Тема работы: «Разработка криптостойкого генератора псевдослучайной последовательности».

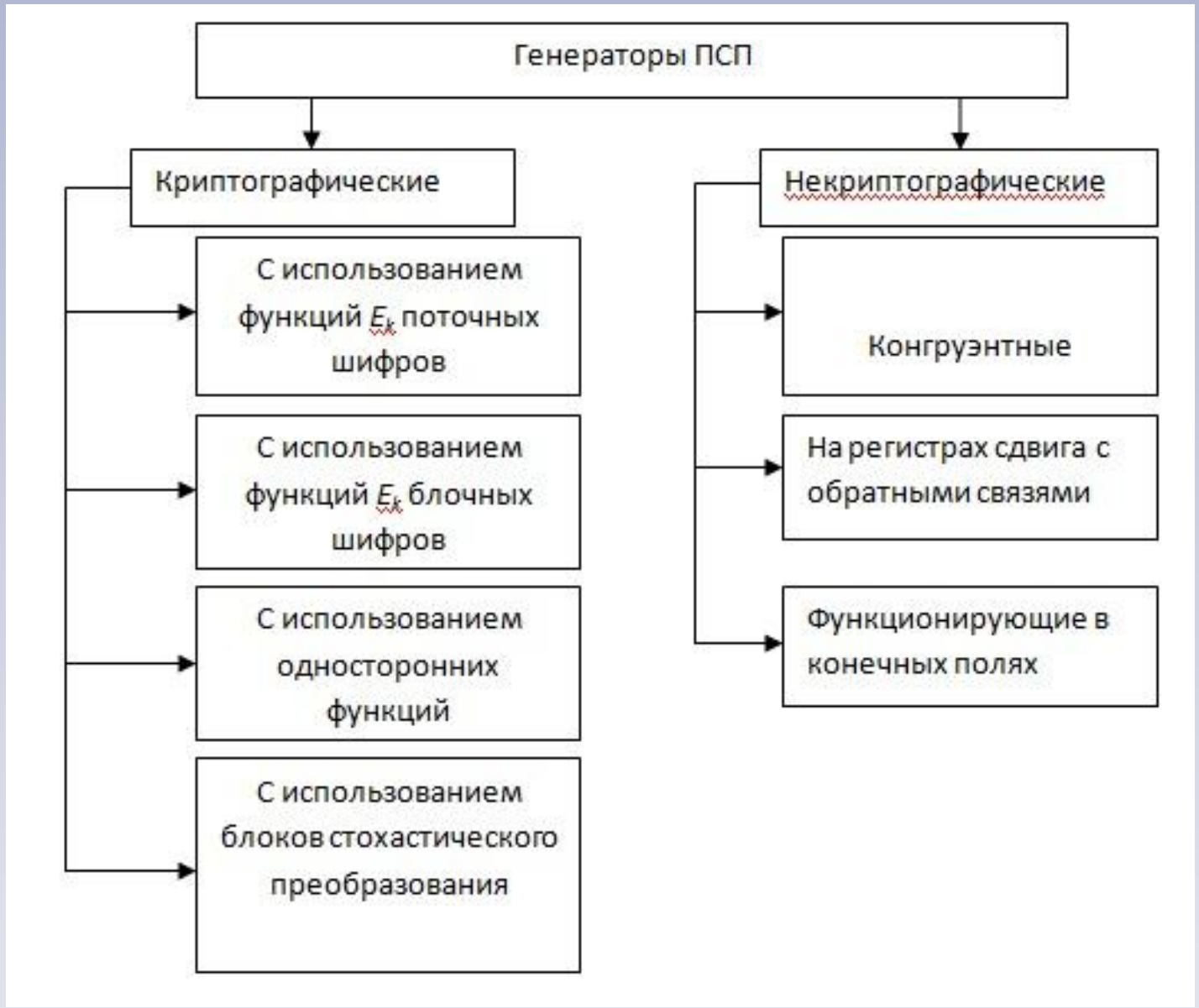
- Цель работы: разработка криптостойкого генератора псп, для применения его в системе защиты информации от несанкционированного доступа.
- Актуальность заключается в том, что с расширением компьютерных сетей участились всевозможные атаки на информацию, представляющую определенную значимость , для предотвращения это используются криптостойкие системы защиты, неотъемлемой частью которых являются генераторы псп.

Генераторы ПСП решают такие задачи, как:

- Внесение неопределенности в работу средств защиты.
- Генерация гамма-последовательностей при построении синхронных поточных шифров.
- Внесение неопределенности в работу защищаемых средств.
- Хэширование информации.
- Формирование случайных запросов при реализации большого числа криптографических протоколов (протоколов аутентификации, электронной подписи, привязки к биту и тд.)
- Формирование ключевой информации, на которой основана стойкость алгоритма.
- Построение самосинхронизирующихся поточных шифров.

- Качественный генератор ПСП должен удовлетворять следующим требованиям:
- Криптографическая стойкость;
- Хорошие статистические свойства. ПСП по своим свойствам не должна отличаться от истинно случайной последовательности;
- Большой период формируемой последовательности: например, при шифровании для преобразования каждого элемента входной последовательности необходимо использовать свой элемент псевдослучайной гаммы;
- Эффективная аппаратная и программная реализация.

Классификация генераторов ПСП:



- Достоинства стандарта:
- бесперспективность атаки полным перебором (XSL-атаки в учёт не берутся, так как их эффективность на данный момент полностью не доказана);
- эффективность реализации и, соответственно, высокое быстродействие на современных компьютерах;
- наличие защиты от навязывания ложных данных (выработка имитовставки) и одинаковый цикл шифрования во всех четырёх алгоритмах стандарта.

Недостатки связаны с неполнотой стандарта в части генерации ключей и таблиц замен. Считается, что у стандарта существуют «слабые» ключи и таблицы замен, но в нем не описываются критерии выбора и отсева «слабых». В связи с этим могут возникнуть такие проблемы как:

- нельзя определить криптостойкость алгоритма, не зная заранее таблицы замен;
- реализации алгоритма от различных производителей могут использовать разные таблицы замен и могут быть несовместимы между собой;
- возможность преднамеренного предоставления слабых таблиц замен лицензирующими органами РФ;
- потенциальная возможность (отсутствие запрета в стандарте) использования таблиц замены, в которых узлы не являются перестановками, что может привести к чрезвычайному снижению стойкости шифра.

- Возможные применения:
- Использование в S/MIME (PKCS#7, Cryptographic Message Syntax).
- Использование для защиты соединений в TLS (SSL, HTTPS, WEB).
- Использование для защиты сообщений в XML Encryption.

Результаты анализа статистической безопасности криптографических генераторов ПСП:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
A5															
1 бит	994	982	976	976	991	984	992	88	963	869	886	993	991	988	908
RC4															
8 бит	987	991	967	965	988	988	994	121	954	883	877	991	990	984	904
4 бита	995	989	977	974	990	987	990	93	978	888	891	991	989	993	914
2 бита	991	991	977	972	987	985	995	103	963	879	879	985	993	987	899
1 бит	991	994	975	965	991	984	989	90	958	885	882	990	998	988	915
ГОСТ 28147-89															
64 бита	990	990	979	973	991	990	994	99	968	891	894	986	987	988	922
32 бита	998	1000	983	992	998	1000	997	98	994	915	926	999	998	997	922
16 бит	993	993	970	970	991	988	993	104	962	893	884	988	991	990	909
8 бит	987	987	965	968	985	990	987	97	970	867	876	983	988	985	922
4 бита	991	991	969	981	987	987	988	90	966	876	897	992	990	988	905
2 бита	993	994	979	980	993	993	989	93	976	881	889	989	993	986	898
1 бит	988	983	976	971	992	981	990	91	961	885	886	986	990	986	917

Продолжение таблицы:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
AES **- 128**															
128 бит	991	989	977	980	993	992	990	104	974	866	885	986	989	987	918
64 бита	987	995	972	975	988	991	996	95	954	888	892	987	990	985	901
32 бита	986	994	974	966	985	992	990	79	968	892	888	983	992	984	910
16 бит	990	986	974	976	993	990	987	103	962	868	884	987	984	989	918
8 бит	995	988	971	965	985	984	991	101	964	860	889	988	988	990	909
4 бита	989	995	977	969	991	994	992	91	961	875	903	985	990	988	923
2 бита	992	992	983	977	995	990	985	105	960	883	883	989	990	990	919
1 бит	994	991	978	981	996	986	989	100	972	878	874	990	985	988	921
Rgen **- 1**															
128 бит	992	991	966	970	995	983	990	108	969	876	891	987	993	987	900
64 бита	983	987	967	965	990	982	991	95	958	886	892	987	989	984	910
32 бита	986	987	982	971	996	995	985	108	963	872	908	989	990	984	916
16 бит	988	991	970	968	988	985	988	112	950	898	903	989	991	985	918
8 бит	991	994	965	974	987	989	988	95	966	886	880	983	992	986	914
4 бита	989	987	975	973	990	995	989	84	959	873	884	980	991	988	905
2 бита	991	989	965	966	989	990	995	102	966	881	879	989	983	987	923
1 бит	990	989	976	974	991	989	991	122	970	880	886	987	986	989	890

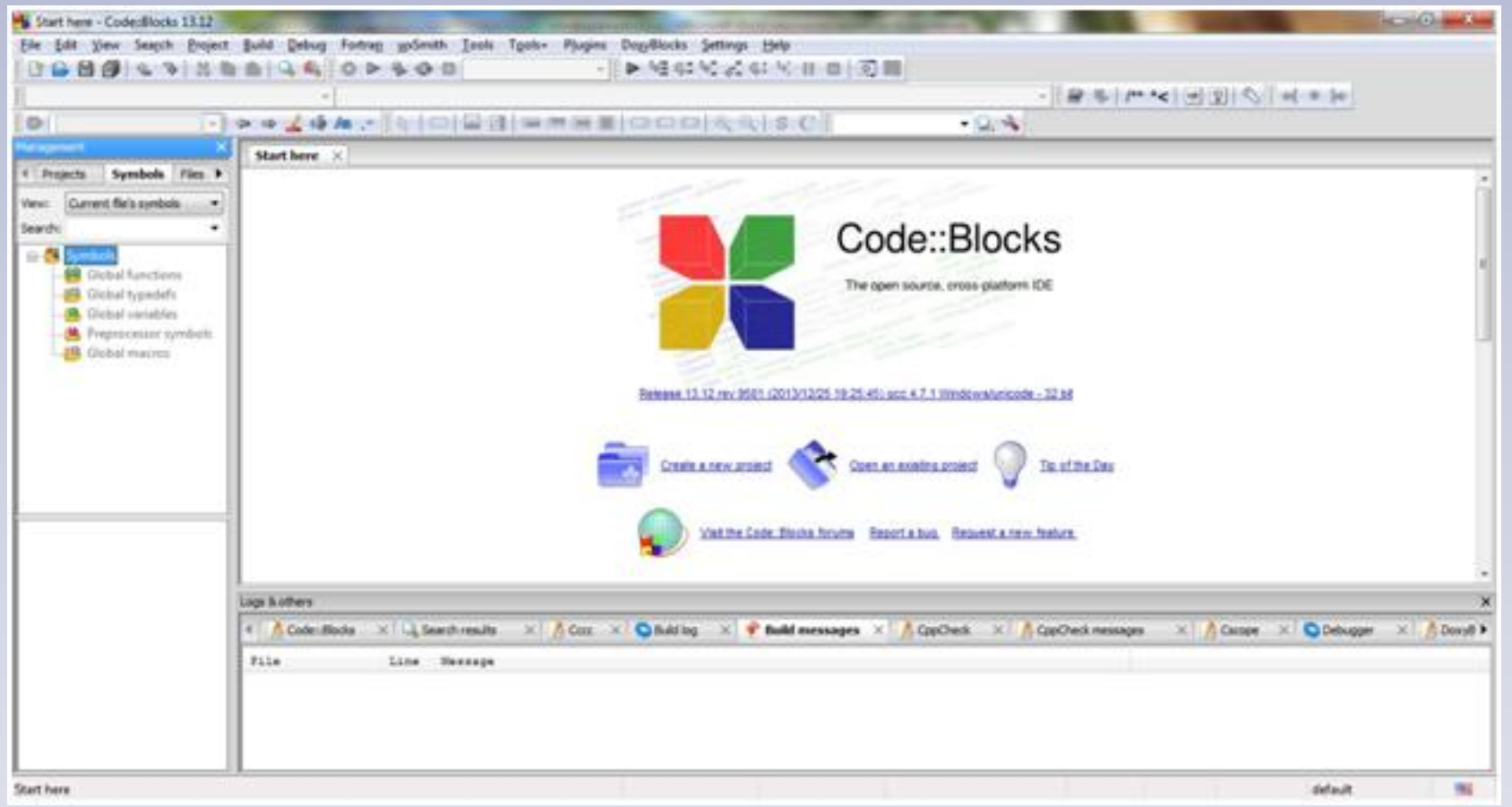
Алгоритм ГОСТ 28147-89 предусматривает четыре режима работы:

- шифрование данных в режиме простой замены;
- шифрование данных в режиме гаммирования;
- шифрование данных в режиме гаммирования с обратной связью;
- выработка имитовставки.

Проблемы, которые нужно изучить для реализации поставленой цели:

1. Выбор среды разработки и языка программирования
2. Анализ схемы генератора ПСП ГОСТ 28147-89
3. Разработка программного кода для реализации генератора
4. Проверить удовлетворяет ли генератор ПСП требованиям, описаным выше

Рабочее окно среды разработки CodeBlocks 13.12



Блок-схема одного цикла шифрования

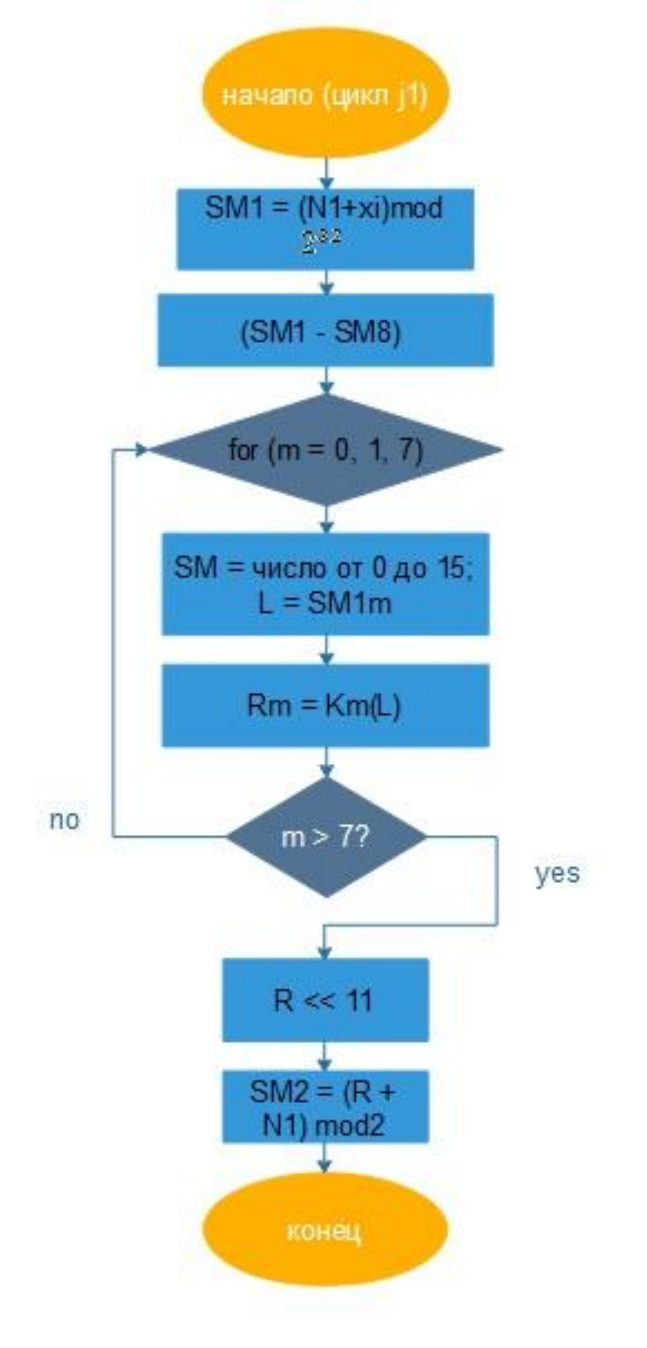


Таблица замен:

	8	7	6	5	4	3	2	1
0	1	13	4	6	7	5	14	4
1	15	11	11	12	13	8	11	10
2	13	4	10	7	10	1	4	9
3	0	1	0	1	1	13	12	2
4	5	3	7	5	0	10	6	13
5	7	15	2	15	8	3	13	8
6	10	5	1	13	9	4	15	0
7	4	9	13	8	15	2	10	14
8	9	0	3	4	14	14	2	6
9	2	10	6	10	4	15	3	11
10	3	14	8	9	6	12	8	1
11	14	7	5	14	12	7	1	12
12	6	6	9	0	11	6	0	7
13	11	8	12	3	2	0	7	15
14	8	2	15	11	5	9	5	5
15	12	12	14	2	3	11	9	3

Блок-схема алгоритма :