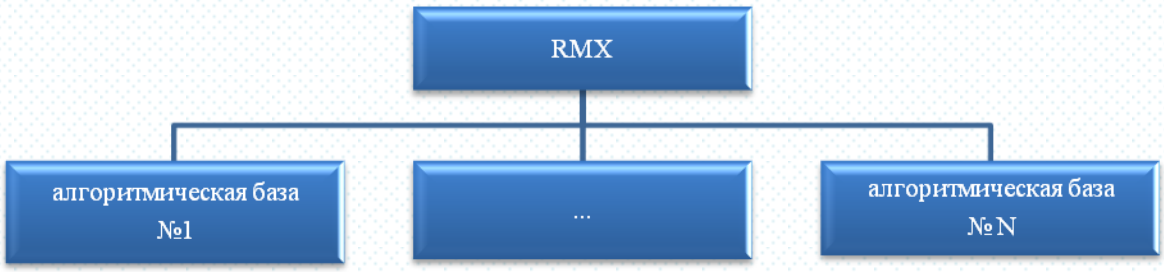
ПАСПОРТ
КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ

1. ОСНОВНЫЕ СВЕДЕНИЯ О ПРОГРАММНОМ ПРОДУКТЕ RMX.

Дата начала разработки RMX.	1996.
Дата окончания разработки RMX.	2012.
Уровень защиты информации.	Защита информации уровня А1.
Классификация системы защиты.	Абсолютная система защиты информации.
Язык исходных файлов системы RMX.	Delphi. C++.
Назначение программы.	Защита информации шифрованием.
Размер программы без оболочки.	5 - 40 килобайт. (в зависимости от алгоритма и выбранного режима работы).
Отрасли применения.	- Национальная безопасность государств. - Военные объекты. - Банковская сфера. - Сотовая телефонная связь. - Коммуникации. - Онлайн платежи. - Биопаспорт. - Интернет. - Компьютерные сети. - ЭВМ. - Сейфы, охранные устройства и т.д.
Условия поставки ПО.	- Установочный пакет программы. - Программно-аппаратный комплекс (микрочип).
Основной спектр услуг системы RMX.	Система RMX предоставляет весь спектр услуг по защите информации: - Аутентификация. - Цифровая подпись. - Режим “Свой-Чужой”. - Шифрование любого вида информации. - Многопользовательский режим с неограниченным количеством пользователей. - Работа в режиме реального времени практически на любой вычислительной технике. - Шифрование сотовой связи. - Защита от имитации, проникновения, эмуляции. - Возможность использования универсального ключа. - Возможность использования полиморфных ключей. - Защита любых сетей. - Возможность установки RMX в любую точку пространства. - Поддержка большинства ОС и т.д.

2. СОСТАВ СИСТЕМЫ RMX.

2.1 Система защиты RMX имеет огромное количество алгоритмических баз, которые задаются специальными коэффициентами.

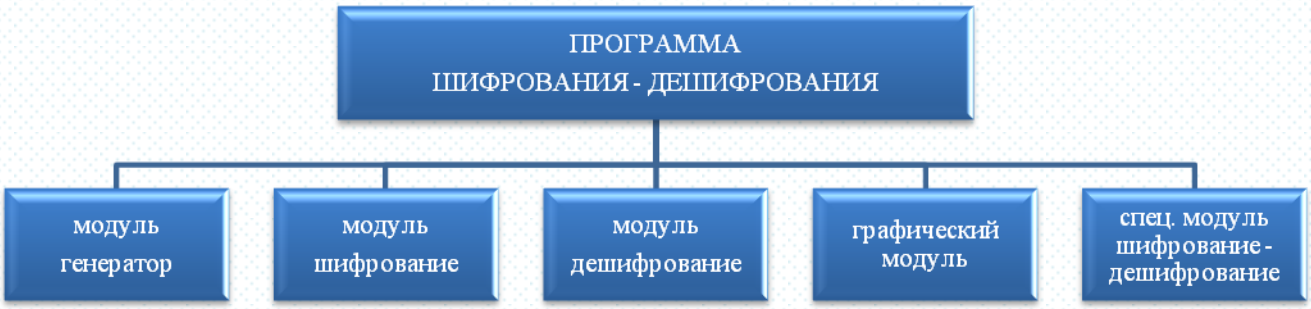


2.2 Состав алгоритмической базы:

- программа подготовки начальных данных,
- программа генерирования универсального ключа в многопользовательском режиме,
- программа шифрования - дешифрования.

2.3 Состав программы шифрования-дешифрования*:

- Модуль «Генератор».
- Модуль «Шифрование».
- Модуль «Дешифрование».
- Модуль «Графический».
- Модули шифрования-дешифрования со специальными функциями.



*Также подключаются и другие специальные модули.

3. ФУНКЦИИ СИСТЕМЫ RMX.

3.1 Полная защита информации при передаче ее от пользователя к пользователю на всем протяжении сети во всех физических средах и в любых каналах (Интернет, телефонные сети и т.д.).
3.2 Обеспечение многопользовательского режима с неограниченным количеством пользователей в масштабе реального времени и с неограниченным количеством алгоритмических баз для каждой группы пользователей.
3.3 Шифрование любой информации (символьной, графической, двоичной).
3.4 Обеспечение режима электронной подписи.
3.5 Шифрование информации в любых сетях: Internet, сотовой телефонной сети и др. (возможна поддержка протоколов сетей).
3.6 Создание многопользовательских закрытых сетей любой конфигурации с использованием стандартных каналов связи (сети с удаленными терминалами в т. ч. банковские).
3.7 Полная защита от имитации каждого пользователя сети, станции (даже при попытке имитации с подключением к каналу связи). Работа в режиме «Свой-Чужой».
3.8 Полная защита станции от потери начальных данных пользователей при работе с универсальным ключом.

4. МИНИМАЛЬНЫЕ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ ДЛЯ РАБОТЫ СИСТЕМЫ RMX.

4.1 Частота процессора: 100МГц.
4.2 ОЗУ: 32 Мб
4.3 Место на винчестере для установки RMX без оболочки: 50-60 кб.

5. РЕКОМЕНДУЕМЫЕ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ ДЛЯ РАБОТЫ СИСТЕМЫ RMX.

5.1 Частота процессора: 2ГГц и выше.
5.2 ОЗУ: 1 Гб и выше.
5.3 Место на винчестере для установки RMX с оболочкой: 15-50 Мб.

6. ТЕХНИЧЕСКИЕ ПАРАМЕТРЫ КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ RMX:

• АРХИТЕКТУРА СИСТЕМЫ RMX

Архитектура системы RMX	N-мерные вероятностно-детерминированные самоорганизующиеся структуры.

• ЧИСЛО РАУНДОВ ШИФРОВАНИЯ СИСТЕМЫ RMX

Число раундов.	1 раунд. 2 раунда. 3 раунда.

• АЛГОРИТМЫ СИСТЕМЫ RMX

1.	Алгоритмы системы RMX.	1. Симметричный недетерминированный алгоритм: - поточное гаммирование; - блочное шифрование: ▪ 256 байт, ▪ 512 байт, ▪ 1 кб, ▪ 2 кб, ▪ 4 кб, ▪ … , ▪ 128 кб и более. 2. Ассиметричный недетерминированный алгоритм.
2.	Количество алгоритмов RMX.	200 алгоритмических баз системы RMX. Каждая алгоритмическая база представляет собой самостоятельную систему шифрования. Разные алгоритмические базы RMX не дешифруют друг друга. Количество алгоритмов определяется: - полями генератора, - алгоритмами генератора, - длиной ключей, - методами преобразования и их последовательностью.

• ФУНКЦИИ РАУНДОВ ШИФРОВАНИЯ СИСТЕМЫ RMX

	Функции раундов шифрования.	- Гаммирование (сложение по модулю 2). - Побитовая операция скремблирования случайным равномерно распределенным многобайтовым ключом. - Нелинейная операция замены случайным равномерно-распределенным многобайтовым ключом для блока размером 256 байт и более. - И другие функции.

• КЛЮЧИ СИСТЕМЫ RMX

1.	Длина ключа.	1 024 байт, 2 048 байт, 4 096 байт, 8 192 байт, 16 384 байт и более (в зависимости от выбранного режима).

2.	Количество независимых ключей	Количество независимых ключей: $10^{1\,000} - 10^{50\,000}$ Количество независимых ключей зависит от выбранного режима (система позволяет создавать ключи любой длины и мощности, соизмеримой с количеством независимых ключей, формируемых в течение одного цикла).
3.	Характеристика ключа RMX.	Система RMX позволяет создавать на выходе ключ: - N-мерный в пространстве, - случайный, - байтовый/многобайтовый.
4.	Возможности операций ключа системы RMX.	- Линейные/нелинейные операции шифрования на всем битовом поле файла; - Блочное или поточное шифрование любого количества поступающих на вход битов/байтов.
5.	Процесс формирования ключей.	В процессе формирования ключей идет многократный процесс нелинейного отображения с разрывами первого и второго рода одного множества в другое и N-мерных защелок для выхода в случайные распределенные пространства (все преобразования необратимые).
6.	Состав независимого ключа.	Независимый ключ состоит из случайного набора чисел, формируемых в течение одного цикла (периода) для каждого пользователя.
7.	Возможность работы с универсальными ключами.	Да.
8.	Размер универсального ключа.	5-50 килобайт
9.	Универсальный ключ.	Система позволяет создавать универсальный ключ для шифрования-дешифрования для любой группы пользователей (причем у каждого пользователя сохраняются свои начальные данные, которые позволяют создавать неограниченное количество независимых ключей). Количество пользователей в группе и количество групп ничем не ограниченно. Между начальными данными пользователей и универсальным ключом (а так же между универсальными ключами, созданными для различных групп пользователей) отсутствует всякая зависимость. Наличие одного универсального ключа позволяет поместить программу и ключ в одну интегральную микросхему, что полностью исключает утечку начальных данных со станции.
10.	Генерация	Универсальные ключи генерируются самими

	универсальных ключей.	пользователями или владельцами станций.
11.	Сложные полиморфные ключи.	Система RMX предоставляет возможность создания побитового шифрования информации случайным полиморфным ключом (случайным алгоритмом).
12.	Наличие элементов ключей в зашифрованной информации.	Отсутствуют.
13.	Формирование ключей.	Ключи формируют сами пользователи или провайдер.
14.	Формирование ключей у пользователей.	RMX вырабатывает бесконечное количество ($10^{1\,000}$ - $10^{50\,000}$) случайных ключей у каждого пользователя (один и тот же текст каждый раз шифруется случайными, равномерно - распределенными, никогда не повторяющимися ключами).

• НАЧАЛЬНЫЕ ДАННЫЕ СИСТЕМЫ RMX

1.	Подготовка начальных данных	Подготовка начальных данных (порождающих чисел) для каждого пользователя осуществляется только один раз на все время пользования программой.
2.	Режим подготовки начальных данных.	Подготовка начальных данных осуществляется в автоматическом режиме и носит случайный характер. Каждый пользователь может иметь несколько различных вариантов начальных данных.
3.	Передача начальных данных по сетям.	Начальные данные никогда не передаются по сетям.
4.	Хранение начальных данных.	Начальные данные хранятся в зашифрованном виде.
5.	Защита начальных данных.	Начальные данные защищены от потери случайными паролями (длина пароля составляет 30-40 байт).
6.	Объем памяти начальных данных.	2048 - 12288 байт.
7.	Генерация начальных данных.	Начальные данные генерируются самими пользователями или владельцами станций.
8.	Расшифровка начальных данных.	Расшифровка начальных данных идет по N-мерному образу.

9.	Начальные данные пользователей.	Каждый пользователь формирует случайные начальные данные 5—50 кбайт (в зависимости от алгоритмической базы), которые являются основой работы генератора. В случае работы с универсальным ключом, провайдер выдает каждому пользователю его начальные данные, которые формируются автоматически и могут находиться (как и универсальный ключ) в чипе.
10.	Хранение начальных данных.	Начальные данные могут храниться и в зашифрованном виде (без хранения ключа вскрытия). Ключ вскрытия начальных данных очень короткий, но он является отображением на бесконечное пространство и перебором вычислить его невозможно.

• ГЕНЕРАТОР СИСТЕМЫ RMX

1.	Нелинейность генератора и методов преобразования.	Генератор обладает супервысокой алгебраической сложностью и высокой степенью нелинейности структуры (все параметры генератора возможно изменять в любую сторону, доводя нелинейность структуры до сколь угодно больших степеней). Нелинейность как генератора так и методов преобразования чрезвычайно высока: достаточно изменить начальные данные на один бит (любого байта) и дешифрация будет невозможна (формирование случайных пространств идет по-другому пути).
2.	Математическая функция генератора.	Самоорганизующаяся вероятностно - детерминированная N-мерная необратимая функция.
3.	Диапазон чисел генератора.	Диапазон чисел, вырабатываемых генератором, ничем не ограничен (0-255, 0-511, 0-1023 и т.д.), поэтому система может работать как с ANSI, так и с UNICODE.
4.	Внутренняя структура генератора и алгоритмы.	Внутренняя структура генератора позволяет реализовывать большое количество различных алгоритмических конструкций, что в совокупности с различными методами преобразования информации дает огромное количество алгоритмов.
5.	Случайные числа генератора.	Генератор позволяет вырабатывать случайные числа, аналогичные получаемым с помощью неприводимых многочленов над полем Галуа, но в любом диапазоне с бесконечным периодом повторения и в любом функциональном окружении.
6.	Последовательности генератора.	Генератор позволяет одновременно генерировать последовательности с бесконечно большим периодом и с шагом больше (3-25): - случайные, равномерно распределенные последовательности для операции суммирования по модулю N, умножения по модулю N; - случайные, равномерно распределенные последовательности на всем протяжении периода для нелинейной операции замены, стохастического преобразования (блоками по 256 ,512, 1024 и более байт). Количество блоков ничем не ограниченно.

Количество подстановок (зависящих от преобразуемых данных или не зависящих от преобразуемых данных) от 2^8! до 2^{32}! и более (! - факториал);

- случайные, равномерно распределенные последовательности на всем протяжении периода для побитовой/побайтовой операции перестановки (блоками по 256, 512, 1024 и более байт (количество блоков ничем не ограниченно). Количество перестановок, зависящих от преобразуемых данных или не зависящих от преобразуемых данных, от 2^8! до 2^{32}! и более (! - факториал);

- случайные, равномерно распределенные последовательности на всем протяжении периода для других сложных математических нелинейных операций.

Генератор позволяет вырабатывать последовательности и для других операций шифрования:
- суммирования по модулю N,
- умножения по модулю N и некоторых других (обратимых и даже необратимых операций; обратимых с помощью специально вырабатываемых ключей при дешифрации).

7. Структура генератора.

Генератор представляет собой полуоткрытое множество, т.е. при работе никогда не вырождается (это позволяет создавать бесконечно большие, равномерно распределенные, случайные периоды).

8. Установка и подводка генератора.

Генератор автоматически устанавливается в любую точку пространства до:

$$10^{50\,000}$$

При этом новый файл шифруется другими случайными никогда неповторяющимися ключами.

Специально подводить генератор не нужно.

• ПОЛЬЗОВАТЕЛИ СИСТЕМЫ RMX

Количество пользователей в системе RMX	Не имеет практических ограничений.

• ЗАЩИТА СТАНЦИЙ СИСТЕМОЙ RMX

Защита станций.	Абсолютная защита станций от проникновения при использовании микрочипа RMX.

• МАТЕМАТИКА СИСТЕМЫ RMX

1.	Отличительные особенности математики системы RMX.	В математическом аппарате системы решены две сложнейшие задачи - одновременно выполняются два взаимоисключающихся процесса: - детерминирование, - случайный хаос решето-случайных чисел. Система RMX работает на специальных математических функциях, которые разработаны автором и являются закрытыми. Только система RMX выполняет сложнейшие математические операции с битами и с байтами информации: полное побитовое скремблирование нескольких килобит информации случайным, никогда неповторяющимся, равномерно распределенным, полиморфным ключом.
2.	Математический аппарат системы RMX.	Самоорганизующиеся случайные открытые/полуоткрытые N-мерные множества, которые могут размножаться подобно живым клеткам и которые никогда не теряют своей структуры в бесконечном N-мерном пространстве). N-мерные вложенные, связанные, случайные фракталы никогда не вырождаются.
3.	Выполняемые математические тесты системой RMX.	Система RMX выполняет ряд тестов, которые ни одна даже «закрытая» система выполнить не может. Пример: случайные, равномерно распределенные последовательности на всем протяжении бесконечного периода (количество ключей: $10^{50\,000}$).

• ОТЛИЧИТЕЛЬНЫЕ ОСОБЕННОСТИ СИСТЕМЫ RMX

1.	Абсолютная равномерность случайного байтового /многобайтового поля.	Абсолютная равномерность случайного байтового/многобайтового поля позволяет реализовать битовую операцию скремблирования, никогда неповторяющуюся (ключи никогда не повторяются) на всем битовом/байтовом поле шифруемого файла. Каждый шаг работы генератора вырабатываются новые случайные ключи и на другом отрезке файла происходит побитовая операция скремблирования. Длина отрезка файла и длина ключей ничем не ограниченна. Абсолютная равномерность случайного байтового/многобайтового поля позволяет реализовать нелинейную операцию замены элементов блока шифруемого файла - стохастическое преобразование, байтовую или битовую замену (длина блока может достигать десятки килобайт).

		Каждый шаг работы генератора вырабатываются новые случайные ключи и таблица замены обновляется каждый шаг (формируется случайным образом).
2.	Генератор случайный чисел.	В отличие от многих криптографических систем в основе RMX лежит генератор случайных чисел который генерирует случайные, равномерно распределенные байтовые/многобайтовые последовательности, которые самоорганизуются над полем натурального ряда вещественных чисел и даже комплексных чисел.
3.	НОУ-ХАУ.	Система RMX в математической и алгоритмической реализации содержит ряд НОУ-ХАУ, которые позволили решить сложнейшие математические задачи, такие как: - решето случайные числа, - генерация универсального ключа, - установка генератора в любую точку пространства до $10^{50\,000}$, - генерация случайных и одновременно равномерно-распределенных последовательностей и др.
4.	Основа RMX.	В основу RMX положены самоорганизующиеся случайные открытые/полуоткрытые N-мерные множества, которые могут размножаться как живые клетки и никогда не теряют своей структуры в бесконечном N-мерном пространстве. N-мерные вложенные, связанные, случайные фракталы никогда не вырождаются.
5.	Хранение информации, идентифицирующей пользователей.	При использовании системы защиты RMX в головном офисе не сохраняются пароли, начальные данные (ключи) и другая информация, идентифицирующая пользователей.

RMX • ПРОЦЕСС ШИФРОВАНИЯ СИСТЕМЫ RMX

1.	Скорость шифрования – дешифрования.	Скорость шифрования – дешифрования составляет: (50 кб - 50 Мб) / сек (в зависимости от выбранного режима; платформы компьютера; аппаратного и программного метода реализации).
2.	Изменение размера информации после шифрования.	Объем информации после шифрования значительно не увеличивается.

• ПОДДЕРЖКА ОПЕРАЦИОННЫХ СИСТЕМ RMX

Поддержка операционных систем.	Система независимо поддерживает различные платформы: - DOS; - WINDOWS (95,98,2000,NT,XP,7,8); - LINUX; - UNIX и др. RMX может быть адаптирована под любую ОС под заказ.

• РЕЖИМ РЕАЛЬНОГО ВРЕМЕНИ СИСТЕМЫ RMX

Работа RMX в реальном масштабе времени.	Система RMX работает в масштабе реального времени даже на бытовых ЭВМ.

• РЕЖИМ «СВОЙ-ЧУЖОЙ» СИСТЕМЫ RMX

Режим “Свой-Чужой”	Система RMX позволяет работать в режиме “Свой - Чужой” с помощью случайных, неповторяющихся посылок (авиация, охранные устройства, сейфы и т.д.).

• ЗАЩИТА СОТОВОЙ СВЯЗИ СИСТЕМОЙ RMX

.	Защита сотовых телефонных сетей.	Да.

• ЗАЩИТА СПУТНИКОВЫХ СИСТЕМ СИСТЕМОЙ RMX

Защита телевизионных каналов, спутниковых систем.	Да.

• ЗАЩИТА ОТ ПРОНИКНОВЕНИЯ И ЭМУЛЯЦИИ

Проникновение и эмуляция.	Проникновение и эмуляция невозможны.

• РЕЖИМ ЦИФРОВОЙ ПОДПИСИ СИСТЕМЫ RMX

Цифровая подпись.	Да.

• АУТЕНТИФИКАЦИЯ СИСТЕМЫ RMX

Аутентификация.	Да.

• ЗАЩИТА НОСИТЕЛЕЙ ИНФОРМАЦИИ СИСТЕМОЙ RMX

Защита носителей информации системой RMX.	RMX позволяет защитить от копирования: - CD, - DVD, - Жесткие диски, - Flash-накопители и другие накопители информации.

• ОСНОВА КРИПТОСКТОЙКОСТИ СИСТЕМЫ RMX

Основа криптостойкости системы RMX.	Криптостойкость системы RMX основана на: 1. закрытии начальных данных, хранящихся у каждого пользователя, и универсального ключа, хранящегося на станции; 2. длине случайного ключа и абсолютной равномерностью гаммы; 3. количестве полиморфных случайных ключей; 4. количестве алгоритмов; 5. защите станции (изготовление в чипе); 6. количестве и длине паролей в многопользовательском режиме; 7. длине начальных данных у каждого пользователя; 8. очень высокой алгебраической сложности случайных нелинейных структур и наличии необратимых функций;

9. новой математике, разработанной автором;
10. операциях преобразования со сверхдлинными случайными ключами:
    - побитовом скремблировании,
    - нелинейных операциях замены и ряде других преобразований и НОУ-ХАУ.

Знание алгоритмов программы и исходных программных текстов не уменьшают криптостойкость.

Разные алгоритмические базы системы RMX не дешифруют друг друга.

Разные алгоритмические базы системы RMX выступают в роли самостоятельной системы шифрования

7. ГАРАНТИИ.

Разработчики системы RMX гарантируют абсолютную защиту информации для пользователя при условии правильной эксплуатации, указанной в договоре.

8. ОТВЕСТВЕННОСТЬ.

Пользователи системы RMX несут ответственность, оговоренную в договоре.

Система RMX предназначена исключительно для личного использования покупателем.

Относительно RMX запрещена любая деятельность (перепродажа, любое копирование, изменение ПО и т.п.), которое носит коммерческий характер, не относящийся к автору RMX, или вредит имиджу технологии RMX.

Данный паспорт является документом, идентифицирующим систему RMX.

info@lesantint.com