УДК 004.056.57

Попов П.И. студент 2 курса КИТ
Северо-Восточный Федеральный университет
Россия, г.Якутск
Николаев Э.И. студент 2 курса КИТ
Северо-Восточный Федеральный университет
Россия, г.Якутск
Протодьяконова Галина Юрьевна
Кандидат педагогических наук, заведующая кафедрой
Россия, г. Якутск

ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ КРИПТОГРАФИИ

***Аннотация*:** *Статья посвящена основным методам и средствам криптографической защиты к анализу и их применениям*

Ключевые слова: *информация, защита информации, криптография.*

Annotation: *The article is devoted to the main methods and means of cryptographic protection to the analysis and their applications.*

Key words: *information, information security, cryptography.*

В современном мире, компьютеры, электронные средства передачи, обработки и хранения информации играют важную роль. Что касается информационных технологий в других областях, вы обязаны в первую очередь заняться своей безопасности и надежности. В самом широком смысле "безопасность" означает способность сохранять свою целостность и эффективность под внешним воздействием.

Самые простые методы шифрования существуют уже давно. Сегодня криптография содержит множество теорем и алгоритмов, как прикладных, так и фундаментальных. Невозможно работать с криптографией без серьезной

подготовки. На самом деле, вам нужно знать дискретную математику, теорию чисел и алгоритмы.

Криптография - это серия методов, предназначенных для защиты информационных взаимодействий от обычных регулярных потоков, путем злонамеренных действий различной тематики, методов, основанных на секретных алгоритмах преобразования информации, в том числе алгоритмах, которые на самом деле не просто секретные, а с секретными параметрами. В связи со сложностью взаимодействия информации в человеческом обществе возникают и развиваются новые вызовы.

Алгоритм преобразования криптографических данных

Предназначен для реализации аппаратного или программного обеспечения, он отвечает криптографическим требованиям и не ограничивает степень конфиденциальности защищенных данных.

Алгоритмы шифрования.

Ключевые алгоритмы шифрования предполагают, что никто не может читать данные, но нет ключа для их дешифрования.

Шифр простой подстановки

При замене шифрования символы в зашифрованном тексте заменяются символами того же или другого ошеломителя с правилом переопределения. В простом коде замены каждый символ в исходном тексте заменяется одинаковыми алфавитными символами в тексте. Часто простые заменяющие шифры называются простыми алфавитными заменяющими шифрами. Частым случаем простого заменяющего кода является фигура императора.

Криптографические средства защиты

Основными видами криптографической блокировки являются шифрование и кодирование защищаемых данных.

- Замена
- Перестановка
- Гаммирование
- Аналитическое преобразование шифруемых данных
- Комбинированные шифры и т.д

Средство криптографической защиты информации

Это специализированный программно-аппаратный инструмент компьютерной техники, реализуемый путем криптографического преобразования информации для обеспечения ее безопасности.

- Расшифровка-процесс извлечения обычного текста без знания криптографического ключа на известном шифровании. Термин "декодирование" обычно используется в процессе шифрования зашифрованного текста.

- Принудительное шифрование способность криптографического алгоритма шифрования чтобы выдержать.

Функция - шифрование безопасности, которая определяет его прочность для расшифровки, не зная ключа. Криптографические системы защиты информации можно разделить на два типа:

- Симметричные (одноключевые, с секретным ключом)
- Несимметричные (с открытым ключом)

Методы шифрования для защиты информации в системе автоматизации могут быть использованы для защиты данных, которые обрабатываются в компьютере или хранятся на различных типах устройств хранения данных, а также для остановки информации между различными элементами системы по линиям связи.

Своевременно стоит необходимость защиты информации, выраженная в создании национальной системы информационной безопасности (НСЗ). Правовые основы информационной безопасности. Принимаются и

реализуются законы о государственной тайне, об информации, информатизации и информационной безопасности, о правовой защите программ для ЭВМ и электронных баз данных и других целях защиты информации: предотвращение ущерба, который может возникнуть в результате утраты (кражи, утери, изменения, обработки информации) в одной из ее форм. Осуществлять соответствующие меры по защите от угроз информационной безопасности в соответствии с действующим законодательством и в сфере регулирования информационной безопасности, потребностей владельцев (пользователей) информации. Каждая документированная информация, которая может быть утеряна их владельцами, владельцами, пользователями и третьими лицами, может быть защищена таким образом, что может нанести ущерб владельцу. "Любое современное предприятие (учреждение, компания и другое), независимо от характера деятельности и формы собственности, не может успешно развиваться и осуществлять хозяйственную и иную деятельность, без создания надежной системы защиты вашей информации, которая не ограничивается только высокими нормативными мерами, но и методами контроля и обеспечения информационной безопасности при обработке, хранении и передаче в системе автоматизации, главным образом аппаратно-программных средств.

Средств защиты информации должны иметь сертификат, подтверждающий их соответствие требованиям информационной безопасности. Современные компьютеры за последние годы приобрели большую вычислительную мощность, но в то же время с ними стало намного проще работать. Пользоваться ими стало проще, поэтому все новые и новые, как правило, не квалифицированные лица, которым предоставлен доступ к компьютерам, что значительно облегчает задачу правонарушителям, поскольку в результате в облаке "мой стиль" большинство пользователей, которые управляют компьютерами самостоятельно.

Широкое внедрение сетевых технологий позволило объединить отдельные машины с локальными сетями, использующими общие ресурсы, а использование клиент-серверных и кластерных технологий превратило эти сети в распределенные вычислительные среды. Безопасность сети, безопасность всех компьютеров и сетевых устройств в сети, а также атака должны иметь только один компонент, чтобы нарушить всю сеть под угрозой. Современные телекоммуникации имеют локальные компьютерные сети, глобальная информационная среда-интегрированный интернет. Развитие Интернета вызвало растущий интерес к проблеме безопасности и вопросу об обязательном наличии средств защиты для сетей и систем, связанных с Интернетом, независимо от типа содержащейся в них информации. Дело в том, что интернет злоумышленников предлагает возможность глобальных уязвимостей безопасности. Если компьютер, являющийся объектом атаки, подключен к Интернету, для атаки не важно, где он находится-в соседней комнате или на другом континенте

Шифрование является одним из наиболее мощных средств обеспечения конфиденциальности и целостности информации. Во многих отношениях ключевое программное и аппаратное обеспечение не имеет первостепенного значения. Например, для ноутбуков, которые очень трудно защитить физически, только кодирование может гарантировать "конфиденциальность" даже в случае кражи.

Список литературы

1. Протодьяконова Г.Ю - Методы и средства защиты информации, изд. дом СВФУ, 2014. - 224 с
2. Бондарев В.В - Введение в информационную безопасность автоматизированных систем, Издательство: МГТУ им. Н. Э. Баумана, 2016г. -252с