Технология генерации перестановок в программно-информационном комплексе защищенной передачи данных

О. А. Бистерфельд, email: bist19@yandex.ru [1]
Н. С. Бистерфельд, email: bist18@yandex.ru [2]

[1] Средняя общеобразовательная школа № 66 г. Пензы
имени Виктора Александровича Стукалова
[2] МИРЭА – Российский технологический университет

Аннотация. *В данной работе представлен образ программно-информационного комплекса защищенной передачи данных, включающего программно-информационный компонент «Генератор перестановок», программы «Преобразование файла» и «Восстановление файла». Приведено описание компонента «Генератор перестановок», предназначенного для формирования последовательностей перестановок, в соответствии с которыми проводится преобразование передаваемого файла (на передающей стороне) и восстановление файла (на приемной стороне).*

Ключевые слова: *информационная безопасность, передача данных, шифрование, метод перестановки.*

Введение

Одним из отрицательных явлений развивающейся в настоящий период цифровизации экономики являются разнообразные киберпреступления. Борьба с киберпреступностью обявляется государственной политикой, предпринимаются активные действия, выделяются громадные финансовые ресурсы по недопущению несанкционированного доступа к данным на уровне значимых предприятий и организаций различных форм собственности. Проводятся попытки организации согласованной политики по борьбе с киберпреступностью на международном уровне. Несанкционированный доступ к разнообразным данным возможен и при передаче данных. Такой вид преступлений является одним из самых распространенных.

Как правило, для передачи данных создаются организационно-технические системы разной сложности, в которых важной составной частью является персонал. Перед персоналом ставятся сложные задачи по защите от несанкционированного доступа, и снижение затраты персонала на осуществление защищенных передач данных также актуально.

С целью повышения уровня защиты сетевой передачи данных в виде файлов предлагается использовать программно-информационный комплекс защищенной передачи данных. Предлагаемый комплекс включает: программно-информационный компонент «Генератор перестановок» (КГП), программы «Преобразование файла» и «Восстановление файла». С помощью КГП формируются последовательности перестановок, в соответствии с которыми проводится преобразование передаваемого файла (на передающей стороне) и восстановление файла (на приемной стороне).

1. Программно-информационный компонент «Генератор перестановок»

Генерация перестановок широко известная процедура (например, [2]). Однако, в предлагаемом подходе необходимы частые и автоматические процедуры использования целого ряда различных последовательностей перестановок. В связи с этим предлагается реализовать генератор перестановок в виде небольшой базы данных, позволяющей как генерировать последовательности в соответствии с идентификаторами на используемые алгоритмы, так и сохранять и предоставлять сгенерированные последовательности перестановок.

Генератор перестановок предлагается использовать в средствах защищенной передачи данных по вычислительным сетям. Как вариант скрытия передаваемых данных могут быть использованы перестановки блоков передаваемых данных (групп символов). При выборе размера блока данных не кратного размеру данных, представляющих символы, преобразовываются и символы передаваемых данных, что повышает уровень защищенности при передаче в сети. В таких средствах необходим генератор перестановок как на передающей стороне (для перестановок символов или групп символов в передаваемых по сети данных), так и на приемной стороне (для восстановления принимаемых данных). Генераторы на передающей и на приемной стороне должны формировать одинаковую последовательность перестановок.

Для усложнения несанкционированного доступа к данным периодически необходимо менять используемую последовательность перестановок (одна из задач персонала).

В разработанном действующем прототипе генератора перестановок максимально возможный размер группы (гр) равен 10. При необходимости гр может быть увеличен.

В пределах размера группы меняются позиции передаваемых в канал связи символов (групп, части символов). На практике, конечно, представляют интерес существенные размеры групп (7, 8, 9 и 10 в действующем прототипе). Для каждой следующей группы символов

используется очередная перестановка из применяемой последовательности. После исчерпания всех перестановок последовательности, для следующих групп передаваемых в канал символов, использование последовательности перестановок повторяется.

Чередование перестановок в последовательности зависит от алгоритма генерации. В предлагаемом КГП реализованы несколько алгоритмов.

2. Информационная схема генератора перестановок

Генератор перестановок выполнен в виде базы данных (наименование БД - db1ПерестановкиW2). Схема таблиц БД представлена ниже (рис. 1**Ошибка! Источник ссылки не найден.**).

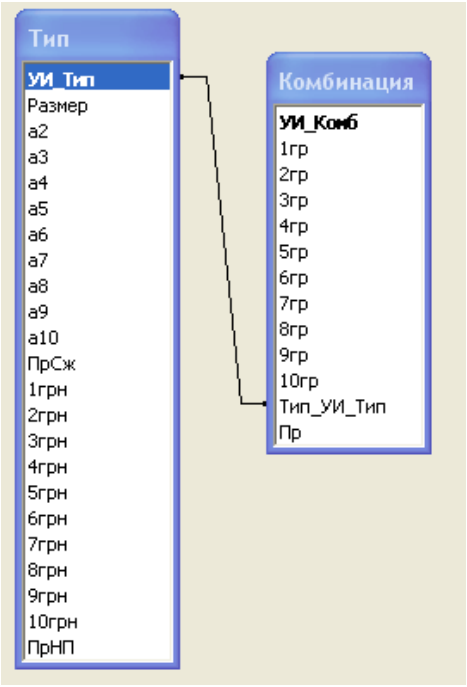

Рис. 1. Схема таблиц БД «db1ПерестановкиW2»

В таблице «Тип» сохраняют данные по размеру группы гр (колонка «Размер»), идентифицирующему кортежу используемых алгоритмов (колонки «a2», «a3», «a4», «a5», «a6», «a7», «a8», «a9», «a10»), признаку

сжатия последовательности (колонка «ПрСж»), идентифицирующему заданной начальной перестановки (колонки «1грн», «2грн», «3грн», «4грн», «5грн», «6грн», «7грн», «8грн», «9грн», «10грн»), признаку использования опции начальной перестановки (колонка «ПрНП»).

В таблице «Комбинация» сохраняют данные по сформированным последовательностям перестановок.

3. Форма, отчет и запрос генератора перестановок

Вид формы для генерации последовательностей перестановок представлен на рис. 2.

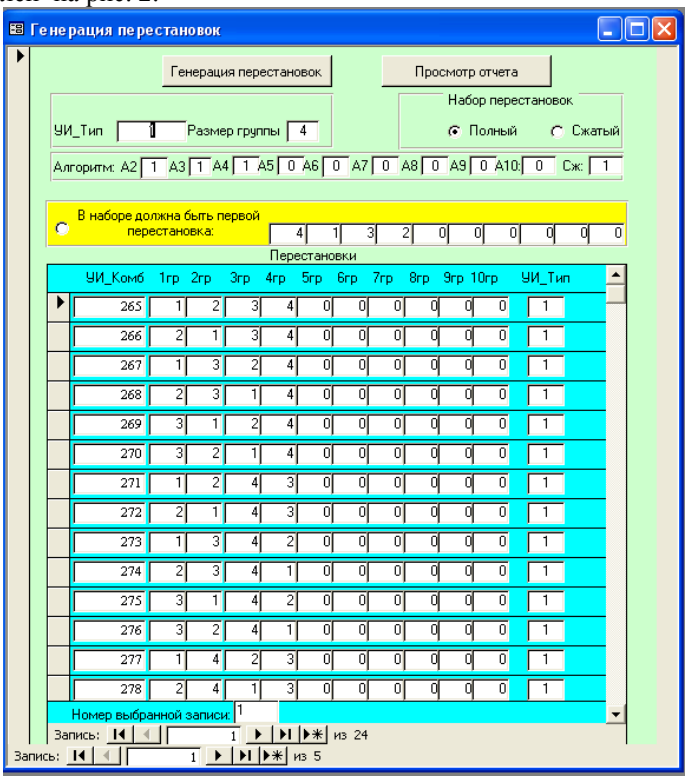

Рис. 2. Вид формы для генерации последовательностей перестановок

Идентифицирующие данные (размер группы, признак последовательности /полный или сжатый набор, кортеж используемых алгоритмов, признак начальной перестановки, сама начальная

перестановка) формируемой последовательности перестановок задаются в верхней части формы (с зеленым фоном).

Генерация последовательности запускается кнопкой «Генерация перестановок».

Сгенерированная последовательность заносится в подчиненную форму «Перестановки» (с голубым фоном, в нижней части формы, рис. 2).

По кнопке «Просмотр отчета» открывается отчет со сгенерированными последовательностями (рис. 3).

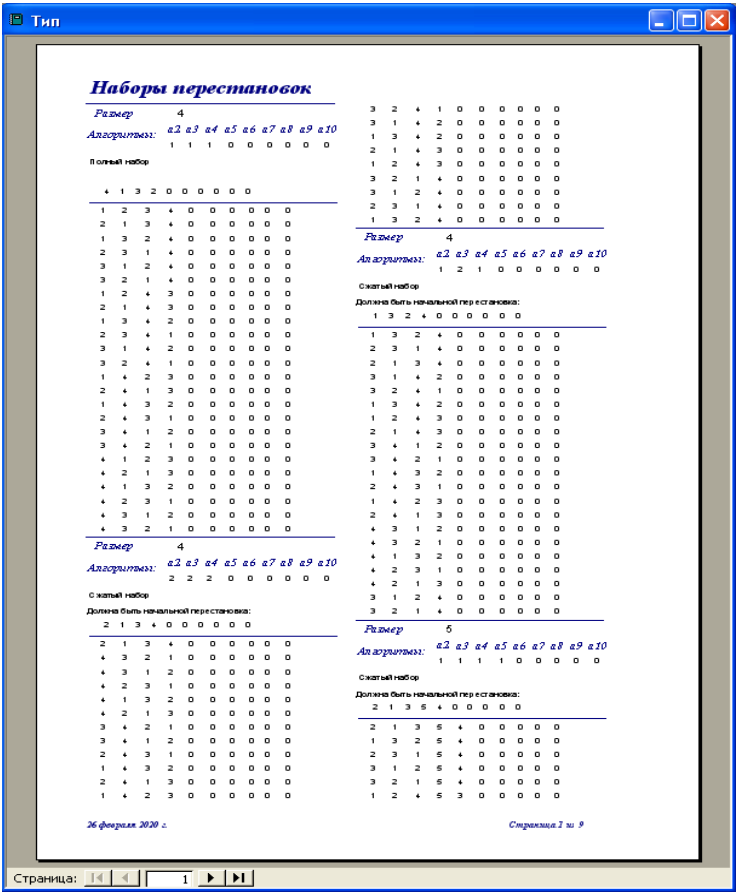

Рис. 3. Вид отчета с последовательностями перестановок

4. Программы «Преобразование файла» и «Восстановление файла»

В простейших схемах защиты передачи файла данных в компьютерных сетях:

- при передаче данных используют телекоммуникационные протоколы с подтверждением;
- перед передачей файла намеренно искажают содержимое файла, чем обеспечивают скрытие его содержимого; например, разбивают файл на группы (группы кодов символов или последовательности блоков двоичных бит файла); в пределах группы в соответствии с некоторой перестановкой (заранее известной и на передающей, и на приемной стороне; периодически такие перестановки меняют синхронно и на передающей и на приемной стороне) меняют порядок следования символов или блоков бит в файле; или криптографически преобразуют [1];
- передают преобразованный файл по сети от передающей к приемной стороне;
- на приемной стороне проводят обратное преобразование.

Такие способы недостаточно скрывают содержимое передаваемых данных. Существуют и другие способы намеренного искажения содержимого файла, но все они предусматривают определенный и неизменный в процессе передачи порядок начальной переработки и конечного восстановления файла; порядок преобразования известен заранее на приемной и на передающей стороне; предусматривают систематическое изменение, например, смена используемой перестановки на приемной и передающей стороне, но частая смена правила преобразования требуют от пользователей приемной и передающей стороны организационных затрат, вызывающих некоторое раздражение при использовании подобных средств защиты.

Предлагается ввести многократную и автоматическую смену правил преобразования файла по ходу первоначального формирования (а, следовательно, и соответствующие смены правил по ходу передачи файла в сети). Использование программы автоматической генерации перестановок (применяемой и на приемной и на передающей стороне) позволяет сократить организационные расходы администраторов системы безопасности. В большинстве случаев достаточно изменить только идентификатор алгоритма формирования перестановок и этого будет достаточно для смены правил преобразований файлов при их передаче по компьютерной сети.

Предлагаются следующие положения, реализуемые в разрабатываемых программах «Преобразование файла» и «Восстановление файла» для защищенной передачи файлов по сети:

- использование последовательностей перестановок при передаче файла;
- при генерации последовательностей перестановок исключение перестановки с последовательным возрастанием нескольких позиций (например, три и более позиции, что позволяет исключить практически все случаи последовательной передачи групп символов исходного файла);
- использование одной и той же программы генерации последовательности перестановок на приемной и передающей стороне и идентификаторов алгоритмов генерации, что позволяет при организационных решениях исключить необходимость передачи содержательных данных по защищенной трансляции файлов;
- в качестве дополнительной возможности исключение из оборота использование существующих общепринятых средств передачи файлов (программ трансляции файлов, транспортных протоколов с подтверждением) и переход к нестандартным средствам передачи файлов – пользовательским средствам, заменяющим стандартные; это затрудняет доступ к передаваемому и намеренно преобразованному файлу, а, кроме того позволяет в ряде случаев существенно ускорить передачу файлов.

Заключение

Внедрение программно-информационного комплекса защищенной сетевой передачи данных между устройствами существенно сократить затраты системных администраторов защиты данных, повысить уровень защищенности передаваемых данных, а в случае применения альтернативного транспортного протокола, сократить затраты и на собственно передачу данных.

Список литературы

1. Способ криптографического преобразования данных [Текст] : пат. 2734829, Российская Федерация : МПК: H04L 9/00 (2006.01) / Мартынов А. П. и др. ; Патентообладатели: Российская Федерация, от имени которой выступает Государственная корпорация по атомной энергии "Росатом" (Госкорпорация "Росатом"), Федеральное государственное унитарное предприятие "Российский федеральный ядерный центр - Всероссийский научно-исследовательский институт

экспериментальной физики" (ФГУП "РФЯЦ-ВНИИЭФ"). – № 2020109438; заявл. 03.03.2020 опубл. 23.10.2020.

2. Генератор перестановок. Перестановки без повторений и с повторениями [Электронный ресурс] – Режим доступа : https://prog-cpp.ru/permutation/