсистема тестирования;

– подсистема восстановления;

– подсистема регистрации;

– подсистема аудита;

– подсистема взаимодействия с аппаратной платформой;

– подсистема установки МЭ.

2.5. Сетевая подсистема обеспечивает взаимодействие МЭ на сетевом уровне по протоколу IP, на канальном уровне по протоколу Ethernet, а также приоритизацию трафика, туннелирование ipip, отслеживание соединений, статическую и динамическую маршрутизацию, сбор статистики.

2.6. Подсистема межсетевого экрана и обнаружения вторжений обеспечивает фильтрацию принимаемых и передаваемых данных с использованием правил, определяемых администраторами МЭ.

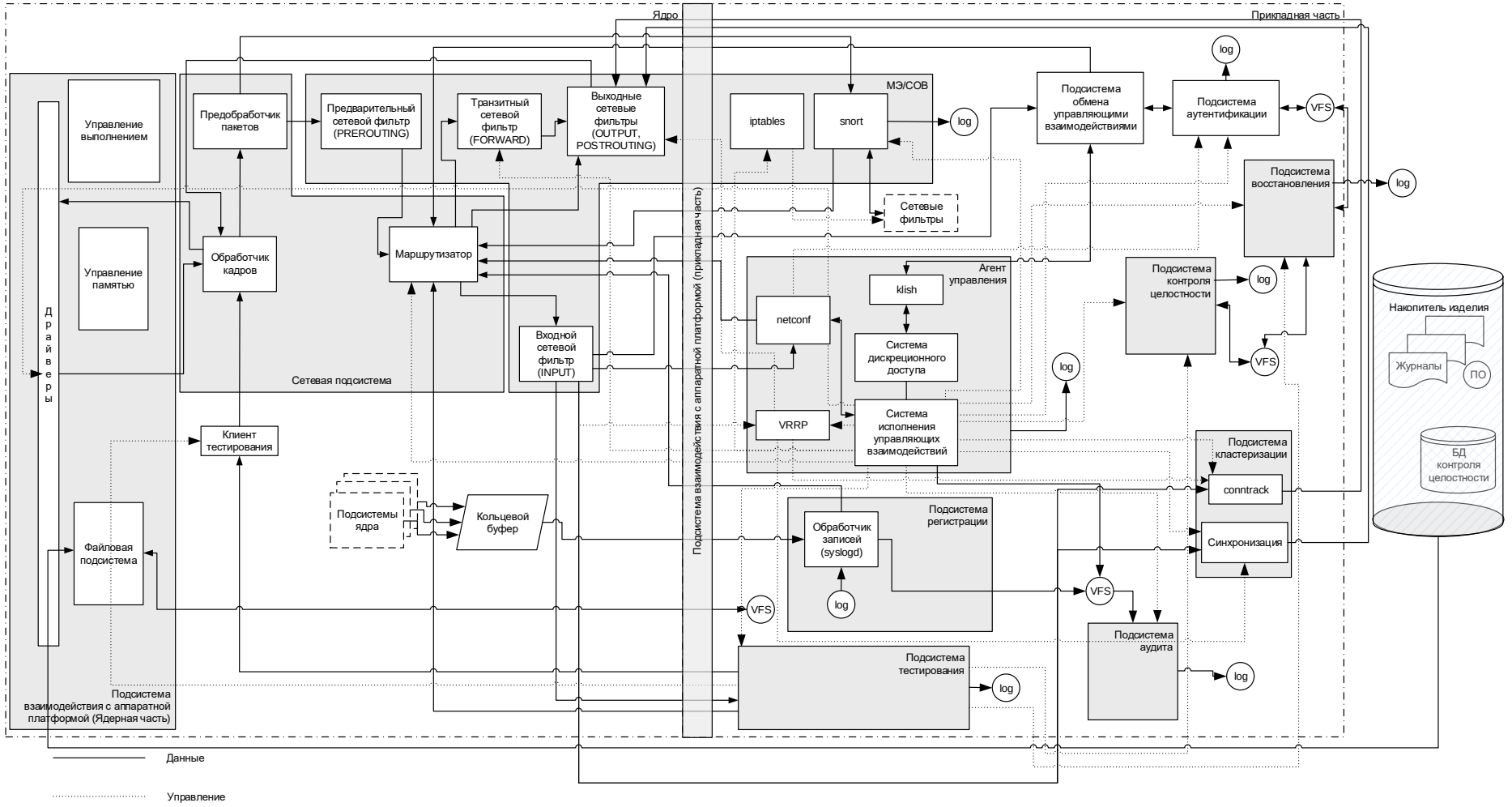
Ядро
Прикладная часть
Управление выполнением
Управление памятью
Драйверы
Предобработчик пакетов
Предварительный сетевой фильтр (PREROUTING)
Транзитный сетевой фильтр (FORWARD)
Выходные сетевые фильтры (OUTPUT, POSTROUTING)
МЭ/СОВ
iptables
snort
log
Подсистема обмена управляющими взаимодействиями
Подсистема аутентификации
VFS
Подсистема восстановления
Сетевые фильтры
Обработчик кадров
Маршрутизатор
Сетевая подсистема
Входной сетевой фильтр (INPUT)
Агент управления
klish
netconf
Система дискреционного доступа
VRRP
Система исполнения управляющих взаимодействий
Подсистема контроля целостности
Накопитель изделия
Журналы
ПО
БД контроля целостности
Клиент тестирования
Подсистемы ядра
Кольцевой буфер
Подсистема кластеризации
conntrack
Синхронизация
Подсистема регистрации
Обработчик записей (syslogd)
Файловая подсистема
Подсистема взаимодействия с аппаратной платформой (прикладная часть)
Подсистема тестирования
Подсистема аудита
Подсистема взаимодействия с аппаратной платформой (Ядерная часть)
Данные
Управление

Рис. 1

Примечание. Для редактирования правил СОВ создан графический интерфейс, который входит в состав МЭ и устанавливается на ПЭВМ, функционирующую под управлением ОС Astra Linux Special Edition версии 1.3 или выше. Кроме этого, необходим файловый сервер с запущенными службами SSH-сервер или FTP-сервер. Описание работы с графическим интерфейсом приведено в приложении 3 к руководству оператора ИСКП.00022-01 34 01-4.

2.7. Подсистема кластеризации предназначена для настройки и управления работой МЭ в режиме двухузлового отказоустойчивого кластера вида Active\Passive и обеспечивает:

– объединение сетевых интерфейсов в виртуальную кластерную группу с общим адресом доступа (виртуальный IP-адрес);

– автоматическое определение состояний узлов кластерной группы (Active/Passive);

– перенаправление входящих запросов на активный узел кластерной группы;

– синхронизацию таблицы текущих подключений между узлами кластерной группы;

– синхронизацию управляющих команд, выполняемых на активном узле, между узлами кластерной группы.

Примечания:

1. В кластерную группу можно объединять до 20 узлов.

2. Для корректной работы кластерной группы предварительные настройки должны быть выполнены администратором вручную на каждом узле. Эти настройки должны быть идентичными (различия лишь в приоритетах).

3. Синхронизирующаяся информация (команды настроек, таблицы соединений) передаётся по сети «открытым текстом» (plain text), рекомендуется использовать для синхронизации обособленный канал передачи данных.

2.8. Логически подсистема кластеризации состоит из следующих модулей:

– конфигурирования;

– VRRP;

– Conntrack;

– синхронизации настроек.

Модуль конфигурирования состоит из набора CLI-команд, с помощью которых администратор настраивает работу кластера (задание настроек кластерной группы, интерфейса синхронизации).

Модуль VRRP, реализованный на основе работы утилиты Keepalived, управляет функционированием кластерной группы - приём и отправка информационных сообщений протокола VRRP. Модуль автоматически управляет сменой состояния узла (MASTER\BACKUP) в случае возникновения отказов в кластерной группе и рассылает соответствующие широковещательные запросы для перенаправления входящих сетевых пакетов.

Модуль Conntrack, реализованный на основе работы утилиты Conntrack, следит за состоянием таблицы текущих подключений и в случае возникновения новых производит широковещательное оповещение для всех подключенных узлов кластерной группы. В режиме узла BACKUP информация о подключениях аккумулируется и при смене состояния в MASTER таблица соединений обновляется на полученную.

Модуль синхронизации настроек, реализованный на основе утилиты «uftp» и вспомогательных скриптов на языке BASH, производит синхронизацию корректно выполненных CLI-команд на узле MASTER. В случае включенной кластеризации головной модуль производит сохранение корректно выполненных команд в файл. Модуль синхронизации контролирует этот файл и производит с помощью утилиты «uftp» широковещательную отправку этого файла всем узлам кластера. На узлах с состоянием BACKUP в этот момент запущена утилита-слушатель (uftpd), принимающая данный файл. После приёмки модуль синхронизации инициализирует выполнение всех команд из принятого файла.

2.9. Подсистема управления обеспечивает:

– автономное управление изделием, включая конфигурацию портов;

– настройку маршрутизации, приоритизации трафика;

– настройку межсетевого экранирования, сбора статистики и ведения журналов работы;

– настройку печати и печать журналов;

– взаимодействие с администраторами МЭ.

2.10. Программа печати, входящая в состав агента управления, состоит из следующих python-модулей:

– «getch» – модуль работы с клавиатурным буфером;

– «console_dialog» – базовый класс для поддержки консольных меню;

– «config» – модуль работы с конфигурационными данными;

– «text2pdf» – модуль вывода текста в формат pdf;

– «logprinter» – главный модуль программы, обеспечивает настройку необходимых параметров и вывод документа на печать.

Для настройки печати используется команда «printer_config», которая вызывает модуль «logprinter». Выдача команды без параметров командной строки предназначена для просмотра и изменения текущих настроек программы, при этом в консоль выводится меню-подсказка. Каждому параметру или группе параметров в меню соответствует номер (от «1» до «7»).

Главное меню включает в себя:

– выбор принтера – вывод на экран списка доступных принтеров;

– выбор сервера – для печати через удаленный сервер печати, для изменения текущих настроек следует ввести пару <сервер>:<порт> (например, localhost:631). После выбора сервера небходимо выбрать принтер;

– формат страницы – вывод меню для настройки формата и ориентации страницы, размера полей в мм, включения или отключения заголовка страницы и нижнего колонтитула и их формата, настройки основного текста (нужна ли нумерация строк, печатать или нет учетную карточку документа, выбор шрифта);

– текущие установки – для просмотра установленных значений;

– очередь печати – просмотр и удаление выбранных заданий из очереди;

– выключить (включить) службу печати – команда доступна только для локального сервера печати;

– выход – сохранение настроек в конфигурационный файл и выход из программы печати.

Настройки, доступные для изменения в интерактивном режиме, сохраняются в файле «logprinter.conf». В файле «logprinter-fonts.conf» содержится информация о доступных шрифтах. Этот файл создается на этапе установки и может быть изменен администратором системы при добавлении или удалении системных шрифтов вручную.

2.11. Подсистема обмена управляющими взаимодействиями обеспечивает взаимодействие администраторов МЭ с агентом управления по протоколам Telnet, SSH и через порты RS-232.

2.12. Подсистема аутентификации обеспечивает проверку правильности аутентификационных данных, используя механизм настраиваемых присоединяемых аутентификационных модулей.

2.13. Подсистема контроля целостности осуществляет контроль целостности программы и базы данных.

2.14. Подсистема восстановления обеспечивает восстановление изменяемых контролируемых файлов в случае их повреждения.

2.15. Подсистема тестирования обеспечивает проверку функционирования подсистем изделия, в частности:

– правил фильтрации;

– аутентификации/идентификации;

– регистрации действий администраторов МЭ;

– контроля за целостностью программной и информационной части МЭ;

– процедуры восстановления;

– регистрации фильтрации;

– целостность базы решающих правил СОВ.

2.16. Подсистема регистрации обеспечивает запись в журналы сообщений от компонент подсистем и включает в себя:

– подсистему регистрации событий безопасности;

– подсистему регистрации прочих событий.

Подсистема регистрации является распределенной и состоит из:

– программы-демона «rsyslogd», ее настроек, скриптов обработки информации;

– модуля отображения, архивации, настройки;

– интерфейса CLI в части отображения и настройки журналов.

Программа позволяет вести следующие журналы:

– журнал регистрации сетевых пакетов «access_lists» (при выводе ответа на некоторые команды может называться «firewall»);

– журнал событий аутентификации «auth»;

– журнал агента управления «daemon»;

– журнал сообщений СОВ «snort»;

– журнал команд пользователя «commands»;

– журнал тестирования «testing»;

– журнал сетевых соединений «netflow»;

– журнал событий групповой маршрутизации «multicast»;

– журнал сообщений клиента и сервера VPN «vpn»;

– журнал печати «print»;

– системный журнал «syslog».

Для печати журналов используются команды «show log <имя журнала> print» и «show security_log <имя журнала> print».

Использование аргумента «print» приводит к формированию документа в соответствии с параметрами, заданными в конфигурационном файле. Когда документ готов для вывода на печать, оператору предлагается ввести сведения, необходимые для регистрации в системном журнале и печати учетной карточки документа (вид, шифр, код, получатель документа). Пустые строки в сведениях недопустимы.

2.17. Подсистема аудита обеспечивает возможность анализа журналов.

2.18. Подсистема взаимодействия с аппаратной платформой осуществляет управление компонентами аппаратной платформы, обеспечивает обмен данными программных компонентов МЭ с компонентами аппаратной платформы.

2.19. Подсистема взаимодействия с аппаратной платформой состоит из двух групп программных компонентов – ядра и прикладной части. Ядро обеспечивает выполнение низкоуровневых функций:

– непосредственное взаимодействие с компонентами аппаратной платформы;

– управление выполнением – управление процессорами и таймерами для реализации многопоточного выполнения программного обеспечения (ПО);

– управление оперативной памятью в части распределения блоков памяти между процессами ядра и прикладной части;

– реализация работы сетевых функций коммутации, маршрутизации и фильтрации;

– разграничение ресурсов пользователей;

– обеспечение работы файловых систем.

Ядро в оперативной памяти существует в одном экземпляре и обеспечивает для каждого процесса в системе собственное изолированное адресное пространство. Данный механизм изоляции основан на страничном механизме защиты памяти, а также механизме трансляции виртуального адреса в физический, поддерживаемый модулем управления памятью. Одни и те же виртуальные адреса преобразуются в разные физические для разных адресных пространств.

Процесс не может несанкционированным образом получить доступ к пространству другого процесса, так как непривилегированный пользовательский процесс лишен возможности работать с физической памятью напрямую.

Адресное пространство ядра защищено от прямого воздействия пользовательских процессов с использованием механизма страничной защиты. Страницы пространства ядра являются привилегированными и доступ к ним из непривилегированного кода вызывает исключение процессора, которое обрабатывается корректным образом ядром изделия.

Единственным санкционированным способом доступа к ядру изделия из пользовательской программы является механизм системных вызовов, который гарантирует возможность выполнения пользователем только санкционированных действий.

Для взаимодействия с прикладной частью используется программный интерфейс функций с двоичными аргументами.

Прикладная часть обеспечивает взаимодействие ядра с пользователями или ПО через программный интерфейс системных команд, реализованных в виде отдельных программ, библиотек функций и файлов настроек. Любой из этих компонентов может существовать в оперативной памяти во множестве экземпляров, если не установлены специальные ограничения.

2.20. Подсистема установки МЭ обеспечивает выполнение следующих функций:

– автоматический запуск подсистемы установки МЭ с установочного компакт-диска (при соответствующей настройке свойств загрузки аппаратной платформы);

– разделение целевого носителя данных на три логических раздела;

– форматирование указанных выше разделов в файловые системы (первый и второй разделы в ext4, третий раздел в nilfs2);

– перенос программных пакетов с установочного компакт-диска в первый раздел целевого диска;

– настройка программных пакетов;

– создание базы данных (БД) контроля изменяемых файлов;

– создание БД контроля ПО;

– блокировка изменения файлов, перечисленных в базе данных контроля ПО.

3. НАСТРОЙКА ПРОГРАММЫ

3.1. Общие сведения

3.1.1. Для установки программы на аппаратную платформу к ней должны быть подключены следующие устройства:

– технологический монитор;

– клавиатура.

Примечание. Если аппаратная платформа не имеет возможности подключения монитора и клавиатуры, то необходимо соединить ее с технологической ПЭВМ кабелем консольного управления (через порт RS-232).

3.1.2. Возможны следующие варианты установки МЭ на аппаратную платформу:

– локальная установка, при которой технологический дисковод DVD-ROM подключается непосредственно к порту USB аппаратной платформы;

– установка по сети, при которой Ethernet-кабель соединяет аппаратную платформу с сетью установки.

Примечание. Перед установкой программы на аппаратную платформу должны быть установлены сетевые карты в соответствии с конструкторской документацией, однако кабели к сетевым картам на время установки не подключать.

3.2. Проверка целостности программы

3.2.1. Непосредственно перед установкой должна быть проверена контрольная сумма инсталляционного компакт-диска ИСКП.00022-01.

Примечание. Проверка контрольной суммы осуществляется на ЭВМ, на которую установлена ОС «Astra Linux Special Edition» РУСБ.10015-01 версии 1.4.

3.2.2. Для проверки контрольной суммы дистрибутива необходимо выполнить следующую последовательность действий:

– войти в ОС под именем и паролем, которые установлены на ЭВМ при инсталляции ОС;

– дождаться приглашения ввода консоли;

– вставить компакт-диск ИСКП.00022-01 в дисковод DVD-ROM;

– смонтировать компакт-диск, набрав в командной строке команду без кавычек «mount /media/cdrom»;

– в командной строке набрать команду без кавычек для подсчета контрольной суммы «cd /media/cdrom; ls -A1 | sort | tar c -T - | md5sum»;

– нажать клавишу «Enter» и дождаться окончания выполнения введенной команды (выключения индикатора активности дисковода);

– наблюдать на следующей строке подсчитанную контрольную сумму;

– в командной строке набрать команду без кавычек «cd /; umount /media/cdrom» для размонтирования компакт-диска;

– извлечь компакт-диск ИСКП.00022-01 из дисковода DVD-ROM.

3.2.3. МЭ считается готовым к установке, если контрольная сумма, отображенная на мониторе ЭВМ для компакт-диска ИСКП.00022-01, совпала с контрольной суммой этого диска, записанной в формуляре ИСКП.00022-01 30 01.

Примечание. При несовпадении контрольных сумм запрещается производить дальнейшие действия по установке программы.

3.3. Подготовка установки программы по сети

3.3.1. Для установки программы по сети требуется наличие сети установки, включающей в себя серверы DHCP, TFTP и FTP, а также оборудование, обеспечивающее доступность МЭ к ним.

Примечания:

1. МЭ и сервер DHCP должны располагаться в одном сегменте локальной сети.

2. Серверы TFTP и FTP должны иметь один IP-адрес и могут находиться за пределами сегмента локальной сети, однако рекомендуется для ускорения установки располагать их в одном сегменте с МЭ. В частном случае, все серверы могут быть объединены в одной ЭВМ.

3.3.2. Настройка DHCP-сервера сводится к настройке раздачи IP-адресов с выдачей параметра «DHCP 66», равного IP-адресу TFTP-сервера и параметра «DHCP 67», равного строке «pxelinux.0».

Например, для Linux-сервера «dhcpd» параметр «DHCP 66» имеет название «next-server», а параметр «DHCP 67» – «filename».

Пример файла конфигурации сервера «dhcpd»:

```
ddns-update-style none;
deny duplicates;
one-lease-per-client true;
authoritative;

subnet 200.168.2.0 netmask 255.255.255.0 { # Подсеть, для которой
                                           #производится раздача адресов
default-lease-time 3600;
#Описание набора адресов для раздачи по DHCP
 pool {
  range 200.168.2.7 200.168.2.36;          #Диапазон адресов IP
  max-lease-time 90000;
  option routers 200.168.2.100;  # IP-адрес шлюза, если нужен выход за
                                 # пределы локальной сети
  next-server 200.168.2.139;     # Адрес TFTP-сервера (параметр 66)
  server-name "200.168.2.100"; # Имя сервера DHCP
  filename "pxelinux.0";         # Имя файла
   allow all clients;
   }
}
```

3.3.3. Настройка TFTP-сервера сводится к копированию содержимого каталога «netboot» компакт-диска ИСКП.00022-01 в домашний каталог сервера.

3.3.4. Для настройки FTP-сервера необходимо выполнить следующие действия:

– добавить пользователя «installer» с паролем «1234567890»;

– создать каталог «cdrom». В зависимости от настроек сервера создание каталога производится в корневом каталоге или домашнем каталоге пользователя;

– скопировать содержимое компакт-диска ИСКП.00022-01 в каталог «cdrom» или примонтировать компакт-диск к этому каталогу.

3.4. Установка программы

3.4.1. Если к аппаратной платформе удалось подключить технологический монитор, клавиатуру и дисковод DVD-ROM, то необходимо выполнить последовательность действий, начиная с 3.4.8, исключая 3.4.11.

Далее описывается последовательность установки программы с технологической ПЭВМ, соединенной с портом COM1 (ttyS0) аппаратной платформы кабелем консольного управления.

3.4.2. Включить технологическую ПЭВМ с установленной ОС, имеющей в своем составе программу «minicom».

3.4.3. Ввести логин и пароль, заданные при установке ОС на технологическую ПЭВМ.

3.4.4. На экране монитора отобразится окно (рис. 2).

3.4.5. В появившейся командной строке набрать команду без кавычек «minicom –s» и нажать клавишу «Enter».

3.4.6. Появится окно «Конфигурация» (рис. 3), в котором выбрать пункт «Настройка последовательного порта» и нажать клавишу «Enter».

3.4.7. В появившемся окне (рис. 4) выбрать последовательный порт технологической ПЭВМ, к которому подключена аппаратная платформа.

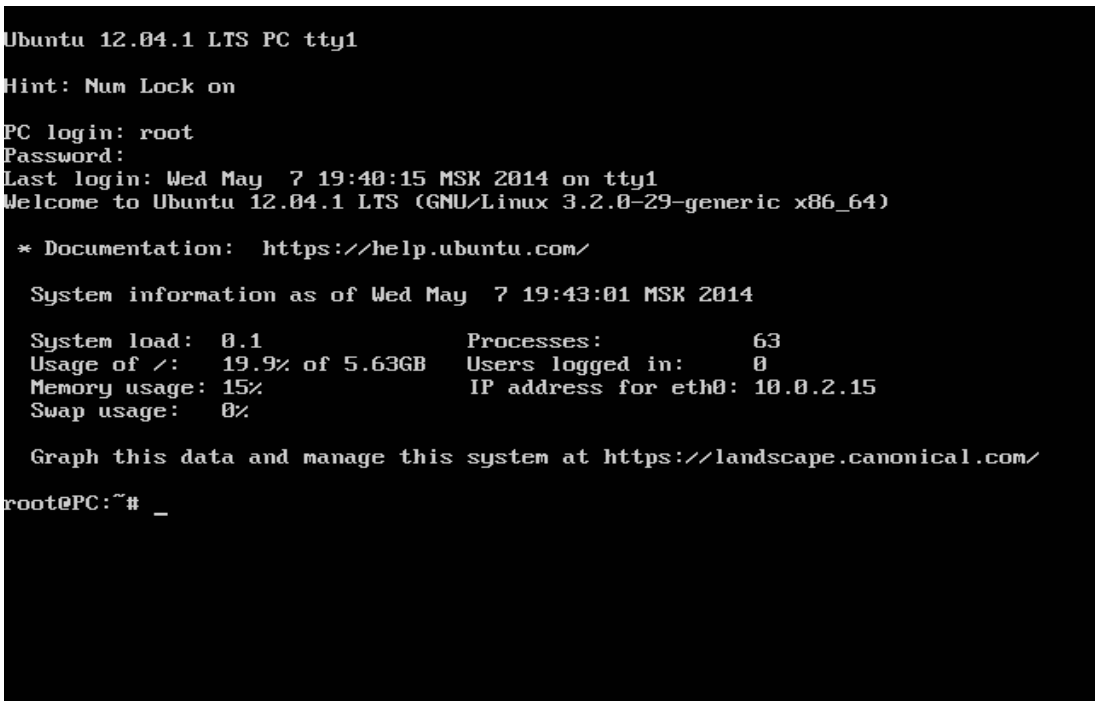

Рис. 2

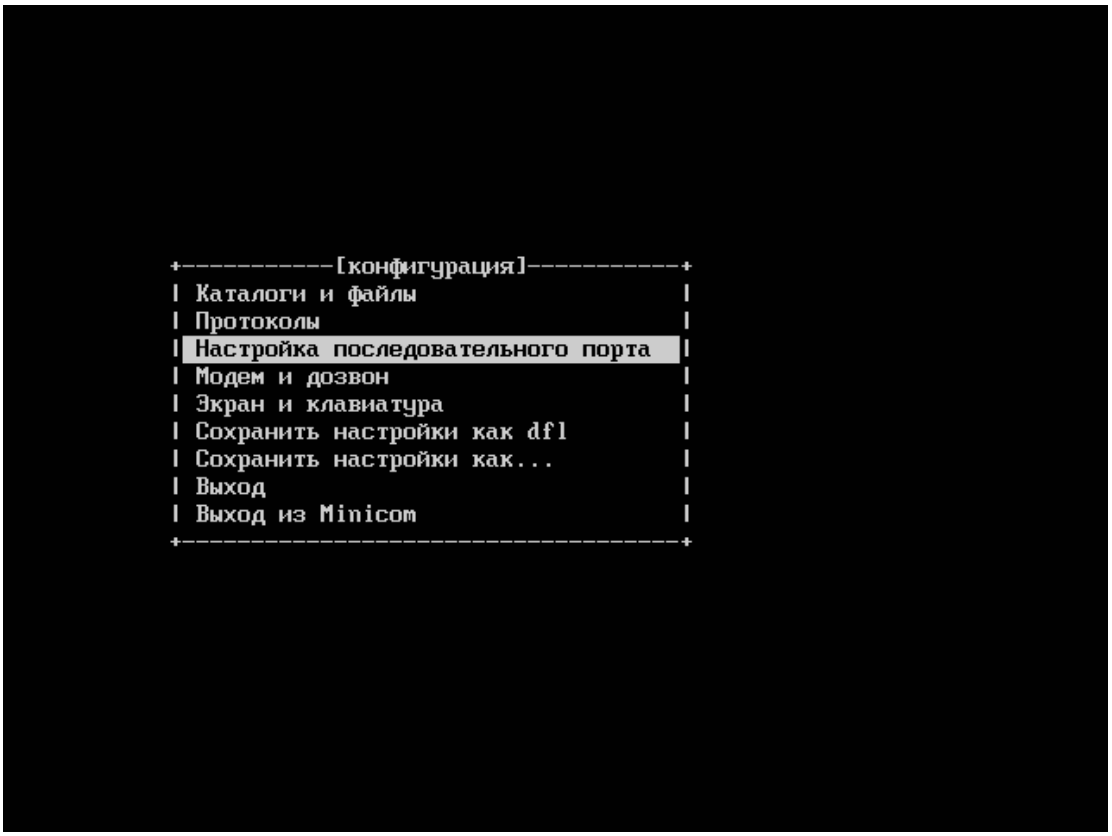
[конфигурация]
Каталоги и файлы
Протоколы
Настройка последовательного порта
Модем и дозвон
Экран и клавиатура
Сохранить настройки как dfl
Сохранить настройки как...
Выход
Выход из Minicom

Рис. 3

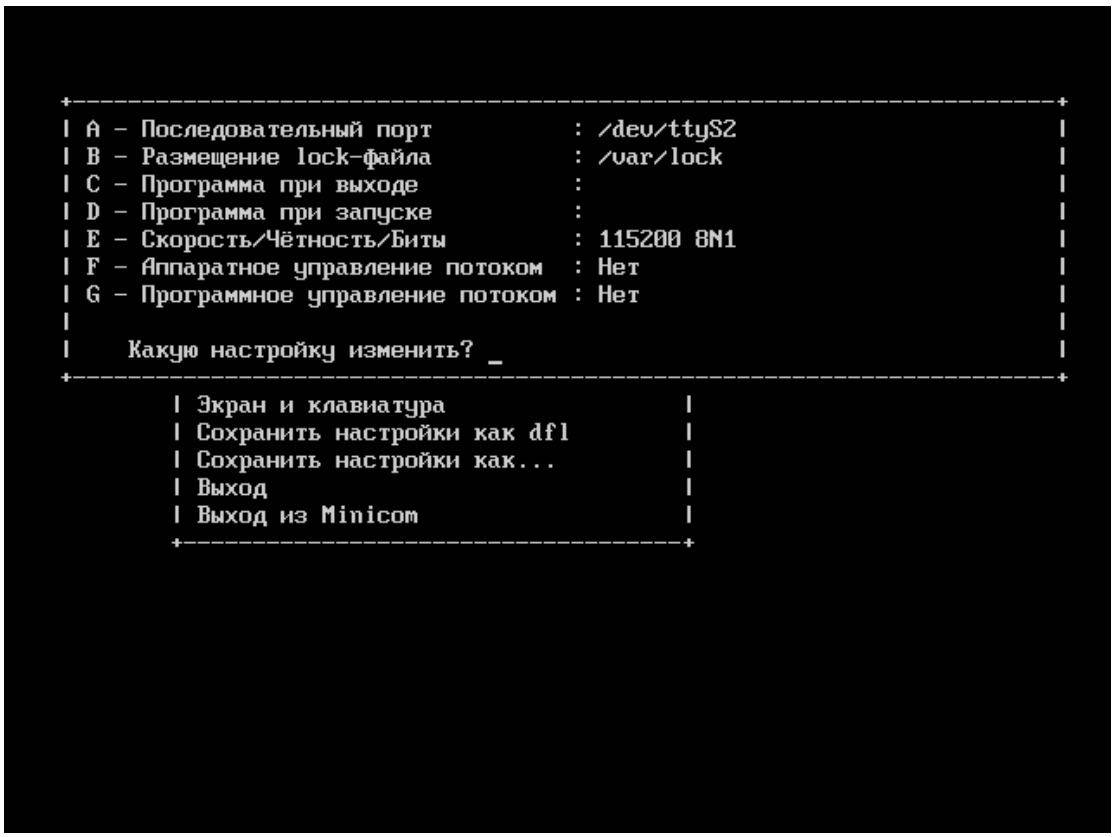
A - Последовательный порт : /dev/ttyS2
B - Размещение lock-файла : /var/lock
C - Программа при выходе :
D - Программа при запуске :
E - Скорость/Чётность/Биты : 115200 8N1
F - Аппаратное управление потоком : Нет
G - Программное управление потоком : Нет
Какую настройку изменить? _
Экран и клавиатура
Сохранить настройки как dfl
Сохранить настройки как...
Выход
Выход из Minicom

Рис. 4

Указать в строке «Скорость/Четность/Биты» значение «115200 8N1». В строке «Аппаратное управление потоком» указать «Нет», в строке «Программное управление потоком» также указать «Нет» и нажать клавишу «Enter».

После этого вновь откроется окно «Конфигурация» (см. рис. 3), в котором выбрать пункт «Выход» и нажать клавишу «Enter».

На экране откроется окно, приведенное на рис. 5.

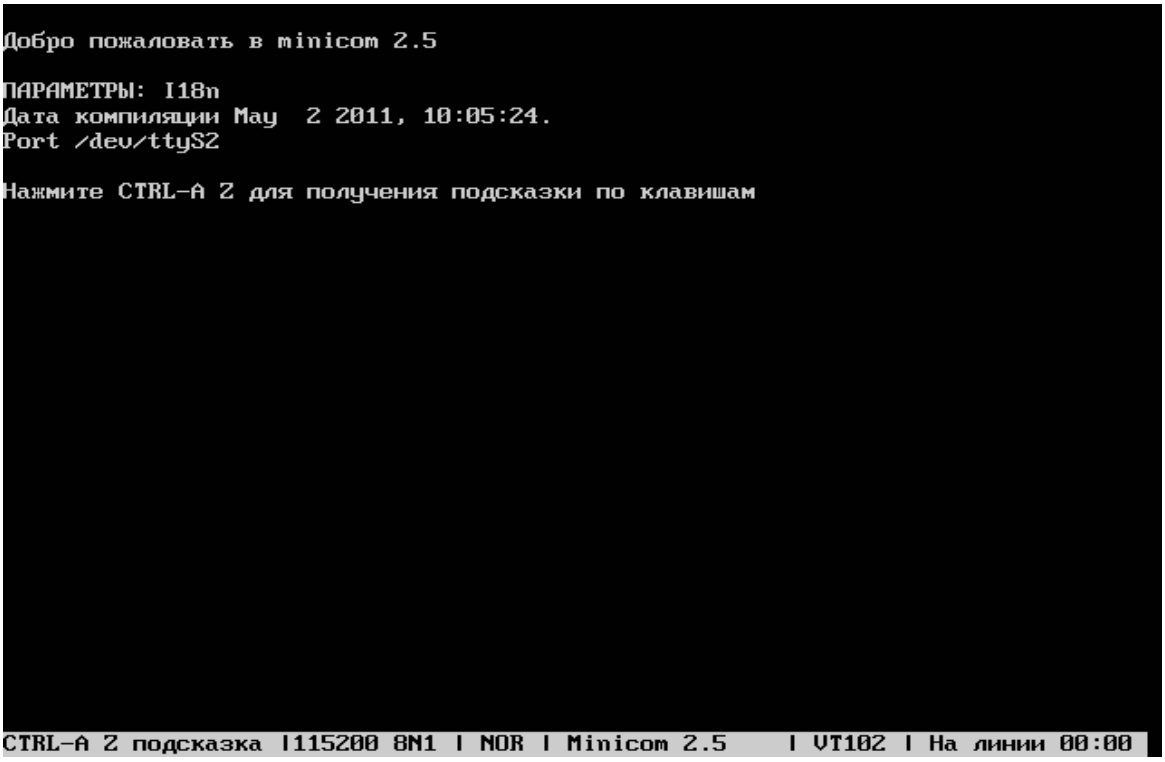

Рис. 5

3.4.8. При локальной установке подключить к порту USB аппаратной платформы внешний DVD-ROM и вставить в него компакт-диск ИСКП.00022-01, а для сетевой установки подключить Ethernet-кабель, соединяющий аппаратную платформу с сетью установки.

3.4.9. Включить аппаратную платформу и выполнить следующие действия:

1) войти в редактирование настроек BIOS аппаратной платформы;

2) произвести сброс всех настроек на настройки «по умолчанию»;

3) выставить текущую дату («System Date») и время («System Time»);

4) для Т-платформы необходимо выставить конфигурацию PCI-express плат с помощью следующих действий:

– в меню «IntelRCSetup» стрелками «вверх-вниз» выбрать «IIO Configuration» и нажать клавишу «Enter»;

– в меню «CardEdge/RiserC-RCIE2» изменить параметр «RCIE3/RiserD Link Width» с «X16» на «X8X8»;

5) выбрать в качестве загрузочного носителя для локальной установки – DVD-ROM, а для установки по сети – Ethernet-контроллер с младшим номером с использованием PXE. При этом если во время установки в дальнейшем загрузка по сети не начинается, то необходимо перезапустить аппаратную платформу, войти в редактирование настроек BIOS и выбрать другой Ethernet-контроллер;

6) сохранить сделанные настройки.

Примечание. Меню «CardEdge/RiserC-RCIE2» для некоторых аппаратных платформ может отсутствовать.

3.4.10. После перезапуска аппаратной платформы начнется загрузка с компакт-диска или с сервера в сети, в зависимости от настроек, сделанных ранее.

Примечание. Если аппаратная платформа имеет возможность подключения монитора и клавиатуры, то необходимо перейти к 3.4.12.

3.4.11. Необходимо подождать появления окна со строкой «boot:», в которой набрать команду без кавычек «serial» и нажать клавишу «Enter».

Еще раз нажать клавишу «Enter».

3.4.12. Если на экране монитора появится приглашение выбора видеорежима, необходимо прописать видеорежим «F00» и нажать клавишу «Enter».

3.4.13. Дождаться появления окна «Configuring tzdata», в котором выбрать временную зону «Europe» и нажать клавишу «Enter». В следующем окне выбрать «Moscow» и нажать клавишу «Enter».

3.4.14. Дождаться появления вопроса «May I update your system?» и нажать клавишу «Enter».

3.4.15. В следующих окнах «DHCP Relay» (рис. 6 - рис. 8) необходимо нажимать клавишу «Enter».

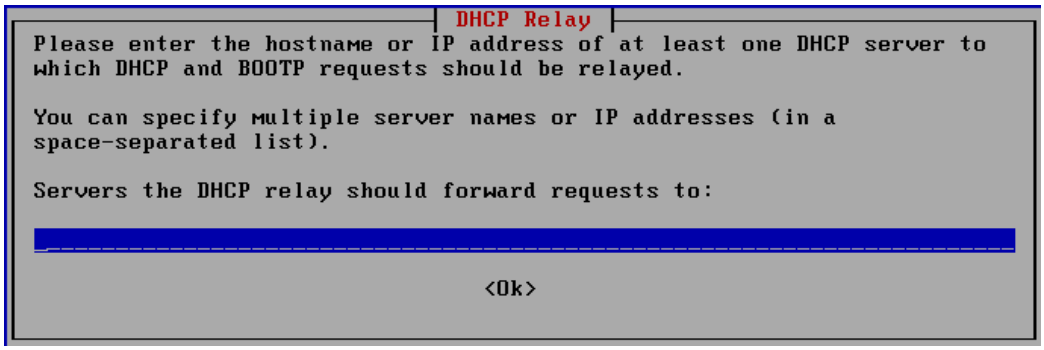

Рис. 6

Рис. 7

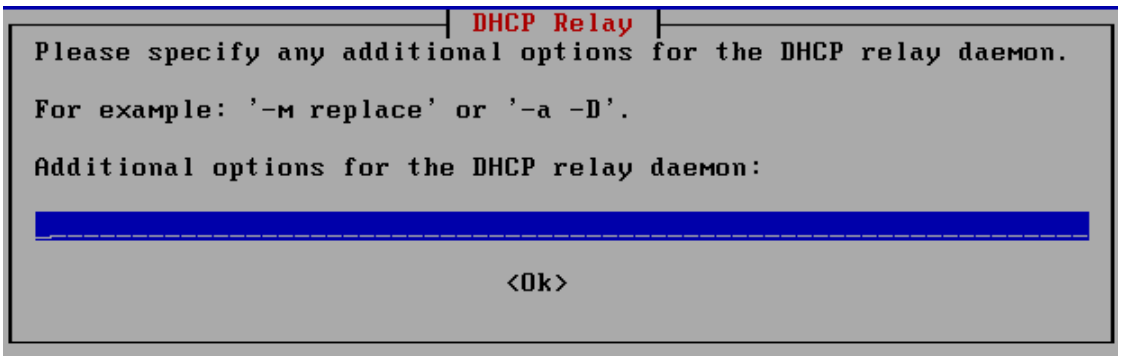

Рис. 8

3.4.16. После этого последовательно откроются два окна «Configuring keyboard-configuration» (рис. 9, рис. 10), в которых последовательно выбрать раскладку клавиатуры «Russian», сочетание клавиш смены языка ввода и нажать клавишу «Enter».

Рис. 9

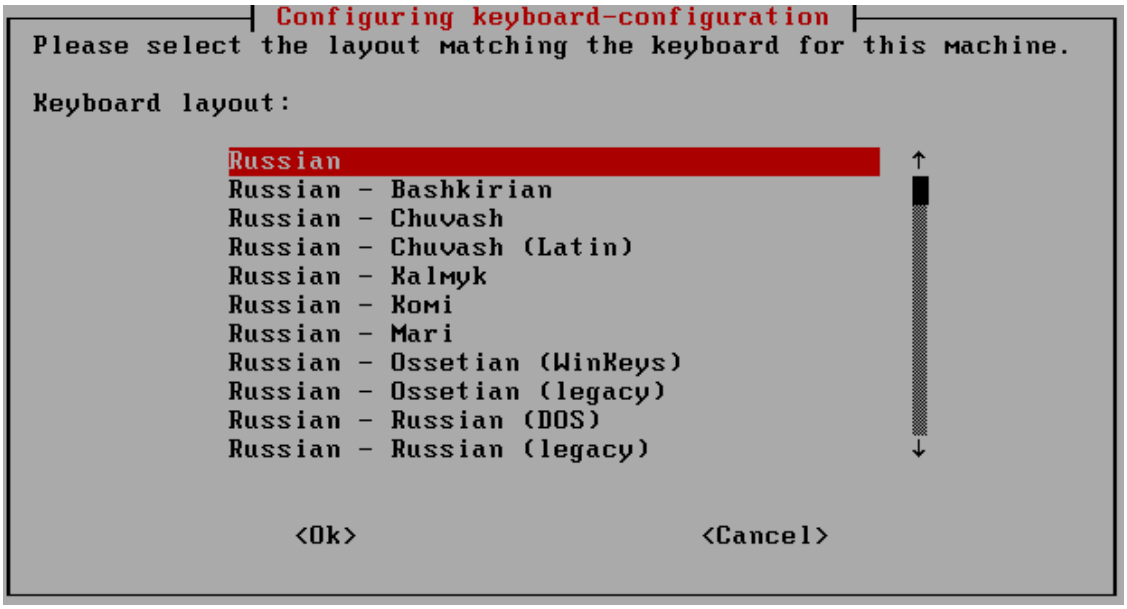

Рис. 10

3.4.17. В следующем окне «Configuring racoon» (рис. 11) выбрать «direct» и нажать клавишу «Enter».

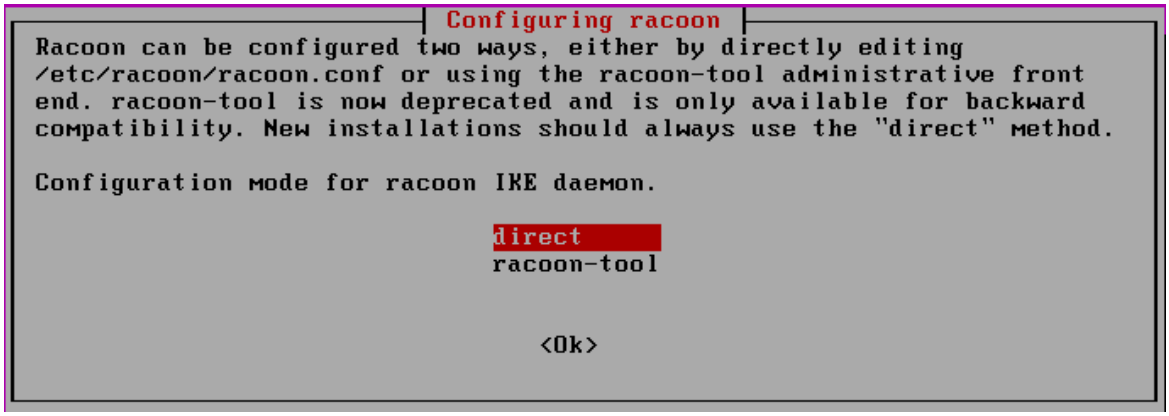

Рис. 11

3.4.18. После этого в окне «Configuring dash» (рис. 12) выбрать ответ «No» (клавиша →) и нажать клавишу «Enter».

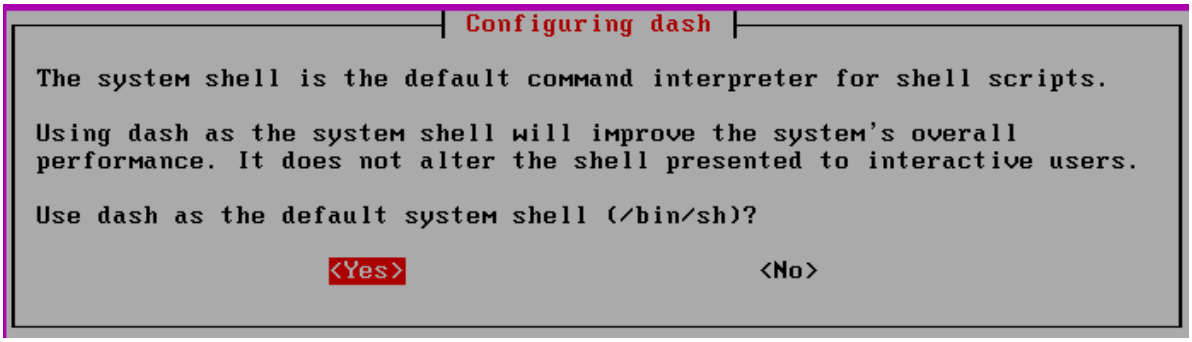

Рис. 12

3.4.19. В следующих окнах «DECnet node configuration» (рис. 13, рис. 14) необходимо нажимать клавишу «Enter».

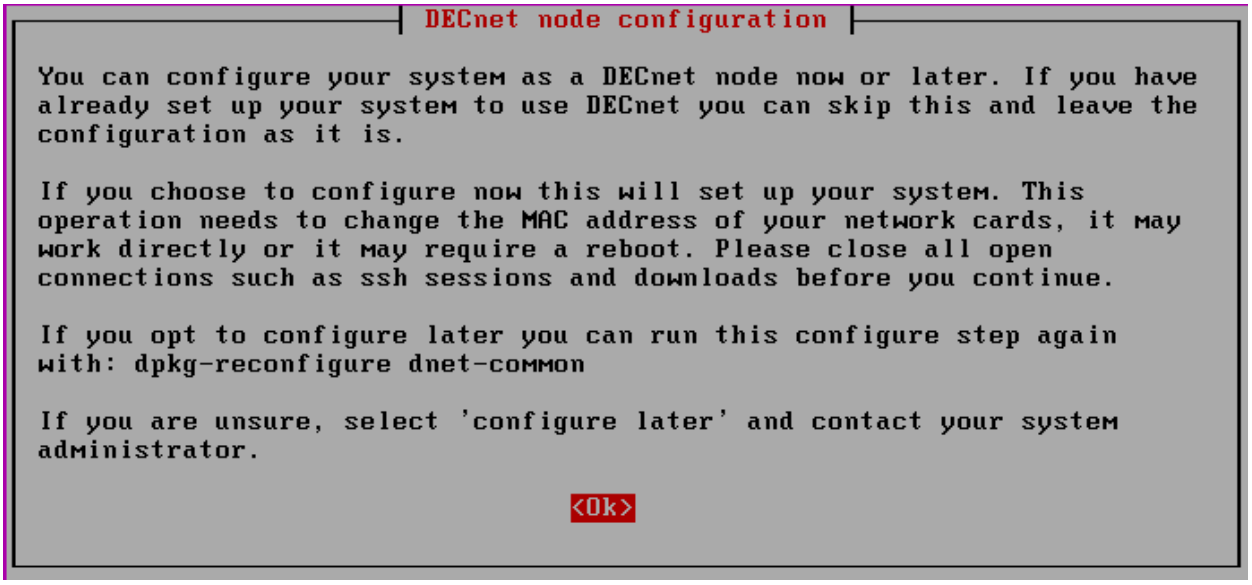

Рис. 13

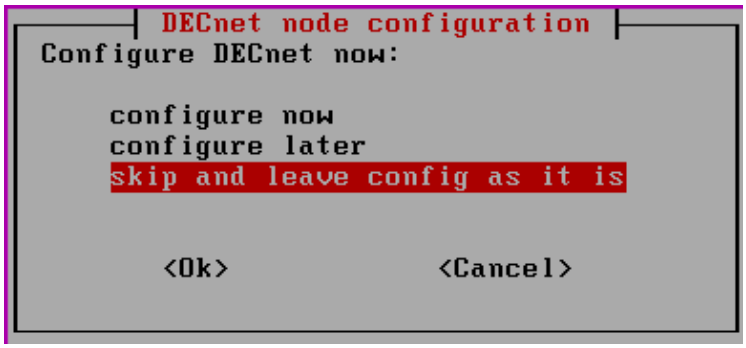

Рис. 14

3.4.20. Далее в первом окне «Configuring grub-pc» (рис. 15) нажать клавишу «Enter», а во втором окне выбрать устройство для начального загрузчика (первое в списке) с помощью клавиши «Пробел» (рис. 16), а затем нажать клавиши «Tab» (переход на «ОК») и «Enter».

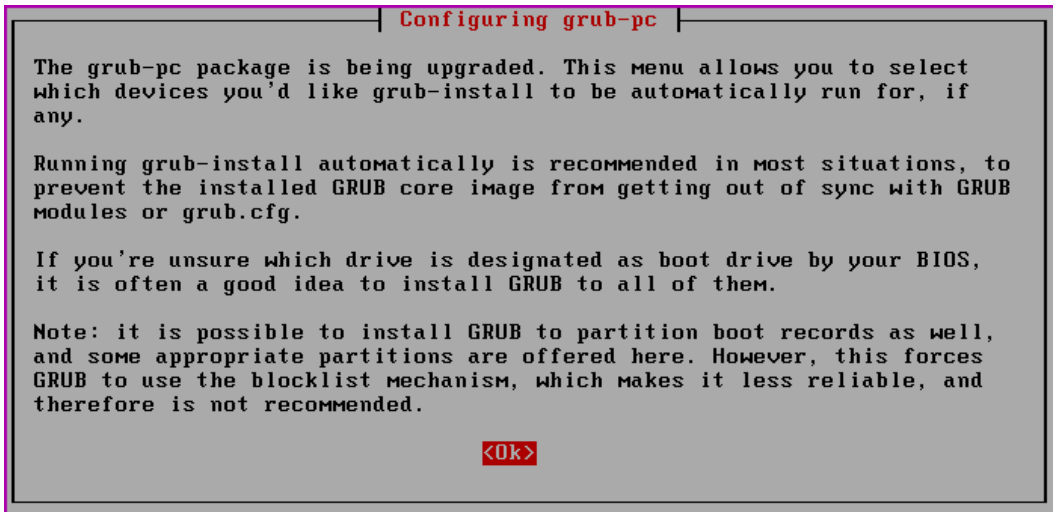

Рис. 15

Рис. 16

3.4.21. После этого откроется окно «Configuring console-setup» (рис. 17), в котором выбрать кодировку «UTF-8», а в следующем окне «Combined – Latin; Slavic Cyrillic; Greek» (рис. 18).

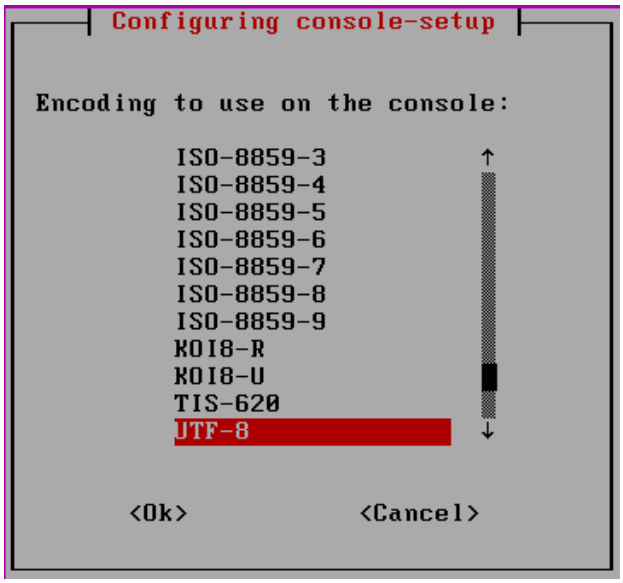

Рис. 17

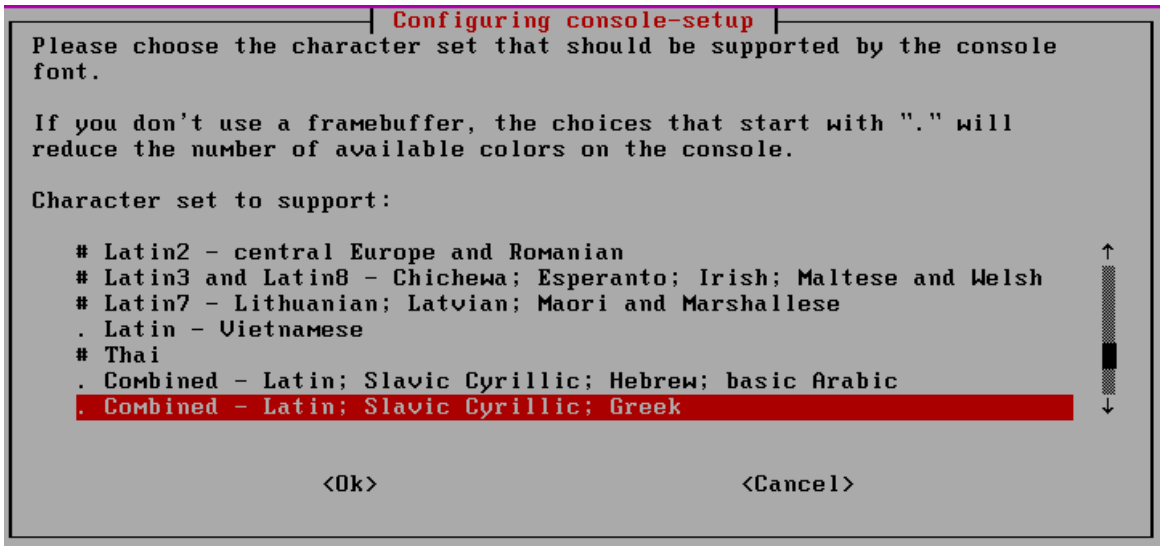

Рис. 18

3.4.22. При успешном окончании установки будет выведена надпись «READY TO REBOOT. Press key ENTER». При локальной установке одновременно будет произведено автоматическое открытие лотка CD/DVD-дисковода, из которого необходимо извлечь компакт-диск ИСКП.00022-01. При установке по сети необходимо отсоединить от аппаратной платформы Ethernet-кабель, соединяющий ее с сетью установки.

После нажатия на клавишу «Enter» будет произведён перезапуск аппаратной платформы.

3.4.23. После перезапуска необходимо войти в редактирование настроек BIOS аппаратной платформы и установить в качестве загрузочного носителя накопитель на жёстком магнитном или твердотельном диске.

3.4.24. При выполнении всех указанных выше действий программа считается установленной.

В МЭ существует три группы пользователей, соответствующих различным ролям:

– «admin» – администраторы сети;

– «admsec» – администраторы безопасности;

– «admaud» – администраторы аудита.

3.4.25. После первоначальной установки созданы следующие учётные записи:

– «admin», «cluster», «json_ctl» – в группе «admin»;

– «admsec», «clustersec», «json_ctlsec» – в группе «admsec»;

– «admaud», «clusteraud», «json_ctlaud» – в группе «admaud».

Примечания:

1. Для учётных записей «admsec» и «json_ctlsec» изначально установлен пароль «12345678i.» без кавычек. Остальные учётные записи заблокированы после установки программы и разблокируются путем установки пароля.

2. Учётные записи «cluster», «clustersec» и «clusteraud» являются служебными (используются для автоматической синхронизации изделий в составе кластерной группы) и не должны использоваться администраторами изделия.

3.4.26. Дальнейшую настройку программы необходимо производить из-под учетной записи «admin» или «admsec».

3.4.27. Последовательность настройки программы и описание команд, используемых в процессе настройки и выполнения программы, приведены в руководстве оператора ИСКП.00022-01 34 01-1, ИСКП.00022-01 34 01-2.

4. ПРОВЕРКА ПРОГРАММЫ

4.1. При включении аппаратной платформы автоматически запускается МЭ и начинается процедура самотестирования, при этом осуществляются следующие проверки:

– целостности файловой системы;

– целостности программного обеспечения;

– целостности аппаратной конфигурации;

– работы СОВ.

4.2. Результаты тестирования выдаются на консоль управления перед запросом имени пользователя в виде сообщений:

– при отсутствии ошибок «Autocheck: no errors»;

– при наличии ошибок «Autocheck: ERRORS: disk_check=<результат> hardware_check=<результат> software_check=<результат> ids_check=<результат>», где «<результат>» может принимать значения «OK» для положительного или «ERROR» для отрицательного результатов;

«disk_check» отображает суммарный результат проверки целостности файловой системы при старте МЭ;

«hardware_check» отображает суммарный результат проверки целостности аппаратной конфигурации;

«software_check» отображает суммарный результат проверки целостности программного обеспечения агента управления;

«ids_check» отображает суммарный результат проверки работы СОВ.

4.3. Для дальнейшей проверки программы после появления запроса имени пользователя необходимо набрать имя пользователя «admsec» и пароль «12345678i.» (установлен «по умолчанию» в процессе инсталляции). На экране появится сообщение «Welcome admsec».

Примечания:

1. Перед началом эксплуатации МЭ рекомендуется поменять этот пароль.

2. Пароль может включать в себя строчные буквы, цифры и знаки пунктуации.

3. Длина пароля должна быть не менее девяти символов.

4. Пароль на экране не отображается.

4.4. Более подробные результаты тестирования можно запросить на консоль управления с помощью следующих команд:

– «show log fscheck» - вывод сообщений проверки целостности файловой системы;

– «show log hwcheck» - вывод сообщений проверки целостности аппаратной конфигурации;

– «show log swcheck» - вывод сообщений проверки целостности программного обеспечения агента управления;

– «show log idscheck» - вывод сообщений проверки работы СОВ.

Примечания:

1. Первоначально МЭ запускается с конфигурацией «по умолчанию», в которой все сетевые интерфейсы выключены, кроме RS-232, который используется для консоли управления. После настройки необходимых интерфейсов выполнить команду «no shutdown».

2. Первоначально также запрещено прохождение трафика. Для полного или выборочного разрешения прохождения сетевого трафика используется команда «ip filter».

4.5. Для проверки версии программы в командной строке ввести команду без кавычек «show version» и нажать клавишу «Enter».

4.6. Для проверки версии ядра в командной строке ввести команду без кавычек «show version kernel» и нажать клавишу «Enter».

4.7. Для проверки версии «iptables» в командной строке ввести команду без кавычек «show version iptables» и нажать клавишу «Enter».

4.8. Для получения информации о модуле анализа сетевого трафика NETFLOW в командной строке ввести команду без кавычек «show version netflow» и нажать клавишу «Enter».

4.9. Для проверки целостности файлов программы необходимо выполнить команду без кавычек «check all». На экране появятся сообщения «No damage», если целостность файлов не нарушена, в противном случае выводится перечень ошибок.

5. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

5.1. Дополнительные функциональные возможности программы

5.1.1. Для выполнения программой «быстрой» фильтрации необходимо после завершения работ, связанных с изменением/применением списков доступа (ACL-листов), выполнить команду «ip filter fast».

5.1.2. Для изменения количества буферов на интерфейсах МЭ необходимо выполнить команду «buffers {max | 'N' }».

5.1.3. Для включения/выключения промежуточного буфера (кеша) маршрутных таблиц необходимо выполнить команду «cache { on | off | flush }».

5.1.4. Для перезагрузки маршрутизатора необходимо выполнить команду «system reboot».

5.1.5. Для выключения маршрутизатора необходимо выполнить команду «system shutdown».

5.1.6. Существует команда для вывода загрузки процессора и занятости памяти «show usage [dynamic]».

Примечание. Если указан параметр «dynamic», то вывод формируется не однократно, а обновляется каждые две секунды.

5.2. Установка локального времени, даты и часового пояса

5.2.1. Вывод текущего времени, даты и часового пояса выполняется с помощью команды «show clock».

5.2.2. Установка локального времени выполняется с помощью команды «system clock time 'HH:MM[:SS]'».

Примечание. Запрещается устанавливать время более раннее, чем указано в выводе команды «show clock».

5.2.3. Установка даты выполняется с помощью команды «system clock date 'dd.mm.yyyy'».

Примечание. Запрещается устанавливать дату более раннюю, чем указано в выводе команды «show clock».

5.2.4. Установка часового пояса выполняется с помощью команды «system clock timezone».

5.3. Восстановление пароля администратора

5.3.1. Восстановление пароля администратора осуществляется путем установки нового пароля. Для этого необходимо выполнить следующую последовательность действий:

– произвести перезапуск (включение) МЭ;

– после прохождения процедуры POST или в её конце нажать и удерживать клавишу «Shift» до появления меню загрузчика;

– в меню выбрать пункт «Restore of admin password» и нажать клавишу «Enter».

5.3.2. По окончании загрузки будет предложено ввести логин администратора, чей пароль необходимо изменить.

В случае, если такой пользователь есть в системе, будет предложено ввести новый пароль дважды.

Если такого пользователя нет в системе, либо был неудачно два раза введен пароль (первый ввод пароля не совпадает со вторым вводом пароля), будет предложено повторить попытку путем ввода слова без кавычек «yes» и нажатия клавиши «Enter», либо перезагрузкой компьютера (просто путем нажатия клавиши «Enter»).

6. СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

6.1. Сообщения системному программисту, выдаваемые на экран во время установки, настройки и проверки программы, приведены в разделах 3, 4 и 5 настоящего документа.

6.2. Действия системного программиста должны осуществляться в соответствии с подсказками, выдаваемыми в процессе установки и настройки МЭ на экран монитора.

Перечень принятых сокращений

БД	– база данных
ОС	– операционная система
МЭ	– программный комплекс межсетевого экрана с функциями системы обнаружения вторжений
ПО	– программное обеспечение
ПЭВМ	– персональная электронно-вычислительная машина
СЗИ	– средства защиты информации
СОВ	– система обнаружения вторжений

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (стра-	Номер доку-мента	Входящий номер сопроводи-тельного докум. и дата	Подп.	Да-та
	изме-ненных	заме-ненных	новых	анну-лиро-ванных					
