XXI Международная конференция
«Информатика: проблемы, методы, технологии»

МИРЭА - Российский технологический университет
Институт комплексной безопасности
и специального приборостроения

Средняя общеобразовательная школа № 66 г. Пензы
имени Виктора Александровича Стукалова

Технология генерации перестановок в программно-информационном комплексе защищенной передачи данных

Бистерфельд Н.С.
Бистерфельд О.А.

2021

АКТУАЛЬНОСТЬ ТЕМЫ

«Все последние годы мы отмечаем рост угроз в сфере информационной безопасности», участились случаи «масштабных и скоординированных кибератак». «Особое внимание нужно уделить защите компьютерных систем органов власти, государственных электронных сервисов, операторов связи, банковских организаций и крупных компаний».

В.В. Путин

Выступление на расширенной коллегии ФСБ 21.02.2020

«Вопросы кибербезопасности, применение передовых цифровых технологий заслуживают самого серьезного разговора… Важно услышать, воспринять опасения людей, насколько в новую эпоху будут защищены их права, права на частную жизнь, собственность, безопасность».

В.В. Путин

Выступление на 75-й сессии Генассамблеи ООН 22.02.2020

Один из самых распространенных видов киберпреступлений – несанкционированный доступ к передаваемым данных.

ЦЕЛИ РАБОТЫ

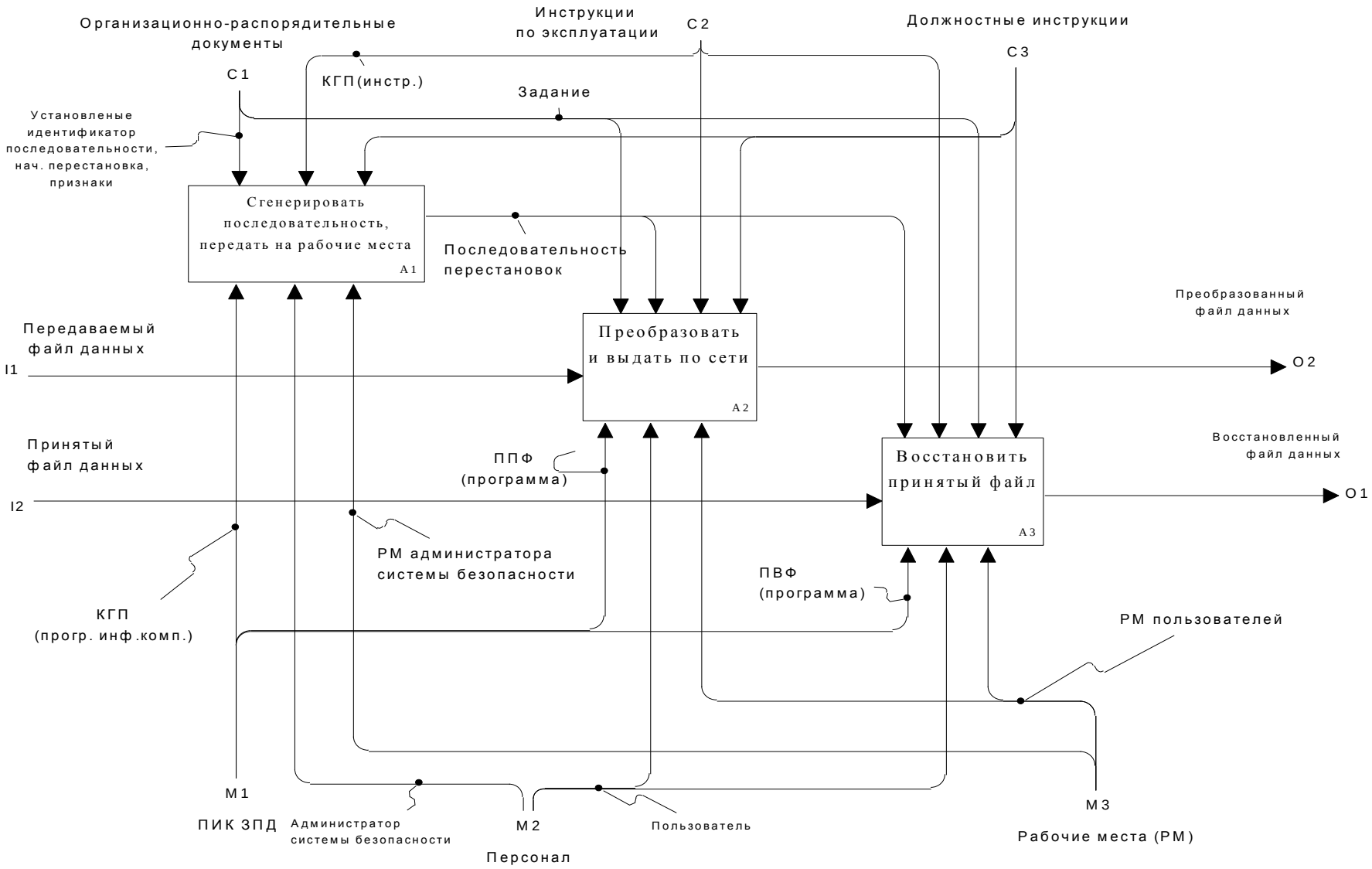
Цели работы:

✓повышение уровня защиты сетевой передачи данных в виде файлов;

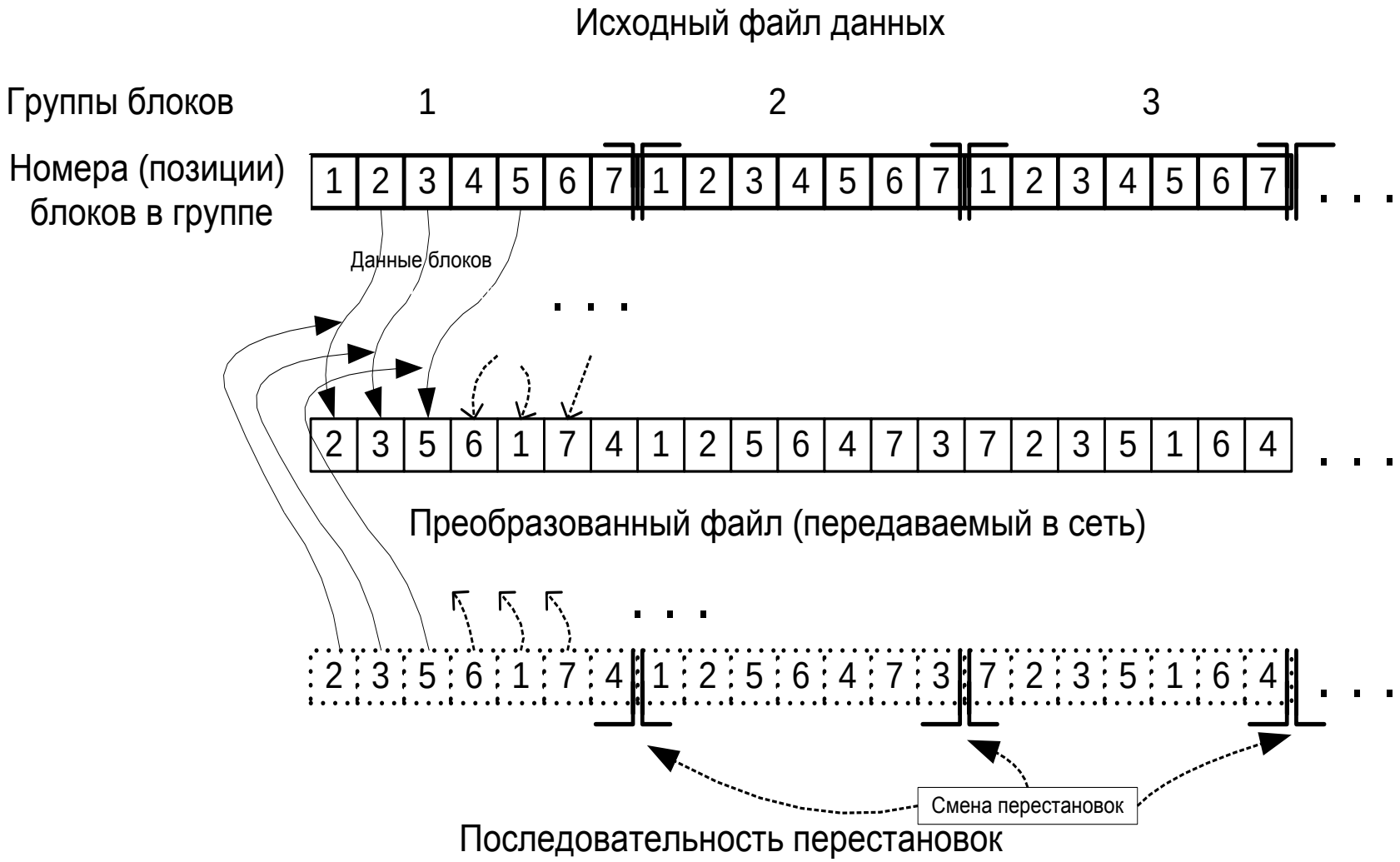
✓снижение затраты персонала на осуществление защищенных передач данных

путем создания и внедрения программно-информационного комплекса защищенной передачи данных.

ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ КОМПЛЕКСА



ПРЕДЛАГАЕМОЕ ПРЕОБРАЗОВАНИЕ ДАННЫХ



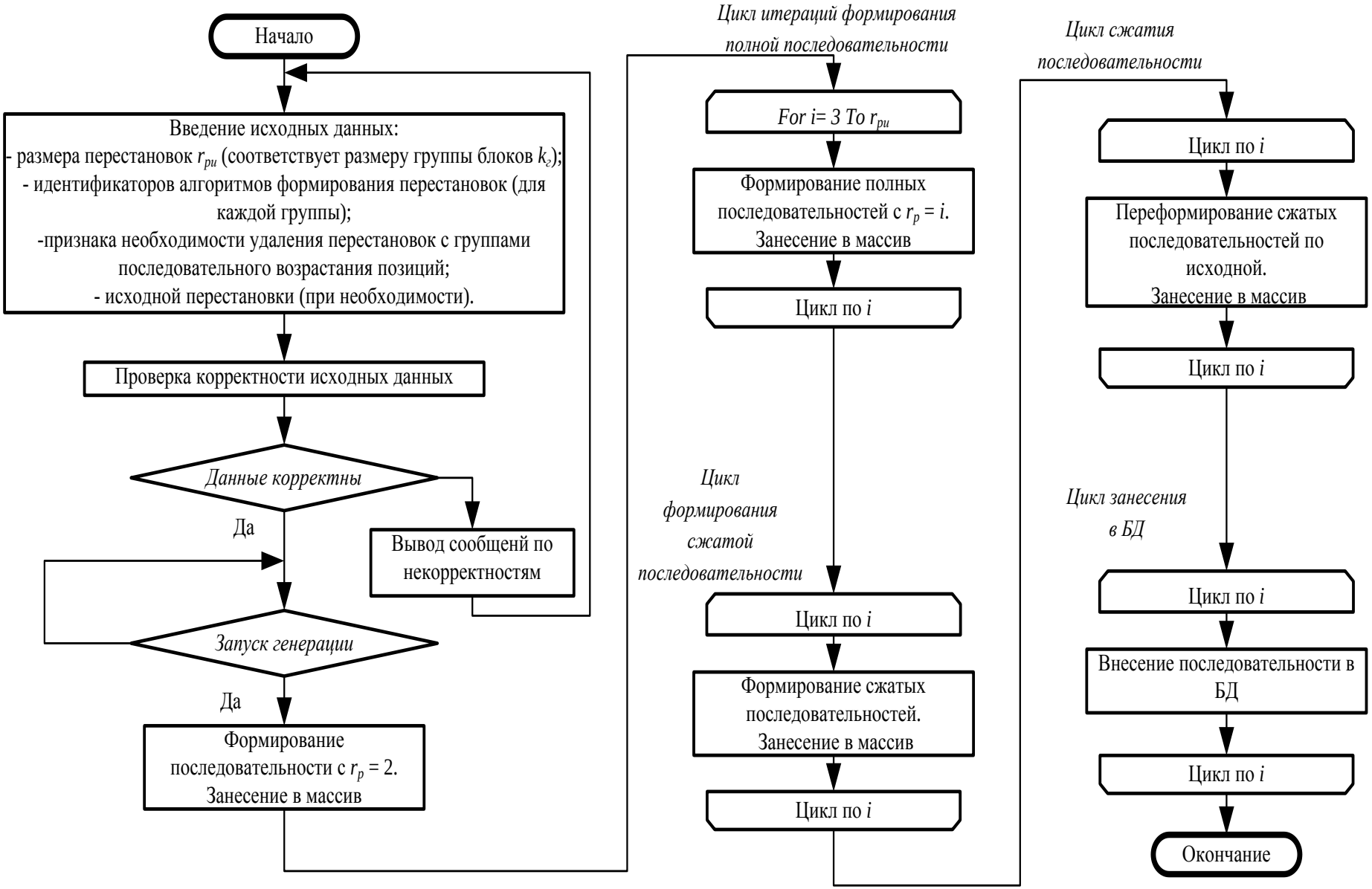
МЕХАНИЗМ КОДИРОВАНИЯ

Преобразуемый файл разбивается на группы блоков. Каждой группе блоков соответствует своя перестановка, в соответствии с которой переставляется содержимое блоков в формируемом файле. Переформированный файл передается в сеть. На приемной стороне проводится восстановление порядка следования блоков данных.

При выборе размера блока данных, не кратного размеру данных, представляющих символы, преобразовываются и символы передаваемых данных, что повышает криптостойкость алгоритма.

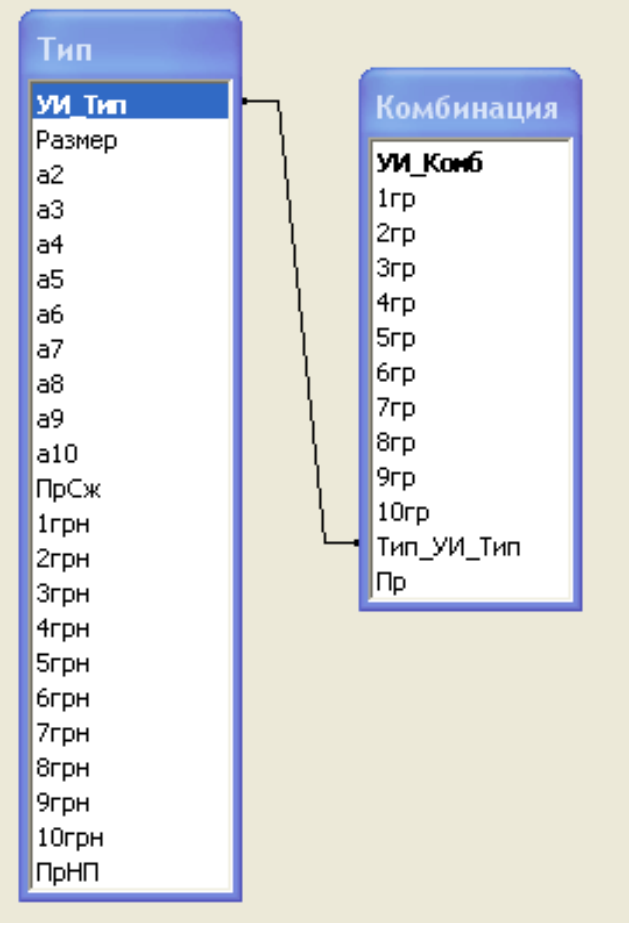
ГЕНЕРАТОР ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПЕРЕСТАНОВОК

Алгоритм

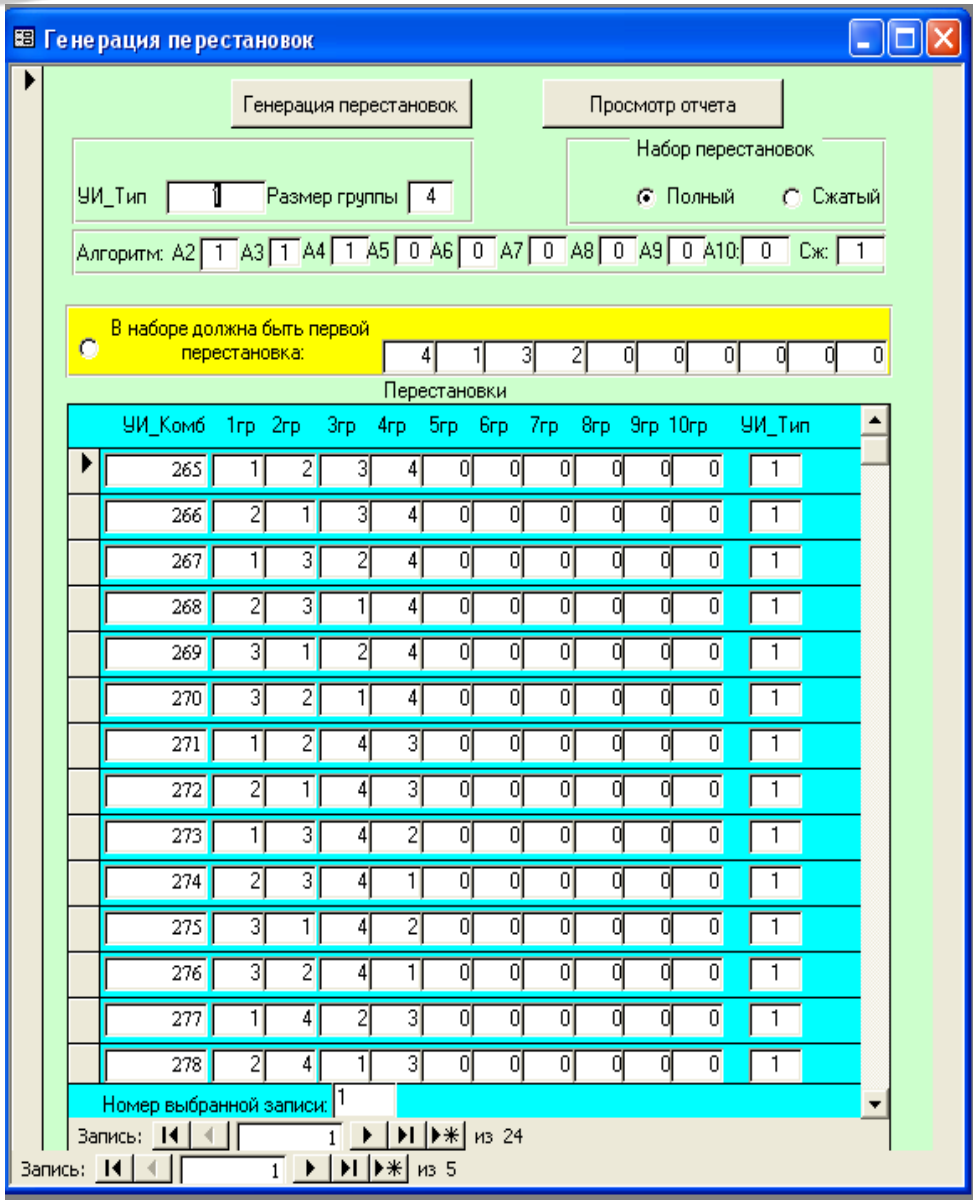


ГЕНЕРАТОР ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПЕРЕСТАНОВОК

Информационная модель



Экранная форма



РАЗРАБОТКА ГЕНЕРАТОРА ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПЕРЕСТАНОВОК

Отчет

Тип

Наборы перестановок

Размер 4

Алгоритмы: a2 a3 a4 a5 a6 a7 a8 a9 a10

1 1 1 0 0 0 0 0 0

Полный набор

4 1 3 2 0 0 0 0 0 0

1	2	3	4	0	0	0	0	0	0
2	1	3	4	0	0	0	0	0	0
1	3	2	4	0	0	0	0	0	0
2	3	1	4	0	0	0	0	0	0
3	1	2	4	0	0	0	0	0	0
3	2	1	4	0	0	0	0	0	0
1	2	4	3	0	0	0	0	0	0
2	1	4	3	0	0	0	0	0	0
1	3	4	2	0	0	0	0	0	0
2	3	4	1	0	0	0	0	0	0
3	1	4	2	0	0	0	0	0	0
3	2	4	1	0	0	0	0	0	0
1	4	2	3	0	0	0	0	0	0
2	4	1	3	0	0	0	0	0	0
1	4	3	2	0	0	0	0	0	0
2	4	3	1	0	0	0	0	0	0
3	4	1	2	0	0	0	0	0	0
3	4	2	1	0	0	0	0	0	0
4	1	2	3	0	0	0	0	0	0
4	2	1	3	0	0	0	0	0	0
4	1	3	2	0	0	0	0	0	0
4	2	3	1	0	0	0	0	0	0
4	3	1	2	0	0	0	0	0	0
4	3	2	1	0	0	0	0	0	0

Размер 4

Алгоритмы: a2 a3 a4 a5 a6 a7 a8 a9 a10

2 2 2 0 0 0 0 0 0

Сжатый набор

Должна быть начальной перестановка:

2 1 3 4 0 0 0 0 0 0

2	1	3	4	0	0	0	0	0	0
4	3	2	1	0	0	0	0	0	0
4	3	1	2	0	0	0	0	0	0
4	2	3	1	0	0	0	0	0	0
4	1	3	2	0	0	0	0	0	0
4	2	1	3	0	0	0	0	0	0
3	4	2	1	0	0	0	0	0	0
3	4	1	2	0	0	0	0	0	0
2	4	3	1	0	0	0	0	0	0
1	4	3	2	0	0	0	0	0	0
2	4	1	3	0	0	0	0	0	0
1	4	2	3	0	0	0	0	0	0
3	2	4	1	0	0	0	0	0	0
3	1	4	2	0	0	0	0	0	0
1	3	4	2	0	0	0	0	0	0
2	1	4	3	0	0	0	0	0	0
1	2	4	3	0	0	0	0	0	0
3	2	1	4	0	0	0	0	0	0
3	1	2	4	0	0	0	0	0	0
2	3	1	4	0	0	0	0	0	0
1	3	2	4	0	0	0	0	0	0

12 декабря 2020 г *Страница 1 из 13*

Тип

4	5	3	2	1	6	0	0	0	0
5	2	1	3	4	6	0	0	0	0
5	1	3	2	4	6	0	0	0	0
5	2	3	1	4	6	0	0	0	0
5	3	1	2	4	6	0	0	0	0
5	3	2	1	4	6	0	0	0	0
5	1	2	4	3	6	0	0	0	0
5	2	1	4	3	6	0	0	0	0
5	1	3	4	2	6	0	0	0	0
5	3	1	4	2	6	0	0	0	0
5	3	2	4	1	6	0	0	0	0
5	1	4	2	3	6	0	0	0	0
5	2	4	1	3	6	0	0	0	0
5	1	4	3	2	6	0	0	0	0
5	2	4	3	1	6	0	0	0	0
5	3	4	1	2	6	0	0	0	0
5	3	4	2	1	6	0	0	0	0
5	4	2	1	3	6	0	0	0	0
5	4	1	3	2	6	0	0	0	0
5	4	2	3	1	6	0	0	0	0
5	4	3	1	2	6	0	0	0	0
5	4	3	2	1	6	0	0	0	0
2	1	3	4	6	5	0	0	0	0
1	3	2	4	6	5	0	0	0	0
2	3	1	4	6	5	0	0	0	0
3	1	2	4	6	5	0	0	0	0
3	2	1	4	6	5	0	0	0	0
1	2	4	3	6	5	0	0	0	0

12 декабря 2020 г *Страница 13 из 13*

Страница: 13

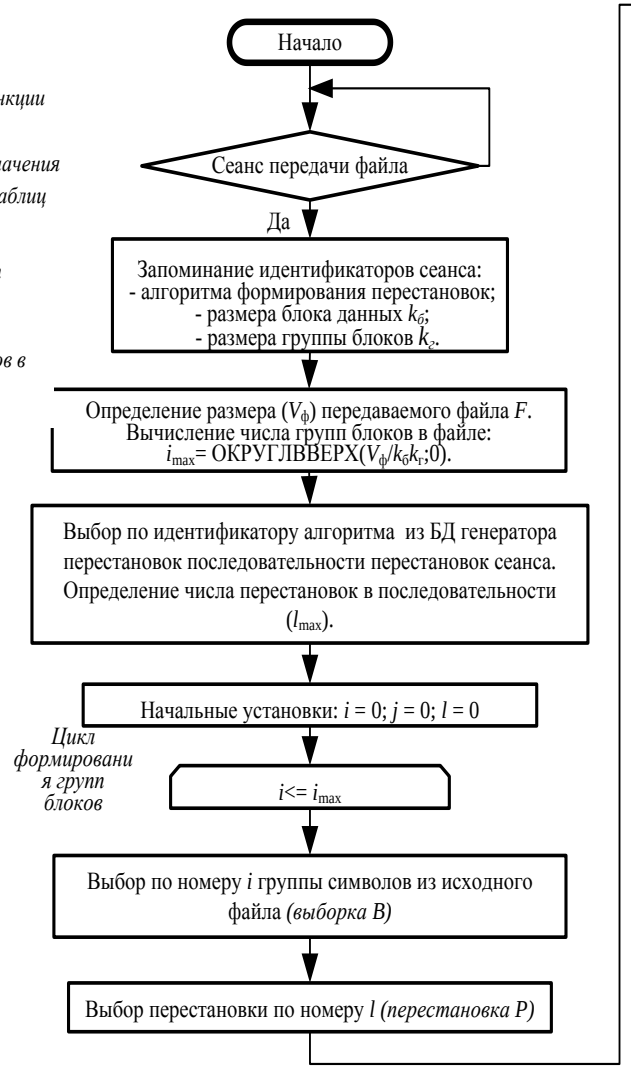
ПРОГРАММА ПРЕОБРАЗОВАНИЯ ФАЙЛА
Алгоритм

В обозначении функции округления используются обозначения из электронных таблиц Excel

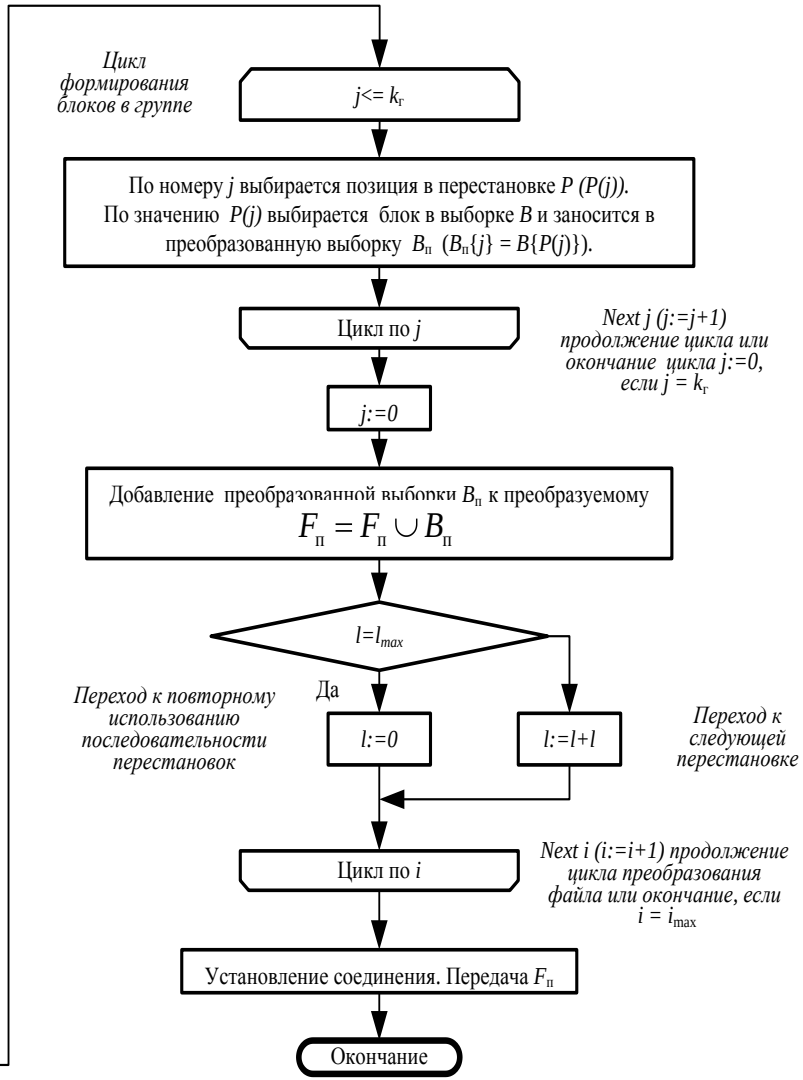
i – переменная цикла групп блоков;

j – переменная цикла блоков в группе;

l – переменная выбора перестановок.



В перестановке P: число позиций = $k_г$; P{позиция 1; позиция 2;...позиция $k_г$}



ПРОГРАММА ВОССТАНОВЛЕНИЯ ФАЙЛА
Алгоритм

В обозначении функции округления используются обозначения из электронных таблиц Excel

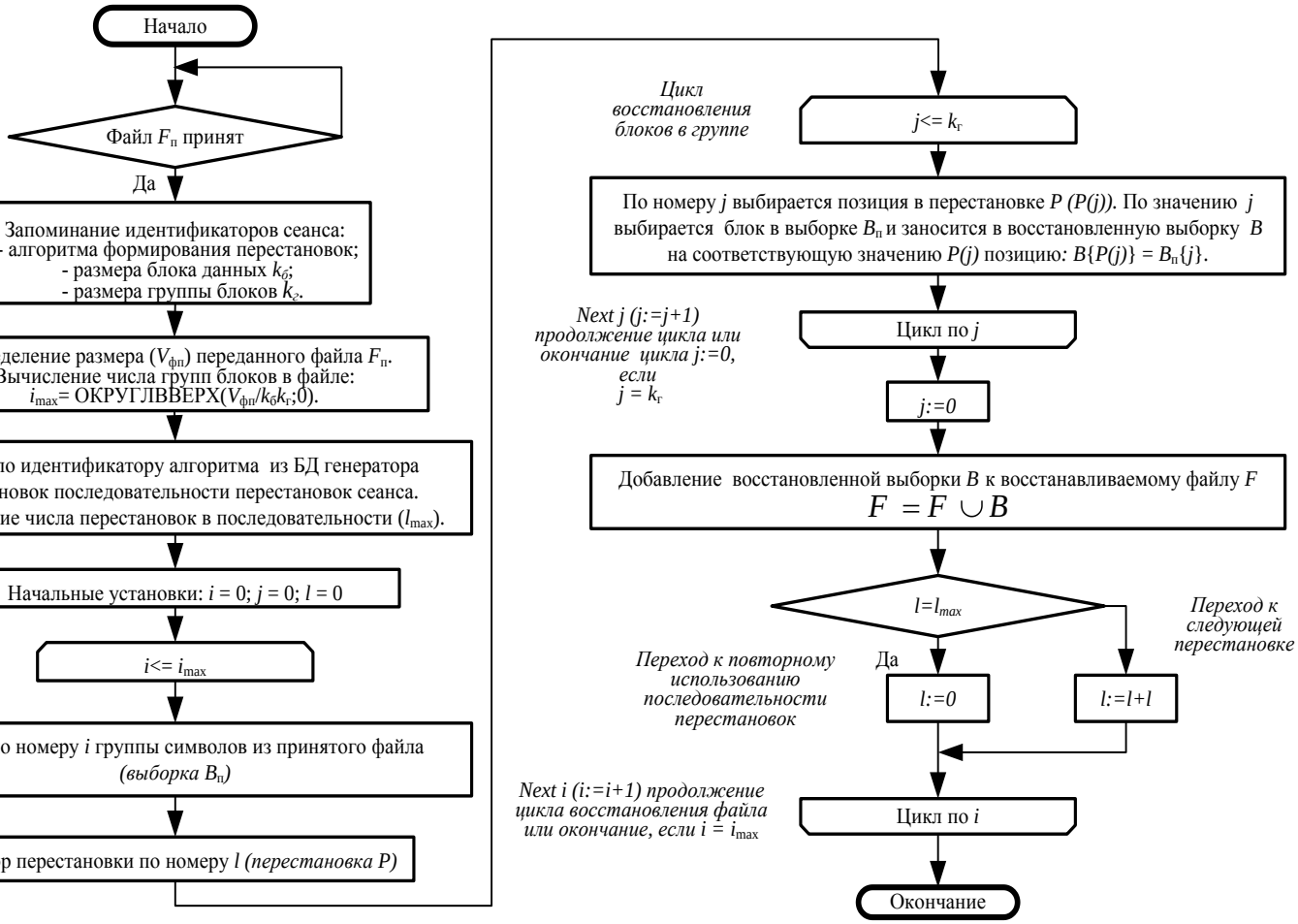
i – переменная цикла групп блоков;

j – переменная цикла блоков в группе;

l – переменная выбора перестановок.

В выборке $B_п$: число символов (бит) = $k_б k_г$; $k_г$ блоков по $k_б$ символов (бит) в каждом $B_п${блок 1;блок 2; ...блок $k_г$}

В перестановке P: число позиций = $k_г$; P{позиция 1; позиция 2;...позиция $k_г$}



ЗАКЛЮЧЕНИЕ

Был разработан программно-информационный комплекс защищенной передачи данных, включающий:

- программно-информационный компонент «Генератор перестановок»;
- программу «Преобразование файла»;
- программу «Восстановление файла».

Внедрение разработанного комплекса позволяет дополнительно повысить уровень зашиты данных, передаваемых между устройствами по сетевым каналам связи.

Кроме того, автоматизация процесса кодирования и декодирования информации существенно сократит затраты системных администраторов защиты данных.

Доклад закончен

Благодарю за внимание!