Докторов Александр Вячеславович
соискатель, заместитель начальника отдела
Научно-исследовательский испытательный центр
г. Знаменск, Астраханская область

РАЗРАБОТКА КРИПТОГРАФИЧЕСКОГО МЕТОДА ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ КОМБИНИРОВАННОГО ШИФРОВАНИЯ

***Аннотация**: в статье рассматривается актуальная проблема защиты информации. В работе автором выделяются ключевые методы защиты информации.*

***Ключевые слова**: защита информации, криптография, метод гаммирования, метод Виженера.*

В настоящее время в современном мире проблема защиты информации имеет огромное значение, особенно в военной сфере. Без использования криптографии сегодня немыслимо решение задач по обеспечению безопасности информации, связанной с конфиденциальностью и целостностью при передаче информации в сетях общего пользования.

Широкое внедрение в сферу обработки информации автоматизированных систем на базе электронной вычислительной техники, а также утверждение за информацией статуса материального ресурса потребовали разработки специальных мер, средств и систем защиты информации.

Уязвимость информации возрастает по мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации в автоматизированных системах управления. Это связано с процессами интеграции информации в базах данных, расширением крута лиц, имеющих доступ к интегрированным базам данных через компьютерные сети и системы коллективного пользования, широким распространением персональных ЭВМ и подключением их к компьютерным сетям; совершенствованием средств разведки и шпионажа различных уровней. Причем информация, обладая всеми свойствами

материальных ресурсов, имеет специфическую особенность – неисчерпаемость ресурса, что усложняет фиксацию факта ее хищения.

Проблема защиты информации представляет собой совокупность тесно связанных подпроблем в области права, организации управления, разработки технических средств, программирования и математики.

Анализ отечественной и зарубежной литературы позволил выделить следующие объективные причины, определяющие важность проблемы защиты информации:

− широкое применение ПЭВМ в самых различных сферах

− человеческой деятельности;

− высокие темпы роста парка ПЭВМ, находящихся в эксплуатации;

− высокая степень концентрации информации в ПЭВМ;

− совершенствование способов доступа пользователей к ресурсам ПЭВМ;

− усложнение вычислительного процесса в ПЭВМ.

Под защитой информации понимается совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач:

− проверки целостности информации;

− исключения несанкционированного доступа к ресурсам ПЭВМ и хранящимся в ней программам и данным;

− исключения несанкционированного использования хранящихся в ПЭВМ программ;

− защита программ и данных от несанкционированного копирования.

К основным современным методам шифрования можно отнести представленные ниже.

Шифрование заменой (подстановка).

Наиболее простой метод – прямая замена символов шифруемого сообщения другими буквами того же самого или другого алфавита. Однако такой шифр имеет низкую стойкость.

Шифрование методом перестановки.

Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов.

Стойкость простой перестановки однозначно определяется размерами используемой матрицы перестановки. Стойкость усложненных перестановок еще выше. Однако следует иметь ввиду, что при шифровании перестановкой полностью сохраняются вероятностные характеристики исходного текста, что облегчает криптоанализ.

Шифрование методом гаммирования.

Суть метода состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, называемой гаммой. Иногда такой метод представляют как наложение гаммы на исходный текст, поэтому он получил название «гаммирование».

Стойкость гаммирования однозначно определяется длиной периода гаммы. При использовании современных ПСЧ реальным становится использование бесконечной гаммы, что приводит к бесконечной теоретической стойкости зашифрованного текста.

Шифрование с помощью аналитических преобразований.

Достаточно надежное закрытие информации может обеспечить использование при шифровании некоторых аналитических преобразований. Например, можно использовать методы алгебры матриц – в частности умножение матрицы на вектор.

Метод Виженера.

Этот метод является простой формой многоалфавитной замены. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

Шифр Виженера «размывает» характеристики частот появления символов в тексте, но некоторые особенности появления символов в тексте остаются. Главный недостаток шифра Виженера состоит в том, что его ключ повторяется.

Проведя анализ всех вышеперечисленных методов выявлено, что каждый метод является недостаточно эффективным средством защиты информации в автоматизированных системах при несанкционированном доступе к ней.

Достаточно эффективным средством повышения стойкости шифрования является комбинированное использование нескольких различных способов шифрования, т.е. последовательное или параллельное шифрование исходного текста с помощью двух или более методов шифрования.

В связи с этим предлагается объединить два существующих метода, а именно метод гаммирования и метод Виженера и на их основе разработать новый метод комбинированного шифрования на языке высокого уровня, который позволит при смене ключей кодирования осуществлять несколько циклов кодирования для улучшения стойкости шифра, при этом стойкость повышается многократно. Достаточным является смена ключа и стартового кода без смены таблицы шифрования.

Усложнение методов и средств организации машинной обработки информации ведет к тому, что информация становится все более уязвимой. Этому способствуют такие факторы как постоянно возрастающие объемы обрабатываемых данных, накопление и хранение данных в ограниченных и фиксированных местах, постоянное расширение круга пользователей, имеющих доступ как к ресурсам ПЭВМ, так к программам и данным, хранящимся в них, усложнение режимов эксплуатации вычислительных систем и т. п.

Список литературы

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты / Б. Шнайер. – М.: Триумф, 2015. – 816 с.

2. Рябко В.Г. Криптографические методы защиты информации: учебное пособие для вузов / В.Г. Рябко, А.Н. Фионов. – М.: Горячая линия Телеком, 2017. – 225 с.

3. Гашков С.Б. Криптографические методы защиты информации: учебное пособие для вузов / С.Б. Гашков, Э.А. Применко, М.А. Черепнев. – М.: Академия, 2018. – 3014 с.

4. Панасенко С. Алгоритмы шифрования: специальный справочник / С. Панасенко. – СПб.: БХВ-Петербург, 2016. – 576 с.

5. Алферов А.П. Основы криптографии: учебное пособие / А.П. Алферов, А.К. Зубов. – 2-е изд. – М.: Гелиос АРВ, 2019. – 480 с.

6. Климова Л.М. Delphi 7. Основы программирования. Решение типовых задач: самоучитель / Л.М. Климова. – СПб.: Кудиц-Образ, 2016. – 480 с.

7. Глушаков С.В. Delphi 2017 г. / С.В. Глушаков. – М.: Хранитель, 2017. – 230 с.

8. Ященко В.В. Основные понятия криптографии / В.В. Ященко // Математическое просвещение. – 2018. – №2. – С. 170.

9. Карацуба А.А. Основы аналитической теории чисел / А.А. Карацуба. – М.: Наука, 2017. – 240 с.