ZENATOR SE Fw

Руководство системного программиста

ИСКП.30330-01 32 01

Листов 32

2023

АННОТАЦИЯ

Данный документ является руководством системного программиста для Zenator SE Fw (программное обеспечение межсетевого экрана 2 класса защиты с функцией системы обнаружения вторжений), далее по тексту – Zenator SE Fw или программа.

Документ описывает назначение, структуру, последовательность установки и настройки программы, рекомендации и требования, исполнение которых необходимо для корректного функционирования программы.

Настоящее руководство 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. Zenator SE Fw выполняет функции программного обеспечения (ПО) межсетевого экрана уровня сети 2 класса защиты с функцией обнаружения вторжений.

1.1.2. Zenator SE Fw, имеющий самостоятельную поставку и функционирующий на аппаратных платформах (АП) на базе процессоров с архитектурой x86, обеспечивает возможность работы под управлением гипервизора системы виртуализации.

1.1.3. Zenator SE Fw обеспечивает явное задание скорости интерфейса Ethernet (10/100/1000), режима работы (half duplex, full duplex), автосогласование.

1.1.4. Zenator SE Fw обеспечивает явную настройку максимального размера полезного блока данных (MTU) на сетевых интерфейсах, в том числе и на туннельных.

1.1.5. Zenator SE Fw обеспечивает функционирование по протоколу IPv4 и IPv6.

1.1.6. В Zenator SE Fw реализован прием и передача IP-пакетов по протоколам семейства TCP/IP.

1.1.7. Zenator SE Fw обеспечивает вывод в интерфейс управления статистики по сетевым интерфейсам (тип/количество ошибок, тип/количество переданных/принятых пакетов).

1.1.8. Zenator SE Fw имеет возможность назначения и (или) изменения MAC-адреса на своих интерфейсах и подынтерфейсах.

1.1.9. Zenator SE Fw обеспечивает поддержку loopback-интерфейсов.

1.1.10. Zenator SE Fw обеспечивает возможность назначения нескольких IP-адресов на своих интерфейсах и подынтерфейсах.

1.1.11. Zenator SE Fw обеспечивает статическое и динамическое заполнение таблицы MAC-адресов с помощью протокола разрешения адресов (ARP).

1.1.12. Zenator SE Fw имеет возможность функционирования как ARP-proxy.

1.1.13. Zenator SE Fw обеспечивает:

– производительность не менее 2000000 пакетов/с (минимально необходимая таблица маршрутизации, отсутствует фильтрация и приоритизация пакетов, длина пакета 64 байта);

– производительность не менее 800000 пакетов/с (при заполненной таблице маршрутизации – 1000 маршрутов, заполненной таблице фильтрации – 1000 записей и настроенной приоритизации – 1000 классов, длина пакета 64 байта).

1.1.14. Zenator SE Fw обеспечивает пропускную способность в режиме межсетевого экранирования не менее 400 Мбит/с (при минимально допустимой заполненной таблице маршрутизации, заполненной таблице фильтрации – 1000 записей и ненастроенной приоритизации, длина пакета 1500 байт).

1.1.15. В Zenator SE Fw реализована поддержка групповой передачи данных – multicast routing (сетевой пакет одновременно направляется определенной группе адресатов).

1.1.16. В Zenator SE Fw реализована возможность маршрутизации IP-трафика.

1.1.17. В Zenator SE Fw обеспечивается статическая маршрутизация пакетов.

1.1.18. Zenator SE Fw обеспечивает функционирование по протоколам динамической маршрутизации:

– протокол маршрутизации (RIPv2);

– протокол динамической маршрутизации (OSPFv2);

– пограничный межсетевой протокол (BGPv4).

Примечание. Блокировка протоколов динамической маршрутизации обеспечивается программным способом.

1.1.19. Zenator SE Fw обеспечивает настройку таймеров OSPFv2.

1.1.20. Zenator SE Fw обеспечивает маршрутизацию на основе политик (policy-routing), включая «ToS» (DSCP), длину IP-пакета, входной интерфейс, маршрутизацию выделенных абонентов/подсетей через определенный шлюз.

1.1.21. Zenator SE Fw обеспечивает возможность балансировки нагрузки при наличии нескольких маршрутов с одинаковой метрикой.

1.1.22. В Zenator SE Fw реализована возможность автоматического переключения на резервный канал по сетевому протоколу, объединяющему группу маршрутизаторов в один виртуальный маршрутизатор (VRRP).

1.1.23. Zenator SE Fw обеспечивает функционирование по протоколу управления групповой передачей данных (IGMPv3).

1.1.24. В Zenator SE Fw реализовано функционирование по протоколу PIM SM, протоколу групповой маршрутизации для IP-сетей, обеспечивающему эффективный механизм доставки дейтаграмм для групп хостов без организации соединений.

1.1.25. Zenator SE Fw обеспечивает настройку маршрутизации выделенных IP-потоков в туннели PPPoE и PPTP как с клиентской, так и с серверной стороны туннеля.

1.1.26. Zenator SE Fw обеспечивает функционирование туннелей с использованием:

– туннельного протокола типа «точка-точка» в стандартной, незащищенной сети (PPTP);

– сетевого протокола канального уровня передачи кадров PPP через Ethernet (PPPoE);

– протокола туннелирования сетевых пакетов (GRE);

– протокола туннелирования «IP over IP» (IPIP).

1.1.27. Zenator SE Fw обеспечивает защиту данных, передаваемых по межсетевому протоколу IP (IPSec).

1.1.28. Zenator SE Fw поддерживает протокол туннелирования второго уровня L2TP.

1.1.29. Zenator SE Fw обеспечивает функционирование защищенной виртуальной частной сети (VPN) на основе OpenVPN.

1.1.30. Zenator SE Fw обеспечивает фильтрацию фрагментированных пакетов.

1.1.31. Zenator SE Fw обеспечивает фильтрацию на всех интерфейсах (реальных и виртуальных).

1.1.32. Zenator SE Fw поддерживает правила фильтрации при перераспределении маршрутной информации.

1.1.33. Zenator SE Fw обеспечивает возможность снятия бита DF на сетевых интерфейсах.

1.1.34. Zenator SE Fw обеспечивает возможность изменения значения максимального размера полезного блока данных (MSS) в TCP-пакетах для предотвращения Path MTU Discovery Black Hole.

1.1.35. Zenator SE Fw обеспечивает фильтрацию входящего, исходящего и пересылаемого трафика.

1.1.36. Zenator SE Fw 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:

– порт (TCP/UDP) отправителя;

– порт (TCP/UDP) получателя;

– IP-адрес отправителя;

– IP-адрес получателя;

– MAC-адрес отправителя;

– значение поля «Протокол» заголовка IP;

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

– длина пакетов;

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

– совокупность указанных критериев.

1.1.37. Zenator SE Fw имеет возможность осуществления тестирования (вручную) реализации правил фильтрации и прохождения сетевых пакетов.

1.1.38. В Zenator SE Fw реализована фильтрация IP-пакетов в соответствии с заданными правилами фильтрации на основе:

– IP-адресов отправителя и получателя;

– сетевых интерфейсов;

– протоколов;

– номеров портов UDP/TCP;

– флагов TCP/IP-пакетов;

– состояния соединений;

– прикладных протоколов с использованием регулярных выражений;

– мандатных меток, с возможностью преобразования форматов.

1.1.39. В Zenator SE Fw обеспечивается возможность просмотра средствами локального управления таблицы состояний TCP-соединений.

1.1.40. В Zenator SE Fw обеспечивается поддержка не менее 2000000 конкурирующих TCP-сессий.

1.1.41. В Zenator SE Fw обеспечивается маркировка IP-пакетов, предусматривающая обработку поля DSCP в заголовке IP-пакета с возможностями:

– сохранения имеющегося значения;

– маркировки DSCP;

– перемаркировки DSCP.

1.1.42. В Zenator SE Fw реализована возможность ограничения числа одновременных соединений с одного IP-адреса.

1.1.43. В Zenator SE Fw реализована возможность поддержки добавления, удаления мандатных меток безопасности в поле опций IP-заголовка.

1.1.44. Zenator SE Fw обеспечивает три базовые концепции трансляции адресов:

– статическая (SNAT);

– динамическая (DAT);

– маскарадная – преобразование сетевых адресов и портов (NAPT), преобразование сетевых адресов (NAT) Overload, трансляция сетевого адреса в зависимости от TCP/UDP-порта получателя (PAT).

1.1.45. Zenator SE Fw поддерживает настройку демилитаризованной зоны (DMZ) в сочетании с маршрутизацией и трансляцией адресов NAT или трансляцией портов PAT.

1.1.46. Zenator SE Fw обеспечивает запрашивающие хосты IP-адресами и другими конфигурационными параметрами с помощью протокола динамической конфигурации хоста (DHCPv4).

1.1.47. Zenator SE Fw обеспечивает распределение IP-адресов на определенный срок.

1.1.48. Zenator SE Fw обеспечивает распределение IP-адресов с помощью DHCP тремя способами:

– ручное распределение;

– автоматическое распределение;

– динамическое распределение.

1.1.49. Zenator SE Fw обеспечивает настройку интерфейса автоконфигурированием с помощью DHCPv4.

1.1.50. Zenator SE Fw обеспечивает ретрансляцию сообщений DHCP между клиентами и серверами в разных подсетях.

1.1.51. Zenator SE Fw предоставляет возможность конфигурирования себя с помощью интерфейса командной строки (CLI) следующими способами:

– локально (путем ввода с клавиатуры текстовых команд);

– удаленно (при подключении по сетевому протоколу прикладного уровня (SSH) или Telnet).

1.1.52. Zenator SE Fw обеспечивает проверку корректности основных задаваемых параметров функционирования.

1.1.53. Zenator SE Fw обеспечивает вывод текстового предупреждения в CLI при некорректно задаваемом параметре.

1.1.54. Zenator SE Fw обеспечивает сохранение сконфигурированных профилей.

1.1.55. Zenator SE Fw имеет возможность вывода информации о текущей загруженности центрального процессора и оперативного запоминающего устройства.

1.1.56. Zenator SE Fw имеет возможность поддерживать работу сервиса сторожевого таймера («watchdog») для выполнения автоматической перезагрузки устройства в случае прекращения нормального функционирования демона (зависания).

1.1.57. Zenator SE Fw имеет возможность вывода имеющихся в системе профилей, а также их копирования.

1.1.58. Zenator SE Fw обеспечивает применение сохраненных профилей.

1.1.59. В Zenator SE Fw разработан механизм управления очередями, предусматривающий поддержку методов CBQ, HFSC, FIFO, PQ, TBF, HTB.

1.1.60. Zenator SE Fw обеспечивает возможность задания полосы пропускания для определенного администратором типа трафика.

1.1.61. В Zenator SE Fw реализована возможность приоритезации IP-трафика.

1.1.62. Zenator SE Fw обеспечивает классификацию и приоритетную обработку пакетов по следующим критериям:

– порт (TCP/UDP) отправителя;

– порт (TCP/UDP) получателя;

– IP-адрес отправителя;

– IP-адрес получателя;

– MAC-адрес отправителя;

– значение поля «Протокол» заголовка IP;

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

– длина пакетов;

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

– совокупность указанных критериев.

1.1.63. В Zenator SE Fw реализовано распределение трафика в соответствии с классом трафика между каналами.

1.1.64. В Zenator SE Fw реализовано предупреждение перегрузок с поддержкой механизмов RED, ECN, GRED.

1.1.65. Zenator SE Fw обеспечивает функционирование протокола передачи точного времени (NTPv4) клиента/сервера с возможностью явно задать часовой пояс клиента/сервера с возможностью явно задать часовой пояс.

1.1.66. Zenator SE Fw обеспечивает функционирование виртуальной локальной сети (VLAN) согласно стандарту Института Инженеров Электротехники и Электроники (IEEE) 802.1Q.

1.1.67. В Zenator SE Fw обеспечивается поддержка технологии VXLAN.

1.1.68. Zenator SE Fw обеспечивает возможность агрегации сетевых интерфейсов в группу согласно IEEE 802.3ad.

1.1.69. Zenator SE Fw обеспечивает функционирование протокола оповещения канального уровня (LLDP).

1.1.70. Zenator SE Fw обеспечивает перенаправление (зеркалирование) трафика.

1.1.71. В Zenator SE Fw реализована возможность мониторинга состояния каналов Ethernet по протоколам TCP, ICMP.

1.1.72. Zenator SE Fw обеспечивает возможность программного объединения портов Ethernet на втором уровне модели ISO/OSI с возможностью назначения общего IP-адреса.

1.1.73. Zenator SE Fw имеет возможность переадресации DNS-запросов от клиента к удаленному DNS-серверу (DNS-proxy).

1.1.74. В Zenator SE Fw реализована функция отказоустойчивого кластера в конфигурации «Активный»/«Пассивный».

1.1.75. В Zenator SE Fw реализована система ролевого доступа со следующими пользователями:

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

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

– администратор аудита (с функцией доступа на чтение).

1.1.76. Zenator SE Fw обеспечивает ведение следующих журналов регистрации:

– журнал «ids» (журнал системы обнаружения вторжений);

– журнал «auth» (журнал информации о фактах идентификации, аутентификации);

– журнал «ipfilter» (журнал событий срабатывания правил межсетевого экранирования);

– журнал «router» (информация о работе протоколов динамической маршрутизации);

– журнал «commands» (команды администратора Zenator SE Fw, вводимые с консоли управления);

– журнал «daemon» (внутренний журнал агента управления Zenator SE Fw);

– журнал «testing» (информация о самотестировании);

– журнал «syslog» (информация от ядра операционной системы и системных утилит).

1.1.77. В Zenator SE Fw обеспечивается регистрация следующих событий:

– загрузка и инициализация системы и её остановка;

– вход/выход пользователей в систему/из системы с фиксацией ошибок авторизации;

– результат фильтрации входящих/исходящих пакетов.

1.1.78. В Zenator SE Fw при регистрации событий фиксируются:

– дата и время регистрируемого события;

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

1.1.79. В Zenator SE Fw осуществляется автоматический контроль целостности ПО.

1.1.80. В составе Zenator SE Fw предусмотрена система обнаружения вторжений, соответствующая следующим требованиям и обладающая возможностями:

– обнаружения попыток несанкционированного доступа;

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

– работы в режиме предотвращения компьютерных атак;

– контроля нескольких сетей с разными скоростями;

– централизованного управления и мониторинга с помощью CLI, используя удаленное подключение по протоколу SSHv2;

– гибкости системы генерации отчетов;

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

1.1.81. Zenator SE Fw поддерживает протокол экспорта информации по IP-потоку (IPFIX).

1.1.82. Zenator SE Fw поддерживает миграцию базовых настроек между версиями ПО.

1.1.83. Zenator SE Fw поддерживает возможность программного отключения неиспользуемых портов и сервисов.

1.1.84. Zenator SE Fw поддерживает передачу данных о событиях на удаленный сервер (syslog, SNMP trap).

1.1.85. Zenator SE Fw обеспечивает программное определение позиций интерфейсов.

1.1.86. Zenator SE Fw обеспечивает получение обновлений с локальных серверов с последующей полной переустановкой ПО силами администратора сети.

1.1.87. Zenator SE Fw поддерживает режим удаленного управления с помощью прикладного программного интерфейса передачи состояния представления (REST API).

1.1.88. Zenator SE Fw обеспечивает возможность архивации и просмотра журналов регистрации.

1.2. Требования к техническим и программным средствам

1.2.1. Zenator SE Fw функционирует на аппаратной платформе (АП) «Сервер MS-3040» ЦРМП.466219.001 или на АП со следующими характеристиками:

1) процессор с архитектурой x86;

2) оперативная память – не менее 4 Гбайт;

3) постоянное запоминающее устройство – не менее 16 Гбайт;

4) интерфейс USB – не менее одного;

5) интерфейс стандарта RS-232 – не менее одного;

6) интерфейс Ethernet 10/100/1000BaseT, соответствующий требованиям IEEE 802.3u, 802.3ab – не менее двух;

7) интерфейс Ethernet 1000Base-X – не менее двух;

8) интерфейсный модуль SFP – не менее двух с характеристиками:

– стандарт Ethernet – 1000Base-LX;

– тип разъема – LC;

– тип волокна – одномодовое;

– длина волны – не менее 1310 нанометра;

– скорость передачи данных – до 1,25 Гбайт/с;

– рабочая дистанция – не менее 2000 м;

– количество волокон – не менее двух;

9) интерфейсный модуль SFP с характеристиками:

– стандарт Ethernet – 1000Base-T;

– тип разъема – RJ-45;

– тип кабеля – UTP-5;

– скорость передачи данных – до 1,25 Гбайт/с;

– рабочая дистанция – не менее 100 м.

Примечания:

1. Порт RS-232 необходим для технологического управления изделием в отсутствии подключаемых клавиатуры и монитора. На некоторых аппаратных платформах он может отсутствовать.

2. Zenator SE Fw, имеющий самостоятельную поставку и функционирующий на аппаратных платформах на базе процессоров с архитектурой x86, должен

обеспечивать возможность работы под управлением гипервизора системы виртуализации.

3. Количество интерфейсов Ethernet и SFP определяется договором поставки. Допускается применение интерфейсов SFP+.

1.2.2. В зависимости от версии ПО и комплектации оборудования функциональные возможности программы могут отличаться.

2. СТРУКТУРА ПРОГРАММЫ

2.1. В Zenator SE Fw реализован принцип модульного построения ПО, когда каждый отдельный модуль отвечает за решение узкоспециализированной задачи.

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).

Структурная схема программы представлена на рис. 1.

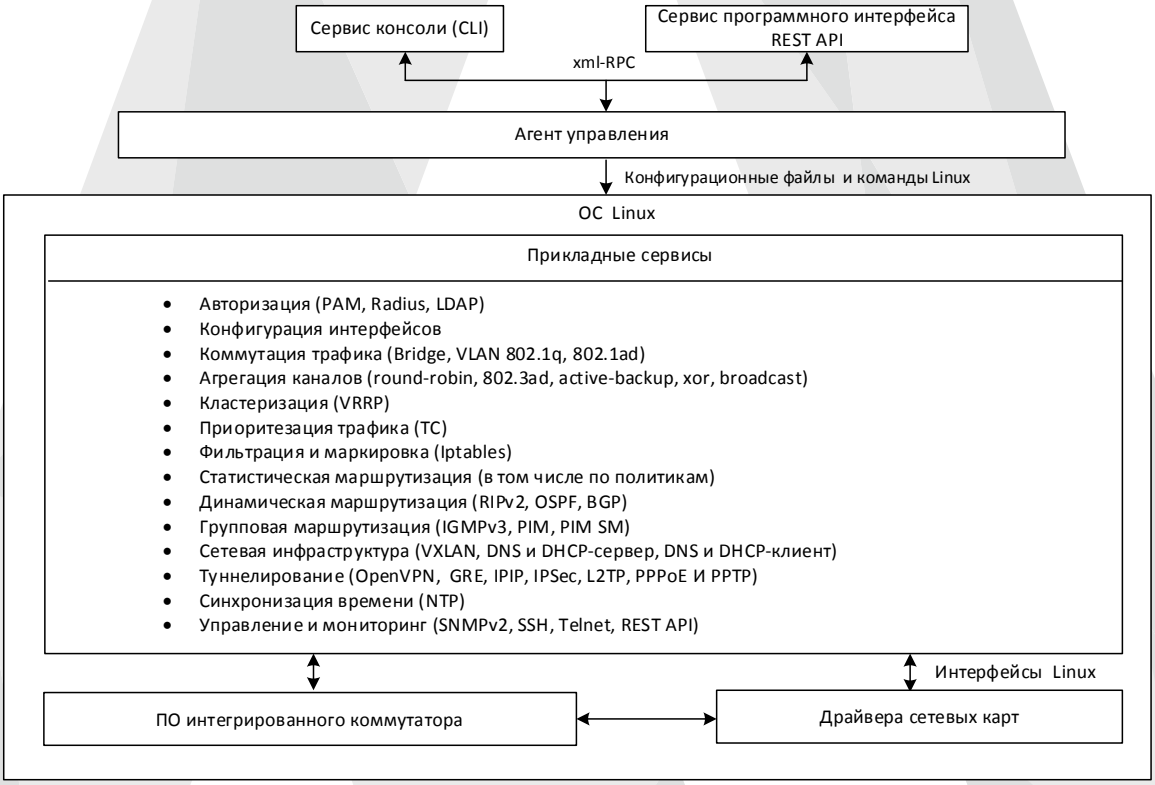

Рис. 1

2.3. Поступающая из контроллеров Ethernet информация обрабатывается в соответствии с семиуровневой моделью взаимодействия открытых систем.

На каждом уровне производится проверка корректности параметров данных этого уровня.

На канальном и сетевом уровнях производится фильтрация информации в соответствии с установленными правилами и выбор порта, через который будет производиться передача информации.

На транспортном уровне осуществляется обмен данными между программными объектами и сетевым уровнем через транспортные точки доступа.

2.4. Программные объекты, осуществляющие функции управления изделием, анализируют принимаемую информацию, выполняют управляющие действия в соответствии с алгоритмом. В том случае, если принятая информация является командой, формируется ответ, отправляемый инициатору команд через транспортные точки доступа.

2.5. Агент управления – это самостоятельная программная система, имеющая возможность принимать воздействие с сервисов консоли и REST API, она определяет свою реакцию на это воздействие и формирует ответное действие. Эта программа обладает возможностью изменения своего поведения с течением времени в зависимости от накопленной информации и извлеченных из нее знаний.

Агент управления обеспечивает передачу управляющих воздействий, разграничение прав доступа, а также ведение журналов.

Агент управления взаимодействует с прикладными сервисами, сервисом обработки и передачи трафика, а также через протокол xml-RPC с сервисом консоли и сервисом REST API.

Запрос, переданный пользователем через сервис консоли и сервис REST API, передается агенту управления через протокол xml-RPC. Посредством агента управления запрос перенаправляется соответствующему сервису. Обработанный сервисом запрос через агента управления выдается в консоль или REST API.

2.6. Сервис REST API – программный интерфейс взаимодействия, предоставляющий доступ к изделию с помощью HTTP-запросов. Является точкой сопряжения со всеми внешними по отношению к изделию системами управления. HTTP-запросы в своем теле отражают функционал изделия, к которому применяется управляющее воздействие.

В ответ на управляющее воздействие REST API возвращает документ в формате json, информирующий об успешности воздействия и корректности запроса.

2.7. Сервис консоли CLI – это текстовый интерфейс общения с ОС. Интерфейс командной строки обеспечивает взаимодействие с агентом управления с помощью XML-файлов.

2.8. Прикладные сервисы взаимодействуют с агентом управления с помощью конфигурационных файлов и команд Linux.

Прикладные сервисы включают в себя следующие сервисы:

– авторизация (PAM, SNMP, LDAP);

– конфигурация интерфейсов;

– коммутация трафика (Bridge, VLAN 802.1q, 802.1ad);

– агрегация каналов (round-robin, 802.3ad, active-backup, xor, broadcast);

– кластеризация (VRRP);

– приоритезация трафика (TC);

– фильтрация и маркировка (Iptables);

– статическая маршрутизация (в том числе по политикам);

– динамическая маршрутизация (RIPv2, OSPF, BGP);

– групповая маршрутизация (IGMPv3, PIM, PIM SM);

– сетевая инфраструктура (VXLAN, DNS и DHCP клиент и сервер);

– туннелирование (OpenVPN, GRE, IPIP, IPSec, L2TP, PPPoE, PPTP);

– синхронизация времени (NTP);

– управление и мониторинг (SNMPv2, SSH, Telnet, REST API).

2.9. Прикладные сервисы взаимодействуют с ПО интегрированного коммутатора и высокопроизводительными драйверами сетевых карт с помощью API.

2.10. Высокопроизводительные драйвера сетевых карт взаимодействуют непосредственно с АП.

3. НАСТРОЙКА ПРОГРАММЫ

3.1. Общие сведения

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

– технологический монитор;

– клавиатура.

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

3.2. Проверка целостности программы

3.2.1. Непосредственно перед установкой должна быть проверена контрольная сумма инсталляционного компакт-диска ИСКП.30330-01.

Примечание. Проверка контрольной суммы выполняется на персональной электронно-вычислительной машине (ПЭВМ), на которой установлена программа фиксации и контроля целостности информации исходного состояния программного комплекса «ФИКС-UNIX 1.0» 643.53132931.501492-02. Программа «ФИКС-UNIX 1.0» функционирует под управлением ОС «Astra Linux Special Edition» версии 1.6.

3.2.2. Подсчет КС осуществляется в следующей последовательности:

– включить АРМ с установленной программой «ФИКС-UNIX 1.0»;

– установить компакт-диск ИСКП.30330-01, подлежащий проверке, в дисковод DVD-ROM;

– смонтировать компакт-диск любыми доступными средствами ОС, например, командой

mount /media/cdrom

– перейти в каталог, где находится исполняемый файл «ufix» программы «ФИКС-Unix 1.0» с помощью команды

cd <путь к файлу ufix>

– проверить, существует ли файл проекта «listfile.prj» в данном каталоге. Если указанный файл проекта существует, то новая информация будет добавлена в его конец. Поэтому следует его удалить перед началом подсчета, выполнив команду

rm listfile.prj

– в командной строке набрать команду, которая формирует список файлов (включая каталоги) для контрольного суммирования и выводит его в файл «listfile.txt»

./ufix -jR /media/cdrom > listfile.txt

– дождаться окончания выполнения введенной команды и набрать команду для подсчета контрольных сумм

./ufix -eP listfile.txt

– в результате будет создан файл проекта «listfile.prj»;

– создать отчет в формате HTML командой

./ufix -h listfile.prj

– в результате будет создан файл отчета «listfile.html»;

– открыть файл отчета «listfile.html» любыми доступными средствами ОС и проверить значение контрольной суммы компакт-диска в файле «listfile.html»;

– после подсчета контрольной суммы следует удалить файл проекта «listfile.prj» из данного каталога командой

rm listfile.prj

– размонтировать компакт-диск любыми доступными средствами ОС, например, командой

umount /media/cdrom

– извлечь проверяемый компакт-диск из дисковода DVD-ROM.

3.2.3. Zenator SE Fw считается готовым к установке, если полученная контрольная сумма совпала с контрольной суммой, приведенной на маркировке этого диска.

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

3.3. Установка программы

3.3.1. Если к АП удалось подключить технологический монитор, клавиатуру и дисковод DVD-ROM, то необходимо выполнить последовательность действий, начиная с 3.3.5.

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

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

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

3.3.4. На технологической ПЭВМ выполнить следующие действия:

1) запустить «minicom» с помощью команды

minicom -s

2) в открывшемся окне «Конфигурация» выполнить следующие действия:

– выбрать пункт «Настройка последовательного порта» и нажать клавишу «Enter»;

– в появившемся окне выбрать последовательный порт технологической ПЭВМ, к которому подключена АП;

– убедиться (при необходимости выставить) в том, что для параметра «Скорость/Четность/Биты» выставлено значение «115200 8N1»;

– для параметров «Аппаратное управление потоком» и «Программное управление потоком» выставить значение «нет» и нажать клавишу «Enter»;

– выбрать пункт «Сохранить настройки как df1» и нажать клавишу «Enter»;

– выбрать пункт «Выход из Minicom» и нажать клавишу «Enter»;

3) в консоли включить «minicom» с помощью команды

minicom -D /dev/ttyUSB0

где ttyUSB0 – имя и номер последовательного порта, к которому подключена АП.

3.3.5. Подключить внешний дисковод DVD-ROM с вставленным компакт-диском ИСКП.30330-01 к АП.

3.3.6. Запустить АП по питанию.

3.3.7. В зависимости от возможностей АП дальнейшая установка программы производится либо с консоли технологической ПЭВМ с включённым «minicom», либо напрямую с АП. Для установки необходимо выполнить следующие действия:

1) несколько раз нажать клавишу «Delete»;

2) в открывшемся меню выбрать пункт «Boot», для поля «Boot Option #1» нажать клавишу «Enter», а затем выбрать подключённый внешний дисковод DVD-ROM (рис. 2);

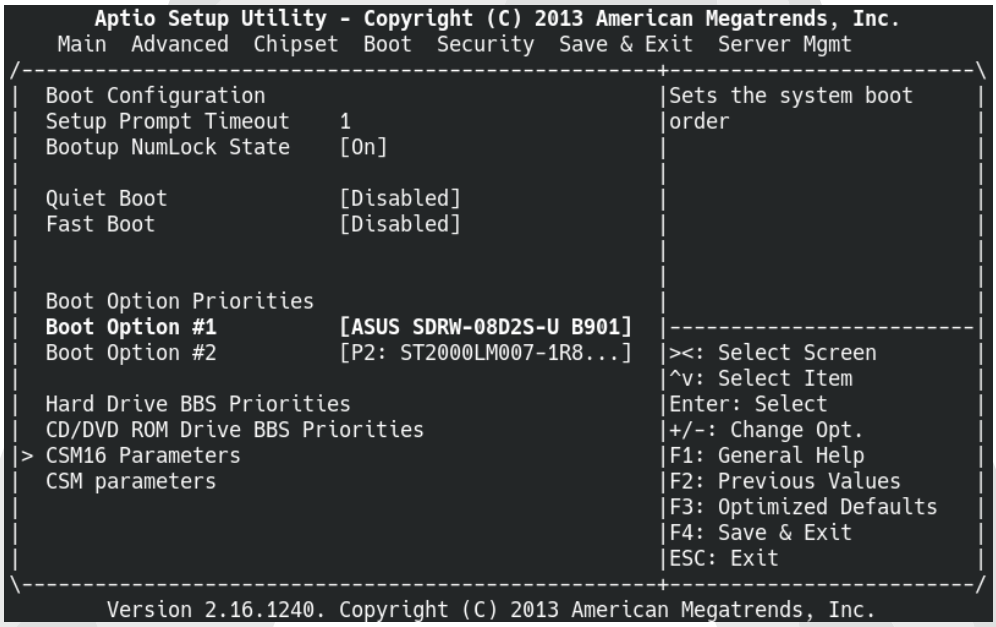

Рис. 2

3) нажать клавишу «F4» и согласиться с сохранением изменений, выбрав «Yes» (рис. 3) и нажав клавишу «Enter»;

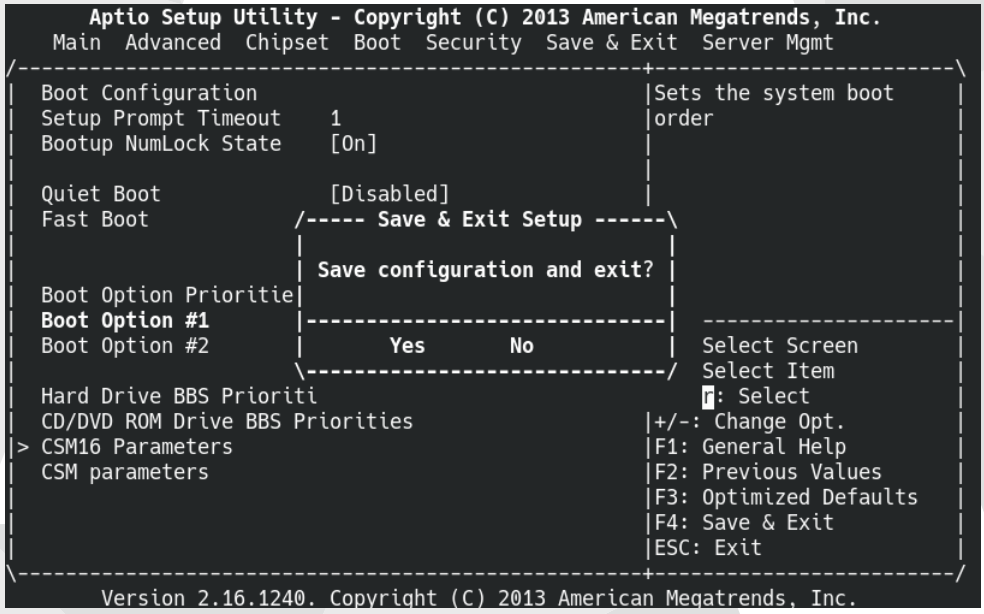

Рис. 3

4) в загрузочном меню (рис. 4) выбрать пункт «Install with serial console» и нажать клавишу «Enter»;

Рис. 4

3.3.8. АП перейдёт в режим установки ПО.

3.3.9. В появившемся окне (рис. 5) нажать клавишу «Enter».

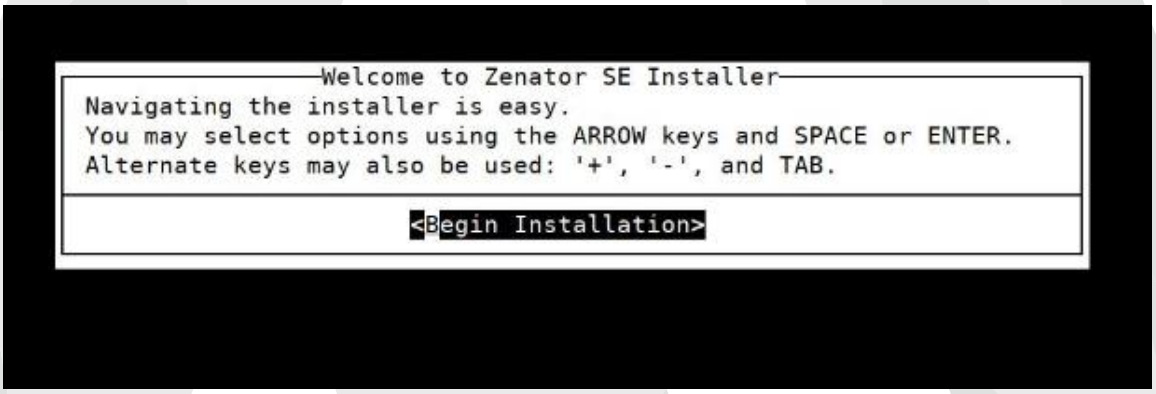

Рис. 5

3.3.10. В следующем окне (рис. 6) для поля «Disk to partition:» выбрать диск для установки системы «/dev/sda» и нажать «Enter»;

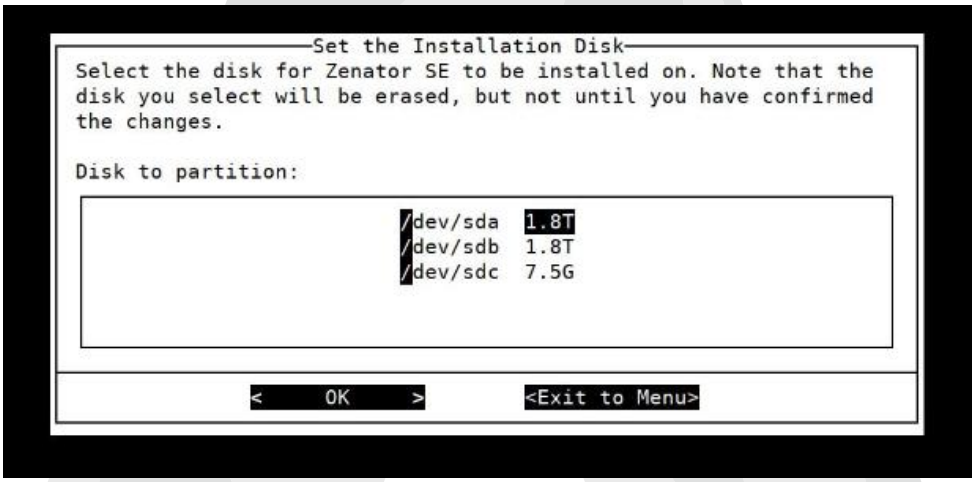

Рис. 6

3.3.11. В открывшемся окне предупреждения (рис. 7) подтвердить удаление всех данных на диске «/dev/sda» выбрав «Yes» и нажав клавишу «Enter».

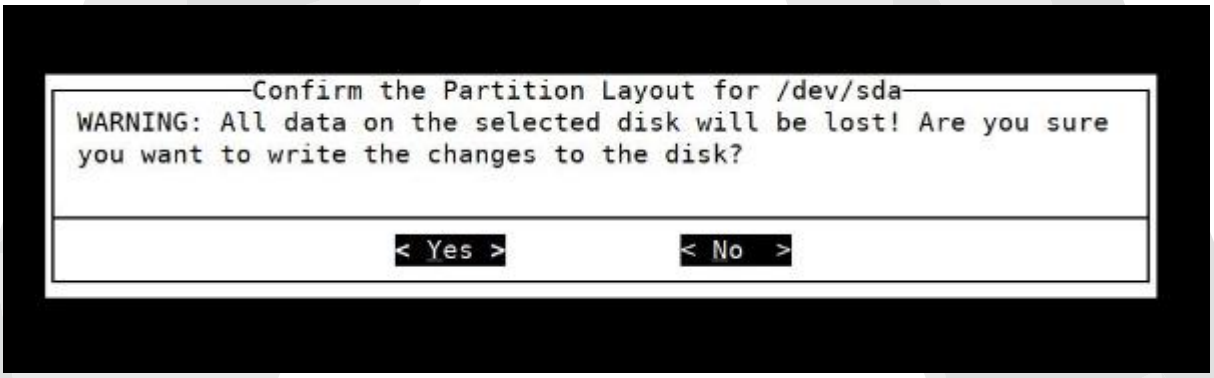

Рис. 7

3.3.12. В следующем окне (рис. 8) подтвердить установку Zenator SE Fw выбрав «Yes» и нажав клавишу «Enter».

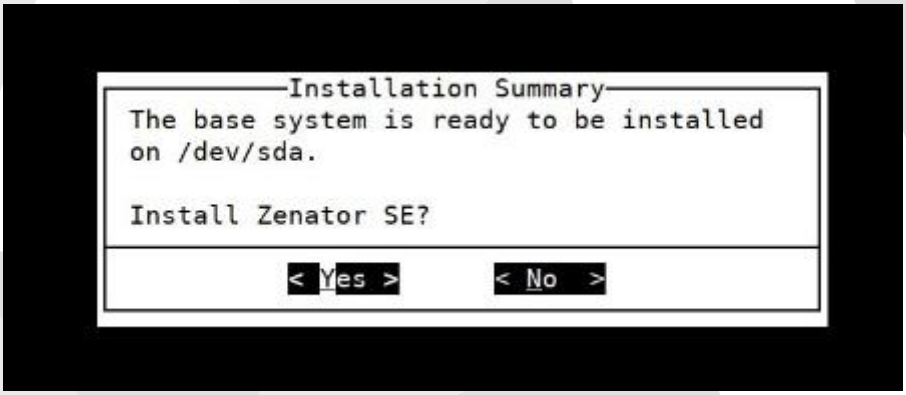

Рис. 8

3.3.13. Наблюдать процесс установки ПО.

3.3.14. После завершения установки в открывшемся окне (рис. 9) нажать клавишу «Enter».

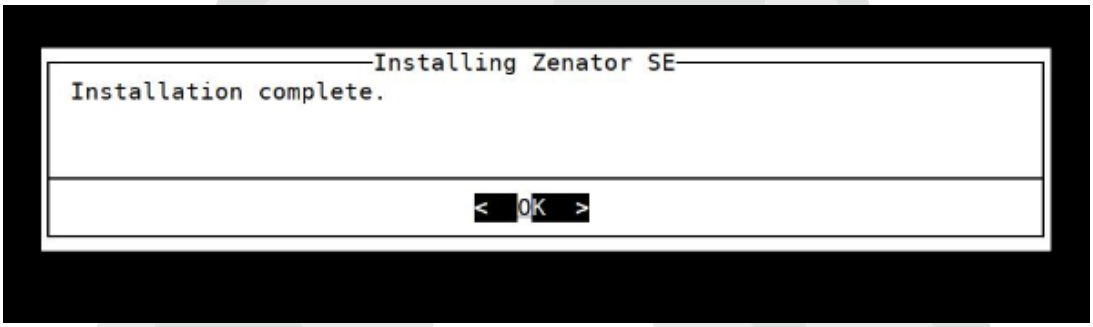

Рис. 9

3.3.15. В следующем окне (рис. 10) выбрать из предложенного списка пункт «Reboot system» и перегрузить систему нажав «OK».

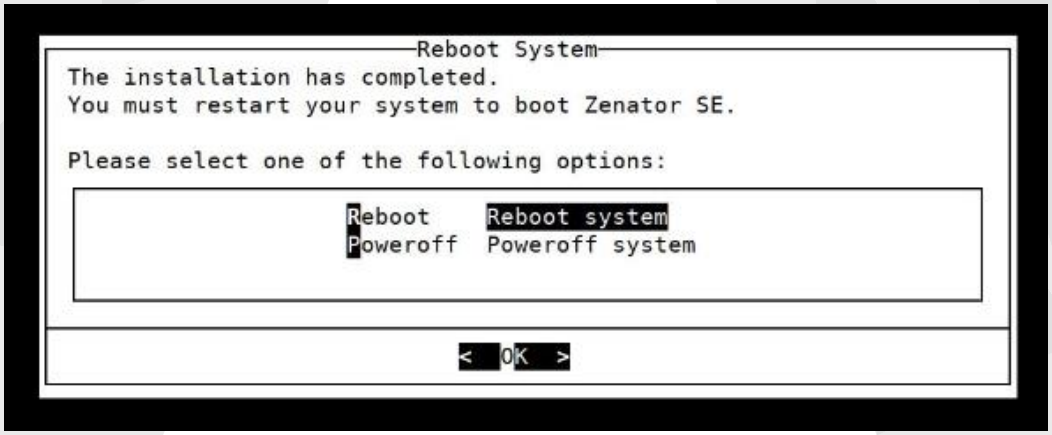

Рис. 10

3.3.16. Дождаться перезагрузки АП и в появившемся окне (рис. 11) в меню загрузчика grub выбрать «Zenator (serial console)».

Рис. 11

3.3.17. На экране ПЭВМ появятся строки:

Zenator SE Fw ИСКП.30330-01

zenator login:

3.3.18. Отключить внешний дисковод DVD-ROM с вставленным компакт-диском ИСКП.30330-01 от АП.

3.3.19. Дальнейшую настройку программы необходимо производить под учетными записями «admin» или «admsec» (пароль «по умолчанию» – без кавычек «12345678i.») либо напрямую с АП, либо с консоли ПЭВМ после включения «minicom» с помощью команды

minicom -D /dev/ttyUSB0

где ttyUSB0 – имя и номер последовательного порта, к которому подключена АП.

3.3.20. Последовательность настройки программы и описание команд, используемых в процессе настройки и выполнения программы, приведены в руководстве оператора ИСКП.30330-01 34 01 и в приложении к нему ИСКП.30330-01 34 01-1.

4. ПРОВЕРКА ПРОГРАММЫ

4.1. При включении АП автоматически запускается Zenator SE Fw и начинается процедура самотестирования, при этом осуществляются следующие проверки:

– целостности файловой системы;

– целостности ПО;

– целостности аппаратной конфигурации.

4.2. Для дальнейшей проверки программы необходимо выполнить процедуру авторизации.

В поле «zenator login: » необходимо ввести имя пользователя «admsec» и нажать клавишу «Enter».

В поле «Password: » необходимо ввести пароль «12345678i.» и нажать клавишу «Enter».

Примечания:

1. Пароль на экране не отображается. Данный пароль устанавливается «по умолчанию» в процессе инсталляции программы.

2. При первом запуске рекомендуется сменить пароль на более безопасный.

3. Длина задаваемого пароля не должна превышать 32 символа.

После входа в систему на экране появятся следующие сообщения:

1) «Welcome <name>!» – приглашение входа в систему с учетной записью «name» («name» – имя пользователя);

2) «zenator>» – строка приглашения к вводу команд.

4.3. Для проверки состояния сетевых интерфейсов необходимо в строке приглашения ввести команду «show interfaces». Если программа функционирует корректно, будет выведен перечень всех физических сетевых интерфейсов системы.

5. ОБНОВЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

5.1. После запуска Zenator SE Fw необходимо произвести процедуру авторизации.

В поле «zenator login: » необходимо ввести имя пользователя «admsec» и нажать клавишу «Enter».

В поле «Password: » необходимо ввести пароль «12345678i.» и нажать клавишу «Enter».

Примечание. Пароль на экране не отображается.

После входа в систему на экране появится сообщение «Welcome admsec!» и строка приглашения «zenator>».

5.2. Далее необходимо задать сервер обновления, выполнив команду

system update-server <address>

где <address> – адрес сервера обновлений.

Примечание. Адрес сервера обновлений можно получить, обратившись в службу технической поддержки АО «НИИ «Масштаб».

5.3. После этого необходимо получить список обновлений Zenator SE Fw, выполнив команду

system update

5.4. Обновление общесистемного ПО выполняется командой

system upgrade

6. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

6.1. Для вывода текущего времени и даты используется команда

show system clock

6.2. Для установки даты и времени используется команда

system clock <YYYYMMDDhhmmss>

где YYYYMMDD – год, месяц, день соответственно;

hhmmss – часы, минуты, секунды соответственно.

Примечание. Запрещается устанавливать дату и время более ранние, чем указано в выводе команды «show system clock».

7. СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

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

Действия системного программиста должны осуществляться в соответствии с подсказками, выдаваемыми в процессе инсталляции и настройки программы на экран монитора.

Перечень принятых сокращений

АП	– аппаратная платформа
ОС	– операционная система
ПО	– программное обеспечение
ПЭВМ	– персональная электронно-вычислительная машина
ARP	– Address Resolution Protocol (протокол разрешения адресов)
BGP	– Border Gateway Protocol (пограничный межсетевой протокол)
CLI	– Command Line Interface (интерфейс командной строки)
DAT	– Dynamic Address Translation (динамическое преобразование адресов)
DHCP	– Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста)
DMZ	– демилитаризованная зона
GRE	– Generic Routing Encapsulation («общая инкапсуляция маршрутов», протокол туннелирования сетевых пакетов)
IEEE	– Institute of Electrical and Electronics Engineers (Институт Инженеров Электротехники и Электроники)
IGMP	– Internet Group Management Protocol (протокол управления групповой передачей данных)
IPFIX	– Internet Protocol Flow Information Export (протокол экспорта информации по IP-потоку)
IPIP	– IP over IP («IP поверх IP», протокол туннелирования)
LLDP	– Link Layer Discovery Protocol (протокол оповещения канального уровня)
MSS	– Maximum Segment Size (максимальный размер полезного блока данных)
MTU	– Maximum Transmission Unit (максимальный размер полезного блока данных)
NAPT	– Network Address Port Translation (преобразование сетевых адресов и портов)

NAT – Network Address Translation (преобразование сетевых адресов)
NTP – Network Time Protocol (протокол передачи точного времени)
OSPF – Open Shortest Path First («первоочередное открытие кратчайших маршрутов», протокол динамической маршрутизации)
PAT – Port Address Translation (технология трансляции сетевого адреса в зависимости от TCP/UDP-порта получателя)
PPP – Point-to-Point Protocol (туннельный протокол типа «точка-точка»)
PPPoE – Point-to-Point Protocol Over Ethernet (сетевой протокол канального уровня передачи кадров PPP через Ethernet)
PPTP – Point-to-Point Tunneling Protocol (туннельный протокол типа «точка-точка» в стандартной, незащищенной сети)
REST API – прикладной программный интерфейс передачи состояния представления
RIP – Routing Information Protocol (протокол маршрутизации)
SNAT – Static Network Address Translation (статический NAT)
SNMP – Simple Network Management Protocol (простой протокол сетевого управления)
SSH – Secure Shell (сетевой протокол прикладного уровня)
VLAN – Virtual Local Area Network (виртуальная локальная сеть)
VPN – Virtual Private Network (виртуальная частная сеть)
VRRP – Virtual Router Redundancy Protocol (сетевой протокол, объединяющий группу маршрутизаторов в один виртуальный маршрутизатор)

Лист регистрации изменений

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