УДК 004.056.5 : 519.72

Климова Екатерина Алексеевна
Студентка
Научный руководитель:
Половинко Екатерина Владимировна
кандидат пед. наук, доцент кафедры математики

ПРИМЕНЕНИЕ ТЕОРИИ ИНФОРМАЦИИ В КРИПТОГРАФИИ

Аннотация: работа посвящена исследованию теоретических основ и практических приложений теории информации в криптографии. Подробно рассмотрены основные понятия, такие как энтропия, неопределенность и мера информации, играющие ключевую роль в оценке стойкости криптографических систем. Изучены методы и алгоритмы, основанные на принципах теории информации, включая симметричное и асимметричное шифрование, а также хеширование и квантовую криптографию. Сделаны выводы о необходимости применения этих методов для повышения уровня информационной безопасности в современных условиях.

Ключевые слова: теория информации, криптография, энтропия, шифрование, хеширование, квантовая криптография, информационная безопасность, защита данных.

Криптография — наука о математических методах обеспечения конфиденциальности, целостности данных, аутентификации и шифрования. Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого текста на основе секретного алгоритма или ключа в шифрованный текст (шифротекст)

История применения теории информации в криптографии начинается в середине XX века, когда американский ученый Клода Элвуда Шеннон опубликовал революционную статью «The Mathematical Theory of

Communication» 1948, ставшую фундаментом современной теории информации. В этой работе Шеннон впервые предложил математическое описание природы информации и разработал идеи, впоследствии оказавшие огромное влияние на криптографию [1, с. 22].

До появления трудов Шеннона криптография была областью скорее искусства, нежели точной науки. Основой защиты служили примитивные алгоритмы шифрования, полагавшиеся главным образом на сложность алфавита и математические хитрости. Но Шеннон представил совершенно иное видение проблемы, введя понятие энтропии как меры неопределенности и открыв пути к разработке действительно надежных криптографических систем.

Ключевое открытие Шеннона состояло в том, что информация должна быть представлена в виде двоичных сигналов, причем величина неопределенности, связанная с любым источником информации, может быть выражена численно. Исходя из этого, стало возможным разработать строгие методы оценки надежности шифров и оценить пределы возможного разрушения защитных систем.

Одно из первых значительных приложений теории информации в криптографии произошло вскоре после публикации статьи Шеннона. Ученые начали понимать, что энтропия ключа шифрования напрямую влияет на стойкость криптосистемы. Другими словами, чем больше энтропия ключа, тем сложнее его восстановить. Этот вывод стал началом революции в подходе к разработке криптографических алгоритмов, породил переход от простых замещающих шифров к современным методам шифрования с высоким уровнем энтропии.

Особенно важное значение имела идея идеальной тайны Perfect Secrecy, изложенная Шенноном. Согласно ей, шифр идеально защищает информацию, если никакие предположения о содержании сообщения не улучшат шансы на его разгадку. Самым известным примером такого шифра стала одноразовая

лента One Time Pad, где секретный ключ равен длине самого сообщения и меняется для каждого нового послания.

Дальнейшие шаги привели к появлению новых идей, связанных с вероятностными моделями и стохастическими процессами, позволивших детально изучить слабость многих существовавших ранее шифров. Было показано, что традиционные методы вроде полиалфавитных шифров или шифров Цезаря могут быть преодолены статистическими методами, поскольку они недостаточно хорошо скрывают структуру текста.

Параллельно развивались математические основы для понимания криптостойкости на уровне полной системы, а не отдельно взятых фрагментов. Исследование энтропии помогло установить границы того, насколько мощным может быть ключ шифрования, каким образом определить уровень безопасности системы и какими свойствами должен обладать идеальный шифр.

Сегодня применение теории информации в криптографии продолжает развиваться. Уже появились системы, основанные на квантовом шифровании, где ключевым понятием вновь оказывается неопределенность, понимаемая теперь уже в квантовом смысле. Новые прорывы, связанные с энтропией и неопределенностью, продолжают открывать горизонты, создавая более надежные и сложные криптографические системы, способные надежно защищать данные в будущем.

Ее основными целями являются обеспечение трёх ключевых атрибутов информационной безопасности: конфиденциальности, целостности и аутентификации [2, с. 7].

Конфиденциальность означает невозможность прочтения сообщения посторонними лицами без владения специальным ключом. Цель целостности — гарантировать отсутствие изменений или подмены данных в процессе передачи или хранения. Аутентификация направлена на подтверждение истинности происхождения информации и идентификации субъектов обмена данными.

Основные направления современной криптографии включают:

- разработку и оценку надёжности криптографических алгоритмов и протоколов.

- создание и анализ алгоритмов, генерирующих уникальные короткие коды, используемые для верификации целостности данных.

- разработку цифровых подписей методов подтверждения авторства и целостности документов.

- исследование квантовой криптографии нового направления, основанного на уникальных свойствах квантово-механических явлений, обеспечивающих принципиально новую степень безопасности.

Методы криптографии традиционно подразделяются на две группы: симметричное и асимметричное шифрование. Симметричное шифрование предполагает использование единого секретного ключа как для шифрования, так и для дешифрации данных. Асимметричный подход, напротив, задействует пары ключей — открытый и закрытый, что позволяет решить проблему распространения ключей безопасным способом.

Широко применяемым дополнительным механизмом является хеширование, суть которого заключается в преобразовании произвольного набора данных в короткую строку фиксированной длины, называемую хэшем. Хэш функционирует как уникальный идентификатор объекта и используется для проверки целостности информации.

Включение в школьный курс информатики материалов, посвященных применению теории информации в криптографии, представляется целесообразным и важным этапом формирования у школьников представлений о механизмах защиты информации. Основываясь на понимании понятий энтропии, взаимной информации и неопределенности, учащиеся смогут глубже осознать природу криптографических алгоритмов и их роль в повседневной жизни.

Привнесение элементов теории информации позволит расширить представление учеников о сути криптографической защиты и повысит их

уровень осознанности при взаимодействии с конфиденциальными данными. Изучение таких тем, как распределение ключей, симметричное и ассиметричное шифрование, обеспечит прочную базу для последующего углубленного изучения программирования и безопасности в старших классах и вузах.

Важно отметить, что ознакомление с основами теории информации способствует формированию критического мышления и развивает умения самостоятельно анализировать проблемы, связанные с передачей и хранением информации. Интеграция рассматриваемых вопросов в уроки информатики сделает содержание курса ближе к реалиям современности и облегчит дальнейшее профессиональное самоопределение учащихся в области информационных технологий и защиты данных.

Практическое применение криптографии чрезвычайно обширно. Оно охватывает сферу финансовой безопасности, телекоммуникаций, электронную торговлю, персональные коммуникации и государственные службы. Криптографические методы обеспечивают защиту финансовых транзакций, аутентификацию пользователей, конфиденциальность электронных писем и чат-коммуникаций, а также безопасность мобильных устройств и облачных сервисов.

Список литературы

1. Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии. Учебное пособие. Москва : Горячая Линия – Телеком, 2006 – 42с.
2. Глухов М. М., Круглов И. А., Пичкур А. Б. Введение в теоретико-числовые методы криптографии. М.: Лань. 2024. 396 с.
3. Жданов О. Н., Лубкин И. А. Алгоритм RSA. Методические указания к выполнению лабораторных работ. Красноярск : СибГАУ, 2007. – 38с.