УДК 003.26

С. А. Гулевич,
факультет педагогики, менеджмента и информационных технологий в образовании,
Филиал Омского государственного педагогического университета в г. Таре
Научный руководитель: канд. пед. наук, доц. А. П. Федосеева

Общие сведения о современной криптографии и подходах к ее изучению

Аннотация. В статье рассмотрены основные понятия современной криптографии как основы обеспечения информационной безопасности общества; отмечены авторские подходы к ее изучению в научной и учебной литературе.

Ключевые слова: криптография, шифр, зашифрование, ключ, дешифрование, информационная безопасность.

Большинство развитых стран мира, в число которых входит Российская Федерация, переходят к информационному построению общества. Ключевым фактором такого изменения стало использование информационных технологий, обеспечение безопасности которых — основная задача криптографии.

Рассмотрим некоторые определения криптографии, которые предлагают современные ученые. Так, А. В. Аграновский дает следующее определение: «Криптография — область знания, объединяющая в себе разделы иных наук, основной целью которой принято считать изучение и создание криптографических преобразований и алгоритмов» [1, с. 4]. На основе сведений, представленных Л. К. Бабенко, удается сформулировать иное определение: криптография — наука, призванная с помощью различных вариантов кодирования информации защищать сведения от несанкционированного доступа к ним [2].

У криптографии как области знания имеется собственный перечень основных понятий. В первую очередь криптография связана с понятием конфиденциальности. Под конфиденциальностью понимают невозможность получения информации из преобразованного массива без знания дополнительной информации. Шифр — одно из ключевых понятий криптографии; некоторого рода преобразования имеющихся данных в закрытую информацию с использованием определенного алгоритма криптопреобразования. Зашифрование — преобразование имеющихся данных в закрытую информацию с помощью шифра. Встречается и несколько иное определение понятия «зашифрование», под которым понимается преобразование некоторого открытого текста в криптограмму. Под дешифрованием понимается обратный зашифрованию процесс, заключающийся в преобразовании закрытой информации в исходную путем использования неизвестного ключа или алгоритма. Иногда встречается понятие «расшифрование», синонимичное и носящее аналогичное термину «дешифрование» значение. Каждый шифр может быть дешифрован с помощью ключа. Ключ — определенное защищенное состояние алгоритма криптографии, позволяющего выбрать один вариант из множества для текущего алгоритма. При этом ключ бывает открытым и закрытым. В зависимости от того, насколько трудно дешифровать шифр без использования ключа, принято говорить о различных уровнях криптостойкости шифрования. Криптостойкость — свойство шифра, заключающееся в степени его защищенности от процесса дешифрования.

Вопросы, связанные с рассмотрением криптографии, отражены в научной и учебной литературе такими авторами, как Г. В. Басалова [3], Ж. Земор (в переводе В. В. Шуликовской) [5], П. П. Бескид [4], М. Ю. Пляскин [6] и др.

Книга Г. В. Басаловой «Основы криптографии» включает в себя ряд тематических лекций на тему криптографии. В них излагаются базовые структурные знания из данной области, в частности рассматриваются различные виды криптографического шифрования, алгоритмы шифрования и принципы их построения, а также основные направления применения криптографии и задачи информационной безопасности [3].

Более современный взгляд на криптографию как науку наблюдается в книге Ж. Земора «Курс криптографии». Автор предлагает новые идеи и решения для актуальных проблем информационной безопасности, в том числе описывает известные криптографические протоколы и указывает на их неточности, приводит коды, в которых выделяются и исправляются ошибки [5].

Особое внимание теоретическим аспектам криптографии уделено в учебном пособии П. П. Бескида и Т. М. Татарниковой «Криптографические методы защиты информации». Авторы последовательно ведут повествование от самых простых понятий, проиллюстрированных наглядными примерами и схемами, к более углубленным элементам криптографии. Немалое внимание уделено реально существовавшим в истории шифрам, к которым приводятся задания, а также иллюстрации в формате таблиц или рисунков [4].

В коллективной монографии В. А Майстренко, А. А. Соловьева, М. Ю. Пляскина, А. И. Тихонова «Современные радиоэлектронные средства и технологии информационной безопасности» дается полное математическое обоснование основным криптографическим методам шифрования и дешифрования информации, приводится краткий экскурс в историю с этапами развития и становления криптографии как части информационной безопасности, а также рассматриваются понятия открытых, закрытых ключей, их применение в процессе алгоритмизации шифрования и расшифрования информации [6].

Наиболее доступным языком изложены основные аспекты современной криптографии со всеми ее составляющими в учебном пособии Л. К. Бабенко «Криптографическая защита информации: симметричное шифрование». Особое внимание автор уделяет одному из самых больших разделов криптографии — симметричному блочному шифрованию [2].

Таким образом, криптография — одна из самых актуальных наук с точки зрения обеспечения не только безопасности отдельно взятых людей, но и всего государства в целом. Как говорил Натан Ротшильд, «кто владеет информацией — тот владеет миром», а криптография, в свою очередь, призвана защитить эту информацию от несанкционированного доступа.

1. *Аграновский А. В., Хади Р. А*. Практическая криптография: алгоритмы и их программирование. — М. : СОЛОН-Пресс, 2009. — 256 с.

2. *Бабенко Л. К., Ищукова Е. А.* Криптографическая защита информации: симметричное шифрование : учеб. пособие. — М. : Юрайт, 2019. — 220 с.

3. *Басалова Г. В.* Основы криптографии. — М. : Национальный Открытый Университет «ИНТУИТ», 2016. — 282 с.

4. *Бескид П. П., Татарникова Т. М.* Криптографические методы защиты информации. Ч. 1. Основы криптографии : учеб. пособие. — СПб. : Рос. гос. гидрометеороло г. ун-т, 2010. — 95 с.

5. *Земор Ж*. Курс криптографии / пер. В. В. Шуликовская. — М. ; Ижевск : Регулярная и хаотическая динамика : Ижев. ин-т компьютер. исследований, 2006. — 256 с.

6. Современные радиоэлектронные средства и технологии информационной безопасности : моногр. / В. А. Майстренко, А. А. Соловьев, М. Ю. Пляскин, А. И. Тихонов. — Омск : Изд-во Ом. гос. техн. ун-та, 2017. — 356 с.