АО «Концерн ГРАНИТ»

Россия, 119019, г. Москва, ул. Гоголевский бульвар, д. 31, стр. 2, эт. 2, пом.1
т. +7 495 642 97 42, ф. +7 499 558 15 29
office@granit-concern.ru, granit-concern.ru

QUANTUM SECURE STORAGE

Описание функциональных характеристик

Листов 14

2023

Акционерное общество «Концерн ГРАНИТ»
ОКПО 78089277 к/с 30101810400000000225, БИК 044525225
, ОГРН 1055011347093, ИНН/КПП 5003056699/770401001
р/с 40702810738000014569 в ПАО «Сбербанк России»,

АННОТАЦИЯ

Настоящий документ содержит сведения по задачам и функциям «Quantum Secure Storage» (далее QSS, Программа), предназначенной для криптографической защиты конфиденциальности и целостности информации, в том числе для защиты персональных данных. Кроме того, в документе содержится информация по техническим требованиям, входным и выходным данным.

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ

1.1. Наименование продукта

Программа, предназначенная для криптографической защиты конфиденциальности и целостности информации, в том числе для защиты персональных данных, «Quantum Secure Storage» (далее по тексту – QSS, Программа, Программный комплекс).

1.2. Краткое описание продукта

Программный комплекс представляет собой программный продукт, написанный на языке Rust, с использованием встроенной библиотеки, реализующей криптографические алгоритмы. СКЗИ обеспечивает возможность осуществления следующих операций с пользовательскими данными: шифрование и расшифрование (через UNIX сокеты и разделяемую память), вычисление хеш-кода, формирование электронной подписи, а так же обеспечивает возможность выработки общих ключей.

В качестве интерфейса взаимодействия использованы разделяемая библиотека и административная утилита. Разделяемая библиотека предоставляет программный интерфейс и берёт на себя сериализацию, пересылку, принятие и десериализацию пользовательских сообщений, передаваемых по UNIX сокету, а также установление соединений по UNIX сокету. Административная утилита предоставляет консольный интерфейс для администраторов QSS.

2. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

Разработанное СКЗИ QSS предназначено для криптографической защиты (обеспечение конфиденциальности и целостности) информации на территории Российской Федерации в системах защиты информации, не содержащей сведений, составляющих государственную тайну. Программный комплекс выполняет криптографические операции в соответствии с требованиями следующих стандартов и рекомендаций по стандартизации ТК26:

- ГОСТ 34.10-2018 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;
- ГОСТ 34.11-2018 «Информационная технология. Криптографическая защита информации. Функция хэширования»;
- ГОСТ 34.12-2018 «Информационная технология. Криптографическая защита информации. Блочные шифры»;
- ГОСТ 34.13-2018 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров»;
- Р 1323565.1.026–2019 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование»;
- Р 50.1.111-2016 «Информационная технология. Криптографическая защита информации. Парольная защита ключевой информации»;
- Р 50.1.113-2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования».

ПК СКЗИ QSS не предназначен для защиты речевой информации.

Реализована возможность совместной работы с системой управления базами данных «Квант-гибрид».

3. СОСТАВ ФУНКЦИЙ

Программный комплекс обладает набором следующих функциональных характеристик:

1) аутентификация при установлении административного соединения по паролю и дополнительной случайной информации (с опциональным её хранением на внешнем носителе) с использованием алгоритма выработки ключа из пароля по алгоритму «PBKDF2» в соответствии с «Р 50.1.111-2016»;
2) диверсификация ключей с использованием алгоритма KDF_GOSTR3411_2012_256 в соответствии «Р 50.1.113-2016»;
3) аутентифицированное шифрование/расшифрование данных (с использованием разделяемой памяти/ через сокеты) в соответствии с «Р 1323565.1.026—2019» (алгоритмом «Кузнечик» в соответствии «ГОСТ 34.12—2018»);
4) формирование и проверка электронной подписи в соответствии с «ГОСТ 34.10-2018» и параметрами эллиптических кривых, определёнными в «Р 1323565.1.024-2019»;
5) формирование общих ключей по алгоритму «VKO» в соответствии с «Р 50.1.113-2016»;
6) вычисление хеш-суммы от блока данных в соответствии с «ГОСТ 34.11-2018»;
7) управление ключевой информацией;
8) хранение ключей в зашифрованном и имитозащищенном виде в долговременном хранилище (диске);
9) стирание из оперативной памяти ключевой информации после окончания её использования путем перезаписи псевдослучайной последовательностью;
10) защита ключевой информации в оперативной памяти путем ее маскирования;
11) контроль жизненного цикла ключа: запрет техническими средствами на использование ключа для шифрования и формирования цифровой подписи после истечения времени его жизни (не может составлять более 15 месяцев) и

заблаговременное уведомление администраторов о необходимости смены ключа;

12) управление пользователями.

4. РЕАЛИЗОВАННЫЕ МЕРЫ ЗАЩИТЫ

В Программном комплексе реализованы следующие меры защиты.

- Ролевая модель.

  Предусмотрены роли администратора и пользователя. Доступ ограничивается средствами операционной системы (принадлежит ли пользователь к нужной группе в ОС или нет). Для учетных записей администратора предусмотрены расширенные средства защиты.
- Ограничение на одновременное подключение нескольких администраторов к системе.
- Возможность задавать период неактивности администратора, по истечении которого соединение с администратором будет закрыто.
- Идентификация и аутентификация субъектов доступа.

  Для аутентификации используется символьный периодически изменяющийся пароль из не менее чем 8 символов ASCII. Пароль должен содержать минимум по одному символу в верхнем и нижнем регистрах и минимум один символ пунктуации. Максимальное время жизни пароля 6 месяцев.
- Очистка памяти.

  В СКЗИ осуществляется перезапись участков оперативной памяти, хранящих ключевую, криптографически опасную и чувствительную информацию, ПСП, выработанной ПДСЧ.
- Электронный журнал регистрации событий.

  В СКЗИ QSS осуществляется регистрация входа/выхода субъектов доступа QSS, всех административных действий в СКЗИ и функций управления ключевой информацией. В параметрах регистрации указываются время и дата регистрируемого события и его описание.
- Контроль целостности.

  СКЗИ проверяет целостность библиотеки для доступа к ФДСЧ, целостность бинарных файлов СКЗИ, целостность рабочих ключей. При обнаружении нарушения контроля целостности СКЗИ вносит

соответствующую запись в электронный журнал регистрации событий и прекращает работу.

- Контроль работоспособности.

  В СКЗИ имеются функции регламентного и периодического контроля, проверяющие работоспособность криптографических алгоритмов. При обнаружении нарушения работоспособности криптографических алгоритмов СКЗИ вносит соответствующую запись в электронный журнал регистрации событий и прекращает работу.

- Контроль последовательностей, выработанных ДСЧ.

  В СКЗИ имеется функция регламентного контроля, проверяющая ДСЧ: если тестовая последовательность не прошла проверку, то генерируется новая последовательность и тесты прогоняются заново, после нескольких неуспешных попыток ошибка возвращается пользователю. Алгоритм из нескольких итераций снижает риски ложных результатов. При обнаружении ошибок в рамках данных проверок СКЗИ вносит соответствующие записи в электронный журнал регистрации событий и прекращает работу.

  В СКЗИ имеется функция статистического контроля последовательностей, выработанных ДСЧ, которая применяется для любой сгенерированной последовательности. При обнаружении ошибок в рамках данных проверок СКЗИ вносит соответствующие записи в электронный журнал регистрации событий.

Реализованные меры указаны при использовании QSS в качестве функционально законченного изделия. При использовании QSS в качестве встраиваемого решения, прикладное ПО, вызывающее QSS, должно дополнительно реализовывать собственный стартовый и регламентный контроль целостности.

5. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Взаимодействие с системой предусмотрено через программный интерфейс (API) и через консольный интерфейс, путем ручного ввода команд. В качестве входных данных предусмотрены команды из указанного в документе Руководство системного программиста списка команд, в качестве атрибутов могут быть использованы файлы для расшифрования и зашифрования информации, а также файлы, используемые в качестве криптографической соли. В качестве выходных данных являются сообщения - ответы программы, расшифрованные и зашифрованные данные, информация в журналах регистрации событий.

6. УСЛОВИЯ ПРИМЕНЕНИЯ

Программа функционирует на ПЭВМ. В таблице (Таблица 1) представлены требования к Программе и программному обеспечению.

Таблица 1 - Требования к Системе

№ п/п	Техническое средство	Требования
1	Процессор	Процессоры архитектуры (только для 64 битных CPU): x86-64 с тактовой частотой 2 ГГц
2	Оперативная память	Не менее 4 ГБ оперативной памяти
3	Жесткий диск	Не менее 1 ГБ (не учитывая требования ОС)

QSS функционирует на всех вышеуказанных архитектурах в среде ОС на базе Linux:

- CentOS 7 и 8;
- РЕД ОС 7;
- ROSA Enterprise Linux Server (RELS) 7;
- Альт 8 СП;
- Альт Сервер 9;
- Fedora 33, 34 и 35;
- Debian 9 и Astra Linux Special Edition «Смоленск» 1.6, 1.7;
- Ubuntu 22.04 LTS;
- openSUSE Leap 15.4.

Аппаратные средства Программного комплекса должны эксплуатироваться в условиях, соответствующих требованиям по установке и эксплуатации, указанным в документации производителей технических средств.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

Термин/ Сокращение, обозначение	**Расшифровка**
CPU	Центральный процессор (с англ. «Central processing unit»)
QHB	Система управления базами данных «Квант-гибрид»
QSS	Quantum Secure Storage Программа, предназначенная для криптографической защиты конфиденциальности и целостности информации, в том числе для защиты персональных данных
Гб	Гигабайт, единица измерения количества информации
ГОСТ	Государственный стандарт
ГОСТ Р 34.11-2012	ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования
ГОСТ 34.11-2018	ГОСТ 34.11-2018 Информационная технология. Криптографическая защита информации. Функция хэширования.
ГОСТ Р 34.12-2015	ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры.
ГОСТ 34.12-2018	ГОСТ 34.12-2018 Информационная технология. Криптографическая защита информации. Блочные шифры.
ГОСТ Р 34.13-2015	ГОСТ Р 34.13-2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров.
ГОСТ 34.13-2018	ГОСТ 34.13-2018 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров.
Ключ хранения	Ключ, которым производится зашифрование рабочего ключа
МДЗ	Модуль доверенной загрузки
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение

Термин/ Сокращение, обозначение	**Расшифровка**
Пользовательский ключ, ключи пользователей	Ключи, хранимые на отчуждаемых носителях, которыми производится зашифрование ключа хранения
ПС	Программные средства
Рабочий ключ	Ключ, которым производится зашифрование/расшифрование информации
Р 1323565.1.026–2019	Р 1323565.1.026–2019 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицирующее шифрование.
Р 50.1.111-2016	Р 50.1.111-2016 Информационная технология. Криптографическая защита информации. Парольная защита ключевой информации.
Р 50.1.113-2016	Р 50.1.113-2016 Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования.
ТЗ	Техническое задание
ФСБ	Федеральная служба безопасности
ЭВМ	Электронно-вычислительная машина
ЭЦП	Электронная цифровая подпись

Лист регистрации изменений

Изм.	*Номера листов (страниц)*				*Всего листов (страниц) в документе*	*Номер документа*	*Входящий номер сопроводительного документа и дата*	*Подпись*	*Дата*
	измененных	*замененных*	*новых*	*аннулированных*					