Спецификация ПО СКЗИ

Раздел "Документация"

|  |  |  |
| --- | --- | --- |
| Код документа | Наименование и файл | Содержание / Назначение |
| СКЗИ-ТП-001 | Текст программы (файл: magma.c) | Основной исполняемый код системы, реализация ГОСТ "Магма" в режиме OFB |
| СКЗИ-ОП-002 | Описание программы | Реализация криптографических операций, аутентификации, тестов, журналирования |
| СКЗИ-РП-003 | Руководство пользователя | Инструкция по работе через CLI, описание запуска и параметров тестирования |
| СКЗИ-ЛОГ-004 | Формат журнала аудита (crypto\_audit.log) | Запись событий аутентификации и критических операций |

Раздел "Комплексы"

|  |  |  |
| --- | --- | --- |
| Код комплекса | Наименование комплекса | Краткое описание |
| СКЗИ-КОМПЛЕКС-001 | Криптографический модуль "Магма" | Включает реализацию ГОСТ "Магма" (ГОСТ Р 34.12-2015) в режиме OFB и тестовые функции |

Раздел "Компоненты"

|  |  |  |
| --- | --- | --- |
| Код компонента | Наименование компонента | Краткое описание |
| СКЗИ-МОДУЛЬ-001 | Модуль аутентификации (authenticate\_user) | Проверка пароля, блокировка после 5 неудачных попыток |
| СКЗИ-МОДУЛЬ-002 | Модуль логирования (log\_event) | Запись событий в crypto\_audit.log |
| СКЗИ-МОДУЛЬ-003 | Модуль генерации случайных байтов (generate\_random) | Генерация случайных данных для ключей и IV |
| СКЗИ-МОДУЛЬ-004 | Модуль безопасного обнуления памяти (secure\_zero) | Очистка секретных данных из памяти |
| СКЗИ-МОДУЛЬ-005 | Модуль шифрования и расшифрования (magma\_ofb, magma\_encrypt\_block, key\_schedule) | Реализация алгоритма "Магма" в режиме OFB, обработка блоков |
| СКЗИ-МОДУЛЬ-006 | Модуль тестирования (test\_file\_encryption, test\_key\_rotation, main) | Проведение тестов корректности, производительности, смены ключей |

Примечания

1. В разделе "Документация" коды видов документов указаны в соответствии с внутренней классификацией.
2. В компонентах используются стандартные заголовочные файлы C и perf\_metrics.h.
3. Реализация соответствует требованиям ГОСТ Р 34.12-2015 ("Магма").
4. Для защиты от перебора пароля предусмотрена блокировка после 5 неудачных попыток.
5. Для тестирования реализованы проверки корректности, производительности и смены ключей.

Описание ПО СКЗИ

Основные сведения о составе ПО СКЗИ

Состав программного обеспечения включает следующие файлы:

magma.c (SHA-256: пример: 3e23e8160039594a33894f6564e1b1348bbd7a0088d42c4acb73eeaed59c009d) — основной исполняемый код системы, реализующий алгоритм блочного шифрования "Магма" (ГОСТ Р 34.12-2015) в режиме OFB, аутентификацию пользователя, тесты производительности и журналирование.

perf\_metrics.h (SHA-256: пример: 486ea46224d1bb4fb680f34f7c9ad96a8f24ec88be73ea8e5a6c65260e9cb8a7) — заголовочный файл для замеров производительности.

Вспомогательные стандартные заголовочные файлы C: stdio.h, stdlib.h, string.h, time.h и др

Логическая структура ПО СКЗИ

1. Модули и функции:
   1. Аутентификация: Проверка пароля пользователя (authenticate\_user), блокировка при превышении попыток (MAX\_FAILED\_AUTH)
2. Логирование
   1. Запись событий в файл crypto\_audit.log (log\_event).
3. Генерация случайных данных:
   1. Функция generate\_random для получения случайных байтов (используется для генерации ключей и IV).
4. Шифрование/расшифровка:
   1. Использование алгоритма "Магма" (функции magma\_encrypt\_block, magma\_ofb), генерация раундовых ключей (key\_schedule), обработка данных в режиме OFB.
5. Тестирование производительности:
   1. Функции test\_file\_encryption и test\_key\_rotation для проверки скорости обработки и смены ключей.
6. Безопасное обнуление памяти:
   1. Функция secure\_zero для очистки конфиденциальных данных.
7. Основной модуль (main):
   1. Координирует аутентификацию, логирование, тесты, очистку памяти и завершение работы.

Взаимодействие модулей: основной модуль (main) управляет аутентификацией, логированием, генерацией ключей, вызовом криптографических функций и тестированием.

Описание ПО СФ СКЗИ

1. Специальные функции:
   1. Аутентификация: Статическая проверка пароля "securepass" с блокировкой после 5 неудачных попыток.
   2. Шифрование: Использование алгоритма "Магма" (режим OFB) с мастер-ключом и вектором инициализации (IV).
   3. Логирование: Фиксация всех критических событий (успешные/неудачные попытки входа, ошибки, начало и завершение операций).
   4. Защита данных: Безопасное обнуление ключей, IV и рабочих буферов после завершения работы.

Методы и правила эксплуатации

1. Требования к запуску:
2. Программа запускается через командную строку:

*./magma*

Пароль для доступа: "*securepass*".

1. Ограничения:

Блокировка доступа на 10 секунд после 5 неудачных попыток ввода пароля.

Для корректной работы требуется поддержка стандартных функций C и наличие файла журнала (crypto\_audit.log).

1. Рекомендации:

Использовать ОС, поддерживающую функции secure\_zero и стандартные файловые операции.

Инструкция по сборке

1. Скомпилировать исходные файлы:

*gcc -o magma magma.c -O2 -Wall*

1. Проверить целостность файлов (контрольные суммы из п. а).
2. Запустить исполняемый файл:

*./magma*

Описание применения ПО СКЗИ

Назначение ПО СКЗИ

Программное обеспечение СКЗИ реализует криптографическую защиту информации с помощью алгоритма блочного шифрования "Магма" (ГОСТ Р 34.12-2015) в режиме OFB (Output Feedback). Основное назначение — обеспечение конфиденциальности и целостности информации при потоковой обработке данных.  
ПО также реализует базовую аутентификацию пользователя с журналированием событий для контроля и фиксации доступа к криптографическим операциям.

Область применения ПО СКЗИ

ПО предназначено для использования в информационных системах общего назначения, где требуется защита данных от несанкционированного доступа, модификации и подделки.  
Возможные области применения:

1. хранение и резервное копирование защищённых файлов;
2. передача конфиденциальных данных по незащищённым каналам связи;
3. защита служебных и конфигурационных файлов
4. тестирование и обучение по стандартам ГОСТ.
5. ПО ориентировано на применение в условиях, не связанных с государственной тайной.

Класс решаемых ПО СКЗИ задач

Программное обеспечение предназначено для решения следующих задач:

1. симметричное шифрование и расшифрование данных по ГОСТ Р 34.12-2015 ("Магма") в режиме OFB;
2. обеспечение потоковой защиты данных (шифрование/расшифрование произвольной длины);
3. контроль доступа к криптографическим операциям с применением аутентификации;
4. ведение аудита (журналирования) событий, связанных с криптографическими операциями;
5. тестирование производительности и корректности реализации алгоритма "Магма".

Ограничения при применении ПО СКЗИ

1. ПО не предназначено для защиты информации, содержащей сведения, составляющие государственную тайну.
2. Аутентификация реализована в виде заглушки и не должна использоваться в продуктивной среде без замены на полноценный механизм.
3. Поддерживается только работа с данными, размещёнными в оперативной памяти (файловый ввод-вывод реализован только в тестах).
4. Не реализована защита от атак по сторонним каналам (например, по времени выполнения).
5. В текущей реализации не выполняется постоянное отслеживание повторного использования вектора инициализации (IV).

Минимальная конфигурация технических средств

Архитектура: x86 или ARM (32/64-бит);

Оперативная память: не менее 64 МБ;

Процессор: не ниже Intel Pentium III / ARM Cortex-A7;

ОС: POSIX-совместимая (Linux, FreeBSD), bash или sh-оболочка;

Доступ к файловой системе (для создания журнала аудита);

Доступ к устройству генерации случайных чисел (/dev/urandom).

Сведения о среде функционирования (СФ)

Среда функционирования включает:

1. POSIX-совместимую ОС (Linux);
2. стандартную библиотеку языка C (libc)
3. модуль perf\_metrics.h для тестирования производительности;
4. файловую систему с поддержкой прав доступа
5. потоковый ввод-вывод (системные вызовы open, read, write).

Порядок работы ПО СКЗИ

1. Пользователь запускает ПО из командной строки.
2. Выполняется проверка времени блокировки (если ранее было превышено количество неуспешных аутентификаций).
3. Пользователь проходит процедуру аутентификации (пароль "securepass").
4. Генерируются ключ и вектор инициализации (IV) для алгоритма "Магма".
5. Выполняется операция шифрования и расшифрования тестового сообщения или буфера (режим OFB).
6. Производится проверка корректности расшифрования (сравнение исходных и расшифрованных данных).
7. Ведётся журнал событий (успешные/неуспешные попытки входа, начало и завершение операций).
8. Все секретные данные (ключ, IV, буферы) очищаются из памяти.
9. Программа завершает выполнение

Пояснительная записка

Назначение компонентов, входящих в состав ПО СКЗИ

Программное обеспечение состоит из следующих компонентов.  
Модуль **magma.c** управляет выполнением программы, реализует пользовательский интерфейс, аутентификацию пользователя, генерацию ключей и вектора инициализации, вызов криптографических функций, тестирование производительности, обработку ошибок и ведение журнала событий.  
Модуль **perf\_metrics.h** предназначен для замеров производительности при шифровании и расшифровании больших объёмов данных.  
Встроенные функции обеспечивают: генерацию случайных байтов (generate\_random), безопасное обнуление памяти (secure\_zero), аутентификацию пользователя (authenticate\_user), журналирование событий (log\_event), реализацию алгоритма "Магма" (key\_schedule, magma\_encrypt\_block, magma\_ofb), тестирование производительности и корректности.

Перечень всех реализованных в ПО СКЗИ функций

1. main — основная управляющая функция, координирующая выполнение программы, аутентификацию, тестирование и очистку данных.
2. authenticate\_user — функция аутентификации пользователя.
3. log\_event — функция записи событий в журнал аудита.
4. secure\_zero — функция безопасного обнуления памяти.
5. generate\_random — функция генерации случайных байтов для ключей и IV.
6. key\_schedule — функция генерации раундовых ключей для алгоритма "Магма".
7. magma\_encrypt\_block — функция шифрования одного блока данных.
8. magma\_ofb — функция реализации режима OFB для потокового шифрования и расшифрования.
9. test\_file\_encryption — функция тестирования производительности шифрования/расшифрования файловых буферов.
10. test\_key\_rotation — функция тестирования производительности при частой смене ключей.

Сведения о параметрах реализованных функций

1. authenticate\_user не принимает аргументов, возвращает логическое значение (1 — успех, 0 — неудача).
2. log\_event принимает строку с сообщением и записывает её в файл журнала.
3. secure\_zero принимает указатель на память и размер области, очищает её.
4. generate\_random принимает буфер и его размер, заполняет буфер случайными байтами.
5. key\_schedule принимает указатель на ключ и массив для раундовых ключей.
6. magma\_encrypt\_block принимает указатель на входной и выходной блок (8 байт), а также массив раундовых ключей.
7. magma\_ofb принимает IV, ключ, входные и выходные буферы, длину данных.
8. test\_file\_encryption принимает имя файла и размер тестируемого файла в мегабайтах.
9. test\_key\_rotation принимает количество блоков между сменами ключа.

Сведения о формируемых кодах возврата реализованных функций

1. main возвращает код 0 при успешном завершении работы, в случае ошибок (например, превышено число попыток аутентификации, сбой генерации ключа) — завершает выполнение с помощью exit(1).
2. authenticate\_user возвращает 1 при успешной аутентификации, 0 при ошибке.
3. В случае критических ошибок (например, сбой открытия файла журнала или генерации случайных данных) также вызывается exit(1).

Перечень экспортируемых функций ПО СКЗИ

Из модуля perf\_metrics.h экспортируются функции для замеров производительности (используются при тестировании).

Все основные криптографические функции реализованы непосредственно в magma.c и используются внутри данного файла.

Описание используемых переменных

1. key — массив из 32 байт (256 бит), используется как симметричный ключ для алгоритма "Магма".
2. iv — массив из 8 байт (64 бита), используется как вектор инициализации (IV) в режиме OFB.
3. failed\_attempts — количество неудачных попыток аутентификации.
4. blocked\_until — время, до которого заблокирован повторный ввод пароля.
5. ciphertext, decrypted — буферы для хранения шифротекста и расшифрованных данных.
6. s\_box — таблица S-блоков для алгоритма "Магма".
7. round\_keys — массив раундовых ключей для шифрования.
8. metrics — структура для замеров производительности.

Описание алгоритмов функционирования ПО СКЗИ

После запуска программа проверяет, истекло ли время блокировки пользователя. Если блокировка не активна, пользователь проходит процедуру аутентификации. При успешной аутентификации генерируются ключ и вектор инициализации. Далее выполняются тесты корректности (шифрование и расшифрование тестового сообщения, сравнение результата с исходными данными), а также (при необходимости) тесты производительности и смены ключей. Все события (успешная или неуспешная аутентификация, ошибки, начало и завершение операций) фиксируются в журнале аудита. После завершения работы все секретные данные (ключ, IV, буферы) очищаются из памяти функцией secure\_zero. Программа завершает выполнение.

Описание критериев, методики и результатов тестирования

В качестве критериев тестирования использовались: корректность шифрования и расшифрования (совпадение исходных и расшифрованных данных), обработка ошибок доступа и аутентификации, ведение журнала, очистка памяти, производительность при обработке больших объёмов данных, корректность смены ключей.  
Методика включала ручное тестирование: ввод корректного и некорректного пароля, анализ содержимого журнала аудита, проверку очистки секретных данных, сравнение исходных и расшифрованных данных, измерение скорости шифрования/расшифрования, тестирование частой смены ключей.  
В результате тестирования установлено, что при корректных входных данных функция magma\_ofb обеспечивает обратимость шифрования, программа блокирует доступ при ошибках аутентификации, а журнал фиксирует все ключевые события. Все функции отработали в соответствии с требованиями.