127018, Москва, ул. Сущёвский вал, д. 18
Телефон: +7 (495) 995 4820
Факс: +7 (495) 995 4820
https://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство Криптографической Защиты Информации

КриптоПро HSM версия 2.0 Комплектация 3

Описание реализации

ЖТЯИ.00096-02 96 01

Листов 69

2020 г.

Содержание

Список сокращений

ДСЧ	—	Датчик случайных чисел
НСД	—	Несанкционированный доступ
ОС	—	Операционная система
ПАКМ	—	Программно-аппаратный криптографический модуль
ПО	—	Программное обеспечение
СВТ	—	Средства вычислительной техники
СКЗИ	—	Средство криптографической защиты информации
CRL	—	Список отозванных сертификатов (Certificate Revocation List)
ITU-T	—	Международный комитет по телекоммуникациям (International Telecommunication Union)

1. Основные технические данные и характеристики ПАКМ

ПАКМ «КриптоПро HSM» — программно-аппаратный криптографический модуль, предназначен для использования в сетях/системах хранения и обработки информации, не составляющей государственной тайны.

ПАКМ «КриптоПро HSM» представляет собой сетевое устройство, подключаемое либо непосредственно к серверу (хосту), использующему криптографические сервисы ПАКМ, либо в сегмент локальной сети через стандартные сетевые устройства (коммутаторы, маршрутизаторы, концентраторы) для обслуживания групп серверов и компьютеров пользователей сети.

ПАКМ может быть использован в качестве СКЗИ в различных системах/подсистемах криптографической защиты информации, поддерживающих криптографические интерфейсы «КриптоПро CSP» (Microsoft CryptoAPI 2.0).

ПАКМ «КриптоПро HSM» предназначен для выполнения следующих функций:

- формирования/проверки электронной подписи (ЭП) под блоком данных по запросу пользователей;
- шифрования/расшифрования блоков данных по запросам пользователей.

При этом ПАКМ «КриптоПро HSM» обеспечивает:

- реализацию криптографических функций и интерфейс взаимодействия с серверами и рабочими станциями пользователей;
- интерфейс к прикладным криптографическим функциям в соответствии со спецификацией Microsoft Cryptographic Service Provider;
- возможность использования функций ПАКМ «КриптоПро HSM» через интерфейсы Microsoft CryptoAPI;
- идентификацию и аутентификацию пользователей при локальном и удаленном доступе к ПАКМ «КриптоПро HSM»;
- проверку целостности критичного к безопасному функционированию ПО при инициализации ПАКМ «КриптоПро HSM»;
- генерацию случайных чисел с использованием аппаратного ДСЧ;
- генерацию закрытых ключей обмена и ключей ЭП с использованием исходного материала, предоставленного уполномоченной организацией;
- срок действия ключей ЭП, являющихся неэкспортируемыми, составляет не более 3-х лет. Максимальный срок действия ключей проверки ЭП — 15 лет после окончания срока действия соответствующего ключа ЭП. Максимальный срок действия открытых ключей обмена — не более 3-х лет. Максимальный срок действия неэкспортируемых закрытых ключей обмена составляет не более 3-х лет. Срок действия иных ключей не превышает 1 года 3 месяцев[1];
- сопряжение с сервером/серверной группой по отдельному сегменту Ethernet;
- ввод закрытого ключа с ключевых носителей на интеллектуальной карте;
- выполнение функций создания и проверки электронной подписи (ЭП) согласно ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018),

вычисление хэш-функции согласно ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018);

- шифрование и имитозащита согласно ГОСТ 28147-89;
- опционально, поддержку алгоритмов RSA в части генерации ключей, формирования и проверки ЭП, шифрования и расшифрования;
- опционально, поддержку алгоритмов RSA в части генерации ключей, формирования и проверки ЭП;
- возможность встречной работы ПАКМ «КриптоПро HSM» с СКЗИ «КриптоПро CSP»;
- уничтожение ключей;
- сопряжение с устройством доступа по криптографически защищенному каналу «К2». Канал «К2» – локальный защищенный канал, используется для защищенного обмена информацией между ПАКМ и устройством доступа к ПАКМ;
- сопряжение с устройством доступа по криптографически защищенному каналу «К». Канал «К» – локальный защищенный канал, используется для защищенного обмена информацией между ПАКМ и устройством доступа к ПАКМ[2];
- регистрация событий в журнале аудита криптографических вызовов ПАКМ.

Примечания:

1. Сроки действия ключей ЭП и закрытых ключей обмена могут уточняться при проведении работ по встраиванию ПАКМ «КриптоПро HSM» в системы по ТЗ, согласованным с 8 Центром ФСБ России.

2. Канал «К» используется только в рамках Головного удостоверяющего центра.

ПАКМ «КриптоПро HSM» удовлетворяет классу КВ/КВ2 (Комплектация 1 Исполнение 1) или классу КС3 (Комплектация 1 Исполнения 2-5) при выполнении требований эксплуатационной документации на ПАКМ.

ПАКМ «КриптоПро HSM» может быть использован в качестве СКЗИ в различных системах/подсистемах криптографической защиты информации, поддерживающих криптографический интерфейс (Cryptographic Service Provider (CSP)) КриптоПро CSP 4.0/5.0.

ПАКМ обеспечивает одновременное обслуживание до 100 устройств доступа с возможностью формирования до 3000 подписей хэш-значений в секунду.

ПАКМ «КриптоПро HSM» обеспечивает хранение до 500000 ключевых контейнеров пользователей.

1.1. Операционные системы серверных приложений ПАКМ

Программные средства ПАКМ «КриптоПро HSM» функционируют на базе Альт Линукс СПТ 7.0 с защитой ядра ОС средствами пакета GRSecurity.

ОС Альт Линукс СПТ 7.0 сертифицирована Федеральной службой по техническому и экспортному контролю (ФСТЭК России). Классификация по уровню контроля отсутствия недекларированных возможностей - 4 уровень. Показатели защищенности от несанкционированного доступа к информации - по 5 классу защищенности.

ПАКМ предназначен для использования с серверными приложениями, приложениями пользователей на базе операционных систем семейств Windows и Unix/Linux (см. п. 4 документа «ЖТЯИ.00096-02 30 01. КриптоПро HSM. Формуляр»).

1.2. Ключевые носители ПАКМ

Ключевая система СКЗИ ПАКМ «КриптоПро HSM» включает в себя ключи ЭП, шифрования и обмена (экспорта ключей).

Ключи ЭП представляются ключевой парой: ключ ЭП – для формирования ЭП, ключ проверки ЭП.

Ключи шифрования – симметричные ключи сообщения (пакета), случайные или диверсифицированные из случайного ключа сессии по открытому заголовку сообщения (пакета).

Ключи обмена строятся на основе открытого распределения ключей по алгоритму Диффи-Хеллмана на базе ключевых пар закрытый/открытый ключи алгоритма ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018).

На ключевых носителях ключи хранятся в формате ключевого контейнера. Ключевой контейнер содержит также информацию, необходимую для обеспечения криптографической защиты ключей и их целостности.

Закрытые ключи, хранящиеся в памяти ПАКМ, шифруются прямо или косвенно (через промежуточные ключи – ключи шифрования) на ключе активации ПАКМ.

Ключ активации ПАКМ использует схему разделения секрета с вводом ключевой информации с любых 3-х (k) из 5-ти (n) носителей для формирования функционального ключа. При этом обеспечивается защита функционального ключа при компрометации ключевой информации на любых не более k-1 носителях. В случае компрометации ключевой информации хотя бы с одного носителя, необходимо перевыпустить все 5 (n) ключей.

Интеллектуальные карты поставляются с ПАКМ «КриптоПро HSM» отформатированными, с предустановленным pin-кодом «11111111». При записи ключей на карту pin-код необходимо сменить.

При выпуске/записи карт с ключами на карту наносится тип карты: номер компоненты ключа защиты, символ «К» (для карты аутентификации Администратора UNIX/Linux Сервера – ПАК «КриптоПро HSM»), символ «К2» (для карты аутентификации Пользователь/Администратор Windows сервера – ПАК «КриптоПро HSM»). Кроме этого на карту записывается фамилия лица (пользователя - владельца), ответственного за данный ключевой носитель.

Надписи производятся разборчивым почерком (предпочтительно – печатными буквами), фломастером типа Staedtler Lumocolor permanent № 318 (с водостойким красителем).

2. Состав и назначение компонент программного обеспечения ПАКМ

2.1. Состав компонент ПО ПАКМ

Программная компонента ПАКМ включает две составляющие:

- системное программное обеспечение – ОС Альт Линукс СПТ 7.0;
- программное обеспечение ПАКМ (ПО ПАКМ).

Штатные средства ОС «Альт Линукс СПТ 7.0» включают:

- МЭ – межсетевой экран;
- TCP/IP –стек протокола TCP/IP;
- RPC – процедура удаленных вызовов;
- SYS Log – модуль работы с log-файлами;
- ACL – система управления доступом;
- Драйвер COM-порта;
- Библиотека libc, обеспечивающая взаимодействие прикладного программного обеспечения с программными средствами ОС.

Состав устанавливаемых пакетов ОС Альт Линукс СПТ 7.0 при изготовлении ПАКМ и настройка ОС описаны в документе «ЖТЯИ.00096-02 94 01. КриптоПро HSM. Описание процедуры сборки».

Программное обеспечение ПАКМ включает:

- ЖТЯИ.00096-01 99 01. КриптоПро HSM. Базовые модули;
- ЖТЯИ.00096-01 99 02. КриптоПро HSM. Интерфейсные модули.

Базовые модули ПАКМ являются составной частью изделия ПАКМ и устанавливаются при изготовлении ПАКМ «КриптоПро HSM».

Интерфейсные модули поставляются на отдельном CDROM и служат для создания систем, использующих СКЗИ ПАКМ «КриптоПро HSM», подсистем криптографической защиты информации. Данные модули должны быть установлены на ЭВМ, использующей СКЗИ ПАКМ «КриптоПро HSM».

2.2. Базовые модули ПАКМ «КриптоПро HSM»

При изготовлении ПАКМ помимо базовой установки операционной системы Альт Линукс СПТ 7.0 в изделие устанавливаются следующие пакеты с программным обеспечением:

lsb-cprocsp-base-4.0.0-4.noarch.rpm

lcprocsp-fenixm-server-64-4.0.0-4.x86_64.rpm

lsb-cprocsp-rdr-64-4.0.0-4.x86_64.rpm

lsb-cprocsp-rdr-sobol-64-4.0.0-4.x86_64.rpm

cprocsp-rdr-pcsc-64-4.0.0-4.x86_64.rpm

lsb-cprocsp-capilite-64-4.0.0-4.x86_64.rpm

lcprocsp-hsm_db-64-4.0.0-4.x86_64.rpm

cprocsp-pam_hsm-64-4.0.0-4.x86_64.rpm

cprocsp-stunnel-64-4.0.0-4.x86_64.rpm

cprocsp-hsm_webadmin-64-4.0.0-4.x86_64.rpm

В названиях дистрибутивов СКЗИ используется нотация:

Lsb – префикс LSB (Linux standard base) совместимости пакета

cpro – префикс организации разработчика;

csp – криптопровайдер;

x86_64 – 64 -разрядная платформа Intel.

noarch – независимый от платформы пакет

Пакет lsb-cprocsp-base-4.0.0-4.noarch.rpm содержит модули:

- **cprocsp** – модуль старта/останова сервисов (демонов) обработки криптографических вызовов
- локализированные версии мануала (man)
- сценарий создания всех каталогов, необходимых для установки и функционирования СКЗИ.

Пакет **cprocsp-fenixm-server-64-4.0.0-4.x86_64.rpm** содержит основные модули криптопровайдера:

- **fenixmsrv** – модуль реализации канала К, управления ПАКМ как при помощи LCD панели, так и SOAP интерфейса удаленного Web администрирования, работы с журналами ПАКМ, запускаемый как демон ОС;
- **cryptsrv_hsm** – основной модуль криптопровайдера КриптоПро CSP версии 3.6, обрабатывающий раскодированные запросы на выполнение криптографических операций (направляемые от модулями fenixmsrv и stunnel_hsm). Запускается как демон ОС;
- **srv_wrapper** – модуль обработки команд, требующих запуска второстепенных утилит. Используется для обеспечения большей безопасности путем описания ограничений GRSecurity, позволяющих использование данных утилит только данным модулем. Запускается как демон ОС;
- **libcsp_kb2** – библиотека ГОСТ алгоритмов, реализующая целевые функции криптографической защиты информации, работу с ключами, доступ к ключевым носителям;
- **librsaenh_kb2** – библиотека RSA алгоритмов, реализующая целевые функции криптографической защиты информации, работу с ключами, доступ к ключевым носителям;
- **libcspr** – библиотека, обеспечивающая доступ к криптопровайдеру, функционирующему как отдельный сервис (процесс ОС);

- **libcspsrv** – библиотека, обеспечивающая транспорт вызовов между приложениями и сервисом cryptsrv_hsm;
- **stunnel-K2.conf, stunnel-K2s.conf, stunnel-web.conf** – шаблоны конфигурационных файлов для запуска соответсвующих экземпляров stunnel_hsm;
- **hsm_backup** - утилита, используемая для внутреннего резервирования ключей ПАКМ;
- **dsrfcopy** – утилита, используемая для пополнения ключевого материала, предоставляемого уполномоченной организацией;
- **read_lcd** - скрипт, используемый процедурами загрузки ОС для получения скорости обмена и номера COM порта LCD панели из конфигурационного файла криптопровайдера (см. Приложение 7. Скрипт read_lcd – чтение параметров LCD панели);
- **read_parm** - скрипт, используемый процедурами старта модулей поддержки сети ОС для чтения конфигурации ПАКМ (IP адреса сетевых интерфейсов, их характеристики, доступность), заданной администраторм ПАКМ и хранящейся в БД mysql.
- **genfw** - скрипт, используемый процедурами старта модулей поддержки межсетевого экрана ОС для чтения конфигурации ПАКМ (правила межсетевого экрана), заданной администраторм ПАКМ и хранящейся в БД mysql;
- **lcdfunctions** - скрипт, содержащий набор функций, необходимых для вывода на LCD панель информации о статусе загрузки модулей ОС, прохождении процедуры проверки целостности в момент старта ПАКМ. Содержит саму функцию проверки целостности модулей ПАКМ (см. Приложение 5. Скрипт lcdfunctions – набор функций для вывода строк на LCD панель и проверки целостности);
- **policy_hsm** – список контроля доступа к объектам ПАКМ (ACL), используемый пакетом GRSecurity (см. Приложение 3. Список контроля доступа (ACL));
- **libhsmlcddrv, libhsmlcddrvse, libhsmlcddrvlcm, libhsmlcddrvlcm2x16** – библиотеки драйверов различных исполнений LCD панелей.

Пакет **lsb-cprocsp-rdr-64-4.0.0-4.x86_64.rpm** содержит модули:

- **cpverify** – утилита командной строки для проверки целостности модулей СКЗИ;
- **cpconfig** – утилита командной строки для конфигурирования СКЗИ (работа с конфигурационным файлом);
- **csptest** – утилита командной строки для проверки работоспособности/тестирования СКЗИ. Данный компонент удаляется из ПАКМ в процессе его изготовления;
- **wipefile** - утилита командной строки для удаления файлов вместе с содержимым при штатных и нештатных (свопирование) ситуациях;
- **libcapi10** – библиотека, реализующая основные функции интерфейса CryptoAPI;

- **librdrdsrf** - библиотека поддержки работы с внешней гаммой;
- **librdrfat12** – библиотека поддержки считывателей ключевой информации;
- **librdrrdr** - библиотека поддержки считывателей ключевой информации, обеспечивающая унифицированный интерфейс доступа к ключевым носителям;
- **librdrrndm** - библиотека поддержки ДСЧ ;
- **librdrsup** – библиотека дополнительных функций поддержки работы с оборудованием, обеспечивает реализацию общих функций доступа к различным устройствам хранения ключевых носителей.

Пакет **lsb-cprocsp-rdr-sobol-64-4.0.0-4.x86_64.rpm** содержит модуль:

- **librdrsbl** - библиотека поддержки «Соболь»;

Пакет **cprocsp-rdr-pcsc-64-4.0.0-4.x86_64.rpm** содержит модули:

- **librdrpcsc** - библиотека поддержки считывателей ключевой информации – устройств чтения смарт-карт и eToken, поддерживающих интерфейс PC/SC;
- **librdrric** - библиотека поддержки носителей ключевой информации – смарт-карт ОСКАР, смарт-карты на базе микроконтроллера ST19NR66.

Пакет **lsb-cprocsp-capilite-64-4.0.0-4.x86_64.rpm** содержит модули:

- **cryptcp, csptestf, inittst** - приложения командной строки для работы с сертификатами, шифрования и расшифрования данных, создания и проверки электронной подписи (ЭП), хэширования данных с использованием сертификатов открытых ключей. Данный компонент удаляется из ПАКМ в процессе его изготовления;
- **libasn1data, libcpasn1, libcpext** – библиотека поддержки ASN1 структур PKI, содержит функции преобразования структур данных в машинно-независимое представление;
- **libcapi20** – библиотеки интерфейса CryptoAPI. Интерфейс модуля capilite является подмножеством интерфейса CryptoAPI v. 2.0;
- **libcplib** – библиотека вспомогательных функций для работы с различными форматами даты/времени, двоичными строками (blob);
- **libpkixcmp** – библиотека функций высокого уровня для работы с CMP (Certificate Message Protocol) сообщениями, реализации компонент удостоверяющих центров;
- **libssp** – библиотека поддержки Security Support Provider Interface (SSPI);
- **libpkivalidator** – библиотека функций дополнительной проверки цепочки сертификатов, основанной на политиках использования сертификатов;
- **libenroll –** библиотека поддержки генерации запросов на сертификаты открытых ключей;
- **libtsp, libocsp,libtspcli –** библиотеки поддержки форматов запросов к сервисам штампов времени и онлайн проверки статусов сертификатов.
- **Liburlretrieve –** библиотека поддержки доступа к ресурсам по URL адресам.

Пакет **cprocsp-hsm_db-64-4.0.0-4.x86_64.rpm** – содержит модули:

- **libhsmlogdb** – библиотека поддержки работы с базой данных журнала аудита ПАКМ;
- **libhsmuserdb** – библиотека поддержки работы с базой данных пользователей ПАКМ;
- **libhsmdate** – библиотека поддержки работы с форматами даты/времени;
- **libhsmblob** – библиотека поддержки работы с двоичными данными (блобами).

Пакет **cprocsp-pam_hsm-64-4.0.0-4.x86_64.rpm** – содержит модули:

- **libpamcpx509** – pam модуль дополнительной аутентификации удаленного пользователя по TLS-клиентскому сертификату;
- **libpamhsmlog** – pam модуль дополнительного отражения события аутентификации в журнале аудита ПАКМ.

Пакет **cprocsp-hsm_webadmin-64-4.0.0-4.x86_64.rpm** – содержит модули:

- **default.htm** – html страничка для удаленного web администрирования ПАКМ;
- **CPEnroll.cab** – устанавливаемый как элемент ActiveX в Web интерфейсе администрирования модуль, позволяющий формировать и записывать на ключевые носители ключи и сертификаты ключей доступа пользователей ПАКМ.

Пакет **cprocsp-stunnel-64-4.0.0-4.x86_64.rpm** – содержит модули:

- **stunnel_hsm** – **stunnel_hsm** – модуль, реализующий TLS прокси сервер, обеспечивающий двустороннюю TLS аутентификацию по сертификатам x509 (ГОСТ) и ГОСТ алгоритмы шифрования, обеспечивающий работу канала К2. Запускается как демон ОС;

2.3. Интерфейсные модули ПАКМ «КриптоПро HSM»

В комплект поставки ПАКМ «КриптоПро HSM» входит CDROM «ЖТЯИ.00096-02 99 02. КриптоПро HSM. Интерфейсные модули».

На данном CDROM содержится необходимое ПО для платформ Windows, Атликс («АТЛИКС-2», «АТЛИКС-КВ2»), и LSB-совместимых 32/64-разрядных ОС семейства Unix/Linux, которое должно быть установлено на ПЭВМ, использующую СКЗИ ПАКМ «КриптоПро HSM».

Описание интерфейсных модулей для ОС семейства Unix/Linux/Атликс и их применения можно найти в документе «ЖТЯИ.00096-02 90 02. КриптоПро HSM. Использование интерфейсных модулей».

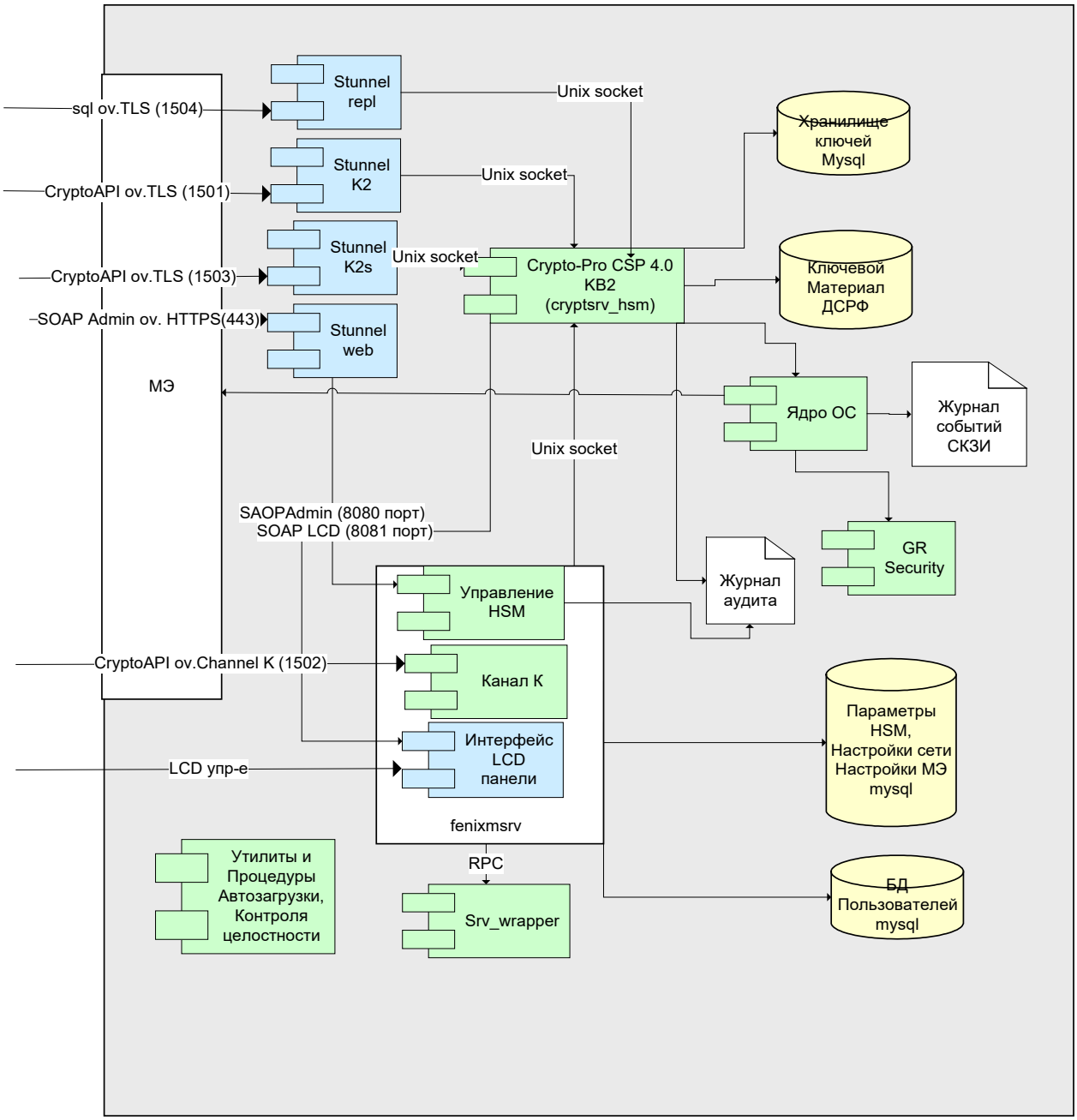
Описание интерфейсных модулей для ОС семейства Windows и их применения можно найти в документе «ЖТЯИ.00096-02 93 01. КриптоПро HSM. Руководство пользователя».

2.4. Взаимодействие основных компонент, модулей ПАКМ

Ниже представлена диаграмма взаимодействия основных модулей ПАКМ.

2.5. Внешние интерфейсы ПАКМ

В рабочем состоянии ПАКМ имеет следущие внешние интерфейсы:



- Интерфейс ручного управления ПАКМ через LCD панель
- Интерфейс канала К
- Интерфейс канала К2
- Интерфейс канала К2s
- Интерфейс Web администрирования
- Интерфейс горячего резервирования (репликации)

2.5.1. Интерфейс ручного управления ПАКМ

Интерфейс ручного управления ПАКМ представляет собой систему меню и вызываемых функций, управляемых с помощью клавиш и экрана LCD панели ПАКМ. Доступ к меню разрешен только привилегированным пользователям с использованием смарт-карт, на которых записан закрытый ключ обмена и сертификат этого ключа, включающий необходимые расширения (признаки Ролей привилегированных пользователей).

Процедура аутентификации привилегированного пользователя выглядит следующим образом: пользователь нажимает на LCD панели любую клавишу, вставляет смарт-карту с ключом и сертификатом доступа, вводит пин код для доступа к контейнеру закрытого ключа обмена на карте. Система извлекает с карты сертификат, разбирает его, получает идентификатор пользователя, по которому извлекает всю информацию о пользователе из БД пользователей ПАКМ. Сравнивает сертификат с хранящимся в БД, проверяет – не заблокирован ли пользователь, сморит флаги привилегий. Далее система запускает процедуру проверки обладания закрытым ключом доступа – предлагает подписать (ГОСТ Р 34.10-2012/ГОСТ 34.10-2018) некую случайную последовательность при помощи ключа ЭП, хранящегося на карте, после чего осуществляет проверку ЭП при помощи извлеченного с карты сертификата. Если все описанные действия прошли без ошибок, система создает контекст пользователя, в котором хранится его идентификатор, флаги привилегий выполнения функций управления и разрешает пользователю с данным контекстом доступ к функциям LCD меню. Любая выполняемая функция проверяется ПАКМ на доступ по флагам привилегий.

Доступ к функциям LCD меню осуществляется при помощи разделенного ключа активации ПАКМ, защитные ключи разделенного секрета которого (5 защитных карт) распределены между привилегированными пользователями ПАКМ. Для этого поочередно вводятся любые 3 из возможных 5-ти частей разделенного секрета. На каждую часть (смарт-карту) пользователь вводит пин-код. После успешного завершения этой процедуры система пытается активировать ключ активации ПАКМ и расшифровать на нем ключи шифрования ПАКМ (описание ключей ПАКМ - см. документ «ЖТЯИ.00096-02 90 01. КриптоПро HSM. Инструкция по использованию»). Если эта процедура заканчивается успехом, то система создает контекст доступа к функциям LCD меню с правами суперпользователя (описание ролевой модели см. в документе «ЖТЯИ.00096-02 90 01. КриптоПро HSM. Инструкция по использованию»). Данный пользователь может выполнять как функции любых других ролей, так и присущие только ему (например, управление привилегированными пользователями).

Все изменения натроек ПАКМ, операций с учетными записями пользователей ПАКМ, и других функций, так или иначе изменяющих внутреннее состояние ПАКМ, попадают в журнал аудита ПАКМ.

2.5.2. Интерфейс канала «К»

Интерфейс канала «К» унаследован от предыдущих реализаций ПАКМ, сертифицированных по классу криптографической защиты КВ, ПК «Феникс-М», ПК «Атликс HSM». В настоящей реализации ПАКМ он оставлен для совместимости, для обслужиания серверов с установленной операционной системой семейства Unix/Linux/Атликс. Канал обеспечивает безопасный обмен данными криптографического интерфейса «КриптоПро CSP» (Microsoft CryptoAPI) между серверами и ПАКМ. ПАКМ использует для данного канала порт входящих соединений 1502. Слушателем данного порта является процесс-демон fenixmsrv. Данный процесс после получения запроса на соединение от сервера производит процедуру аутентификации, выработки сессионного ключа шифрования в канале и создает отдельный поток, который будет обслуживать криптографические запросы интерфейса CryptoAPI сервера.

2.5.3. Интерфейс канала «К2»

Интерфейс канала «К2» обеспечивает безопасный обмен данными криптографического интерфейса «КриптоПро CSP» версии 4.0/5.0 (Microsoft CryptoAPI) между устройствами доступа (серверами и рабочими станциями пользователей) и ПАКМ. Канал К2 полностью реализует протокол TLS с российскими криптографическими алгоритмами ГОСТ. ПАКМ использует для данного канала порт входящих соединений 1501. Слушателем данного порта является процесс-демон **stunnel_hsm**. Данный процесс после получения запроса на соединение от сервера производит процедуру TLS аутентификации, выработки сессионного ключа шифрования в канале и создает отдельный процесс, который будет обеспечивать шифрование/расшифрование протокола TLS и перенаправлять расшифрованные криптографические запросы интерфейса CryptoAPI устройства доступа к внутреннему модулю СКЗИ ПАКМ – процессу cryptsrv_hsm, используя unix сокет.

2.5.4. Интерфейс канала Web администрирования ПАКМ

Интерфейс канала Web администрирования ПАКМ обеспечивает удаленное управление ПАКМ с использованием стандартного протокола HTTPS/TLS, испольующего криптографические алгоритмы ГОСТ. Для этого рабочая станция удаленного WEB администрирования оснащается отдельным СКЗИ «КриптоПро CSP» и подключается по отдельному сегменту локальной сети к ПАКМ на отдельный сетевой интерфейс ПАКМ. Для вызова функций управления ПАКМ поверх протокола TLS используется протокол SOAP. Функции и структуры данных протокола описаны в «Приложение 1. Описание SOAP интерфейса Web администрирования».

ПАКМ использует для данного канала порт входящих соединений 443. Слушателем данного порта является процесс-демон **stunnel_hsm**. Данный процесс после получения запроса на соединение от сервера производит процедуру TLS аутентификации, выработки сессионного ключа шифрования в канале и создает отдельный процесс, запускаемый под UID пользователя, полученного из сертифката TLS клиента, и который будет обеспечивать шифрование/расшифрование протокола TLS и перенаправлять расшифрованные SOAP/HTTP запросы на порт 8080. Слушателем порта 8080 является процесс fenixmsrv, который для обработки поступившего запроса создает отдельный поток. Этот поток запрашивает через /**proc** UID пользователя, под которым запущен соответствующий экземпляр процесса stunnel_hsm, запрашивает информацию из БД пользователей о нем, проверяет – не заблокирован ли пользователь, смотрит флаги привилегий. Если пользователь является привилегированным, система создает контекст пользователя, в котором хранится его идентификатор, флаги привилегий выполнения функций управления и разрешает или запрещает пользователю с данным контекстом доступ к вызываемой функции управления ПАКМ. Любая выполняемая функция проверяется ПАКМ на доступ по флагам привилегий.

При первом HTTPS обращении на IP адрес ПАКМ, после успешного создания TLS соединения (включающего двустороннюю аутентификацию по сертификатам), клиенту в браузер Internet Explorer/Edge выдается html страница с реализованным на ней интерфейсом администрирования ПАКМ, включающим необходимые SOAP вызовы. Дальнейшая работа сводится к выбору того или иного режима на данной странице, который при необходимости осуществляет требуемые SOAP вызовы к ПАКМ по защищенному каналу.

2.5.5. Интерфейс канала К2s

Интерфейс канала K2s (нешифрованный и/или неаутентифицированный канал) обеспечивает обмен данными криптографического интерфейса «КриптоПро CSP» (Microsoft CryptoAPI) между устройствами доступа - серверами и ПАКМ, находящимися в одной контролируемой зоне. Канал K2s может реализовывать протокол TLS с российскими криптографическими алгоритмами ГОСТ в части двусторонней аутентификации. ПАКМ использует для данного канала порт входящих соединений 1503. Слушателем данного порта является процесс-демон **stunnel_hsm**. Данный процесс после получения запроса на соединение от сервера производит процедуру TLS аутентификации и создает отдельный процесс, который будет перенаправлять нешифрованные криптографические запросы интерфейса CryptoAPI устройства доступа к внутреннему модулю СКЗИ ПАКМ – процессу cryptsrv_hsm, используя unix сокет.

Перечисленные каналы и их использвание подробно описаны в документе «ЖТЯИ.00096-02 90 01. КриптоПро HSM. Инструкция по использованию».

2.5.6. Интерфейс горячего резервирования (репликации)

Интерфейс горячего резервирования обеспечивает безопасный обмен данными между базами данных (ключевой информации, информации о пользователях, настроек ПАКМ) основного ПАКМ и ПАКМ горячего резерва. Канал полностью реализует протокол TLS с российскими криптографическими алгоритмами ГОСТ. ПАКМ использует для данного канала порт входящих соединений 1504. Слушателем данного порта является процесс-демон **stunnel_hsm**. Данный процесс после получения запроса на соединение от ПАКМ горячего резерва производит процедуру TLS аутентификации, выработки сессионного ключа шифрования в канале и создает отдельный процесс, который будет обеспечивать шифрование/расшифрование протокола TLS и перенаправлять расшифрованные запросы на измененные данные основного ПАКМ к серверу mysql.

Подробнее о процедуре репликации см. документ «ЖТЯИ.00096-02 95 01. КриптоПро HSM. Правила пользования».

2.6. TLS Прокси сервер – stunnel_hsm

stunnel_hsm - утилита, разработанная для создания TLS защищенного соединения между клиентом и локальным (inetd-запускаемым) или удаленным сервером. Таким образом, не имея поддержки TLS в том или ином демоне (сервисе) системы, можно легко обеспечить защиту (шифрование, одностороннюю или двустороннюю аутентификацию) соединения с использованием TLS. stunnel_hsm может быть использован для добавления функции TLS для популярных inetd сервисов, тиких как POP-2, POP-3, и IMAP, так же для сервисов как NNTP, SMTP и HTTP, или организацию PPP тунелей без изменения кода самих сервисов.

Для реализации TLS протокола stunnel_hsm использует реализацию интерфейса Microsoft Security Support Provider Interface (SSPI) от КриптоПро, обеспечивающую использование российских криптографических алгоритмов ГОСТ.

В ПАКМ «КриптоПро HSM» stunnel_hsm выполняет роль TLS прокси-сервера, прослушивающего входящие защищенные соединения и перенаправляющего расшифрованные запросы соответствующему внутреннему сервису (демону) для их дальнейшей обработки. В частности stunnel_hsm используется для организации каналов K2, K2s и web администрирования (см. п. 3.5).

При этом соответствующие экземпляры stunnel_hsm могут и не запускаться. Процесс stunnel_hsm может быть запущен и остановлен:

при смене состояния ПАКМ (INACTIVE, ADMIN_ONLY, FULL ACTIVE, HALT);

при смене настроек параметров ПАКМ, разрешающих или запрещающих использование соответствующего внешнего канала (Enable K2, Enable K2s, Enable WEB).

Для запуска соответствующего экземпляра stunnel_hsm необходимо:

- активное состояние ПАКМ (FULL ACTIVE для всех или ADMIN_ONLY для канала WEB администрирования);

- разрешение использования соответствующего канала в настройках ПАКМ (опции Enable);

- наличие описания хотя бы одного правила межсетевого экрана для соответствующего канала (порта) и сетевого интерфейса, для которого определен IP адрес в настройках сети;

Если же в режиме управления ПАКМ меняет свое состояние на неактивное или на ADMIN_ONLY (для каналов K2, K2s), или в настройках использование соответствующего канала запрещается, то соответствующий экземпляр stunnel_hsm убивается, т.е. порт перестает прослушиваться.

Перед запуском stunnel_hsm для него формируется конфигурационный файл, который записывается в каталог /var/opt/cprocsp/tmp. Информация для конфигурационнго файла берется из соответствующего шаблона (шаблоны хранятся в каталоге /etc/stunnel) и настроек ПАКМ, таких как:

- Максимальное количество входящих соединений (MaxClients);

- длительность удерживания неактивного соединения (TimeoutIdle);

- IP адрес сетевого интерфейса и соответствующий сертификат TLS сервера (подбирается по правилам межсетевого экрана и описания сетевых интерфейсов)

Перечисленные опции настроек ПАКМ и их использвание подробно описаны в документе «ЖТЯИ.00096-02 90 01. КриптоПро HSM. Инструкция по использованию».

Сразу после получения запроса на входящее соединение stunnel_hsm запускается стандартная процедура двусторонней аутентификации с использованием сертификатов открытых ключей обмена клиента и сервера. После успешной процедуры аутентификации запускается доплнительная процедура аутентификации, реализованная в **pam** модуле libpamcpx509. При этом разбирается сертификат клиента, из которого извлекается идентификатор пользователя. По этому идентификатору из базы данных пользователей ПАКМ извлекается информация об учетной записи пользователя. Происходит сверка сертификатов и проверка на блокировку пользователя. Если всё в порядке, пользователю предоставляется доступ к соответствующему интерфейсу ПАКМ. Обработчик соединения имперсонализируется в UID данного пользователя и транслирует входящий вызов соответствующему модулю – обработчику канала (на порт 8080 (процессу fenixmsrv) или на unix сокет /var/opt/cprocsp/tmp/.cryptsrv_hsm процесса cryptsrv_hsm);

2.7. Просесс cryptsrv_hsm

Процесс cryptsrv_hsm реализует криптографический интерфейс провайдера КриптоПро CSP.

Данный процесс запускается в момент загрузки ПАКМ, создает unix сокет /var/opt/cprocsp/tmp/.cryptsrv_hsm, через который принимает поступающие запросы на выполнение криптографических функций интерфейса Microsoft CryptoAPI. В момент создания соединения производится извлечение аутентификационной информации вызывающего процесса (UID, GID пользователя либо от stunnel_hsm, либо от fenixmsrv), которая запоминается в переменных потока обработчика. Процесс всегда работает под учетной записью root (UID=0, GID=0) и лишь в очень редкие и короткие промежутки

времени (формирование пути к каталогу ключей пользователя, или к личному хранилищу сертификатов пользователя) имперсонализируется, используя сохраненные в переменных потока данные. Таким образом, права на доступ к каталогу с ключами пользователя устанавливаются только для пользователя root, а процесс cryptsrv_hsm выполняет роль диспетчера доступа к этим каталогам. Для каждого пользователя создаются свои каталоги ключей и хранилищ сертификатов в виде UID.GID (например, /var/opt/cprocsp/keys/1025.1025/).

Для своей работы процесс подгружает необходимые библиотеки криптопровайдера, описанные в конфигурационном файле СКЗИ /etc/opt/cprocsp/config64.ini (вся конфигурация хранится в БД MySQL). Для генерации ключей используется аппаратный датчик случайных чисел электронного замка (ЭЗ) «Соболь». Кроме этого, для генерации ключей подписи используется ключевой материал, предоставленный уполномоченной организацией. Данный ключевой материал устанавливается в каталог /var/opt/cprocsp/dsrf/db1/ (копия в /var/opt/cprocsp/dsrf/db1/) в момент изготовления ПАКМ или сервисного обслуживания. Используемый материал уничтожается по мере изготовления ключей.

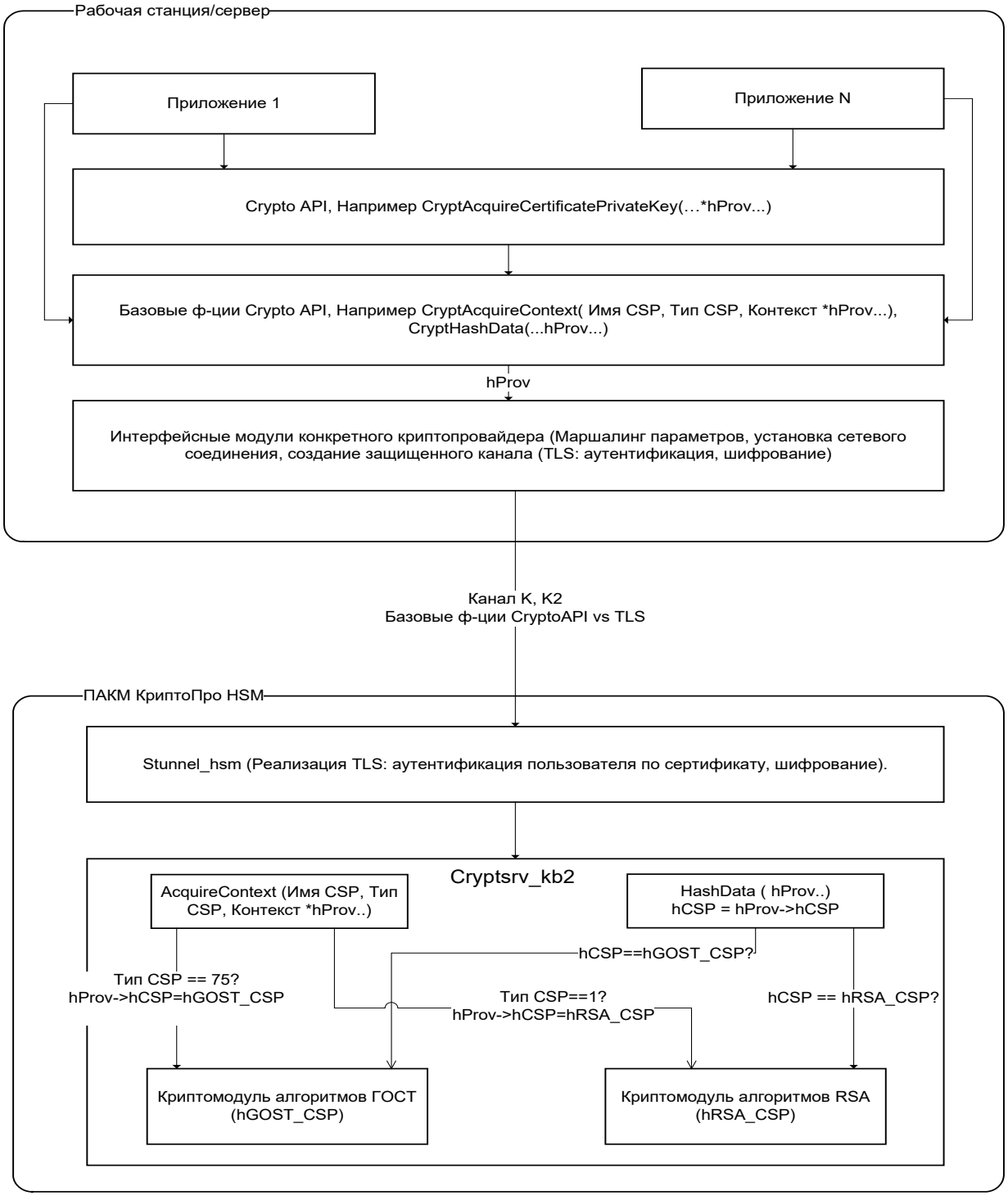
Информация о выполнении/невозможности выполнения криптографических функций записывается в журнал событий СКЗИ и журнал аудита ПАКМ (если в том есть необходимость и произведены соответствующие настройки журнала аудита).

Описание журналов ПАКМ и их использвание подробно описаны в документе «ЖТЯИ.00096-02 90 01. КриптоПро HSM. Инструкция по использованию».

При поступлении некоторых запросов, требующих доступа к закрытым частям ключевых контейнеров (например, к закрытому ключу) процесс вызывает callback функцию запроса pin-кода доступа к ключевому контейнеру. При этом в зависимости от сертификата ключа доступа клиента данный callback транслируется либо обратно на устройство доступа (сервер или рабочую станцию пользователя), либо на LCD панель через процесс fenixmsrv. Для того чтобы вызов транслировался на LCD панель, необходимо, чтобы в сертификате клиента присутствовало расширение «Администратор сервера», т.е. клиентом ПАКМ в данном случае будет сервер приложений. Для трансляции вызова запроса к LCD панели, от процесса cryptsrv_hsm к процессу fenixmsrv, используется SOAP интерфейс LCD панели. Данный интерфейс описан в «Приложение 1. Описание SOAP интерфейса Web администрирования».

При этом устанавливается прямое соединение на порт 8081, который прослушивает процесс fenixmsrv.

Процесс cryptsrv_hsm включает реализацию криптографических алгоритмов ГОСТ и RSA. Логически он объединяет в себе два разных криптомодуля. Криптомодуль RSA реализован в виде разделяемой библиотеки librsaenh.so. Для правильной трансляции криптографических вызовов тому или иному криптомодулю используется следующая схема:



В соответствии с правилами использования интерфейса CryptoAPI перед использованием криптографических вызовов клиентское приложение сначала должно создать контекст требуемого криптопровайдера. В конечном итоге это делается вызовом метода CryptAcquireContext, которому в качестве параметров, как минимум сообщается «Тип криптопровайдера», плюс, возможно, его зарегистрированное имя. По этой информации подгружается специальный модуль, исполняющий или транслирующий эти вызовы далее другим модулям криптопровайдера. Интерфейсные модули криптопровайдера ПАКМ «КриптоПро HSM» устанавливают защищенное сетевое соединение компьютера клиента с ПАКМ (создают TLS соединение с двусторонней аутентификацией), упаковывают параметры криптографического вызова в специальный

пакет (маршаллинг) и передают его по защищенному каналу в ПАКМ. Со стороны ПАКМ сетевое соединение прослушивает процесс stunnel_hsm, основным назначением которого является реализация TLS соединения (аутентификация пользователя по сертификату, шифрование канала). Расшифровав входящий пакет, stunnel_hsm имперсонализируется в UID,GID пользователя (извлеченные из сертификата) и передает пакет и идентификационные данные пользователя через unix socket процессу cryptsrv_hsm.

Процесс cryptsrv_hsm создает поток обработчик вызова, сохраняет в переменных потока цидентификационные данные пользователя (впоследствии они понадобятся для определения раздела, в котором хранятся ключи данного пользователя), распаковывает пакет (демаршаллинг), извлекая параметры вызова. По «Типу криптопровайдера» определяет - какой криптомодуль должен использоваться для создания контекста (RSA или ГОСТ). Создает у себя в памяти структуру контекста, в которой запоминает идентификатор используемого криптомодуля, и перенаправляет вызов данному криптомодулю. После успешного вызова метода CryptAcquireContext процесс cryptsrv_hsm упаковывает в «обратный пакет» результат вызова метода, передавая туда идентификатор (HANDLE) созданной структуры контекста. Все последующие вызовы, использующие данный контекст, в качестве параметра передают указанный идентификатор контекста. Процесс cryptsrv_hsm, распаковав параметры таких вызовов, по переданному идентификатору контекста разыскивает у себя сохраненную структуру контекста, извлекает из неё идентификатор используемого криптомодуля и транслирует вызов указанному криптомодулю.

Кроме всего прочего при разрыве сетевого соединения с клиентом по какой-бы то ни было причине, процесс cryptsrv_hsm закрывает все контексты, созданные с использованием данного сетевого соединения, освобождая при этом ресурсы и удаляя из памяти критически важную информацию о ключах пользователя.

2.8. Просесс fenixmsrv

Процесс fenixmsrv реализует функции управления ПАКМ как через LCD панель ПАКМ, так и через WEB администрирование, а также обеспечивает прием входящих запросов на выполнение криптографических функций по каналу «К».

Функции управления включают изменение состояния ПАКМ, управление настройками ПАКМ, настройками журнала аудита ПАКМ, настройками сети, настройками межсетевого экрана, обычными и привилегированными пользователями, их ключами и сертификатами ключей доступа к ПАКМ; управление ключами и сертификатами ПАКМ (ключи активации, шифрования, ключи и сертификаты подписи ПАКМ, ключи и сертификаты TLS сервера ПАКМ).

Все функции управления подробно описаны в документе «ЖТЯИ.00096-02 90 01. КриптоПро HSM. Инструкция по использованию».

Кроме этого процесс fenixmsrv обеспечивает контроль перепонения журнала аудита ПАКМ и контроль памяти ПАКМ. Для этого он запускает отдельный поток, который в соответствии с настройками ПАКМ, через заданный промежуток времени контролирует заполненность журнала аудита и при необходимости (зависит от настройки сделанной аудитором) запускает процедуру автоочистки журнала. При запрете на автоочистку и достижении порогового значения объема жкрнала аудита, данный поток переводит ПАКМ в состояние «Только для администрирования», т.е. закрывает все каналы обслуживания «клиентов ПАКМ» и оставляя возможность локального и удаленного администрирования. Аудитор при этом может выгрузить очередную порцию журнала и очистить его. После чего администратор ПАКМ может вновь перевести ПАКМ в состояние FULL ACTIVE, позволяющее работать обычным пользователям.

Все настройки ПАКМ хранятся в БД mysql.

2.8.1. Контроль памяти ПАКМ

ПАКМ реализован на аппаратной платформе, включающей ECC (error check & correction) модули памяти. При этом ядро операционной системы включает поддержку контроля ошибок ECC памяти, т.е. оно имеет доступ к внутреннему журналу ошибок ECC памяти.

Операционная система (используется процесс cron и вызываемая им утилита edac_util) периодически вызывает утилиту edac_util, которая обращается к функциям ядра за информацией об ошибках ECC памяти. Данная информация сбрасывается в файл /tmp/ecc_report_simple.txt. Информация содержит количество ошибок памяти, которые были автоматически исправлены, и количество ошибок, которые не могут быть исправлены внутренними механизмами ECC.

Поток fenixmsrv, отвечающий за периодический контроль переполнения журнала аудита, одновременно через тот же интервал времени просматривает файл /tmp/ecc_report_simple.txt. При обнаружении любой ошибки ECC памяти информация об этом пишется в журнал аудита ПАКМ. При обнаружении невосстановимой (unrecoverable) ошибки ECC памяти поток переводит ПАКМ в состояние «Только для администрирования», т.е. закрывает все каналы обслуживания «клиентов ПАКМ» и оставляя возможность локального и удаленного администрирования. В данном случае требуется сервисное обслуживание по замене модуля памяти.

2.9. Просесс srv_wrapper

Процесс srv_wrapper представляет собой модуль обработки команд, требующих запуска второстепенных утилит. Используется для обеспечения большей безопасности путем описания ограничений GRSecurity, позволяющих использование данных утилит только данным модулем. Команды данному процессу поступают от процесса fenixmsrv по RPC протоколу.

В настоящий момент обрабатывается следующие команды:

wipe_user – рекурсивное удаление с диска путем перезаписи нулями файлов и каталогов пользователя с его криптографическими ключами и хранилищами сертификатов;

wipe_root - рекурсивное удаление с диска путем перезаписи нулями файлов и каталогов пользователя с его криптографическими ключами и хранилищами сертификатов, конфигурационных файлов ПАКМ;

wipe_log – удаление с диска путем перезаписи нулями файлов журнала событий СКЗИ;

iptables_restart – вызов сценария рестарта межсетевого экрана (iptables);

network_restart - вызов сценария рестарта поддержки сети (networkd);

cpcsp_restart - вызов сценария рестарта сервисов cryptsrv_hsm и fenixmsrv (при деактивации ПАКМ);

syslog_restart - вызов сценария рестарта сервиса журналирования (syslogd);

stunnel_start – Запуск соответствующего экземпляра stunnel_hsm. В качестве параметров передаются имя конфигурационного файла и pid-файла;

stunnel_kill - останов соответствующего экземпляра stunnel_hsm. В качестве параметра передается имя pid-файла;

backup_root – временное резервирование файлов и каталогов с ключами ПАКМ (активации, подписи, шифрования) и хранилищами сертификатов ключей пользователя root на момент смены ключа активации и ключа шифрования ПАКМ (при сбое происходит восстановление этой информации);

restore_root – восстановление файлов и каталогов с ключами ПАКМ (активации, подписи, шифрования) и хранилищами сертификатов ключей пользователя root, если в процедуре смены ключа активации и ключа шифрования ПАКМ произошел сбой, т.е. она завершилась неудачно;

wipe_backup – удаление временной резервной копии файлов и каталогов с ключами ПАКМ (активации, подписи, шифрования) и хранилищами сертификатов ключей пользователя root, после успешной процедуры смены ключа активации и ключа шифрования ПАКМ, либо после восстановления информации из резервной копии;

backup_hsm – создание резервной копии ПАКМ (включая ключи и хранилища пользователей, ПАКМ, конфигурационные файлы ПАКМ);

restore_hsm – восстановление ПАКМ из указанной резервной копии ПАКМ (включая ключи и хранилища пользователей, ПАКМ, конфигурационные файлы ПАКМ);

2.10. Обеспечение дополнительного контроля доступа при помощи межсетевого экрана ПАКМ

Межсетевой экран ПАКМ реализован на основе встроенного в ОС сервиса iptables.

Промежуточные настройки межсетевого экрана сохраняются в БД mysql.

Администратор ПАКМ изменяет настройки при помощи LCD панели ПАКМ, либо при помощи удаленного рабочего места WEB администрирования. Настройки описываются для каждого канала, каждого сетевого интерфейса и включают:

- Указание порта входящих соединений (канала). Указывается в виде секции конфигурационного файла (например, “[1502]”);
- Указание сетевого интерфейса. Указывается в строке определенной секции (канала), описывающей разрешение на доступ через данный физический сетевой интерфейс (например, “`192_168_70_63__255_255_252_0__`**`eth0`**` = "1"`”);
- Указание сетевого адреса и маски подсети, откуда разрешается доступ. Указывается в строке определенной секции (канала), описывающей разрешение на доступ через физический сетевой интерфейс (например, “**`192_168_70_63__255_255_252_0`**`__eth0 = "1"`”);

Если для канала не описано ни одного правила, то доступ по данному каналу будет запрещен (к тому же соответствующий слушатель порта (экземпляр stunnel_hsm) просто не будет запущен).

Рестарт сервиса iptables вызывает скрипт (genfw), который сначала запрещает любую сетевую активность (входящую и исходящую), потом читает и интерпретирует соответствующим образом информацию из БД mysql, формируя файл /tmp/firewall.ini, содержащий параметры запуска сервиса. При этом в формируемых параметрах явно прописывается только один разрешаемый сетевой протокол – tcp, и никакой другой.

Пример конфигурационного файла межсетевого экрана приведен в «Приложение 2. Структура конфигурационного файла межсетевого экрана ПАКМ».

Используемый скрипт genfw приведен в «Приложение 4. Скрипт genwf – интерпретатор настроек межсетевого экрана».

При изготовлении ПАКМ инсталляционный скрипт заменяет в стандартном файле запуска сервиса iptables команду вывода параметров запуска сервиса «IPTABLES_FILTER» с “cat” на “/opt/cprocsp/sbin/amd64/genfw”:

```
cat /etc/init.d/iptables |sed 's%IPTABLES_FILTER=.*$%IPTABLES_FILTER=/opt/cprocsp/sbin/amd64/genfw%'
>/tmp/iptables.new

mv /tmp/iptables.new /etc/init.d/iptables

chmod 755 /etc/init.d/iptables
```

Таким образом любой перезапуск ПАКМ или только сервиса iptables из кода сервиса srv_wrapper приводит к чтению параметров запуска сервиса iptables из бд mysql, формированию временного конфигурационного файла ПАКМ /tmp/firewall.ini и интерпретации его скриптом genfw.

2.11. Обеспечение дополнительного контроля доступа при помощи механизма ACL

Используемое ядро операционной системы включает в себя поддержку патчей GRSecurity и PaX. Это обеспечивает мандатный контроль доступа на основе списков контроля доступа (ACL), рандомизацию ключевых локальных и сетевых информативных данных, ограничения /proc контроль сетевых сокетов, контроль возможностей, и добавочные функции аудита. PaX, среди прочих других возможностей, отмечает области данных в памяти. Например, стек отмечается как неисполняемый, и область кода программы, как не имеющая возможности записи в неё. Целью этой защиты является защита памяти от записи, что предотвращает множество уязвимостей в безопасности, таких как переполнение буфера. PaX также обеспечивает рандомизацию расположения в адресном пространстве (address space layout randomization, ASLR), которая размещает важные адреса памяти в случайном порядке и таким образом не позволяет атакующему заранее полагаться на знание этих адресов.

ПАКМ использует специально созданные списки ACL установленные в него при изготовлении. Файл со списком ACL – policy_hsm устанавливается в каталог /etc/grsec, после чего переименовывается в “policy”. При загрузке ПАКМ grsec активируется командой gradm –E (добавленной в файл rc.local при изготовлении. см. Приложение 8. Файл автозагрузки rc.local), которая активирует дополнительный контроль доступа, описываемый данным списком. Правила списка ограничивают доступ одних объектов ОС (процессов, файлов, сокетов) к другим, и фактически создают замкнутую систему, в которой отсутствует shell, пользователь root (с его обычными привелегиями), в которой невозможно запустить произвольную утилиту, обратиться к процессу через unix или ip soket, организовать прослушивание порта каким-либо процессом, если это не прописано в списке ACL. Например, доступ на запись к каталогам, в которых хранится ключевая информация пользователей, разрешается только процессу криптопровайдера (cryptsrv_hsm), модулю резервирования (hsm_backup) и утилите криптопровайдера, вычищающей при удалении информацию с диска так, чтобы её невозможно было восстановить (wipefile). Или, например, обращение к процессу fenixmsrv по порту 80 (используется для интерфейса удаленного администрирования ПАКМ) возможно только процессу stunnel_hsm.

Используемый список ACL см. Приложение 3. Список контроля доступа (ACL).

3. Контроль целостности программного обеспечения

В ПАКМ «КриптоПро HSM» В СКЗИ реализован механизм контроля несанкционированного случайного и/или преднамеренного искажения (изменения, модификации) и/или разрушения информации, программных компонентов СКЗИ.

Процедура контроля целостности осуществляется до загрузки ПО ПАКМ. В случае обнаружения искажений программных компонентов ПАКМ прекращает свою работу.

Данный механизм реализован следующим образом. В момент изготовления ПАКМ, после установки в него программного обеспечения производится подсчет контрольных сумм всех файлов в неизменяемых разделах операционной системы, за исключением файлов устройств, сокетов, ссылок на файлы в изменяемых разделах. Список файлов заранее подготовлен, хранится на дистрибутивном диске с модулями и скриптами инсталляции. В момент изготовления ПАКМ скрипты и файлы, необходимые для инсталляции копируются на флэш диск ПАКМ во временный каталог **/var/tmp/post-install**.

Подсчет контрольных сумм осуществляется при помощи утилиты **cpverify** при помощи следующей процедуры:

```
local VERIFY=/opt/cprocsp/bin/amd64/cpverify
local LIST=/var/tmp/post-install/files
local CHK=/boot/hashes/files.chk
local file
cat $LIST|\
(
    while read file
    do
        [ ! -f $file ] && echo "File $file does not exist" && continue
        echo -n $file >>$CHK
        echo -en "\033[;1H$file\033[0K"
            echo -e "\t$($VERIFY -mk $file)" >>$CHK
  done
)
```

Контрольные суммы (результат вычисления хэш функции утилиты) записываются в специальный файл, который помещается в /boot раздел (/boot/hashes/files.chk). Вместе с контрольными суммами в данном файле хранятся и полные имена файлов, подвергаемых контролю. Кроме данного файла - files.chk в каталоге boot/hashes хранятся другие файлы, содержащие контрольные суммы модулей криптопровайдера ПАКМ. Они помещаются туда во время инсталляции соответствующих rpm пакетов дистрибутива криптопровайдера. Процедура контроля целостности обрабатывает все файлы со списками контрольных сумм, находящиеся в каталоге /boot/hashes.

После формирования всех файлов с контрольными суммами в каталоге /boot/hashes, на этапе изготовления ПАКМ запускается расчет контрольной суммы всего раздела /boot при помощи электронного замка (ЭЗ) ПАК «Соболь».

Контроль целостности ПО ПАКМ «КриптоПро HSM» осуществляется всякий раз перед загрузкой операционной системы ПАКМ при помощи ЭЗ «Соболь», который контролирует все содержимое раздела /boot, включая файл с контрольными суммами, рассчитанными утилитой cpverify. В момент загрузки операционной системы осуществляется процедура проверки этих контрольных сумм: утилитой cpverify вновь подсчитываются контрольные суммы файлов, которые затем сравниваются с хранящимися в файлах каталога /boot/hashes, полученными в момент изготовления ПАКМ.

В случае расхождения в значениях контрольных сумм ПАКМ прекращает загрузку ПО и останавливает свою работу (вызывается процедура halt).

Процедура, осуществляющая проверку контрольных сумм файлов, находится в файле /etc/init.d/cprocsp. Она вызывается всякий раз при запуске сервисов криптопровайдера (в момент загрузки операционной системы), а также по расписанию планировщика cron.

В момент изготовления ПАКМ «КриптоПро HSM» в ежедневные планируемые задания cron (/etc/cron.daily) помещается файл сценария cprocsp, содержащий вызов процедуры, осуществляющей проверку контрольных сумм файлов:

```
/etc/init.d/cprocsp check
```

Приложение 1. Описание SOAP интерфейса Web администрирования

```
/* SOAP интерфейс администрирования ПАКМ */
    /* Изменение состояния ПАКМ (различные виды активации, деактивации) */
    //gsoap admin service method-action: ChangeHSMState "urn:admin/ChangeHSMState"
    int admin__ChangeHSMState(
        /* Иддентификатор состояния в которое необходимо перевести ПАКМ */
        enum admin__HSMState HSMState,
        /* Ответное SOAP сообщение - Информация о возможной ошибке при
        выполнении метода */
        struct admin__ChangeHSMStateResponse* Response);

    /* Регистрация нового пользователя в ПАКМ */
    //gsoap admin service method-action: AddUser "urn:admin/AddUser"
    int admin__AddUser(
        /* Структура с информацией о пользователе */
        struct admin__HSMUser UserInfo,
        /* Ответное SOAP сообщение - Информация о возможной ошибке при
        выполнении метода */
        struct admin__AddUserResponse* Response);

    /* Изменение информации о пользователе */
    //gsoap admin service method-action: ModifyUser "urn:admin/ModifyUser"
    int admin__ModifyUser(
        /* Структура с измененной информацией о пользователе */
        struct admin__HSMUser NewUserInfo,
        /* Ответное SOAP сообщение - Информация о возможной ошибке при
        выполнении метода */
        struct admin__ModifyUserResponse* Response);

    /* Удаление информации о пользователе */
    //gsoap admin service method-action: DeleteUser "urn:admin/DeleteUser"
    int admin__DeleteUser(
        /* Серийный номер HSM, в котором изначально регистрировалс
        пользователь.
        Если значение не указано (""), то данный параметр не учитывается, а
        Пользователь идентифицируется по значнию поля UID в текущем ПАКМ. */
        xsd__string HSMID,
        /* Если указано значение параметра HSMID, то данный параметр содержит
        значение поля OriginalUID (изначальный UID пользователя в HSMID). В противном
        случае данный параметр содержит значение поля UID в структуре информации о
        пользователе. Если ПАКМ не участвует в пуле, никогда не синхронизировался с
        другими ПАКМ, то UID и OriginalUID всегда совпадают. */
        xsd__int UID,
        /* Ответное SOAP сообщение - Информация о возможной ошибке при
        выполнении метода */
        struct admin__DeleteUserResponse* Response);

    /* Генерация ключей и сертификата аутентификации пользователя либо пароля.
    Возможно этот метод не понадобится как таковой (всё будет делаться в сервисе
    LCD панели, а новый сертификат сохраняться методом ModifyUser) */
    //gsoap admin service method-action: GenUserToken "urn:admin/GenUserToken"
    int admin__GenUserToken(
        /* Серийный номер HSM, в котором изначально регистрировалс
        пользователь.
        Если значение не указано (""), то данный параметр не учитывается, а
        Пользователь идентифицируется по значнию поля UID в текущем ПАКМ. */
        xsd__string HSMID,
        /* Если указано значение параметра HSMID, то данный параметр содержит
        значение поля OriginalUID (изначальный UID пользователя в HSMID). В противном
        случае данный параметр содержит значение поля UID в структуре информации о
        пользователе. Если ПАКМ не участвует в пуле, никогда не синхронизировался с
        другими ПАКМ, то UID и OriginalUID всегда совпадают. */
        xsd__int UID,
        /* Признак генерация ключа и сертификата или пароля
        0 - генерация ключа и сертификата
        1 - генерация пароля
        -1 - неопределено */
        xsd__int IsPasswordAuth,
        /* Ответное SOAP сообщение - Информация о возможной ошибке при
        выполнении метода */
        struct admin__GenUserTokenResponse* Response);

    /* Блокировка/разблокировка пользователя */
    //gsoap admin service method-action: ChangeUserState "urn:admin/ChangeUserState"
    int admin__ChangeUserState(
```

```
            /* Серийный номер HSM, в котором изначально регистрировалс
            пользователь.
            Если значение не указано (""), то данный параметр не учитывается, а
            Пользователь идентифицируется по значнию поля UID в текущем ПАКМ. */
            xsd__string HSMID,
            /* Если указано значение параметра HSMID, то данный параметр содержит
            значение поля OriginalUID (изначальный UID пользователя в HSMID). В противном
            случае данный параметр содержит значение поля UID в структуре информации о
            пользователе. Если ПАКМ не участвует в пуле, никогда не синхронизировался с
            другими ПАКМ, то UID и OriginalUID всегда совпадают. */
            xsd__int UID,
            /* Идентификатор состояния пользователя:

            0 - рабочее состояние пользователя
            1 - пользователь блокирован
        */
            xsd__int UserState,
            /* Ответное SOAP сообщение - Информация о возможной ошибке при
            выполнении метода */
            struct admin__ChangeUserStateResponse* Response);

        /* Извлечение информации о пользователе */
        //gsoap admin service method-action: GetUserInfo "urn:admin/GetUserInfo"
        int admin__GetUserInfo(
            /* Серийный номер HSM, в котором изначально регистрировалс
            пользователь.
            Если значение не указано (""), то данный параметр не учитывается, а
            Пользователь идентифицируется по значнию поля UID в текущем ПАКМ. */
            xsd__string HSMID,
            /* Если указано значение параметра HSMID, то данный параметр содержит
            значение поля OriginalUID (изначальный UID пользователя в HSMID). В противном
            случае данный параметр содержит значение поля UID в структуре информации о
            пользователе. Если ПАКМ не участвует в пуле, никогда не синхронизировался с
            другими ПАКМ, то UID и OriginalUID всегда совпадают. */
            xsd__int UID,
            /* Ответное SOAP сообщение */
            struct admin__GetUserInfoResponse* Response);

        /* Получение списка с информацией о пользователях. */
        //gsoap admin service method-action: GetUserList "urn:admin/GetUserList"
        int admin__GetUserList(
            /* Условия поиска в БД */
            struct admin__HSMUserSearchCriteria SerachCriteria,
            /* Индекс первой выдаваемой наружу записи в найденном наборе */
            xsd__int LimitIndex,
            /* Количество выдаваемых наружу записи в найденном наборе (размер
            страницы данных) */
            xsd__int LimitCount,
            /* Наименование Поля (колонки), по которому сортировать записи.
        */
            xsd__string SortColumn,
            /* направление сортировки
            1 - asc
            0 - desc */
            xsd__int SortDirection,
            /* Ответное SOAP сообщение для данного метода */
            struct admin__GetUserListResponse* Response);

        /* Получение очередного UID в текущем ПАКМ. */
        //gsoap admin service method-action: GetNextUID "urn:admin/GetNextUID"
        int admin__GetNextUID(
            /* Ответное SOAP сообщение */
            struct admin__GetNextUIDResponse* Response);

        /* Получение набора записей журнала аудита */
        //gsoap admin service method-action: GetAuditLogRecordList
"urn:admin/GetAuditLogRecordList"
        int admin__GetAuditLogRecordList(
            /* Условия поиска в БД */
            struct admin__AuditLogSearchCriteria SerachCriteria,
            /* Индекс первой выдаваемой наружу записи в найденном наборе */
            xsd__int LimitIndex,
            /* Количество выдаваемых наружу записи в найденном наборе (размер
            страницы данных) */
            xsd__int LimitCount,
            /* Условия сортировки записей
            1 - по возрастанию значений поля EventTime
            0 - по убыванию значений поля EventTime
            -1 - не сортировать записи */
            xsd__int SortCriteria,
            /* Возвращаемое SOAP сообщение */
```

```
            struct admin__LogRecordsResponse* Response);

        /* Очистить записи журнала аудита */
        //gsoap admin service method-action: ClearAuditLog "urn:admin/ClearAuditLog"
        int admin__ClearAuditLog(
            /* Дата/время, до которой должны быть удалены все записи журнала
            аудита. */
            xsd__string DateBefore,
            /* Ответное SOAP сообщение - Информация о возможной ошибке при
            выполнении метода */
            struct admin__ClearAuditLogResponse* Response);

        /* Получение audit log total record Count */
        //gsoap        admin        service        method-action:        GetAuditLogRecordCount
"urn:admin/GetAuditLogRecordCount"
        int admin__GetAuditLogRecordCount(
            /* Ответное SOAP сообщение */
            struct admin__GetAuditLogRecordCountResponse* Response);

        /* Получение текущего состояния HSM */
        //gsoap admin service method-action: GetHSMState "urn:admin/GetHSMState"
        int admin__GetHSMState(
            /* Ответное SOAP сообщение */
            struct admin__GetHSMStateResponse* Response);

        /* Получение системной информации о HSM */
        //gsoap admin service method-action: GetSysInfo "urn:admin/GetSysInfo"
        int admin__GetSysInfo(
            /* Ответное SOAP сообщение */
            struct admin__GetSysInfoResponse* Response);

        /* Установка системного времени HSM
      */
        //gsoap admin service method-action: SetHSMTime "urn:admin/SetHSMTime"
        int admin__SetHSMTime(
            /* Системное время ПАКМ, которое должно быть установлено */
            xsd__string CurrentTime,
            /* Ответное SOAP сообщение - Информация о возможной ошибке при
            выполнении метода */
            struct admin__SetHSMTimeResponse* Response);

        /* Получение настроек HSM */
        //gsoap admin service method-action: GetHSMOptions "urn:admin/GetHSMOptions"
        int admin__GetHSMOptions(
            /* Ответное SOAP сообщение  */
            struct admin__GetHSMOptionsResponse* Response);

        /* Установка параметров HSM */
        //gsoap admin service method-action: SetHSMOptions "urn:admin/SetHSMOptions"
        int admin__SetHSMOptions(
            /* Новые настройки ПАКМ */
            struct admin__HSMOptions NewHSMOptions,
            /* Ответное SOAP сообщение - Информация о возможной ошибке при
            выполнении метода */
            struct admin__SetHSMOptionsResponse* Response);

        /* Получение настроек аудита */
        //gsoap admin service method-action: GetHSMAuditOptions "urn:admin/GetHSMAuditOptions"
        int admin__GetHSMAuditOptions(
            /* Ответное SOAP сообщение  */
            struct admin__GetHSMAuditOptionsResponse* Response);

        /* Установка параметров аудита */
        //gsoap admin service method-action: SetHSMAuditOptions "urn:admin/SetHSMAuditOptions"
        int admin__SetHSMAuditOptions(
            /* Новые настройки ПАКМ */
            struct admin__HSMAuditOptions NewHSMAuditOptions,
            /* Ответное SOAP сообщение - Информация о возможной ошибке при
            выполнении метода */
            struct admin__SetHSMAuditOptionsResponse* Response);

        /* Получение сетевых настроек */
        //gsoap admin service method-action: GetNetworkSettings "urn:admin/GetNetworkSettings"
        int admin__GetNetworkSettings(
            /* Ответное SOAP сообщение  */
            struct admin__GetNetworkSettingsResponse* Response);

        /* Установка новых сетевых настроек с перезапуском сети. */
        //gsoap admin service method-action: SetNetworkSettings "urn:admin/SetNetworkSettings"
        int admin__SetNetworkSettings(
            /* Устанавливаемые сетевые настройки */
```

```
            struct admin__NetworkSettings NewNetworkSettings,
            /* Ответное SOAP сообщение - Информация о возможной ошибке при
            выполнении метода */
            struct admin__SetNeworkSettingsResponse* Response);

        /* Получение списка резервных копий HSM */
        int admin__GetBackupsList(
            /* Ответное SOAP сообщение */
            struct admin__GetBackupsListResponse* Response);

        /* Удаление файла с резервной копией HSM */
        int admin__DeleteBackupFile(
            /* Имя файла с резервной копией HSM, без пути к нему */
            xsd__string BackupFileName,
            /* Ответное SOAP сообщение */
            struct admin__DeleteBackupFileResponse* Response);

        /* Получение файла с резервной копией HSM */
        /*int admin_ReceiveBackupFile(*/
            /* Имя файла с резервной копией HSM, без пути к нему */
            /*xsd__string BackupFileName,*/
            /* Ответное SOAP сообщение */
            /*struct admin__ReceiveBackupFileResponse* Response);*/



        /* Получение настроек межсетевого экрана */
        //gsoap admin service method-action: GetFWSettings "urn:admin/GetFWSettings"
        int admin__GetFWSettings(
            /* Ответное SOAP сообщение */
            struct admin__GetFWSettingsResponse* Response);

        /* Добавление одной подсети "разрешенных клиентов" в настройки межсетевого
        экрана. */
        //gsoap admin service method-action: AddFWClientSubnet "urn:admin/AddFWClientSubnet"
        int admin__AddFWClientSubnet(
            /* IP адрес и маска подсети, с которой разрешен вход пользователяи ПАКМ */
            struct admin__FWRule NewClientSubnet,
            /* Ответное SOAP сообщение - Информация о возможной ошибке при
            выполнении метода */
            struct admin__AddFWClientSubnetResponse* Response);

        /* Удаление подсети из настроек межсетевого экрана, из которой разрешен
        вход пользователям ПАКМ. */
        //gsoap         admin         service         method-action:         DeleteFWClientSubnet
"urn:admin/DeleteFWClientSubnet"
        int admin__DeleteFWClientSubnet(
            /* IP адрес и маска подсети, удаляемые из настроек межсетевого экрана */
            struct admin__FWRule ClientSubnet,
            /* Ответное SOAP сообщение - Информация о возможной ошибке при
            выполнении метода */
            struct admin__DeleteFWClientSubnetResponse* Response);

        /* изменение информации о подсети в настройках межсетевого экрана. */
        //gsoap         admin         service         method-action:         ModifyFWClientSubnet
"urn:admin/ModifyFWClientSubnet"
        int admin__ModifyFWClientSubnet(
            /* Старые IP адрес и маска подсети, с которой разрешен вход
            пользователяи ПАКМ */
            struct admin__FWRule OldClientSubnet,
            /* Новые значения IP адреса и маски подсети, с которой разрешен вход
            пользователяи ПАКМ */
            struct admin__FWRule NewClientSubnet,
            /* Ответное SOAP сообщение - Информация о возможной ошибке при
            выполнении метода */
            struct admin__ModifyFWClientSubnetResponse* Response);

        /* Перезапуск межсетевого экрана (после изменения настроек) */
        //gsoap admin service method-action: RestartFW "urn:admin/RestartFW"
        int admin__RestartFW(
            /* Ответное SOAP сообщение - Информация о возможной ошибке при
            выполнении метода */
            struct admin__RestartFWResponse* Response);

        /* получение журнала событий */
        //gsoap admin service method-action: GetEventLog "urn:admin/GetEventLog"
        int   admin__GetEventLog(xsd__string   FromDate,   struct   admin__GetEventLogResponse*
Response);

        //gsoap        admin        service        method-action:        GetRootCertificateList
"urn:admin/GetRootCertificateList"
```

```
            int           admin__GetRootCertificateList(xsd__int           flags,           struct
admin__GetRootCertificateListResponse* Response);

            //gsoap admin service method-action: GetRootCertificate "urn:admin/GetRootCertificate"
            int          admin__GetRootCertificate(xsd__string          SerialNumber,          struct
admin__GetRootCertificateResponse* Response);

            //gsoap admin service method-action: ProcessCertRequest "urn:admin/ProcessCertRequest"
            int admin__ProcessCertRequest(
                /* Серийный номер HSM, в котором изначально регистрировалс
                пользователь.
                Если значение не указано (""), то данный параметр не учитывается, а
                Пользователь идентифицируется по значнию поля UID в текущем ПАКМ. */
                xsd__string HSMID,
                /* Если указано значение параметра HSMID, то данный параметр содержит
                значение поля OriginalUID (изначальный UID пользователя в HSMID). В противном
                случае данный параметр содержит значение поля UID в структуре информации о
                пользователе. Если ПАКМ не участвует в пуле, никогда не синхронизировался с
                другими ПАКМ, то UID и OriginalUID всегда совпадают. */
                xsd__int UID,
               xsd__string CertRequest,
               xsd__int flags,
               struct admin__ProcessCertRequestResponse* Response);

        struct admin__NetworkSettings
        {
                /* Указатель на список структур SOAP_NetworkRule */
                struct admin__NetworkRule *__ptr;
                /* Количество структур в массиве */
                xsd__int __size;
        };

        /* Структура описывающая один файл с резервной копией */
        struct admin__BackupFile
        {
            /* имя файла */
            xsd__string filename;
            /* размер */
            xsd__int flsize;
        };

        /* Список файлов с резервными копиями (массив структур admin__BackupFile) */
        struct admin__BackupFilesList
        {
            /* Указатель список структур SOAP_BackupFile */
            struct admin__BackupFile *__ptr;
            /* Количество структур в массиве */
            xsd__int __size;
        };

        struct admin__AddUserResponse
        {
            /* Информация о новом пользователе с некоторыми полями, которые добавил
            сервер (UID, HSMID, OriginalUID...) */
            struct admin__HSMUser UserInfo;
        };

        struct admin__ChangeHSMStateResponse
        {
        };

        struct admin__ChangeUserStateResponse
        {
        };

        struct admin__ClearAuditLogResponse
        {
        };
        struct admin__DeleteFWClientSubnetResponse
        {
        };

        struct admin__DeleteUserResponse
        {
        };

        struct admin__GenUserTokenResponse
        {
        };

        struct admin__GetEventLogResponse
```

```
{
        xsd__string log;
};

/* Ответное SOAP сообщение для метода GetFWSettings */
struct admin__GetFWSettingsResponse
{
    /* Структура с настройками межсетевого экрана */
    struct admin__FWSettings FWSettings;
};

/* Ответное SOAP сообщение для метода GetHSMOptions */
struct admin__GetHSMOptionsResponse
{
    /* Структура с настройками ПАКМ */
    struct admin__HSMOptions HSMOptions;
};

/* Ответное SOAP сообщение для метода GetHSMAuditOptions */
struct admin__GetHSMAuditOptionsResponse
{
    /* Структура с настройками ПАКМ */
    struct admin__HSMAuditOptions HSMAuditOptions;
};

/* Ответное SOAP сообщение для метода GetHSMState */
struct admin__GetHSMStateResponse
{
    /* Возвращаемый код состояния ПАКМ */
    enum admin__HSMState State;
};

/* Ответное SOAP сообщение для метода GetHSMState */
struct admin__GetAuditLogRecordCountResponse
{
    /* Total audit log recordcount */
    xsd__int count;
};

/* Ответное SOAP сообщение для метода GetNetworkSettings */
struct admin__GetNetworkSettingsResponse
{
    /* Структура с сетевыми настройками ПАКМ */
    struct admin__NetworkSettings NetworkSettings;
};

/* Ответное SOAP сообщение для метода GetNextUID */
struct admin__GetNextUIDResponse
{
    /* Доступный UID в текущем ПАКМ */
    xsd__int UID;
};

/* Ответное SOAP сообщение для метода GetSysInfo */
struct admin__GetSysInfoResponse
{
    /* Структура с внутренней иноформацией ПАКМ */
    struct admin__HSMInfo SysInfo;
};

/* Ответное SOAP сообщение для метода GetUserInfo */
struct admin__GetUserInfoResponse
{
    /* Информация о пользователе ПАКМ */
    struct admin__HSMUser UserInfo;
};

/* Ответное SOAP сообщение на метод получения списка пользователей ПАКМ */
struct admin__GetUserListResponse
{
    /* Возвращаемый список пользователей */
    struct admin__HSMUserList UserList;
    /* всего записей найденных по данному условию */
    xsd__int total;
};

struct admin__GetRootCertificateListResponse
{
    struct admin__CertificateList CertList;
};
```

```
struct admin__GetRootCertificateResponse
{
    xsd__string RootCertificate;
};

struct admin__ProcessCertRequestResponse
{
    xsd__string UserCertificate;
};
/* Список записей журнала аудита (массив сущностей SOAP_AuditLogRecord) */
struct admin__AuditLogRecordList
{
    /* Указатель список структур SOAP_AuditLogRecord */
    struct admin__AuditLogRecord* __ptr;
    /* Количество структур в массиве */
    xsd__int __size;
};

/* Ответное SOAP сообщение на метод получения набора записей журнала аудита
ПАКМ */
struct admin__LogRecordsResponse
{
    /* Возвращаемый список записей журнала аудита */
    struct admin__AuditLogRecordList AuditLogRecords;
    /* всего записей найденных по данному условию */
    xsd__int total;
};

struct admin__ModifyFWClientSubnetResponse
{
};

struct admin__ModifyUserResponse
{
};

struct admin__RestartFWResponse
{
};

struct admin__SetHSMOptionsResponse
{
};

struct admin__SetHSMAuditOptionsResponse
{
};

struct admin__SetHSMTimeResponse
{
};

struct admin__SetNeworkSettingsResponse
{
};

struct admin__GetBackupsListResponse
{
    /* Список файлов с резервными копиями */
    struct admin__BackupFilesList BackupsList;
};

struct admin__DeleteBackupFileResponse
{
};
```

Приложение 2. Структура конфигурационного файла межсетевого экрана ПАКМ

Ниже приводится пример временного конфигурационного файла /tmp/firewall.ini, формируемого скриптом genfw из данных, полученных из БД MySQL

```
[1502]
192_168_70_63__255_255_252_0__eth0 = "1"

[1501]
192_168_68_124__255_255_252_0__eth0 = "1"
192_168_70_0__255_255_252_0__eth0 = "1"
192_168_71_0__255_255_252_0__eth0 = "1"

[443]
192_168_71_191__255_255_252_0__eth1 = "1"

[1503]
192_168_70_67__255_255_252_0__eth2 = "1"
```

Приложение 3. Список контроля доступа (ACL)

```
role admin sA
subject / rvka
        / rwcdmlxi

role shutdown sARG
subject / rvka
        /
        /dev
        /dev/urandom r
        /dev/random r
        /etc r
        /bin rx
        /sbin rx
        /lib rx
        /lib64 rx
        /usr rx
        /proc r
#       $grsec_denied
        -CAP_ALL
        connect disabled
        bind disabled



role default
subject / {
        /                               h
        /tmp    rwcd
        /usr/lib/locale rx
        -CAP_ALL
        connect disabled
        bind    disabled
}
role root uG
role_transitions admin shutdown
role_allow_ip  127.0.0.1/32
role_allow_ip  0.0.0.0/0
subject /  {
        /                               r
        /tmp            rwc
        /bin                            rx
        /dev/initctl
        /lib                            h
        /lib/terminfo
        /lib/terminfo/l/linux           r
        /lib64                          rx
        /opt                            h
        /opt/cprocsp                    h
        /opt/cprocsp/sbin/amd64                 rx
        /opt/cprocsp/bin                rx
        /opt/cprocsp/lib                r
        /opt/cprocsp/lib/hashes         r
        /boot/hashes   r
        /opt/cprocsp/bin/amd64/cpverify         rx
        /sbin                           r
        /sbin/consoletype               x
        /sbin/gradm                     x
        /sbin/initlog           x
        /sbin/minilogd          x
        /sbin/syslogd           x
        /sbin/start-stop-daemon         x
        /sbin/service                   rx
        /usr/sbin/logrotate x
        /usr                            h
        /usr/bin                        rx
        /usr/lib/locale                         rx
        /usr/lib64                      rx
        /usr/share                      rx
        /usr/local                      rx
#       /var                            h
        /var/run                        rw
#TODO: ubrat
        /var/log                        rxw
        /var/opt                        rx
        /var/lib                        h
        /var/etc
```

```
        /var/etc/opt           r
        /var/lib/mysql/cprocsp/db
        /var/lib/mysql/mysql.pid
        /var/lock/subsys/cryptsrv_hsm rwcd
        /var/spool/at
        /var/spool/cron
#       /var/spool/mail
        /dev
        /dev/bus                       rw
        /dev/null                      rw
        /dev/tty                       rw
        /dev/tty2                      rw
        /dev/grsec                     h
        /dev/mem                       h
        /dev/kmem                      h
        /dev/port                      h
        /dev/log                       r
        /dev/urandom        r
        /etc                           rx
        /etc/ssh                       h
        /etc/grsec                     h
        /etc/shadow                    h
        /etc/shadow-                   h
        /etc/gshadow                   h
        /etc/gshadow-                  h
        /etc/ppp/chap-secrets          h
        /etc/ppp/pap-secrets           h
        /etc/samba/smbpasswd           h
        /proc                          r
        /proc/kcore                    h
        /proc/sys                      h
        /proc/bus                      h
        /proc/slabinfo                 h
        /proc/modules                  h
        /proc/kallsyms                 h
        /root                          r
        /sys                           h
        /boot                          h
        /backup                        rwcd
#       /backup/backup.tar             wc
#       /backup/hsmdb_dump.sql         rwc
#       /backup/hsmdb_dump_tmp.sql     rwd
        -CAP_ALL
}

subject /bin/chown o {
        /                              h
        /bin                           h
        /bin/chown                     x
        /etc                           h
        /etc/ld.so.cache               r
        /etc/nsswitch.conf             r
        /etc/passwd                    r
        /lib64                         h
        /lib64/ld-2.17.so              x
        /lib64/libc-2.17.so            rx
        /lib64/libnss_files-2.17.so    rx
        /usr                           h
        /usr/lib64/gconv       r
        /usr/lib/locale                r
        /usr/lib64/locale      r
        /usr/local/mysql
        /var                           h
        /var/lib/mysql/cprocsp/db      w
        /var/run
        /tmp                           w
        -CAP_ALL
        +CAP_CHOWN
        +CAP_DAC_OVERRIDE
        bind    disabled
        connect disabled
}

subject /bin/chmod o {
        /                              h
        /bin                           h
        /bin/chmod                     x
        /etc                           h
        /etc/ld.so.cache               r
        /lib64/ld-2.17.so              x
        /lib64/libc-2.17.so            rx
```

```
        /lib64/libnss_files-2.17.so   rx
        /usr                          h
        /usr/lib/locale                       r
        /usr/lib64/gconv/gconv-modules.cache  r
        /usr/lib64/locale     r
        /usr/local/mysql
        /var
        /var/lib/mysql/cprocsp/db     rw
        /tmp                          w
        -CAP_ALL
        +CAP_DAC_OVERRIDE
        +CAP_FOWNER
        bind    disabled
        connect disabled
}

subject /bin/grep  {
        /                             h
        /bin                          h
        /bin/grep                     x
        /etc                          h
        /etc/ld.so.cache              r
        /etc/sysconfig/i18n           r
        /etc/net                      r
        /lib64                        h
        /lib64/ld-2.17.so             x
        /lib64/libc-2.17.so           rx
        /lib64/libpcre.so.3.15.1      rx
        /usr                          h
        /usr/lib64/gconv       r
        /usr/lib64/locale      r
        /tmp                          r
        -CAP_ALL
        +CAP_DAC_OVERRIDE
        +CAP_DAC_READ_SEARCH
        bind    disabled
        connect disabled
}

subject /bin/cat o {
        /                             h
        /bin                          h
        /bin/cat                      x
        /etc                          h
        /etc/sysconfig         r
        /etc/ld.so.cache              r
        /lib64                        h
        /lib64/ld-2.17.so             x
        /lib64/libc-2.17.so           rx
        /lib64/libnss_files-2.17.so   rx
        /proc
        /boot/hashes           rx
        /proc/cmdline          r
        /usr                          h
        /usr/lib64                    h
        /usr/lib64/gconv/gconv-modules.cache  r
        /usr/lib/locale                       r
        /usr/local                    h
        /usr/local/mysql/share/fill_help_tables.sql  r
        /usr/local/mysql/share/mysql_system_tables.sql       r
        /usr/local/mysql/share/mysql_system_tables_data.sql  r
        /tmp                          r
        /var/lib/mysql/mysql.pid      r
        -CAP_ALL
        +CAP_DAC_OVERRIDE
        bind    disabled
        connect disabled
}

subject /bin/mkdir o {
        /
        /bin                          h
        /bin/mkdir                    x
        /etc                          h
        /etc/ld.so.cache              r
        /lib64                        rx
        /usr                          h
        /usr/lib/locale        r
        /usr/lib64     r
        /usr/local/mysql              r
        /var
```

```
        /var/lib
        /var/lib/mysql
        /var/lib/mysql/cprocsp
        /var/lib/mysql/cprocsp/db     wc
        /var/log                      h
        /dev/grsec                    h
        /proc                         r
        /proc/kcore                   h
        /proc/sys                     h
        /proc/bus                     h
        /dev/mem                      h
        /dev/kmem                     h
        /dev/port                     h
        /dev/log                      h
        /sys                          h
        /boot                         h
        -CAP_ALL
        +CAP_DAC_OVERRIDE
        bind   disabled
        connect disabled
}

subject /bin/rm {
        /opt/cprocsp/bin      r
        /var/run       rwcdls
        /var/lib/mysql
        /var/lib/mysql/mysql.pid rwd
        /var/opt/cprocsp/tmp   rwd
        /var/lock/subsys       rwd
        /etc/ld.so.cache              r
        /lib64/ld-2.17.so             x
        /lib64/libc-2.17.so           rx
        /lib64/libnss_files-2.17.so   rx
        /opt/cprocsp/sbin/amd64               r
    /tmp        rwdc
        /var/lib/mysql/cprocsp/db     wd
        -CAP_ALL
        +CAP_KILL
    +CAP_DAC_OVERRIDE
    +CAP_DAC_READ_SEARCH
        connect disabled
        bind disabled
}
subject /bin/mv {
        /opt/cprocsp/sbin/amd64
        /opt/cprocsp/bin      r
        /var/run       rwcdls
        /var/opt/cprocsp      rwdc
        /var/log                      rwcd
    /var/etc/opt        rwcd
        /var/lock/subsys       rwcd
    /tmp        rwdc
        /var/opt/cprocsp/hsmdb_dump.sql       rwcd
        /var/tmp                      rwd
        /backup
        /backup/hsmdb_dump.sql        rwcd
        /backup/hsmdb_dump_tmp.sql    rwd
        -CAP_ALL
        +CAP_KILL
    +CAP_DAC_OVERRIDE
    +CAP_DAC_READ_SEARCH
        connect disabled
        bind disabled
}

subject /usr/bin/mesg {
    -CAP_ALL
    +CAP_FSETID
    connect disabled
    bind disabled
}
subject /usr/local/sbin/pcscd o {
        /
        /etc/ld.so.cache r
        /etc/localtime r
        /proc/sys/kernel/version r
        /lib rx
    /lib64  rx
        /usr/lib64 rx
        /var/run/pcscd/pcscd.comm rw
        /var/run/pcscd/pcscd.pub rwx
```

```
        /proc/bus/usb rw
        /dev/log rw
        /dev/null rw
        -CAP_ALL
    +CAP_DAC_OVERRIDE
    +CAP_DAC_READ_SEARCH
    connect disabled
    bind disabled
}
#Copy from original for script which restart daemon
subject /usr/sbin/pcscd o {
        /
        /etc/ld.so.cache r
        /etc/localtime r
        /proc/sys/kernel/version r
        /lib rx
    /lib64  rx
        /usr/lib64 rx
        /var/run/pcscd/pcscd.comm rw
        /var/run/pcscd/pcscd.pub rwx
        /proc/bus/usb rw
        /dev/log rw
        /dev/null rw
    /dev/bus/usb    rw
        -CAP_ALL
    +CAP_DAC_OVERRIDE
    +CAP_DAC_READ_SEARCH
    connect disabled
    bind disabled
}
subject /bin/ps {
    /proc   r
    -CAP_ALL
    +CAP_DAC_OVERRIDE
    +CAP_DAC_READ_SEARCH
    connect disabled
    bind disabled
}
subject /sbin/shutdown {
    /dev       rx
    /var/run   rwcd
    -CAP_ALL
    +CAP_SETUID
    +CAP_SYS_TTY_CONFIG
}
subject /sbin/start-stop-daemon {
        /usr/sbin      rx
        /sbin   rx
        /lib    rx
        /usr/lib       rx
        -CAP_ALL
        +CAP_DAC_OVERRIDE
        +CAP_DAC_READ_SEARCH
        connect disabled
        bind disabled
}
subject /sbin/initlog {
        /dev/log       rwcd
    /sbin/iptables-restore  rx
    /sbin/xtables-multi  rx
    /sbin/limited      rx
    /sbin/hwclock      rx
        -CAP_ALL
}

subject /sbin/hwclock {
        /dev/rtc0              rw
        /sbin/hwclock          x
        /var/etc/adjtime       rw
        -CAP_ALL
        +CAP_AUDIT_WRITE
        +CAP_SYS_TIME
}
subject /sbin/limited {
        /dev/log       rwcd
    /usr/lib/locale    rx
        -CAP_ALL
}
subject /bin/getopt {
        /dev/log       rwcd
    /usr/lib/locale    rx
```

```
        -CAP_ALL
}
subject /bin/sed {
        /dev/log       rwcd
    /usr/lib/locale    rx
        -CAP_ALL
}
subject /usr/bin/expr {
        /dev/log       rwcd
    /usr/lib/locale    rx
        -CAP_ALL
}
subject /sbin/minilogd {
        /dev/log       rwcd
        -CAP_ALL
}
subject /sbin/syslogd {
        /sbin          rx
        /etc/services  r
        /etc/syslog.conf       r
        /dev/log       rwcd
        /var/log       rwcd
        /var/lock      rwcd
        -CAP_ALL
        +CAP_KILL
        +CAP_SYS_TTY_CONFIG
}
subject /usr/sbin/logrotate {
        /       rx
        /etc    rx
        /bin/sh x
        /lib64  rx
        /proc                           h
        /proc/filesystems               r
        /selinux
        /var/log       rwcd
        /usr/sbin/logrotate             x
        /var/lib/logrotate rwxcd
        /var/run/logrotate rwxcd
        /tmp    rw
        /dev/null rw
        /dev/tty  rw
        -CAP_ALL
    +CAP_CHOWN
}
subject /bin/sh {
        /               r
        /sbin/reload-syslog    rx
        -CAP_ALL
        +CAP_AUDIT_WRITE
        connect disabled
        bind disabled
}
subject /bin/bash {
        /               r
        /sbin/gradm                     x
        -CAP_ALL
        +CAP_AUDIT_WRITE
        connect disabled
        bind disabled
        sock_allow_family netlink
}
subject /bin/umount {
        /boot          r
        /etc           rwcdl
        /run/mount     rw
        -CAP_ALL
        +CAP_DAC_OVERRIDE
        +CAP_SYS_ADMIN
        connect disabled
        bind disabled
}
subject /sbin/killall5 {
        /sbin/killall5 rx
        /usr/sbin/pcscd        rx
        /usr/sbin/crond        rx
        /lib           rx
        /usr/sbin      rx
        /usr/lib       rx
        -CAP_ALL
        +CAP_KILL
```

```
    +CAP_DAC_OVERRIDE
    +CAP_DAC_READ_SEARCH
       connect disabled
       bind disabled
}
subject /bin/mktemp {
    /tmp    rwcd
    -CAP_ALL
       connect disabled
       bind disabled
}
subject /sbin/init {
    /dev/console    hs
    /dev/log   rwcd
    -CAP_ALL
    bind disabled
    connect disabled
}
subject /bin/stty {
       /dev    r
       -CAP_ALL
       connect disabled
       bind disabled
}
subject /sbin/udevd {
       /dev/.udev  rwcd
    /dev/log    rw
    /dev/console    rwcd
       /dev/vcs12     wcd
       /dev/vcsa12    wcd
    -CAP_ALL
       connect disabled
       bind disabled
}
subject /bin/tar {
       /
       /bin                          h
       /bin/gzip                     x
       /bin/tar                      x
       /etc                          h
       /etc/group                    r
       /etc/ld.so.cache              r
       /etc/nsswitch.conf            r
       /etc/passwd                   r
       /lib64                        rx
       /opt                          h
       /opt/cprocsp/sbin/amd64
       /usr                          h
       /var                          h
       /var/tmp       rwcd
       /var/opt/cprocsp              r
       /backup  rwcd
       /backup/backup.tar            crw
       /backup/hsm_backup.tgz        rwc
       -CAP_ALL
       +CAP_CHOWN
       +CAP_DAC_OVERRIDE
       +CAP_DAC_READ_SEARCH
       +CAP_FOWNER
    connect disabled
    bind disabled
}
subject /bin/touch {
    /var/lock/subsys  rwc
    /var/lock/subsys/mysql           rw
    /lib64             rx
    -CAP_ALL
    connect disabled
    bind disabled
}
subject /usr/bin/tac {
       /tmp    rwcd
    -CAP_ALL
    connect disabled
    bind disabled

}
subject /bin/dumpkeys o {
       /                             h
       /bin                          h
       /bin/dumpkeys                 x
```

```
        /dev                            h
        /dev/tty2                       rw
        /etc                            h
        /etc/ld.so.cache                r
        /lib64                          h
        /lib64/ld-2.17.so               x
        /lib64/libc-2.17.so             rx
        /lib64/libnss_files-2.17.so     rx
        /usr                            h
        /usr/lib64/gconv/gconv-modules.cache  r
        /usr/lib64/locale               r
        /proc
        /proc/kcore                     h
        /proc/sys                       h
        /proc/bus                       h
        -CAP_ALL
        +CAP_SYS_TTY_CONFIG
        bind    disabled
        connect disabled
}

subject /bin/loadkeys o {
        /                               h
        /bin                            h
        /bin/loadkeys                   x
        /dev                            h
        /dev/tty                        rw
        /etc                            h
        /etc/ld.so.cache                r
        /lib64                          h
        /lib64/ld-2.17.so               x
        /lib64/libc-2.17.so             rx
        /lib64/libnss_files-2.17.so     rx
        /proc
        /proc/kcore                     h
        /proc/sys                       h
        /proc/bus                       h
        -CAP_ALL
        +CAP_SYS_TTY_CONFIG
        bind    disabled
        connect disabled
}
subject /bin/login o {
user_transition_allow root
group_transition_allow root shadow

        /
        /bin                            h
        /dev/urandom            r
        /bin/bash                       x
        /bin/login                      x
        /dev                            h
    /dev/log            rw
        /dev/tty2                       rw
        /etc                            r
        /etc/grsec                      h
        /etc/ssh                        h
        /etc/shadow                     h
        /etc/shadow-                    h
        /etc/gshadow                    h
        /etc/gshadow-                   h
        /etc/ppp/chap-secrets           h
        /etc/ppp/pap-secrets            h
        /etc/samba/smbpasswd            h
        /lib64                          rx
        /var                            h
        /var/log/lastlog                rw
        /var/log/wtmp                   a
        /var/run
        /var/run/utmp                   rw
        /var/spool/mail
        /proc
        /proc/sys/kernel/ngroups_max    r
        /proc/kcore                     h
        /proc/bus                       h
        /tmp                            rw
        /sys                            h
        /boot                           h
        /usr/src                        h
        -CAP_ALL
        +CAP_CHOWN
```

```
        +CAP_FSETID
        +CAP_SETGID
        +CAP_SETUID
        +CAP_SYS_TTY_CONFIG
        bind 0.0.0.0/32:0 stream tcp
        connect 127.0.0.1/32:111 stream tcp
}

subject /bin/unicode_start o {
        /                               h
        /bin                            rx
        /etc                            h
        /etc/ld.so.cache                r
        /lib64                          h
        /lib64/ld-2.17.so               x
        /lib64/libc-2.17.so             rx
        /lib64/libdl-2.17.so   rx
        /proc                           h
        /proc/meminfo                   r
        /usr                            h
        /usr/share/locale               r
        /usr/bin/tty                    x
        /usr/lib64/gconv/gconv-modules.cache  r
        /usr/lib64/locale               r
        /dev
        /dev/null                       w
        /dev/tty                        rw
        /dev/grsec                      h
        /dev/mem                        h
        /dev/kmem                       h
        /dev/port                       h
        /dev/log                        h
        /root
        /root/.kbd
        /root/.kbd/.keymap_sv           w
        -CAP_ALL
        bind    disabled
        connect disabled
}

subject /etc/cron.daily o {
        /
        /bin                            rx
    /boot/hashes        r
        /lib64                          rx
        /opt                            h
        /opt/cprocsp                    rx
        /sbin                           h
    /sbin/halt          rx
        /sbin/consoletype               x
        /dev
    /dev/log            rw
        /dev/null                       w
        /dev/tty                        rw
        /dev/grsec                      h
        /dev/mem                        h
        /dev/kmem                       h
        /dev/port                       h
    /dev/urandom        r
        /etc                            rx
        /etc/grsec                      h
        /etc/ssh                        h
        /etc/shadow                     h
        /etc/shadow-                    h
        /etc/gshadow                    h
        /etc/gshadow-                   h
        /etc/ppp/chap-secrets           h
        /etc/ppp/pap-secrets            h
        /etc/samba/smbpasswd            h
        /proc
        /proc/meminfo                   r
        /proc/sys/kernel/ngroups_max    r
        /proc/kcore                     h
        /proc/bus                       h
        /root                           r
        /tmp                            rwcd
        /usr
        /usr/lib                        h
        /usr/lib/perl5/strict.pm        r
        /usr/lib/perl5/vendor_perl
        /usr/local                      h
```

```
        /usr/local/lib
        /usr/bin                        rxi
        /usr/lib64                      rxi
        /usr/libexec                    r
        /usr/sbin                       rxi
        /usr/src                        h
        /var
    /var/lib/logrotate  rwcd
        /var/lock                       h
        /var/lock/makewhatis
        /var/lock/makewhatis/lockdir  wcd
        /var/log                        r
        /var/log/wtmp                   a
        /var/opt                        h
    /var/etc/opt/cprocsp/config64.ini        r
        /var/opt/cprocsp/tmp
        /var/opt/cprocsp/tmp/.registry_lock   w
        /var/run
        /var/run/cprocsp.pid          wcd
        /var/run/utmp                 rw
        /var/spool                    r
#       /var/spool/postfix            r
#       /var/spool/postfix/maildrop   r
#       /var/spool/postfix/maildrop/325794.24903     rwcd
#       /var/spool/postfix/maildrop/4F8D2548116      rwc
#       /var/spool/postfix/public     r
#       /var/spool/postfix/public/pickup      w
#       /var/spool/postfix/var
        /sys                          h
        /boot                         h
        -CAP_ALL
        +CAP_CHOWN
        +CAP_DAC_OVERRIDE
        +CAP_FOWNER
        +CAP_FSETID
        +CAP_SETGID
        +CAP_SETUID
        bind 0.0.0.0/32:0 stream dgram ip tcp
        connect 127.0.0.1/32:111 stream tcp
}
subject /etc/init.d o {
user_transition_allow root mysql
group_transition_allow root mysql
        /
#       /bin                          rxi
        /bin                          rx
        /boot/hashes                  r
        /dev
        /dev/null                     rw
        /dev/tty                      rw
        /dev/ttyS1                    rw
        /dev/grsec                    h
        /dev/mem                      h
        /dev/kmem                     h
        /dev/port                     h
        /dev/sobol                    r
        /dev/log                      rw
        /dev/urandom                  r
#       /etc                          rxwcdi
        /etc                          rxwcd
        /etc/gshadow                  h
        /etc/gshadow-                 h
        /etc/ppp                      h
        /etc/samba/smbpasswd          h
        /etc/shadow                   h
        /etc/shadow-                  h
        /etc/ssh                      h
        /lib/modules                  h
#       /lib64                        rxi
        /lib64                        rx
        /lib64/modules                h
        /opt                          h
        /opt/cprocsp                  rxi
        /proc                         r
        /proc/kcore                   h
        /proc/sys                     h
        /proc/bus                     h
        /proc/sys/net                 r
        /proc/sys/net/ipv4            w
        /proc/sys/net/ipv4/conf              h
        /proc/sys/net/ipv4/conf/all
```

```
        /proc/sys/net/ipv4/conf/all/arp_filter       w
        /proc/sys/net/ipv4/conf/default
        /proc/sys/net/ipv4/conf/default/rp_filter    w
        /proc/sys/net/core/somaxconn  w
        /root                         r
        /run
        /run/mount
        /run/mount/utab                         rw
#       /sbin                         rxi
        /sbin                         rx
        /sys                          h
        /sys/devices/system/cpu/online        r
        /tmp                          rwcd
        /usr                          h
        /usr/bin                      xi
        /usr/lib/locale/      rx
#       /usr/lib64                    rxi
        /usr/lib64                    rx
        /usr/local/mysql              rx
        /usr/sbin
        /usr/sbin/ifplugd
        /var/etc/opt                  r
        /var
        /var/log                      wc
        /var/lib                      rwcd
        /var/lock/subsys
        /var/lock/subsys/cryptsrv_hsm wcd
        /var/lock/subsys/fenixmsrv    wcd
        /var/lock/subsys/mysql        wcd
        /var/lock/subsys/srv_wrapper  wcd
        /var/lock/subsys/syslogd      wcd
        /var/lock/subsys/iptables     wcd
        /var/lock/subsys/network      wcd
        /var/opt                      rwcd
#       /var/opt/cprocsp/dsrf         h
#       /var/opt/cprocsp/dsrf/db1/kis_1       rw
#       /var/opt/cprocsp/dsrf/db2/kis_1       rw
#       /var/opt/cprocsp/log          r
#       /var/opt/cprocsp/log/log_db.dat       rw
#       /var/opt/cprocsp/log/log_db.dat-journal      rwcd
#       /var/opt/cprocsp/mnt
#       /var/opt/cprocsp/tmp          rwcd
        /var/run
        /var/run/cprocsp.pid          rwcd
        /var/run/cryptsrv_hsm.pid     rwcd
        /var/run/fenixmsrv.pid        rwcd
        /var/run/syslogd.pid          rwcd
        /var/run/srv_wrapper.pid      rwcd
        /var/run/pcscd/pcscd.comm     rw
        /var/run/pcscd/pcscd.pub      rwx
        /var/resolv                   rwcd
        /var/run/resolvconf
        /boot                         h
        -CAP_ALL
        +CAP_NET_ADMIN
        +CAP_DAC_READ_SEARCH
        +CAP_NET_RAW
#       +CAP_NET_BIND_SERVICE
        +CAP_SYS_MODULE
        +CAP_SYS_ADMIN
        +CAP_DAC_OVERRIDE
        +CAP_CHOWN
        +CAP_SYS_TTY_CONFIG
        +CAP_SYS_RESOURCE
        +CAP_IPC_LOCK
        +CAP_KILL
        connect disabled
        bind disabled
#       bind 0.0.0.0/32:0 dgram ip
#       bind 0.0.0.0/32 stream tcp
#       bind 0.0.0.0/32:8080 stream tcp
#       bind 0.0.0.0/32:8081 stream tcp
#       bind 0.0.0.0/32:1502 stream tcp
#       bind 0.0.0.0/0:8080 stream tcp
#       connect 0.0.0.0/32:0 raw_sock raw_proto
#       connect 127.0.0.1/32:3306 stream tcp
#       connect 127.0.0.1/32:8083 stream tcp
#       sock_allow_family netlink
}
subject /etc/rc.d/init.d/iptables {
    /tmp            rwcd
```

```
    /etc/passwd r
    /etc/sysconfig  rw
    /var/lock/subsys/network        r
    /opt/cprocsp/sbin/amd64/genfw   rx
    -CAP_ALL
    +CAP_KILL
       connect disabled
       bind disabled
}
#subject /sbin/iptables-restore {
#    /tmp            rwcd
#    /etc/passwd r
#    /etc/sysconfig  rw
#    /var/lock/subsys/network        r
#    /proc                           r
#    /opt/cprocsp/sbin/amd64/genfw   rx
#    -CAP_ALL
#    +CAP_NET_RAW
#    +CAP_NET_ADMIN
#}

subject /sbin/xtables-multi {
    /etc r
    /etc/sysconfig  rw
    /var/lock/subsys/network        r
    /proc                           r
    /opt/cprocsp/sbin/amd64/genfw   rx
    -CAP_ALL
    +CAP_NET_RAW
    +CAP_NET_ADMIN
}


subject /etc/rc.d/init.d/network {
    /etc                        r
    /etc/sysconfig/network      rw
    /etc/net/scripts            rx
    /usr/lib/locale             r
    /usr/sbin                   rx
    /sbin                       rx
    -CAP_ALL
    +CAP_KILL
       connect disabled
       bind disabled
}

subject /etc/net/scripts/ifup {
    /sbin        rx
    -CAP_ALL
       connect disabled
       bind disabled
}
subject /etc/net/scripts/ifup-common {
    /sbin/ip        rx
    /sbin/resolvconf   rx
    -CAP_ALL
       connect disabled
       bind disabled
}

subject /etc/net/scripts/create-eth {
    /sbin/ip        rx
    /sbin/resolvconf   rx
    -CAP_ALL
       connect disabled
       bind disabled
}
subject /etc/net/scripts/ifdown {
    /sbin/ip          rx
    /sbin/resolvconf   rx
    -CAP_ALL
       connect disabled
       bind disabled
}
subject /etc/net/scripts/config-ipv4 {
    /sbin/ip        rx
    /sbin/resolvconf   rx
    -CAP_ALL
    connect disabled
    bind disabled
}
```

```
subject /sbin/ip {
    /sbin/ip           rx
    /sbin/resolvconf   rx
    -CAP_ALL
    +CAP_NET_ADMIN
    +CAP_SYS_MODULE
#TODO: mojet mojno zapretit bind?
}
subject /sbin/ifrename {
    /sbin              rx
    -CAP_ALL
    +CAP_NET_ADMIN
    +CAP_SYS_MODULE
#TODO: mojet mojno zapretit bind?
}

subject /sbin/service {
    /sbin/sd_booted    rx
    -CAP_ALL
}
subject /sbin/sd_booted {
    /sbin/sd_booted    rx
    /sys/fs            r
    -CAP_ALL
}
#Need for network restart.
subject /sbin/sysctl {
    /sbin/sysctl        rx
    /proc/sys/net       rw
    /usr/lib/locale    rx
    -CAP_ALL
    +CAP_SYS_ADMIN
    +CAP_NET_ADMIN
    connect disabled
    bind disabled
}
# Role: root
subject /usr/bin/logger o {
        /                               h
        /dev                            h
        /dev/log                        rw
        /etc                            h
        /etc/ld.so.cache                r
        /etc/localtime                  r
        /lib64                          h
        /lib64/ld-2.17.so               x
        /lib64/libc-2.17.so             rx
        /usr                            h
        /usr/lib/locale                         rx
        /usr/lib64                      r
        /usr/bin/logger                         x
        -CAP_ALL
        bind    disabled
        connect disabled
}
subject /bin/cp {
    /var/opt/cprocsp        rwcdl
    /backup/hsmdb_dump.sql          r
    -CAP_ALL
    +CAP_DAC_OVERRIDE
    +CAP_DAC_READ_SEARCH
    +CAP_CHOWN
    +CAP_FOWNER
    +CAP_FSETID
    connect disabled
    bind disabled
}
subject /bin/find {
    /var/opt/cprocsp        r
    -CAP_ALL
    +CAP_DAC_OVERRIDE
    connect disabled
    bind disabled
}
subject /opt/cprocsp/bin/amd64/cpverify o{
    /       r
    /bin/getopt    rx
        /lib64                      rx
        /usr/lib64                  rx
    /var/opt/cprocsp/keys   h
    /sbin/halt rx
```

```
    /sbin/shutdown     rx
    /usr/include       r
    -CAP_ALL
    +CAP_DAC_OVERRIDE
    +CAP_DAC_READ_SEARCH
    connect disabled
    bind disabled
}
subject /etc/rc.d/init.d/cprocsp {
        /root                           r
        /etc/grsec                      r
        /etc/passwd                     r
        /etc/opt/cprocsp/lcdport.ini    r
        /dev                            rw
        /opt/cprocsp                    h
        /opt/cprocsp/lib/hashes                 r
        /boot/hashes                    r
        /opt/cprocsp/lib/amd64          rx
        /opt/cprocsp/sbin               rx
        /opt/cprocsp/bin                rx
        /var/opt                        r
        /var/opt/cprocsp                r
        /var/opt/cprocsp/mnt
        /var/run                        rwcd
        /var/opt/cprocsp/tmp            rwcd
        /usr                            rx
        /sbin/killall5                  rx
        /sbin/sysctl                    rx
        -CAP_ALL
        +CAP_DAC_OVERRIDE
        +CAP_SYS_TTY_CONFIG
        +CAP_KILL
        +CAP_SYS_RESOURCE
        +CAP_SYS_ADMIN
        connect disabled
        bind disabled
}

#TODO: cross: nado ubrat s finalnoy versii hsmcautil
#subject /opt/cprocsp/bin/amd64/hsmcautil o {
#user_transition_allow root
#group_transition_allow root
#
#       /                               h
#       /etc                            h
#       /etc/ld.so.cache                rx
#       /etc/nsswitch.conf              r
#       /etc/opt/cprocsp/config64.ini   r
#       /etc/passwd                     r
#       /lib64                          rx
#       /opt                            h
#       /opt/cprocsp                    h
#       /opt/cprocsp/bin                h
#       /opt/cprocsp/bin/amd64/hsmcautil        x
#       /opt/cprocsp/lib                h
#       /opt/cprocsp/lib/amd64          rx
#       /usr                            h
#       /usr/lib64/libgpm.so.1.19.0     rx
#       /usr/lib64/libncurses.so.5.6    rx
#       /usr/lib64/libstdc++.so.6.0.17          rx
#       /var                            h
#       /var/log
#       /var/log/hsmcautil.log          w
#       /var/opt/cprocsp/tmp
#       /var/opt/cprocsp/tmp/._hsmcasnpoolfilelock_d73a1832-a567-19fe-2f3caaedfa971d30      wc
#       /var/opt/cprocsp/tmp/.cryptsrv_hsm      rw
#       /var/opt/cprocsp/tmp/.registry_lock     w
#       /var/opt/cprocsp/users/0.0
#       /var/opt/cprocsp/users/0.0/SerialNumberPool     rw
#       /var/opt/cprocsp/users/0.0/hsm.ini      r
#       /var/run
#       -CAP_ALL
#       +CAP_SETGID
#       +CAP_SETUID
#       bind    disabled
#       connect disabled
#}
subject /opt/cprocsp/sbin/amd64/cpconfig {
        /                                       h
        /etc/ld.so.cache        r
        /lib64                          rx
```

```
        /usr/lib64                      rx
        /usr/share/locale   r
        /var/etc/opt/cprocsp/hsmwww h
        /etc/nsswitch.conf      r
        /etc/services           r
        /etc/passwd                     r
        /etc/localtime          r
        /opt/cprocsp/share               r
        /opt/cprocsp/lib                 rx
        /var/opt/cprocsp r
        /var/opt/cprocsp/tmp rwcd
        /usr/local                      h
        /usr/local/mysql/lib/libmysqlclient.so.18.0.0       rx
        /usr/local/mysql/share/charsets/Index.xml    r
        /var/etc/opt                    r
        /var/etc/opt/cprocsp    rwcd
        /var/run                                r
        /tmp/mysql.sock                         rw
        -CAP_ALL
        connect 127.0.0.1/32:3306 stream tcp
        bind disabled
}
subject /opt/cprocsp/sbin/amd64/ecc_check.sh {
        /tmp/ecc_report_simple.txt rwcd
        /tmp/ecc_report_full.txt      rwcd
        -CAP_ALL
        connect disabled
        bind disabled
}
# Role: root
subject /usr/bin/edac-util o {
        /                               h
        /etc                            h
        /etc/ld.so.cache                r
        /lib64                          rx
        /sys                            rx
        /usr                            h
        /usr/bin/edac-util              x
        /usr/lib64                      rx
        -CAP_ALL
        bind   disabled
        connect disabled
}

subject /opt/cprocsp/bin/amd64/wipefile o{
        /                                       h
        /lib64                          rx
        /etc                            r
        /usr/lib64                      rx
        /etc/opt/cprocsp rwcd
        /etc/opt/cprocsp/hsmwww h
        /opt/cprocsp/lib rx
        /var/opt/cprocsp rwcd
        /var/tmp                rwcd
        /var/log                rwcd
        /backup         rwcd
        -CAP_ALL
        +CAP_DAC_OVERRIDE
        +CAP_DAC_READ_SEARCH
        connect disabled
        bind disabled
}
subject /opt/cprocsp/bin/amd64/hsm_backup o {
    /
        /lib64                                          rx
        /opt/cprocsp/bin/amd64/wipefile rx
        /opt/cprocsp/bin/amd64/hsm_backup rx
        /usr/share/locale r
        /usr/lib/locale rx
        /bin/tar rx
        /bin/gzip rx
        /bin/cp     rx
        /bin/mv     rx
        /lib rx
        /usr/lib/gconv rx
        /usr/lib64     rx
        /opt/cprocsp/lib/amd64 rx
        /opt/cprocsp/sbin/amd64/hsmdb_dump.sh x
        /opt/cprocsp/sbin/amd64/hsmdb_repair.sh      x
        /usr/lib64/libstdc++.so.6.0.17        rx
        /usr/local/mysql/lib/libmysqlclient.so.18.0.0       rx
```

```
        /usr/local/mysql/share/charsets/Index.xml    r
        /tmp                            rw
        /etc    r
        /var/etc/opt
        /var/opt/cprocsp rwcd
        /var/tmp                rwcd
        /var/log                rwcd
        /proc   r
        /dev/null rw
        /dev/log    rw
        /etc/opt/cprocsp rwcd
        /etc/opt/cprocsp/hsmwww h
    /backup         rwcd
        -CAP_ALL
        +CAP_DAC_OVERRIDE
        +CAP_KILL
        +CAP_CHOWN
    connect disabled
    bind disabled
}
subject /opt/cprocsp/sbin/amd64/cryptsrv_hsm o {
        /
        /dev                            h
        /dev/log            rw
        /dev/null                       rw
        /dev/sobol                      r
        /dev/random                     r
        /dev/urandom                    r
        /etc                            r
        /etc/localtime                  r
        /etc/passwd                     r
        /etc/grsec                      h
        /etc/ssh                        h
        /etc/shadow                     h
        /etc/shadow-                    h
        /etc/gshadow                    h
        /etc/gshadow-                   h
        /etc/ppp/chap-secrets           h
        /etc/ppp/pap-secrets            h
        /etc/samba/smbpasswd            h
        /etc/ld.so.cache        rx
        /lib64                          rx
        /opt                            h
        /opt/cprocsp                    rx
        /opt/cprocsp/sbin/amd64/cryptsrv_hsm rx
        /usr                            h
        /usr/local/lib          r
        /usr/lib64              rx
        /usr/lib/locale                 rx
        /usr/share                      h
        /usr/share/locale
        /usr/local                      h
        /usr/local/mysql/lib            rx
        /usr/local/mysql/share/charsets/Index.xml    r
        /proc                           r
        /proc/kcore                     h
        /proc/sys                       h
        /proc/sys/vm                    r
        /proc/bus                       h
        /var
        /var/etc            r
        /var/lib                        h
        /var/lib/run
        /var/opt                        rwcd
        /var/run
        /var/run/pcscd
        /var/run/pcscd/pcscd.comm               rw
        /var/run/pcscd/pcscd.pub                rwx
        /var/run/cryptsrv_hsm.pid       rwcd
        /tmp/mysql.sock         rw
        /var/log                        h
        /sys                            h
        /sys/devices/system/cpu/online          r
        /boot                           h
        -CAP_ALL
        +CAP_DAC_OVERRIDE
        +CAP_SYS_RESOURCE
        +CAP_FOWNER
        +CAP_FSETID
        +CAP_SETGID
        +CAP_SETUID
```

```
        +CAP_KILL
        +CAP_IPC_LOCK
        +CAP_SYS_RESOURCE
    connect 127.0.0.1/32:111-1023 dgram udp
    connect 127.0.0.1/32:111-1023 stream tcp
    connect 127.0.0.1/32:8081 stream tcp
    connect 127.0.0.1/32:3306 stream tcp
    bind 0.0.0.0/32:0 stream tcp
}

subject /opt/cprocsp/sbin/amd64/fenixmsrv o {
        /                                   r
        /dev                        rw
        /etc                        rx
        /etc/grsec                  h
        /etc/ssh                    h
        /etc/shadow                 h
        /etc/shadow-                h
        /etc/gshadow                h
        /etc/gshadow-               h
        /etc/ppp/chap-secrets       h
        /etc/ppp/pap-secrets        h
        /etc/samba/smbpasswd        h
        /etc/opt/cprocsp    rwcd
        /etc/opt/cprocsp/hsmwww r
        /sbin/halt                  rx
        /sbin/reboot          rx
        /lib64                      rx
        /opt                        h
        /opt/cprocsp                h
        /opt/cprocsp/lib            h
        /opt/cprocsp/lib/amd64      rx
        /opt/cprocsp/sbin           h
        /opt/cprocsp/sbin/amd64/fenixmsrv     rx
        /usr                        h
        /usr/local/lib      r
        /usr/lib/locale                     rx
        /usr/lib64                  rx
        /usr/local/mysql/lib/libmysqlclient.so.18.0.0       rx
        /usr/local/mysql/share/charsets/Index.xml    r
        /var                        r
        /var/opt/cprocsp/backups rw
        /var/opt/cprocsp/log   rwcd
        /var/opt/cprocsp/tmp rwcd
        /var/opt/cprocsp/users rwcd
        /var/run
        /var/run/pcscd
        /var/run/pcscd/pcscd.pub  rwx
        /var/run/pcscd/pcscd.comm  rw
        /var/run/fenixmsrv.pid      rwcd
        /tmp                        rw
        /proc                       r
        /proc/kcore                 h
        /proc/sys                   h
        /proc/sys/vm                r
        /proc/bus                   h
        /sys                        h
        /sys/devices/system         r
        /boot                       h
        /backup             rwcd
        -CAP_ALL
        +CAP_SETGID
        +CAP_SETUID
        +CAP_NET_BIND_SERVICE
        +CAP_FOWNER
        +CAP_FSETID
        +CAP_SYS_TIME
        +CAP_KILL
        +CAP_DAC_OVERRIDE
        +CAP_DAC_READ_SEARCH
        +CAP_IPC_LOCK
        +CAP_SYS_RAWIO
        bind 0.0.0.0/32 stream tcp
        bind 0.0.0.0/32:8081 stream tcp
        bind 0.0.0.0/32:8080 stream tcp
        bind 0.0.0.0/0:8080 stream tcp
        bind 0.0.0.0/32:1502 stream tcp
        connect 127.0.0.1/32:3306 stream tcp
        connect 127.0.0.1/32:8083 stream tcp
        sock_allow_family all
}
```

```
subject /opt/cprocsp/sbin/amd64/srv_wrapper o {
        /
        /usr/bin/pgrep         rx
        /sbin/killall5         rx
        /bin/sync                      rx
        /bin/umount                    rx
        /dev                           h
        /dev/null                      rw
        /dev/log            rw
        /etc                           h
        /etc/init.d
        /etc/init.d/cprocsp rx
        /etc/init.d/syslogd rx
        /etc/init.d/iptables rx
        /etc/init.d/network rx
        /etc/init.d/mysqld rx
        /etc/init.d/stunneld rx
        /etc/rc.d/init.d
        /etc/rc.d/init.d/cprocsp rx
        /etc/rc.d/init.d/clock rx
        /etc/rc.d/init.d/syslogd rx
        /etc/rc.d/init.d/iptables rx
        /etc/rc.d/init.d/network rx
        /etc/rc.d/init.d/mysqld rx
        /usr/local/mysql/support-files/mysql.server  rx
        /etc/bindresvport.blacklist   r
        /etc/ld.so.cache               rx
        /etc/localtime      r
        /lib64                         h
        /lib64/ld-2.17.so              x
        /lib64/libc-2.17.so            rx
        /lib64/libm-2.17.so    rx
        /opt                           h
        /opt/cprocsp/sbin/amd64/srv_wrapper   rx
        /opt/cprocsp/sbin/amd64/stunnel_hsm   rx
        /opt/cprocsp/bin/amd64/wipefile       rx
        /opt/cprocsp/bin/amd64/hsm_backup     rx
        /var                           h
        /etc/opt/cprocsp rwcd
        /etc/opt/cprocsp/hsmwww h
        /opt/cprocsp/lib rx
        /var/opt/cprocsp rwcd
        /var/tmp               rwcd
        /var/log               rwcd
        /backup         rwcd
        /var/run               rwcd
        /var/etc/opt        r
        /proc                          r
        /proc/kcore                    h
        /proc/sys                      h
        /proc/bus                      h
        /sys                           h
        /boot                          h
        /usr/src                       h
        /proc                          r
        -CAP_ALL
        +CAP_NET_BIND_SERVICE
        +CAP_DAC_READ_SEARCH
        +CAP_DAC_OVERRIDE
        +CAP_NET_ADMIN
        +CAP_KILL
        +CAP_SYS_BOOT
        +CAP_FOWNER
        +CAP_CHOWN
        +CAP_FSETID
        bind 0.0.0.0/32:8083 stream tcp
#       bind 0.0.0.0/32:344-1023 stream dgram tcp udp
#       connect 127.0.0.1/32:111 dgram udp
        connect 127.0.0.1/32:3306 stream tcp
}

# Role: root
subject /usr/bin/pgrep o {
        /                              h
        /etc                           h
        /etc/ld.so.cache               r
        /lib64                         h
        /lib64/ld-2.17.so              x
        /lib64/libc-2.17.so            rx
        /lib64/libprocps.so.1.1.1      rx
```

```
        /sys                            h
        /sys/devices/system/cpu/online        r
        /usr                            h
        /usr/bin/pgrep                  x
        /usr/lib/locale                       rx
        /usr/lib64                      r
        -CAP_ALL
        bind    disabled
        connect disabled
}

subject /opt/cprocsp/sbin/amd64/hsmdb_dump.sh o {
        /       r
        /backup rwcd
        /usr/local/mysql/bin   rx
        /bin/bash      x
        /bin/rm        x
        /bin/mv        x
        /lib/terminfo  r
        /lib64  rx
        /dev/null      w
        /dev/tty       rw
        /op/cprocsp/sbin/amd64/hsmdb_dump.sh  r
        /proc/meminfo  r
        /etc/ld.so.cache       r
        /usr/lib/locale                       rx
        /usr/lib64     r
        -CAP_ALL
        +CAP_DAC_OVERRIDE
        +CAP_DAC_READ_SEARCH
        connect disabled
        bind    disabled
}

subject /opt/cprocsp/sbin/amd64/hsmdb_repair.sh o {
        /
        /backup                         h
        /backup/hsmdb_dump.sql          r
        /bin                            h
        /bin/bash                       x
        /bin/rm                         x
        /etc                            h
        /etc/passwd                     r
        /etc/ld.so.cache                r
        /etc/nsswitch.conf     r
        /var/etc/opt
        /etc/opt/cprocsp/hsmdb_dump.sql       r
        /lib                            h
        /lib/terminfo
        /lib/terminfo/l/linux           r
        /lib64                          rx
        /proc                           h
        /proc/meminfo                   r
        /sbin                           h
        /sbin/service                   x
        /var                            h
        /var/run
        /var/lib/mysql/cprocsp/db
        /dev
        /dev/null                       w
        /dev/tty                        rw
        /dev/grsec                      h
        /dev/mem                        h
        /dev/kmem                       h
        /dev/port                       h
        /dev/log                        h
        /opt
        /opt/cprocsp
        /opt/cprocsp/sbin
        /opt/cprocsp/sbin/amd64
        /opt/cprocsp/sbin/amd64/hsmdb_repair.sh      r
        /root
        /usr
        /usr/lib/locale                       rx
        /usr/lib64/gconv/gconv-modules.cache  r
        /usr/lib64/locale      r
        /usr/local
        /usr/local/mysql
        /usr/local/mysql/bin/mysql    x
        /usr/local/mysql/bin/mysqladmin       x
        /usr/local/mysql/scripts/mysql_install_db    x
```

```
        /usr/src                        h
        -CAP_ALL
        +CAP_DAC_OVERRIDE
        bind    disabled
        connect disabled
}

# Role: root
subject /usr/local/mysql/bin/resolveip o {
        /                               h
        /etc                            h
        /etc/host.conf                  r
        /etc/hosts                      r
        /etc/ld.so.cache                r
        /etc/nsswitch.conf              r
        /etc/resolv.conf                r
        /lib64                          rx
        /lib64/modules                  h
        /usr                            h
        /usr/local/mysql/bin/resolveip          x
        -CAP_ALL
        bind 0.0.0.0/32:0 dgram ip
        connect 127.0.0.1/32:53 dgram udp
}

subject /opt/cprocsp/sbin/amd64/stunnel_hsm o {
user_transition_deny 998
group_transition_deny 998

        /
        /dev                            h
        /dev/urandom                    r
        /dev/log                        rw
        /dev/null                       rw
        /etc                            rx
        /etc/grsec                      h
        /etc/ssh                        h
        /etc/shadow                     h
        /etc/shadow-                    h
        /etc/gshadow                    h
        /etc/gshadow-                   h
        /etc/ppp/chap-secrets           h
        /etc/ppp/pap-secrets            h
        /etc/samba/smbpasswd            h
        /lib64                          rx
        /opt                            h
        /opt/cprocsp                    rx
        /proc
        /proc/stat                      r
        /proc/meminfo                   r
        /proc/cpuinfo                   r
        /sys                            r
        /usr                            h
        /usr/lib/locale                         rx
        /usr/local                      h
        /usr/local/lib      r
        /usr/local/mysql/lib/libmysqlclient.so.18.0.0       rx
        /usr/local/mysql/share/charsets/Index.xml    r
        /usr/share/locale     r
        /usr/lib64     rx
        /var                            h
        /var/etc/opt                    r
        /var/log
        /var/log/stunnel-K2.log                 rwac
        /var/log/stunnel-K2s.log        rwac
        /var/log/stunnel-web.log        rwac
        /var/opt/cprocsp/tmp            rwcd
        /var/opt/cprocsp/log            rwcd
        /var/opt/cprocsp/users     r
        /var/opt/cprocsp/users/stores/my.sto      crw
        /var/opt/cprocsp/users/user_db.dat    r
        /var/opt/cprocsp/users/999.999/stores/my.sto crw
        /var/run
        /tmp                            rwcd
        /boot                           h
        -CAP_ALL
        +CAP_SETGID
        +CAP_FOWNER
        +CAP_SETUID
        +CAP_FSETID
        +CAP_NET_BIND_SERVICE
```

```
        +CAP_AUDIT_WRITE
#Pochemuto snachalo na 0:0 delaet bind
    bind 0.0.0.0:0 stream tcp
    bind 0.0.0.0/0:443 stream tcp
    bind 0.0.0.0/0:1501 stream tcp
    bind 0.0.0.0/0:1502 stream tcp
    bind 0.0.0.0/0:1503 stream tcp
    bind 0.0.0.0/0:1504 stream tcp
    connect 0.0.0.0/0:1504 stream tcp
    connect 127.0.0.1/32:8080 stream tcp
    connect 127.0.0.1/32:3306 stream tcp
    sock_allow_family netlink
}

subject /usr/sbin/crond o {
user_transition_allow root 65534
group_transition_allow 65534 shadow root

        /                               h
        /bin                            h
        /bin/sh                         x
        /dev                            h
        /dev/log            rw
        /etc                            r
        /etc/grsec                      h
        /etc/ssh                        h
        /etc/shadow                     h
        /etc/shadow-                    h
        /etc/gshadow                    h
        /etc/gshadow-                   h
        /etc/ppp/chap-secrets           h
        /etc/ppp/pap-secrets            h
        /etc/samba/smbpasswd            h
        /home                           r
        /lib64                          rx
        /proc                           rw
        /proc/sys/kernel/ngroups_max    r
        /usr                            h
        /usr/sbin/sendmail              x
        /var                            h
        /var/spool/at
        /var/spool/cron
        /root
        /tmp                            rwcd
        /opt/cprocsp/sbin/amd64/ecc_check.sh rx
        -CAP_ALL
        +CAP_SETGID
        +CAP_SETUID
        +CAP_SYS_RESOURCE
        +CAP_SYS_ADMIN
        +CAP_AUDIT_WRITE
        bind 0.0.0.0/32:0 stream tcp
        connect 127.0.0.1/32:111 stream tcp
        sock_allow_family netlink
}
subject /usr/local/mysql/bin/my_print_defaults o {
        /
        /lib64                          rx
        /usr                            h
        /usr/local/mysql
        /usr/local/mysql/bin/my_print_defaults       x
        /var                            h
        /var/lib/mysql/cprocsp/etc/my.cnf     r
        /etc
        /etc/ld.so.cache                r
        /etc/grsec                      h
        /etc/ssh                        h
        /etc/passwd                     h
        /etc/shadow                     h
        /etc/shadow-                    h
        /etc/gshadow                    h
        /etc/gshadow-                   h
        /etc/ppp/chap-secrets           h
        /etc/ppp/pap-secrets            h
        /etc/samba/smbpasswd            h
        -CAP_ALL
        +CAP_DAC_OVERRIDE
        bind    disabled
        connect disabled
}
```

```
subject /usr/local/mysql/bin/mysql o {
        /
        /lib64                          rx
        /usr                            h
        /usr/lib/locale                         rx
        /usr/lib64                      rx
        /usr/lib64/gconv                h
        /usr/lib64/gconv/gconv-modules.cache  r
        /usr/lib64/locale               r
        /usr/local                      h
        /usr/local/mysql
        /usr/local/mysql/bin/mysql      x
        /usr/local/mysql/share/charsets/Index.xml     r
        /var                            h
        /var/lib/mysql/cprocsp/etc/my.cnf     r
        /etc
        /etc/ld.so.cache                r
        /etc/nsswitch.conf              r
        /etc/services                   r
        /etc/grsec                      h
        /etc/ssh                        h
        /etc/passwd                     h
        /etc/shadow                     h
        /etc/shadow-                    h
        /etc/gshadow                    h
        /etc/gshadow-                   h
        /etc/ppp/chap-secrets           h
        /etc/ppp/pap-secrets            h
        /etc/samba/smbpasswd            h
        /tmp                            rw
        -CAP_ALL
        +CAP_DAC_OVERRIDE
        bind    disabled
        connect disabled
}

subject /usr/local/mysql/bin/mysqladmin o {
        /
        /lib64                          rx
        /usr                            h
        /usr/lib/locale                         rx
        /usr/lib64/gconv/gconv-modules.cache  r
        /usr/lib64/libstdc++.so.6.0.17          rx
        /usr/lib64/locale       r
        /usr/local/mysql
        /usr/local/mysql/bin/mysqladmin         x
        /usr/local/mysql/share/charsets/Index.xml     r
        /var                            h
        /var/lib/mysql/cprocsp/db       r
        /var/lib/mysql/cprocsp/etc/my.cnf     r
        /var/lib/mysql/mysql.pid        rwcd
        /etc
        /etc/ld.so.cache                r
        /etc/nsswitch.conf              r
        /etc/services                   r
        /etc/grsec                      h
        /etc/ssh                        h
        /etc/passwd                     h
        /etc/shadow                     h
        /etc/shadow-                    h
        /etc/gshadow                    h
        /etc/gshadow-                   h
        /etc/ppp/chap-secrets           h
        /etc/ppp/pap-secrets            h
        /etc/samba/smbpasswd            h
        /tmp                            rw
        -CAP_ALL
        +CAP_DAC_OVERRIDE
        bind    disabled
        connect disabled
}

subject /usr/local/mysql/bin/mysqld o {
user_transition_allow root mysql
group_transition_allow root mysql

        /                               h
        /lib64                          rx
        /proc/sys/kernel/ngroups_max    r
        /etc
        /etc/group                      r
```

```
        /etc/ld.so.cache              r
        /etc/localtime                r
        /etc/nsswitch.conf            r
        /etc/passwd                   r
        /etc/grsec                    h
        /etc/ssh                      h
        /etc/shadow                   h
        /etc/shadow-                  h
        /etc/gshadow                  h
        /etc/gshadow-                 h
        /etc/ppp/chap-secrets         h
        /etc/ppp/pap-secrets          h
        /etc/samba/smbpasswd          h
        /proc                         r
        /usr
        /usr/lib/locale                       rx
        /usr/lib64/libstdc++.so.6.0.17        rx
        /usr/local
        /usr/local/mysql
        /usr/local/mysql/bin/mysqld   x
        /usr/local/mysql/share/charsets/Index.xml    r
        /usr/local/mysql/share/english/errmsg.sys    r
        /usr/src                      h
        /var
        /var/lib
        /var/lib/mysql
        /var/lib/mysql/cprocsp
        /var/lib/mysql/cprocsp/db     rwcd
        /var/lib/mysql/cprocsp/etc/my.cnf     r
        /var/lib/mysql/mysql.pid      rwcd
        /var/log                      h
        -CAP_ALL
        +CAP_DAC_OVERRIDE
        +CAP_SYS_RESOURCE
        +CAP_SETGID
        +CAP_SETUID
        bind    disabled
        connect disabled
}

subject /usr/local/mysql/bin/mysqld_safe o {
        /                             rw
        /bin                          x
        /etc                          r
        /etc/ld.so.cache              r
        /lib64                                rx
        /lib64/ld-2.17.so             x
        /lib64/libc-2.17.so           rx
        /lib64/libdl-2.17.so   rx
        /proc                         h
        /proc/meminfo                 r
        /usr                          h
        /usr/bin                      x
        /usr/lib/locale                       rx
        /usr/lib64                    h
        /usr/lib64/gconv/gconv-modules.cache  r
        /usr/lib64/locale      r
        /usr/local                    h
        /usr/local/mysql
        /usr/local/mysql/bin          h
        /usr/local/mysql/bin/my_print_defaults       x
        /usr/local/mysql/bin/mysqld
        /usr/local/mysql/bin/mysqld_safe      r
        /usr/local/mysql/lib          h
        /usr/local/mysql/lib/mysql/plugin
        /usr/local/mysql/share        h
        /usr/local/mysql/share/english/errmsg.sys
        /var/lib/mysql/mysql.pid rwcd
        /dev
        /dev/null                     rw
        /dev/tty                      rw
        /dev/grsec                    h
        /dev/mem                      h
        /dev/kmem                     h
        /dev/port                     h
        /dev/log                      h
        /var/log                      h
        /sys                          h
        /boot                         h
        -CAP_ALL
        +CAP_DAC_OVERRIDE
```

```
        bind    disabled
        connect disabled
}

subject /usr/local/mysql/bin/mysqldump o {
        /
        /lib64                          rx
        /usr                            h
        /usr/lib/locale                         rx
        /usr/lib64/libstdc++.so.6.0.17          rx
        /usr/local/mysql        rx
        /usr/local/mysql/bin/mysqldump          x
        /usr/local/mysql/share/charsets/Index.xml     r
        /var                            h
        /var/lib/mysql/cprocsp/etc/my.cnf     r
        /backup
        /backup/hsmdb_dump_tmp.sql     rwcd
        /etc
        /etc/ld.so.cache                r
        /etc/localtime                  r
        /etc/nsswitch.conf              r
        /etc/services                   r
        /etc/grsec                      h
        /etc/ssh                        h
        /etc/passwd                     h
        /etc/shadow                     h
        /etc/shadow-                    h
        /etc/gshadow                    h
        /etc/gshadow-                   h
        /etc/ppp/chap-secrets           h
        /etc/ppp/pap-secrets            h
        /etc/samba/smbpasswd            h
        /tmp                            rw
        -CAP_ALL
        +CAP_DAC_OVERRIDE
        +CAP_DAC_READ_SEARCH
        bind    disabled
        connect disabled
}

subject /usr/local/mysql/scripts/mysql_install_db o {
        /                               h
        /bin                            x
        /etc                            r
        /etc/nsswitch.conf     r
        /etc/passwd                     r
        /etc/ld.so.cache                r
        /lib64                                  rx
        /lib64/ld-2.17.so               x
        /lib64/libc-2.17.so             rx
        /lib64/libdl-2.17.so   rx
        /proc                           h
        /proc/meminfo                   r
        /usr                            h
        /usr/lib/locale                         rx
        /usr/lib64/gconv/gconv-modules.cache  r
        /usr/lib64/locale      r
        /usr/local/mysql
        /usr/local/mysql/bin            h
        /usr/local/mysql/bin/my_print_defaults       x
        /usr/local/mysql/bin/mysqld    x
        /usr/local/mysql/bin/resolveip          x
        /usr/local/mysql/scripts        h
        /usr/local/mysql/scripts/mysql_install_db     r
        /usr/local/mysql/share          h
        /usr/local/mysql/share/fill_help_tables.sql
        /usr/local/mysql/share/mysql_system_tables.sql
        /usr/local/mysql/share/mysql_system_tables_data.sql
        /var                            h
        /var/run
        /var/lib/mysql/cprocsp/db
        /dev
        /dev/null                       w
        /dev/tty                        rw
        /dev/grsec                      h
        /dev/mem                        h
        /dev/kmem                       h
        /dev/port                       h
        /dev/log                        h
        /root
        -CAP_ALL
```

```
        +CAP_DAC_OVERRIDE
        bind    disabled
        connect disabled
}

subject /usr/local/mysql/support-files/mysql.server o {
        /
        /bin                            x
        /etc                            r
        /etc/ld.so.cache                r
        /etc/rc.d/init.d
        /lib64                          rx
        /opt                            h
        /opt/cprocsp/sbin/amd64
        /proc                           h
        /proc/meminfo                   r
        /var                            h
        /var/run
        /var/lib/mysql/cprocsp/db       rw
        /var/lib/mysql/mysql.pid        rwcd
        /var/lock/subsys                rw
        /dev
        /dev/null                       rw
        /dev/tty                        rw
        /dev/grsec                      h
        /dev/mem                        h
        /dev/kmem                       h
        /dev/port                       h
        /dev/log                        h
        /usr
        /usr/bin/expr                   x
        /usr/lib/locale                         rx
        /usr/lib64/gconv/gconv-modules.cache  r
        /usr/lib64/locale     r
        /usr/local
        /usr/local/mysql
        /usr/local/mysql/bin/my_print_defaults       x
        /usr/local/mysql/bin/mysqld_safe     x
        /usr/local/mysql/support-files/mysql.server  r
        /usr/src                        h
        /sys                            h
        /boot                           h
        -CAP_ALL
        +CAP_DAC_OVERRIDE
        +CAP_KILL
        bind    disabled
        connect disabled
}

role cacheman u
role_allow_ip  0.0.0.0/32
subject /  {
        /                               h
        -CAP_ALL
        bind    disabled
        connect disabled
}

subject /etc/cron.daily o {
        /                               h
        /bin                            xi
        /etc                            r
        /etc/grsec                      h
        /etc/ssh                        h
        /etc/shadow                     h
        /etc/shadow-                    h
        /etc/gshadow                    h
        /etc/gshadow-                   h
        /etc/ppp/chap-secrets           h
        /etc/ppp/pap-secrets            h
        /etc/samba/smbpasswd            h
        /lib64                          rxi
        /proc                           h
        /proc/meminfo                   r
        /proc/sys/kernel/ngroups_max  r
        /sbin                           h
        /sbin/consoletype               xi
        /dev
        /dev/null                       w
        /dev/tty                        rw
        /dev/grsec                      h
```

```
        /dev/mem                        h
        /dev/kmem                       h
        /dev/port                       h
        /dev/log                        h
        /tmp                            rwcd
        /usr
        /usr/bin                        xi
        /usr/lib64                      r
        /usr/sbin                       h
        /usr/sbin/makewhatis            rxi
        /usr/X11R6
        /usr/local
        /usr/share                      rxi
        /usr/src                        h
    /var/etc/opt/cprocsp/config64.ini        r
        /var
        /var/cache
        /var/cache/man                  rw
        /var/cache/man/X11R6
        /var/cache/man/X11R6/whatis     w
        /var/cache/man/local
        /var/cache/man/local/whatis     w
        /var/log                        h
        -CAP_ALL
        bind    disabled
        connect disabled
}

role mysql u
role_allow_ip  0.0.0.0/32
role_allow_ip  127.0.0.1/32
subject /  {
        /                               h
        -CAP_ALL
        bind    disabled
        connect disabled
}

subject /etc/init.d o {
        /
        /tmp                            rwcd
        /var/lib/mysql/cprocsp rwcd
        -CAP_ALL
        bind 0.0.0.0/32:3306 stream tcp
        connect disabled
}

subject /usr/local/mysql/bin/mysqld o {
        /
        /tmp                            rwcd
        /var/lib/mysql rwxcd
        /etc            r
        /lib64          r
        /proc/sys/vm    r
        -CAP_ALL
        connect 127.0.0.1/32:1504 stream tcp
        sock_allow_family netlink
        bind disabled
}

role osec u
role_allow_ip  0.0.0.0/32
subject /  {
        /                               h
        -CAP_ALL
        bind    disabled
        connect disabled
}
subject  /usr/bin/osec o {
    /               h
    /etc                h
    /etc/group          r
    /etc/passwd         r
    /usr                h
    /usr/X11R6          h
    /usr/X11R6/bin
    /usr/X11R6/lib          r
    /usr/X11R6/lib/X11
    /usr/X11R6/lib/tls
    /usr/bin            r
    /usr/games
```

```
    /usr/lib            r
    /usr/lib64          r
    /usr/libexec            r
    /usr/sbin           r
    /var                h
    /var/lib/osec           rwcd
    /bin                r
    /lib                r
    /lib64              r
    /root               r
    /sbin               r
    -CAP_ALL
    +CAP_DAC_READ_SEARCH
    connect disabled
    bind disabled
}

subject /etc/cron.daily o {
        /                               h
        /etc                            h
        /etc/group                      r
        /etc/passwd                     r
        /usr                            h
        /usr/X11R6                      h
        /usr/X11R6/bin
        /usr/X11R6/lib                  r
        /usr/X11R6/lib/X11
        /usr/X11R6/lib/tls
        /usr/bin                        r
        /usr/games
        /usr/lib                        r
        /usr/lib64                      r
        /usr/libexec                    r
        /usr/sbin                       r
        /var                            h
        /var/lib/osec                   rwcd
        /bin                            r
        /lib                            r
        /lib64                          r
        /root                           r
        /sbin                           r
        -CAP_ALL
        +CAP_DAC_READ_SEARCH
        bind    disabled
        connect disabled
}
role syslogd u
role_allow_ip          0.0.0.0/32
subject / {
        /       h
        /var/resolv
        -CAP_ALL
        bind    disabled
        connect disabled
}

role rpc u
role_allow_ip  0.0.0.0/32
# Role: rpc
subject /  {
        /                               h
        -CAP_ALL
        bind    disabled
        connect disabled
}

# Role: rpc
subject /sbin/rpcbind o {
        /                               h
        -CAP_ALL
        bind 0.0.0.0/32:111 stream tcp
        connect 127.0.0.1/32:712 dgram udp
        connect 127.0.0.1/32:713 dgram udp
}
```

Приложение 4. Скрипт genwf – интерпретатор настроек межсетевого экрана

```
#!/bin/sh
FIREWALL_INI=@localstatedir@/users/0.0/firewall.ini
test -f $FIREWALL_INI || echo -n "" >> $FIREWALL_INI
awk     --posix     -v     ip_address0=`@sbindir@/read_parm     ip_address     eth0`     -v
ip_address1=`@sbindir@/read_parm   ip_address   eth1`   -v   ip_address2=`@sbindir@/read_parm
ip_address     eth2`     -v     ip_address3=`@sbindir@/read_parm     ip_address     eth3`     -v
ip_address4=`@sbindir@/read_parm ip_address eth4` ' BEGIN {
        my_ip["eth0"]=ip_address0
        my_ip["eth1"]=ip_address1
        my_ip["eth2"]=ip_address2
        my_ip["eth3"]=ip_address3
        my_ip["eth4"]=ip_address4
        print "*filter"
        print ":INPUT DROP [0:0]"
        print ":FORWARD DROP [0:0]"
        print ":OUTPUT DROP [0:0]"
        print "[0:0] -A INPUT -s 127.0.0.1/255.0.0.0 -d 127.0.0.1/255.0.0.0 -i lo -j ACCEPT"
        print "[0:0] -A OUTPUT -s 127.0.0.1/255.0.0.0 -d 127.0.0.1/255.0.0.0 -o lo -j ACCEPT"
}
/\[[[:digit:]]*\]/ {
        gsub("\\[","",$1)
        gsub("\\]","",$1)
        port=$1
}
/([[:digit:]]{1,3}_){4}(_[[:digit:]]{1,3}){4}/ {
        ip=$1
        sub("__.*","",ip)
        sub(ip,"",$1)
        gsub("_",".",ip)
        netmask=$1
        sub("^__","",netmask)
        sub("__.*","",netmask)
        gsub("_",".",netmask)
        iface=$1
        sub(".*__","",iface)
        print "[0:0] -A INPUT -s " ip "/" netmask " -d " my_ip[iface] " -i " iface " -p tcp -
m tcp --dport " port " -j ACCEPT"
        print "[0:0] -A OUTPUT -s " my_ip[iface] " -d " ip "/" netmask " -o " iface " -p tcp
-m tcp --sport " port " -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT"
}
END {
        print "COMMIT"
}' <$FIREWALL_INI|grep -v "^[[:space:]]*#"| grep -v '^[[:space:]]*$'
```

Приложение 5. Скрипт lcdfunctions – набор функций для вывода строк на LCD панель и проверки целостности

```
#!/bin/bash
#
# Define LCD port and speed
eval `@sbindir@/read_lcd`
#check mysqld only one time when HSM starts
#if ! test -f /var/run/fenixmsrv.pid ;
wrapper_pid=`/bin/pidof srv_wrapper`
if [ x$wrapper_pid == x ] ;
then
    #check mysqld status
        /etc/init.d/mysqld status 2>&1 > /dev/null
    RET=$?
    if test $RET -ne 0
    then
                # wait 10 sec
                logger -p user.err -t cprocsp.start "Waiting for mysqld to start!"
                for ((retries=0; retries<5; retries++))
                do
                        sleep 2
                        /etc/init.d/mysqld status 2>&1 > /dev/null
                        RET=$?
                        test $RET -eq 0 && break
                        mysqld_pid=`pidof /usr/local/mysql/bin/mysqld`
                        # mysqld is not started?
                        test -z $mysqld_pid && break
                done

        if test $RET -ne 0
        then
                        #try to start mysqld service
                        logger -p user.err -t cprocsp.start "Trying to start mysqld!"
                        /etc/init.d/mysqld start 2>&1 > /dev/null
                        RET=$?
                        if test $RET -ne 0 && test -x /opt/cprocsp/sbin/amd64/hsmdb_repair.sh
&& test -f /backup/hsmdb_dump.sql
                        then
                                # repair mysql db from last regular hsmdb backup
                                logger -p user.err -t cprocsp.start "Trying to repair mysqld
from /backup/hsmdb_dump.sql"
                                /opt/cprocsp/sbin/amd64/hsmdb_repair.sh /backup/hsmdb_dump.sql
                                RET=$?
                        fi
                        if test $RET -ne 0 && test -x /opt/cprocsp/sbin/amd64/hsmdb_repair.sh
&& test -f /etc/opt/cprocsp/hsmdb_dump.sql
                        then
                                # repair mysql db from initial (after HSM installation) hsmdb
backup
                                logger -p user.err -t cprocsp.start "Trying to repair mysqld
from /etc/opt/cprocsp/hsmdb_dump.sql"
                                /opt/cprocsp/sbin/amd64/hsmdb_repair.sh
/etc/opt/cprocsp/hsmdb_dump.sql
                                RET=$?
                        fi
                        test $RET -ne 0 && logger -p user.err -t cprocsp.start "Error: Failed
to start and repair mysqld! HSM is Diyed"
                        # HSM is diyed!!!
                        test $RET -ne 0 && exit 1
        fi
    fi
    # network and iptables services need info from mysql. After mysql starting we need to
restart this services
        service iptables restart 2>&1 > /dev/null
        service network restart 2>&1 > /dev/null
        LCD_LIB=`@sbindir@/cpconfig   -ini   '\config\apppath\libhsmlcddrv.so'   -view`   ||
LCD_LIB=none
else
        LCD_LIB=none
fi
case $LCD_LIB  in
*libhsmlcddrv.so*)

delay_LCD()
{
        LANG= sleep 0.$(printf "%03d" $1)
```

```
        }

        clear_LCD()
        {
                [ x$print_lcd == x1 ] && echo -en "\0376\0376\001" > $LCD_PORT && delay_LCD 500
        }

        set_LCD()
        {
                stty                                    -F                                      $LCD_PORT
402:0:cfb:0:3:1c:7f:15:4:0:1:0:11:13:1a:0:12:f:17:16:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0
                stty -F $LCD_PORT speed $LCD_PORT_SPEED
                export print_lcd=1
                export reset_lcd=0
                clear_LCD
        }

        unset_LCD()
        {
                print_lcd=0
        }

        send_LCD()
        {
                if [ x$print_lcd == x1 ];then
                        [ x$reset_lcd == x1 ] && set_LCD
                        echo -en "$*" > $LCD_PORT
                        delay_LCD 300
                fi
        }

        clear_1_LCD()
        {
                send_LCD "\0376\0200                "
        }

        clear_2_LCD()
        {
                send_LCD "\0376\0300                "
        }

        send_LCD_1()
        {
                clear_1_LCD
                send_LCD "\0376\0200$*"
        }

        send_LCD_2()
        {
                clear_2_LCD
                send_LCD "\0376\0300$*"
        }

        dprint_LCD()
        {
                print_LCD_1 $*
                if [ x$2 == xcprocsp ];then
                        [ $1 == U ] && unset_LCD
                        [ $1 == D ] && set_LCD
                fi
        }
        ;;
        *libhsmlcddrvlcm.so*)
        delay_LCD()
        {
                LANG= sleep 0.$(printf "%03d" $1)
        }

        clear_LCD()
        {
                [ x$print_lcd == x1 ] && echo -en "\x4D\x0D" > $LCD_PORT && delay_LCD 500
        }

        set_LCD()
        {
                stty                                    -F                                      $LCD_PORT
402:0:8b9:0:3:1c:7f:15:4:0:1:0:11:13:1a:0:12:f:17:16:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0
                stty -F $LCD_PORT speed $LCD_PORT_SPEED
                export print_lcd=1
                export reset_lcd=0
                delay_LCD 300
```

```
        clear_LCD
}

unset_LCD()
{
        print_lcd=0
}

send_LCD()
{
        if [ x$print_lcd == x1 ];then
                echo -en "$*" > $LCD_PORT
                delay_LCD 300
        fi
}

clear_1_LCD()
{
        send_LCD "\x4D\x0C\x00\x10                "
}

clear_2_LCD()
{
        send_LCD "\x4D\x0C\x01\x10                "
}

print_LCD_1()
{
        local A="$*"
        clear_1_LCD
        send_LCD "\x4D\x0C\x00\x`printf "%02x" ${#A}`$A "
}

print_LCD_2()
{
        local A="$*"
        clear_2_LCD
        send_LCD "\x4D\x0C\x01\x`printf "%02x" ${#A}`$A "
}

dprint_LCD()
{
        print_LCD_1 $*
        if [ x$2 == xcprocsp ];then
                [ $1 == U ] && unset_LCD
                [ $1 == D ] && set_LCD
        fi
}
;;
*libhsmlcddrvse.so*)
delay_LCD()
{
        LANG= sleep 0.$(printf "%03d" $1)
}

clear_LCD()
{
        [ x$print_lcd == x1 ] && echo -en "\012\022\001" > $LCD_PORT && delay_LCD 500
}

send_LCD()
{
        if [ x$print_lcd == x1 ];then
                echo -en "$*" > $LCD_PORT
                delay_LCD 300
        fi
}

set_LCD()
{
        stty                                    -F                                      $LCD_PORT
402:0:cfd:0:3:1c:7f:15:4:0:1:0:11:13:1a:0:12:f:17:16:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0
        stty -F $LCD_PORT speed $LCD_PORT_SPEED
        export print_lcd=1
        export reset_lcd=0
        delay_LCD 300
        send_LCD "\012\022\070\014\001"
}

unset_LCD()
{
```

```
                print_lcd=0
        }

        clear_1_LCD()
        {
                send_LCD "\012\022\0200\010                \012\014"
        }

        clear_2_LCD()
        {
                send_LCD "\012\022\0300\010                \012\014"
        }

        print_LCD_1()
        {
                clear_1_LCD
                send_LCD "\012\022\0200\010$*\012\014"
        }

        print_LCD_2()
        {
                clear_2_LCD
                send_LCD "\012\022\0300\010$*\012\014"
        }

        dprint_LCD()
        {
                print_LCD_1 $*
                if [ x$2 == xcprocsp ];then
                        [ $1 == U ] && unset_LCD
                        [ $1 == D ] && set_LCD
                fi
        }
        ;;
        *libhsmlcddrvlcm2x16.so*)
        delay_LCD()
        {
                LANG= sleep 0.$(printf "%03d" $1)
        }

        flush_LCD()
        {
                true
        }

        send_LCD()
        {
                if [ x$print_lcd == x1 ];then
                        echo -en "$*" > $LCD_PORT
                        delay_LCD 300
                        flush_LCD
                fi
        }

        clear_LCD()
        {
                if [ x$print_lcd == x1 ]; then
                        send_LCD "\xB5\x01\x01\x53\x0A"
                        lcd_line1="                "
                        lcd_line2="                "
                fi
        }

        set_LCD()
        {
                stty                                    -F                                                      $LCD_PORT
402:0:8bd:0:3:1c:7f:15:4:1:0:0:11:13:1a:0:12:f:17:16:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0
                stty -F $LCD_PORT speed $LCD_PORT_SPEED
                export print_lcd=1
                export reset_lcd=0
                export lcd_line1="                "
                export lcd_line2="                "
                delay_LCD 300
                send_LCD "\xB5\x01\x01\x60\x17" #Reset LCD
                send_LCD "\xB5\x01\x01\x53\x0A" #Clear LCD
                send_LCD "\xB5\x01\x02\x52\x01\x0B" #Backlight on
        }

        unset_LCD()
        {
                print_lcd=0
```

```
        }

        print_LCD()
        {
                local A B cmd crc i
                if [ x$print_lcd == x1 ];then
                        A="$1"
                        B="$2"
                        [ ${#1} > 16 ] && A="${A:0:16}"
                        [ ${#2} > 16 ] && B="${B:0:16}"
                        for ((i=1; i <= 16-${#1} ; i++))
                        do
                                A="$A "
                        done
                        for ((i=1; i <= 16-${#2} ; i++))
                        do
                                B="$B "
                        done

                        lcd_line1="$A"
                        lcd_line2="$B"
                        A="$A$B"
                        #cmd=`echo -en "\xB5\x01\x22\x55\x02$A"`
                        cmd="\xB5\x01\x`printf "%02x" $[${#A} + 2]`\x55\x02$A"
                        crc=$(printf "\\\x%02x" $[ ( `echo -en "$cmd"|hexdump -e '"0" 37/1 "+%d"'` )
%256 ])
                        send_LCD "$cmd$crc"
                fi
        }

        clear_1_LCD()
        {
                print_LCD  " " "$lcd_line2"
        }

        clear_2_LCD()
        {
                print_LCD  "$lcd_line1" " "
        }

        print_LCD_1()
        {
                print_LCD  "$*" "$lcd_line2"
        }

        print_LCD_2()
        {
                print_LCD  "$lcd_line1" "$*"
        }

        dprint_LCD()
        {
                print_LCD_1 $*
                if [ x$2 == xcprocsp ];then
                        [ $1 == U ] && unset_LCD
                        [ $1 == D ] && set_LCD
                fi
        }
        ;;
        *)
        delay_LCD()
        {
            return 0
        }

        clear_LCD()
        {
            return 0
        }

        set_LCD()
        {
            return 0
        }

        unset_LCD()
        {
            return 0
        }

        send_LCD()
```

```
{
    return 0
}

clear_1_LCD()
{
    return 0
}

clear_2_LCD()
{
    return 0
}

print_LCD_1()
{
    return 0
}

print_LCD_2()
{
    return 0
}

dprint_LCD()
{
    return 0
}
;;
esac

unset check_func
check_func() {
  check_stop=0
  trap "check_stop=1"  2 3 15
  FTOTAL=$[ $# / 2 ]
  FNUM=0
  FPRINT=$[ 5 * ( ( $FNUM * 20 ) / $FTOTAL ) ]
  set_LCD
  print_LCD_1 "Checking..."
  print_LCD_2 " $FPRINT%"

  file=$1
  hash=$2
  shift 2
  CPVERIFY=@bindir@/cpverify
  echo $$ >$PID_FILE
  while test $check_stop = 0 && test -n "$*"
  do
    if $CPVERIFY $file $hash
    then
        O_FPRINT=$FPRINT
        FNUM=$[ $FNUM + 1 ]
        FPRINT=$[ 5 * ( ( $FNUM * 20 ) / $FTOTAL ) ]
        [ $FPRINT != $O_FPRINT ]  && print_LCD_2 " $FPRINT%"
    else
        print_LCD_2 "FAILURE!"
        logger -p user.err -t cpcsp.check "File $file corrupted!"
        sleep 10
        /sbin/halt -p
    fi
    file=$1
    hash=$2
    shift 2
  done
  print_LCD_2 "Done."
  rm $PID_FILE
  trap 2 3 15
}
```

Приложение 6. Скрипт read_parm – чтение параметров конфигурации ПАКМ

```
#!/bin/bash
dm()
{
        echo $1|(
                IFS='.'
                read w1 w2 w3 w4
                bits=0;
                for ((i=1;i<5;i++)) do
                        eval tmp=\$w$i
                        case $tmp in
                                        255) bits=$[ $bits + 8];;
                                        254) bits=$[ $bits + 7];;
                                        252) bits=$[ $bits + 6];;
                                        248) bits=$[ $bits + 5];;
                                        240) bits=$[ $bits + 4];;
                                        224) bits=$[ $bits + 3];;
                                        192) bits=$[ $bits + 2];;
                                        128) bits=$[ $bits + 1];;
                        esac
                done
                echo $bits
                )
}
echo `@sbindir@/cpconfig -ini "/network/$1/ip_address" -view`/`dm \`@sbindir@/cpconfig -ini "/network/$1/net_mask" -view\``
```

Приложение 7. Скрипт read_lcd – чтение параметров LCD панели

```
#!/bin/bash
#
# Этот файл содержит информацию, являющуюся
# собственностью компании Крипто Про.
#
# Любая часть этого файла не может быть скопирована,
# исправлена, переведена на другие языки,
# локализована или модифицирована любым способом,
# откомпилирована, передана по сети с или на
# любую компьютерную систему без предварительного
# заключения соглашения с компанией Крипто Про.
#

get_lcd_param()
{
        awk 'BEGIN{FS="=";LN=0;LCD_PORT_SPEED=0;my_sect=0}
        /^[[:blank:]]*\[lcdport\][[:blank:]]*$/ {
                my_sect=1;
                next;
        }
        /^[[:blank:]]*\[.*\][[:blank:]]*$/ {
                my_sect=0;
                next;
        }
        /^[[:blank:]]*Number[[:blank:]]*=[[:blank:]]*[[:digit:]]*[[:blank:]]*$/ {
                if (my_sect == 1){
                        LN=$2;
                        gsub("[[:blank:]]*","",LN);
                }
                next;
        }
        /^[[:blank:]]*Speed[[:blank:]]*=[[:blank:]]*[[:digit:]]*[[:blank:]]*$/ {
                if (my_sect == 1){
                        LCD_PORT_SPEED=$2;
                        gsub("[[:blank:]]*","",LCD_PORT_SPEED);
                }
        next;
        }
        END      {printf      "LN=%s;\nLCD_PORT_SPEED=%s;\n",LN,      LCD_PORT_SPEED;}'      <
@sysconfdir@/lcdport.ini

}
test -f @sysconfdir@/lcdport.ini || exit 1
eval `get_lcd_param`

if [ -n "$LN" ] && [ $LN -ge 1 ] && [ $LN -le 2 ]
then
        let "LN -= 1"
        LCD_PORT="/dev/ttyS${LN}"
else
        echo "Wrong LCD port number: '$LN'"
fi

if test -z "$LCD_PORT_SPEED" || test -n "`echo $LCD_PORT_SPEED|tr -d '[0-9]'`"
then
        echo "Wrong LCD port speed: '$LCD_PORT_SPEED'"
fi

echo "LCD_PORT=$LCD_PORT;"
echo "LCD_PORT_SPEED=$LCD_PORT_SPEED;"
```

Приложение 8. Файл автозагрузки rc.local

```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.
/etc/init.d/clock start
clear
gradm -E
echo "
 CCCCC  RRRRRR  Y     Y PPPPPP  TTTTTTTTT  OOOOO
C     C R     R Y     Y P     P T   T   T O     O
C       R     R  Y   Y  P     P     T     O     O
C       RRRRRR    YYY   PPPPPP      T     O     O  ====
C       R     R    Y    P           T     O     O
C     C R     R    Y    P           T     O     O
 CCCCC  R     R    Y    P           T      OOOOO

                   PPPPPP  RRRRRR    OOOOO
                   P     P R     R  O     O
                   P     P R     R  O     O
                   PPPPPP  RRRRRR   O     O
                   P       R     R  O     O
                   P       R     R  O     O
                   P       R     R   OOOOO"
```