

ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00096-06-ЛУ

**СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«ВАЛИДАТА КРИПТОСЕРВЕР» ВЕРСИЯ 4**

Описание применения

ВАМБ.00096-06 31 01

2020

Аннотация

Настоящий документ является описанием применения программного комплекса (ПК) ВАМБ.00096-06 «Средство криптографической защиты информации «Валидата Криптосервер» версия 4» (далее — СКЗИ «Валидата Криптосервер»), предназначенного для обеспечения защиты информации, передаваемой в режимах on-line и off-line между клиентскими рабочими местами и Центрами обработки информации автоматизированных систем эксплуатирующей организации с использованием системы управления сертификатами ключей проверки электронной подписи. В данном документе приведено описание структуры СКЗИ «Валидата Криптосервер», а также сведения о принципах его построения и функционирования.

Перед чтением настоящего описания следует ознакомиться с документацией ПК ВАМБ.00060-06 «СКЗИ «Валидата CSP» версия 6» и ПК ВАМБ.00077-06 ««Валидата Клиент» версия 4».

Содержание

1 НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ	4
1.1 Назначение СКЗИ «Валидата Криптосервер»	4
1.2 Область применения	4
2 СОСТАВ СКЗИ «ВАЛИДАТА КРИПТОСЕРВЕР»	6
3 УСЛОВИЯ ПРИМЕНЕНИЯ	7
3.1 Условия применения СКЗИ «Валидата Криптосервер»	7
3.2 Защита от НСД СКЗИ «Валидата Криптосервер»	7
3.3 Минимальные требования к покупным аппаратно-программным средствам	7
4 ОПИСАНИЕ КРИПТОГРАФИЧЕСКОГО СЕРВЕРА	9
4.1 Назначение криптографического сервера	9
4.2 Функциональная схема КС	9
4.3 Функции КС	10
4.4 Удалённый вызов процедур	11
5 ОПИСАНИЕ БИБЛИОТЕКИ ППИ КС	12
6 ОПИСАНИЕ АРМ УКС	13
6.1 Назначение АРМ УКС	13
6.2 Функции АРМ УКС	13
6.3 Реализация АРМ УКС	14
6.4 Администрирование и управление КС	15
6.5 Просмотр протоколов КС	15
7 ОПИСАНИЕ АРМ ФО	16
8 КОНФИГУРИРОВАНИЕ КРИПТОСЕРВЕРА	17
9 ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ	18
9.1 Само тестирование и контроль целостности ПО КС	18
9.2 Протоколирование работы КС	18
9.2.1 Модуль протоколирования КС	19
9.2.2 Перечень протоколируемых (регистрируемых) событий	19
9.2.3 Используемые конфигурационные параметры КС	20
9.2.4 Обработка протоколов КС	20
ПЕРЕЧЕНЬ СОКРАЩЕНИЙ	20
ПЕРЕЧЕНЬ РИСУНКОВ	22

1 НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Назначение СКЗИ «Валидата Криптосервер»

ПК ВАМБ.00096-06 «Средство криптографической защиты информации «Валидата Криптосервер» версия 4» (далее по тексту - СКЗИ «Валидата Криптосервер») предназначен для:

- предоставления (в качестве сервера) криптографических функций прикладным серверам, клиентским рабочим местам, обращающимся к нему по протоколу удаленного вызова процедур (DCE RPC);
- контроля целостности, подтверждения авторства, неотрекаемости от авторства и обеспечения конфиденциальности электронных документов, передаваемых в режимах on-line и off-line между клиентскими рабочими местами и Центрами обработки информации (ЦОИ) автоматизированных систем (АС) эксплуатирующей организации;
- использования криптографических процедур, реализованных в ПК ВАМБ.00060-06 «Средство криптографической защиты информации «Валидата CSP» версия 6»;
- обеспечения работы криптографического сервера (далее - криптосервер или КС) в среде операционной системы (ОС) Windows как на одной ЭВМ, так и на нескольких ЭВМ, объединенных в кластер балансировки сетевой нагрузки (NLB);
- обеспечения удаленной загрузки ключевой информации в КС.

1.2 Область применения

СКЗИ «Валидата Криптосервер» применяется для защиты информации, передаваемой в режимах on-line и off-line между клиентскими рабочими местами и ЦОИ АС эксплуатирующей организации и обеспечивает:

- контроль целостности, подтверждение авторства и конфиденциальность электронных документов;
- применение CMS/PKCS#7 формата защищенных (подписанных и зашифрованных) данных;
- применение в АС эксплуатирующей организации квалифицированной ЭП и квалифицированного сертификата ключей проверки ЭП (далее - квалифицированный сертификат) в соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи», требованиями приказов ФСБ РФ от 27.12.2011 №795 и №796;
- функционирование на ЭВМ с 32-битными (x86) и 64-битными (x64) архитектурами, а также на виртуальных машинах (ВМ), находящихся под управлением гипервизоров Microsoft Hyper-V и VMware ESXi.

Примечание — В том случае, когда в сертификате ключа проверки ЭП установлена область использования ключа «Согласование ключей», ключ проверки ЭП сертификата может использоваться в качестве открытого ключа шифрования, а соответствующий ему ключ ЭП — в качестве закрытого

ключа шифрования.

2 СОСТАВ СКЗИ «ВАЛИДАТА КРИПТОСЕРВЕР»

В состав СКЗИ «Валидата Криптосервер» входят следующие ПК и компоненты:

- ПК ВАМБ.00096-06 12 01 «Криптографический сервер»;
- ПК ВАМБ.00096-06 12 02 «Автоматизированное рабочее место управления криптографическим сервером» (далее — АРМ УКС);
- ПК ВАМБ.00096-06 12 03 «Автоматизированное рабочее место формирования отчётов» (далее — АРМ ФО);
- ВАМБ.00096-06 12 04 «Библиотека прикладного программного интерфейса криптографического сервера для C/C++»;
- ВАМБ.00096-06 12 05 «Конфигурация криптографического сервера» (далее — программа «Конфигурация Криптосервера»);
- ВАМБ.00096-06 12 06 «Монитор криптографического сервера» (далее — программа «Монитор Криптосервера»);
- ВАМБ.00096-06 12 07 «Программа тестирования аппаратно-программных средств криптографического сервера»;
- ВАМБ.00096-06 12 08 «Библиотека прикладного программного интерфейса криптографического сервера для платформ “Java” и “IBM WebSphere Application Server”».

Далее библиотеки прикладного программного интерфейса криптографического сервера для C/C++ и для платформ “Java” и “IBM WebSphere Application Server” будут упоминаться как библиотека ППИ.

3 УСЛОВИЯ ПРИМЕНЕНИЯ

3.1 Условия применения СКЗИ «Валидата Криптосервер»

СКЗИ «Валидата Криптосервер» используется совместно с ПК ВАМБ.00077-06 «“Валидата Клиент” версия 4» и ПК ВАМБ.00060-06 «СКЗИ «Валидата CSP» версия 6».

3.2 Защита от НСД СКЗИ «Валидата Криптосервер»

Защита аппаратного и программного обеспечения от несанкционированного доступа (НСД) при установке и использовании СКЗИ «Валидата Криптосервер» является составной частью общей задачи обеспечения безопасности информации в системе, в состав которой входит СКЗИ «Валидата Криптосервер».

При организации защиты СКЗИ «Валидата Криптосервер» следует руководствоваться рекомендациями, изложенными в документах:

- ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности»;
- ВАМБ.00077-06 93 01 «“Валидата Клиент” версия 4. Руководство администратора информационной безопасности»;
- ВАМБ.00096-06 93 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство администратора информационной безопасности».

При функционировании СКЗИ «Валидата Криптосервер» в виртуальной среде следует дополнительно руководствоваться рекомендациями, изложенными в документе ВАМБ.00060-06 93 03 «СКЗИ «Валидата CSP» версия 6. Функционирование в виртуальной среде. Руководство администратора информационной безопасности».

Парольная аутентификация в ОС Windows на ЭВМ и серверах с установленной СКЗИ «Валидата Криптосервер» должна выполняться в соответствии с требованиями документа ВАМБ.00096-06 93 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство администратора информационной безопасности».

3.3 Минимальные требования к покупным аппаратно-программным средствам

ЭВМ, на которых предполагается эксплуатация СКЗИ «Валидата Криптосервер», должны удовлетворять требованиям по защите информации от утечки по техническим каналам в соответствии с моделью угроз, принятой в АС эксплуатирующей организации.

Минимальные требования к аппаратно-программной среде функционирования СКЗИ «Валидата Криптосервер»:

- персональный компьютер (ЭВМ) с объемом жесткого диска и оперативной памяти, удовлетворяющим минимальным требованиям для установленной на данной ЭВМ версии ОС Microsoft Windows;
- при необходимости — сетевой адаптер и устройство резервного копирования информации на отчуждаемый носитель (например, CD-RW);

- средство защиты информации от несанкционированного доступа (СЗИ от НСД) — при необходимости;
- ОС семейства Windows.

Следует использовать ЭВМ с Intel-совместимым процессором с микроархитектурой Intel Core 2 или более новым, поддерживающим расширения инструкций SSE2, SSE3, SSSE3. Для повышения производительности рекомендуется использовать процессор с поддержкой расширений инструкций SSE4.1, AVX.

Примечания

1 СКЗИ «Валидата Криптосервер» может работать как в 32-битных (x86), так и 64-битных (x64) ОС Windows (выбор производится пользователем при установке СКЗИ «Валидата Криптосервер» на ЭВМ).

2 Необходимость использования СЗИ от НСД при установке и эксплуатации СКЗИ «Валидата Криптосервер» зависит от исполнения СКЗИ «Валидата Криптосервер».

4 ОПИСАНИЕ КРИПТОГРАФИЧЕСКОГО СЕРВЕРА

4.1 Назначение криптографического сервера

Программный исполняемый модуль «Криптографический сервер» (сервис КС) представляет собой модуль, работающий в режиме сервиса под управлением ОС Windows. Сервис КС предоставляет прикладной программный интерфейс к криптографическим функциям КС, взаимодействует с АРМ УКС и ведет протокол своей работы. Все необходимые конфигурационные параметры сервис КС считывает из реестра ОС Windows.

В СКЗИ «Валидата Криптосервер» обеспечивается возможность:

- удаленной загрузки ключей ЭП в КС, при этом установка ключевых носителей выполняется непосредственно на АРМ УКС. Удаленная загрузка ключей ЭП с АРМ УКС в КС может выполняться как одновременно на все КС кластера, так и по отдельности на каждый КС (или группу КС) из состава кластера (по выбору администратора);
- удаленного (с АРМ УКС) выполнения процедуры плановой смены ключей ЭП и сертификатов сессий КС.

При запуске КС загрузка ключа ЭП сессии администрирования (используемого для создания защищенного канала между АРМ УКС и КС) выполняется только локально, т.е. непосредственно с ключевого носителя в интерактивном режиме. При этом плановая смена ключа ЭП сессии администрирования может выполняться удаленно. Проведение подряд двух (и более) плановых смен ключа ЭП сессии администрирования удаленно не допускается.

4.2 Функциональная схема КС

Функциональная схема КС представлена ниже (Рисунок 1).

Используемые библиотеки:

- библиотека функций электронной подписи и шифрования, библиотека поддержки считывателей ключей электронной подписи и/или закрытых ключей шифрования и датчиков случайных чисел и программа конфигурации;
- библиотека прикладного программного интерфейса КС (Remote Procedure Call).

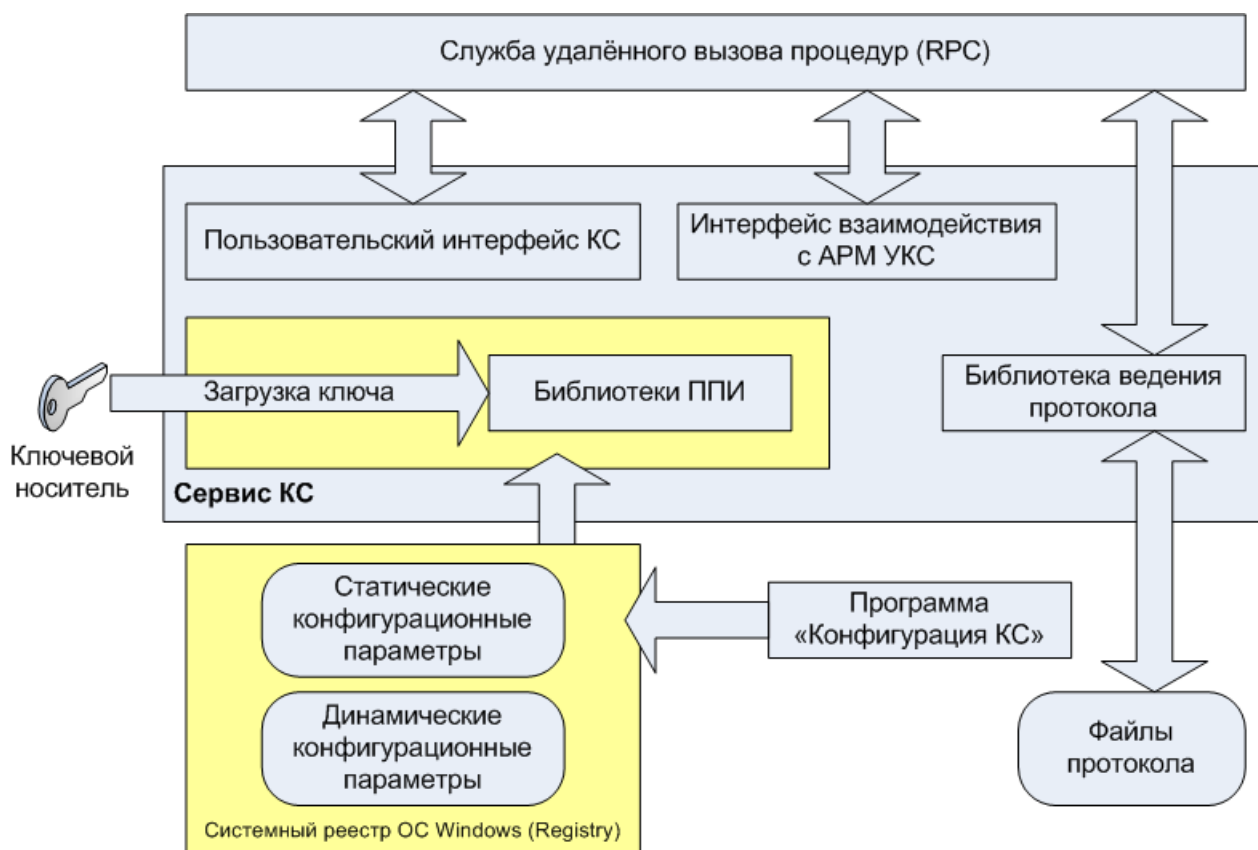


Рисунок 1 – Функциональная схема КС

4.3 Функции КС

КС выполняет следующие функции:

- преобразование форматов сообщений с отдельной электронной подписью (ЭП) и форматов сообщений с присоединённой ЭП;
- вычисление хэш-значения данных, создание и проверку ЭП для значения хэш-функции данных (для дальнейшего преобразования в произвольный формат и из произвольного формата);
- аутентификацию и авторизацию клиентских прикладных процессов для возможности создания ими ЭП (в том числе при выполнении переподписания данных между сессиями КС);
- создание и проверку ЭП файла и блока данных для авторизованных клиентских прикладных процессов;
- блокирование обработки (для каждой из сессий КС) вызовов клиентских прикладных процессов (возможность);
- добавление в файл журнала работы КС сообщения об ошибке поиска сертификата (ошибка «Сертификат не найден») с указанием содержимого шаблона сертификата, по которому производился поиск;
- создание и проверку ЭП (в присоединённом и отсоединённом форматах) файлов;
- зашифрование и расшифрование файлов;

- потоковое зашифрование и расшифрование блоков памяти;
- потоковое создание и проверку ЭП (в присоединённом и отсоединённом форматах) блоков памяти;
- проверку ЭП документов (с возможностью последующего удаления ЭП), подписанных в формате CMS/PKCS#7;
- создание и добавление ЭП к документам в формате CMS/PKCS#7;
- загрузку ключа сессии администрирования и инициализацию датчика случайных чисел без участия пользователя («тихая» инициализация);
- анонимное зашифрование/расшифрование в формате CMS/PKCS#7 с использованием множества сертификатов получателей;
- реализацию механизма простановки и проверки штампов времени ЭП в соответствии с RFC 3161;
- управление настройками авторизации КС с АРМ УКС (добавление, удаление, смена пароля пользователя КС) для каждой сессии в пределах кластера КС;
- получение и изменение уровня протоколирования КС (или кластера КС) с АРМ УКС;
- взаимодействие с сетевым справочником сертификатов эксплуатирующей организации в части построения цепочки сертификации, обновления списка аннулированных сертификатов (САС) и поиска сертификатов пользователей;
- изменение размера диалогового окна программ «Монитор Криптосервера» и «Конфигурация Криптосервера»;
- сортировку по имени сессии в закладке «Сессии» программы «Конфигурация Криптосервер» при выполнении настройки КС;
- удаленную загрузку ключей ЭП с ключевых носителей.

4.4 Удалённый вызов процедур

Серверная часть программного обеспечения КС СКЗИ «Валидата Криптосервер» обеспечивает интерфейс сопряжения КС с прикладным программным обеспечением ЦОИ.

КС допускает возможность масштабирования, т.е. возможность работы КС на нескольких ЭВМ, обеспечивая равномерное распределение запросов, поступающих от прикладного программного обеспечения, и увеличение пропускной способности КС, а также его резервирование.

5 ОПИСАНИЕ БИБЛИОТЕКИ ППИ КС

Библиотека прикладного программного интерфейса криптографического сервера для ОС Windows является составной частью СКЗИ «Валидата Криптосервер» и обеспечивает функции аутентификации в соответствии с рекомендациями Х.509, ЭП по ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 и шифрования по ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015, ГОСТ 28147-89. Доступ к функциям КС осуществляется посредством библиотек API КС, предназначенных для использования в ОС Windows. Реализация функций КС, доступных посредством библиотек API, основана на использовании ПК ВАНБ.00060-06 «СКЗИ «Валидата CSP» версия 6».

Библиотеки API КС обеспечивают обращение к следующим функциям КС:

- зашифрованию и расшифрованию файлов;
- зашифрованию и расшифрованию блоков памяти;
- подписи файла;
- подписи области памяти;
- проверке ЭП файла;
- проверке ЭП области памяти;
- удалению подписи;
- выработке хэш-значения для файла;
- выработке хэш-значения для области памяти;
- выбору и инициализации работы с КС;
- аутентификации при работе КС;
- преобразованию отдельной и совмещенной ЭП;
- выработке случайного числа заданной длины.

Ошибки, возвращаемые библиотекой API КС, приведены в документах ВАНБ.00096-06 33 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство программиста» и ВАНБ.00096-06 33 02 «СКЗИ «Валидата Криптосервер» версия 4. Библиотека прикладного программного интерфейса криптографического сервера для платформ “Java” и “IBM WebSphere Application Server”. Руководство программиста».

6 ОПИСАНИЕ АРМ УКС

6.1 Назначение АРМ УКС

АРМ УКС устанавливается на отдельный компьютер под ОС Windows, подключенный через локальную сеть ко всем КС. Требования к соединению АРМ УКС с КС приведены в документе ВАМБ.00096-06 93 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство администратора информационной безопасности».

АРМ УКС предназначено для работы администратора КС. АРМ УКС позволяет администратору выполнять мониторинг текущего состояния всех КС, управлять всеми КС и просматривать их протоколы, проводить удаленную загрузку ключевой информации. Для автоматизации подготовки отчетов по работе КС используется АРМ ФО.

6.2 Функции АРМ УКС

АРМ УКС обеспечивает поддержку функций КС и выполнение следующих основных функций:

- одновременной загрузки в заданную сессию КС как группы сертификатов из одной директории, так и каждого сертификата по отдельности;
- одновременной загрузки в заданную сессию КС как группы САС, так и каждого САС по отдельности;
- одновременной загрузки всех сертификатов и САС в заданную сессию КС (или кластера КС) из указанной папки;
- выгрузки информации о сертификатах и САС из одной криптографической сессии одного узла КС в текстовые файлы с разбиением по издателю;
- загрузки обновлений, полученных из удостоверяющего центра, в КС;
- запоминания последнего пути к папке, из которой выполнялась загрузка сертификатов, САС или обновлений;
- запуска и остановки заданной сессии КС (или кластера КС), за исключением сессии администрирования;
- плановой смены ключей ЭП и сертификатов КС (с АРМ УКС), которая должна осуществляться как на всех КС кластера одновременно, так и по отдельности на каждом КС (или группе КС) из состава кластера (по выбору пользователя);
- фильтрации записей по типу событий протокола событий просматриваемого журнала КС;
- сортировки в диалоговом окне АРМ УКС и экспорта в текстовый файл списка сертификатов, загруженных в заданную сессию КС;
- просмотра состояния узлов кластера КС (только для NLB-кластера);
- ввода (вывода) узла КС в состав кластера (только для NLB-кластера);
- вывода на экран сообщения о невозможности записи события в системный журнал с предложением вызова администратора. Работа АРМ УКС при этом не блокируется;
- удаления из сессии КС (кластера КС) всех сертификатов пользователей (кроме сертификатов Центра сертификации и Центра регистрации), которые ан-

нулированы/прекратили действие на момент выполнения команды;

- просмотра загруженных сертификатов как всего кластера КС, так и отдельных КС из состава кластера, с возможностью фильтрации;
- добавления и удаления IP-адресов компьютеров, которым разрешен доступ к заданной сессии КС (или кластера КС), с возможностью смены данных аутентификации для ранее добавленных IP-адресов;
- отображения сертификатов заданной сессии КС (кластера КС), которые находятся в САС и время аннулирования/прекращения действия которых уже наступило на момент выполнения команды;
- отображения сертификатов заданной сессии КС (кластера КС), срок действия ключа ЭП которых уже истек на момент выполнения команды;
- визуального отображения хода загрузки сертификатов и САС, отображения процента выполнения загрузки, количества загруженных объектов, общего количества загружаемых объектов, времени начала и окончания загрузки;
- сортировки сессий в окне отображения списка сессий (по имени сессии, имени КС, номеру ключа ЭП, имени владельца, путям к справочникам), а также отображения состояния опции «Принудительно кэшировать сертификаты для шифрования при старте сессии» для каждой сессии;
- детализации информации по коду ошибки — по двойному щелчку «мышью» на строке с ошибкой просматриваемого журнала КС или по введенному коду ошибки из меню АРМ УКС;
- при обнаружении ошибки в журнале (полном или ошибок) КС в протокол работы АРМ УКС записывать данный код в поле «Код события». Отображать информационное окно при обнаружении ошибки в журнале КС или при обнаружении изменения состояния NLB-кластера КС (в случае его использования);
- отображения и очистки статистики для заданной сессии КС (кластера КС), для всех сессий КС (кластера КС);
- получения и изменения уровня протоколирования КС (или кластера КС);
- возможности блокирования обработки пользовательских запросов для заданной сессии КС (или кластера КС) с выводом на экран диалогового окна для подтверждения выполняемой операции.

6.3 Реализация АРМ УКС

Интерактивная диалоговая программа АРМ УКС позволяет запускать для каждого КС отдельное окно мониторинга и управления, которое отображает текущее состояние КС, показывает его протоколы и позволяет управлять этим КС. Текущее состояние и просмотр протокола обновляется автоматически для каждого КС через заданный в конфигурации период времени.

При кластерной реализации криптосервера АРМ УКС обеспечивает:

- просмотр состояния узлов кластера (NLB) КС;
- ввод узла КС в состав кластера (NLB);
- вывод узла КС из состава кластера (NLB).

АРМ УКС обеспечивает просмотр загруженных сертификатов, как всего кла-

стера КС, так и отдельных КС из состава кластера, с возможностью фильтрации по полям сертификата.

6.4 Администрирование и управление КС

АРМ УКС выдаёт (с помощью механизма RPC) для каждого КС команды: блокировки и разблокировки сессий КС, просмотра, добавления, удаления сертификатов, обновления списка аннулированных сертификатов в сессиях КС.

6.5 Просмотр протоколов КС

Администратор АРМ УКС просматривает события КС. Детализация протокола и перечень КС указывается администратором. Обновление протокола КС на экране выполняется как автоматически, так и после нажатия кнопки «**Обновить**».

7 ОПИСАНИЕ АРМ ФО

АРМ ФО функционирует совместно с АРМ УКС и выполняет следующие функции:

- преобразование журнала (полного или ошибок — по выбору пользователя) КС в формат базы данных;
- отображение результата преобразования протокола КС в виде таблицы в главном окне программы;
- разбор, просмотр и анализ преобразованного журнала (полного или ошибок — по выбору пользователя);
- формирование отчёта о выполнении криптографических операций КС за интервал времени до 24 часов по всем пользователям ключевых документов, от имени которых эти операции производились;
- осуществление возможности фильтрации событий в таблице встроенными фильтрами по задаваемому интервалу времени, по задаваемому имени пользователя, по задаваемому наименованию организации и по ошибочным завершениям криптографических функций (каждым фильтром в отдельности и в их комбинациях);
- ввод и запуск на выполнение запроса на языке SQL;
- ограничение импортируемых событий по уровню (порогу) важности события при преобразовании (импорте) протоколов в базу;
- возможность сохранения сформированного отчёта и создаваемых запросов на языке SQL, а также сохранения результатов выполнения SQL-запросов и встроенных фильтров;
- одновременная загрузка журналов (полных или ошибок — по выбору пользователя) со всех узлов кластера КС и предоставление возможности просмотра протоколов на русском языке с возможностью фильтрации.

8 КОНФИГУРИРОВАНИЕ КРИПТОСЕРВЕРА

Установка и настройка КС производится в соответствии с документом ВАМБ.00096-06 91 01 «СКЗИ «Валидата Криптосервер» версия 4. Руководство по установке и настройке».

9 ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ

9.1 Самотестирование и контроль целостности ПО КС

Самотестирование и контроль целостности ПО КС обеспечивают:

- программа тестирования аппаратно-программных средств КС;
- программа контроля целостности ПО из состава ПК ВАМБ.00060-06 «СКЗИ «Валидата CSP» версия 6».

Программа тестирования аппаратно-программных средств КС предназначена для выполнения периодической проверки корректности работы КС. Процедура самотестирования обязательно выполняется один раз при загрузке КС, а затем периодически - через временной интервал, указанный в конфигурации КС. При обнаружении ошибки при проведении самотестирования КС записывает сообщение об этой ошибке в протокол КС и завершает свою работу. Состав тестируемых функций и описание программы приведено в документе ВАМБ.00096-06 92 01 «СКЗИ «Валидата Криптосервер» версия 4. Программа тестирования аппаратно-программных средств криптографического сервера. Руководство пользователя».

Программа контроля целостности ПО предназначена для контроля состава и целостности ПО КС. Программа контроля целостности ПО функционирует в среде ОС Windows.

Контроль целостности обеспечивается за счет использования криптографических функций, а именно вычисления хэш-функции по алгоритму ГОСТ Р 34.11-2012.

Для обеспечения контроля предусматривается создание списка контролируемых файлов с вычисленными значениями хэш-функции для каждого файла и последующая проверка значений хэш-функции для всех файлов из списка.

Описание работы программы контроля целостности приведено в документах ВАМБ.00060-06 92 01 «СКЗИ «Валидата CSP» версия 6. Программа контроля целостности. Руководство пользователя» и ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности».

Программа контроля целостности ПО не контролирует целостность самой себя и списка контроля целостности ПО. Для обеспечения сохранности этих двух файлов в неизменном виде необходимо хранить их на отчуждаемом носителе (например, диске) или выполнять проверку по сети с ЭВМ с установленным АРМ УКС.

9.2 Протоколирование работы КС

В состав ПО КС входит модуль протоколирования выполнения функций КС.

В составе КС модуль протоколирования предназначен для фиксации (согласно нормативным документам эксплуатирующей организации) всех действий, выполняемых КС. Результат работы модуля протоколирования записывается в файлы протокола, которые затем могут быть обработаны на АРМ ФО.

9.2.1 Модуль протоколирования КС

Протоколирование осуществляется загружаемым модулем (библиотекой) записи протоколов КС в файлы на внешнем носителе, который взаимодействует с модулями серверной подсистемы, используя механизмы межпотокowego взаимодействия (ИТС) ОС, что позволяет отделить выполнение операций протоколирования от основного потока запросов пользователей, обрабатываемых КС. На каждом узле КС должно быть запущено по одному потоку записи протоколов, который преобразует записи протоколируемых событий из внутреннего формата во внешнее представление. Разграничение доступа к файлам протоколов для пользователей (процессов) в операционной системе выполняется совместно системным администратором и администратором безопасности средствами операционной системы.

Модуль протоколирования поддерживает следующие файлы протоколов:

- файл протокола элементарных событий;
- файл протокола ошибок;
- файл протокола отладочной информации.

Файлы протоколов создаются ежедневно и содержат суточную информацию. Создание файлов происходит в момент инициализации потока записи протоколов или в момент смены даты (в полночь по Гринвичу). Если происходит перезагрузка криптографической системы несколько раз в сутки, то используется текущий файл протоколов в режиме добавления записей. Имена файлов выглядят следующим образом: YYYYMMDD.CSV,

где

YYYY - год создания файла;

MM - месяц создания файла;

DD - число месяца создания файла.

В файлах протоколов содержится следующая информация:

- время события;
- мнемонический код события;
- сетевой адрес (имя) КС;
- источник события;
- вызванная функция;
- статус завершения события (числовой код);
- сетевой адрес клиента, вызвавшего событие;
- статус завершения события (числовой код);
- адрес прикладного процесса;
- идентификатор сертификата (или ключа);
- информация справочного характера: число запросов, количество обработанной информации.

9.2.2 Перечень протоколируемых (регистрируемых) событий

Протоколируемые (регистрируемые) события:

- запуск КС;
- остановка КС;
- команды управления КС;
- подключение пользовательского процесса к КС;
- выполнение ЭП;
- проверка ЭП;
- выполнение хэширования;
- выполнение шифрования/расшифрования;
- отключение пользовательского процесса;
- события диагностики (при задании в конфигурационном файле).

В некоторых случаях информация о событиях КС дополнительно заносится в системный журнал ОС Windows. Для корректной записи протокола работы КС в системный журнал ОС Windows администратору необходимо увеличить размер файла протокола до 32 МБ.

9.2.3 Используемые конфигурационные параметры КС

Модуль протоколирования использует следующие конфигурационные параметры КС:

- каталог хранения протоколов;
- уровень протоколирования для каждого типа протокола;
- режим работы модуля протоколирования (асинхронный или транзакционный ввод/вывод).

9.2.4 Обработка протоколов КС

Разбор и обработка протоколов КС осуществляется АРМ ФО. АРМ ФО взаимодействует с модулями серверной подсистемы, используя механизмы сетевого файлового взаимодействия ОС Windows.

Также АРМ ФО обеспечивает возможность просмотра администратором АРМ УКС событий, происходящих в КС за промежуток времени, указанный в конфигурации. Детализация протокола и перечень событий КС указывается администратором.

Работа администратора на АРМ ФО и возможности, доступные ему при просмотре протоколов, описаны в документе ВАМБ.00096-06 95 01 «СКЗИ «Валидата Криптосервер» версия 4. АРМ УКС. АРМ ФО. Руководство администратора».

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ УКС	Автоматизированное рабочее место управления криптографическим сервером
АРМ ФО	Автоматизированное рабочее место формирования отчётов
АС	Автоматизированная система
КС	Криптографический сервер
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОС	Операционная система
ПК	Программный комплекс
ПО	Программное обеспечение
ППИ	Прикладной программный интерфейс
САС	Список аннулированных сертификатов
СКЗИ	Средство криптографической защиты информации
ЦОИ	Центр обработки информации
ЭВМ	Электронная вычислительная машина
ЭП	Электронная подпись

ПЕРЕЧЕНЬ РИСУНКОВ

1	Функциональная схема КС	10
---	-----------------------------------	----

[illegible][illegible]