Лекция 6. Криптографические методы защиты информации. Понятие шифра

Цель лекции: Ознакомить студентов с историей развития криптографических методов защиты информации с древних времён до наших дней. Рассмотреть криптографические методы защиты информации.

План лекции:

- Понятие шифров
- Шифр простой замены и его анализ
- Шифры перестановки и их анализ
- Требования к шифрам – принцип Керхгоффса
- Идеальный шифр и классы стойкости шифров

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. История криптографии - ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. Священные книги Древнего Египта, Древней Индии тому примеры.

Разные люди понимают под шифрованием разные вещи. Дети играют в игрушечные шифры и секретные языки. Это, однако, не имеет ничего общего с настоящей криптографией. Настоящая криптография (strong cryptography) должна обеспечивать такой уровень секретности, чтобы можно было надежно защитить критическую информацию от расшифровки крупными организациями - такими, как мафия, транснациональные корпорации и крупные государства. Настоящая криптография в прошлом использовалась лишь в военных целях. Однако сейчас, со становлением информационного общества, она становится центральным инструментом для обеспечения конфиденциальности.

Криптографические методы защиты основаны на возможности осуществления некой операции преобразования информации, которая может выполняться одним (или более) пользователем ИС, обладающим некоторой секретной частью дополнительной информации.

В классической криптографии используется только одна единица конфиденциальной и обязательно сек-ретной информации — ключ, знание которого позволяет отправителю зашифровать информацию, а получа-телю — расшифровать ее. Именно эта операция зашифрования/расшифрования с большой вероятностью невыполнима без знания секретного ключа.

В криптографии с открытым ключом имеется два ключа, по крайней мере один из которых нельзя вычис-лить из другого. Один ключ используется

отправителем для зашифрования информации, сохранность кото-рой должна быть обеспечена. Другой — получателем для обработки полученной информации. Бывают приложения, в которых один ключ должен быть несекретным, а другой — секретным.

Основным достоинством криптографических методов защиты информации является обеспечение ими гарантированной стойкости защиты, которую можно рассчитать и выразить в числовой форме (средним числом операций или количеством времени, необходимым для раскрытия зашифрованной информации или вычисления ключей).

Средства шифрования могут быть реализованы как аппаратно, так и чисто программно. В любом случае они должны быть сертифицированными, т.е. должны соответствовать определенным требованиям (стандар-там). В противном случае, они не могут гарантировать пользователям необходимую стойкость шифрования.

Использование в системе защиты для различных целей нескольких однотипных алгоритмов шифрования нерационально. Оптимальным вариантом можно считать систему, в которой средства криптозащиты — обще-системные, т.е. выступают в качестве расширения функций операционной системы и включают сертифици-рованные алгоритмы шифрования всех типов (блочные и потоковые, с закрытыми и открытыми ключами).

Прозрачное шифрование всей информации на дисках, что широко рекомендуется рядом разработчиков средств защиты, оправдано лишь в том случае, когда компьютер используется только одним пользователем и объемы дисков невелики. Но на практике даже персональные компьютеры используются группами из несколь-ких пользователей. И не только потому, что ПК на всех не хватает, но и в силу специфики работы защищен-ных систем. Так, автоматизированные рабочие места операторов систем управления используются двумя-четырьмя операторами, работающими посменно, и рассматривать их как одного пользователя нельзя в силу требований разделения ответственности.

Очевидно, что в такой ситуации приходится либо отказаться от разделения ответственности и разрешить пользоваться ключом шифра нескольким операторам, либо создавать отдельные закрытые диски для каждо-го из них и запретить им тем самым обмен закрытой информацией, либо часть информации хранить и пе-редавать в открытом виде, что по сути равносильно отказу от концепции прозрачного шифрования всей информации на дисках.

Кроме того, прозрачное шифрование дисков требует значительных накладных расходов ресурсов системы (времени и производительности). И не только непосредственно в процессе чтения-записи данных. Дело в том, что надежное криптографическое закрытие информации пред-полагает периодичес-кую смену ключей шифрования, а это при-водит к необходимости перешиф-

рования всей информации на диске с использованием нового ключа (необходимо всю инфор-мацию расшифровать с использованием старого и зашифровать с использованием нового ключа). Это требует значительного времени. Кроме того, при работе в системе с шифрованными дисками задержки возникают не только при обращении к дан-ным, но и при запуске программ, что значительно замедляет работу компьютера. Поэтому, использовать криптографическую защиту следует ограниченно, защищая только ту информацию, которую действительно надо закрыть от несанкционированно-го доступа.

Основные сведения о криптографии. Под криптологией (от греческого kruptos — тайный и logos сообщение) понимается наука о безопасности (сек-ретности) связи.

Криптология делится на две части: криптографию (шифрование) и криптоанализ. Криптограф пытается найти методы обеспечения секретности и или аутентичности (подлинности) сообщений. Криптоаналитик пытается выполнить обратную задачу: раскрыть шифртекст или подделать его так, чтобы он был принят как подлинный.

Одним из основных допущений криптографии является то, что криптоаналитик противника имеет полный шифртекст и ему известен алгоритм шифрования, за исключением секретного ключа. При этих допущениях криптограф разрабатывает систему, стойкую при анализе только на основе шифротекста. На практике допус-кается некоторое усложнение задачи криптографа. Криптоаналитик противника может иметь фрагменты открытого текста и соответствующего ему шифротекста. В этом случае криптограф разрабатывает систему стойкую при анализе на основе открытого текста. Криптограф может даже допустить, что криптоаналитик противника способен ввести свой открытый текст и получить правильный шифртекст с помощью секретно-го ключа (анализ на основе выбранного открытого текста), и наконец, — объединить две последние возмож-ности (анализ на основе выбранного текста).

Многие из стратегий нарушителя могут быть блокированы с помощью криптографических средств защи-ты информации, но следует отметить, что большинство стратегий нарушителя связано с проблемами аутен-тичности пользователя и сообщений.

Подсистема криптографической защиты. Подсистема объединяет средства криптографической защиты информации и предназначена для обеспече-ния целостности, конфиденциальности, аутентичности критичной информации, а также обеспечения юриди-ческой значимости электронных документов в ИС. По ряду функций подсистема кооперируется с подсистемой защиты от НСД. Поддержку подсистемы криптографической защиты в части управления ключами осуществ-ляет подсистема управления СЗИ.

Структурно подсистема состоит из:

♦ программных средств симметричного шифрования данных;

♦ программно-аппаратных средств цифровой подписи электронных документов (ПАС ЦП). Функции подсистемы предусматривают;

♦ обеспечение целостности передаваемой по каналам связи и хранимой информации;

♦ имитозащиту сообщений, передаваемых по каналам связи;

♦ скрытие смыслового содержания конфиденциальных сообщений, передаваемых по каналам связи и хранимых на носителях;

♦ обеспечение юридической значимости электронных документов;

♦ обеспечение аутентификации источника данных.

Функции подсистемы направлены на ликвидацию наиболее распространенных угроз сообщениям в авто-матизированных системах:

♦ угрозы, направленные на несанкционированное ознакомление с информацией;

♦ несанкционированное чтение информации на машинных носителях и в ЗУ ЭВМ;

♦ незаконное подключение к аппаратуре и линиям связи;

♦ снятие информации на шинах питания;

♦ перехват ЭМИ с линий связи;

♦ угрозы, направленные на несанкционированную модификацию (нарушение целостности) информации:

♦ изменение служебной или содержательной части сообщения;

♦ подмена сообщения;

♦ изъятие (уничтожение) сообщения.

♦ угрозы, направленные на искажение аутентичности отправителя сообщения:

♦ незаконное присвоение идентификаторов другого пользователя, формирование и отправка электрон-ного документа от его имени (маскарад), либо утверждение, что информация получена от некоего пользователя, хотя она сформирована самим нарушителем;

♦ повторная передача документа, сформированного другим пользователем;

♦ искажение критичных с точки зрения аутентичности полей документа (даты формирования, поряд-кового номера, адресных данных, идентификаторов отправителя и получателя и др.).

♦ угрозы, связанные с непризнанием участия:

♦ отказ от факта формирования электронного документа;

♦ отказ от факта получения электронного документа или ложные сведения о времени его получения;

♦ утверждение, что получателю в определенный момент была послана информация, которая в действи-тельности не посылалась (или посылалась в другое время).

Шифр простой замены, простой подстановочный шифр, моноалфавитный шифр — класс методов шифрования, которые сводятся к созданию по определённому алгоритму таблицы шифрования, в которой для каждой буквы открытого текста существует единственная сопоставленная ей буква шифр-текста. Само шифрование заключается в замене букв согласно таблице. Для расшифровки достаточно иметь ту же таблицу, либо знать алгоритм, по которому она генерируется.

Для вскрытия шифра простой замены используется такой метод криптоанализа как Частотный анализ.

Частотный анализ — основывается на предположении о существовании нетривиального статистического распределения отдельных символов и их последовательностей как в открытом тексте, так и в шифротексте, которое, с точностью до замены символов, будет сохраняться в процессе шифрования и дешифрования.

Частотный анализ предполагает, что каждая буква алфавита того или иного языка в довольно длинном тексте встречается с определенной частотой, к примеру, для русского языка известно, что буквы «О», «П», «Р» встречаются очень часто, а вот «Й», «Ъ» — редко. Как же работает данный метод? К примеру, имеется зашифрованный текст, полученный методом какой-либо перестановки букв по определенному алгоритму, и аналитикам требуется его расшифровать. Для этого берется открытый текст, желательно довольно длинный, затем подсчитывается в нем частота каждой буквы, причем, чем больше будет текст, тем точнее получится расшифровка.

Следующий шаг – то же самое проделывается с зашифрованным текстом, подсчитывается частота каждого символа. Собственно говоря, весь процесс расшифровки сводится к тому, что сопоставляются частоты двух текстов. Например, в открытом тексте буква «О» встречается с частотой 33%, то есть от общего количества букв текста, буква «О» составляет 33%, а в зашифрованном тексте с частотой 33% встречается буква «П», значит, с большей вероятностью под буквой «П» подразумевается «О».

К шифрам простой замены относятся многие способы шифрования, возникшие в древности или средневековье, как, например, Атбашь (также читается как этбаш) или шифр Цезаря. Для вскрытия подобных шифров используется частотный криптоанализ. Является частным случаем шифра подстановки.

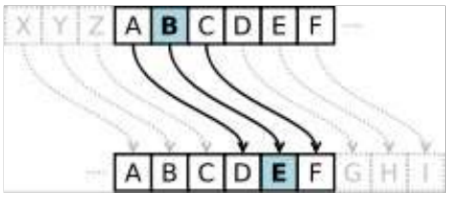


Рисунок 1 Принцип работы шифра Цезаря состоит в «сдвиге» букв на 3 позиции. Для расшифровки нужно произвести обратную операцию

ROT13 (англ. rotate; «сдвинуть на 13 позиций», иногда используется написание через дефис — ROT-13) представляет собой шифр подстановки простой заменой для алфавита английского языка (стандартной латиницы), используемый в интернет-форумах, как средство для сокрытия спойлеров, основных мыслей, решений загадок и оскорбительных материалов от случайного взгляда. ROT13 был охарактеризован как «сетевой эквивалент того, как в журналах печатают ответы на вопросы викторин — перевёрнутыми буквами»[1]. ROT13 — это вариация шифра Цезаря, разработанного в Древнем Риме.

ROT13 является обратимым алгоритмом, то есть отменить ROT13 можно, применив тот же алгоритм; одни и те же действия могут быть использованы для кодирования и декодирования. Алгоритм не дает никакой реальной криптографической безопасности и никогда не должен использоваться для этого. Он часто приводится в качестве канонического примера слабого метода шифрования. Алгоритм ROT13 породил разнообразные онлайн-игры с буквами и словами; алгоритм часто применяется в новостных группах (Usenet).Принцип работы программы ROT13, которая не предназначена для защиты, но лишь для скрытия текста (например, потенциально оскорбительного). Для восстановления текста алгоритм применяется повторно.

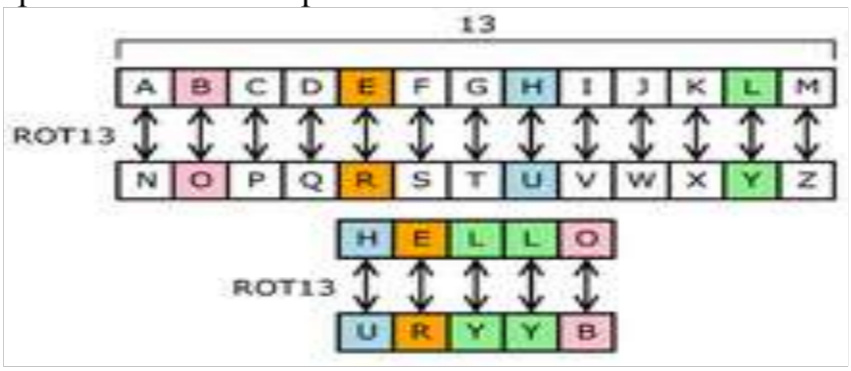


Рисунок 2 Принцип работы программы ROT13

Отметим, что шифр простой замены не всегда подразумевает замену буквы на какую-то другую букву. Допускается использовать замену буквы на число. К примеру представим некий шифр-алфавит: А - 33; Б - 17; В - 8; Г - 16; Д - 2; Е - 15; Ё - 14; Ж - 13; З - 73; И - 98; Й - 10; К - 97; Л - 96; М - 24; Н - 0; О - 11; П - 5; Р - 25; С - 7; Т - 3; У - 64; Ф - 26; Х - 66; Ц - 69; Ч - 4; Ш - 6; Щ - 36; Ь - 21; Ъ - 22; Ы - 23; Э - 37; Ю - 39; Я - 18.

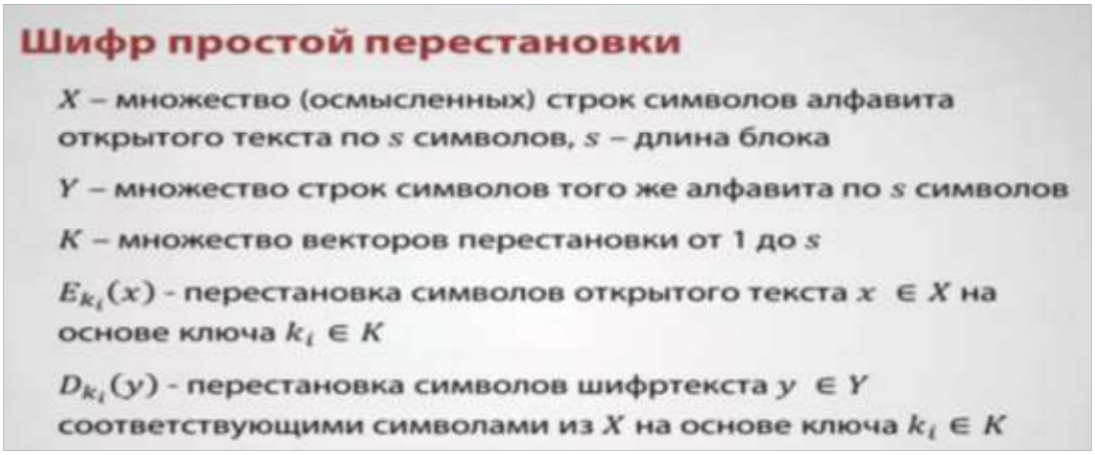
В данном шифре применяются числа, заменяющие буквы. Никакой логики в этих числах нет. Такой простой шифр можно расшифровать, только имея таблицу шифров.

Шифр перестано́вки — это метод симметричного шифрования, в котором элементы исходного открытого текста меняют местами. Элементами текста могут быть отдельные символы (самый распространённый случай), пары букв, тройки букв, комбинирование этих случаев и так далее. Типичными примерами перестановки являются анаграммы. В классической криптографии шифры перестановки можно разделить на два класса:

Шифры одинарной (простой) перестановки — при шифровании символы открытого текста перемещаются с исходных позиций в новые один раз.

Шифры множественной (сложной) перестановки — при шифровании символы открытого текста перемещаются с исходных позиций в новые несколько раз.

В качестве альтернативы шифрам перестановки можно рассматривать подстановочные шифры. В них элементы текста не меняют свою последовательность, а изменяются сами.



Точное время появления шифра перестановки не известно. Вполне возможно, что писцы в древности переставляли буквы в имени своего царя ради того, чтобы скрыть его подлинное имя или в ритуальных целях.

Одно из древнейших известных нам шифровальных устройств — Скитала. Бесспорно известно, что скитала использовалась в войне Спарты против Афин в конце V века до н. э.

Как правило, при шифровании и дешифровании шифра простой перестановки используется таблица перестановок:

1	2	3	...	n
I_1	I_2	I_3	...	I_n

Первая строка — позиция символа в открытом тексте, вторая строка — позиция в шифрограмме. Таким образом, при длине сообщения n символов существует ровно n! ключей.

Требования к шифрам – принцип Керхгоффса

Практическое применение шифров, в первую очередь для военных целей, пролило свет на требования к шифрам, которые возникают по причине того, что они неправильно используются или сами не слишком совершенны: не очень удобны или обладают какими-то неудобствами или изъянами. После гражданской войны Севера и Юга в Соединенных Штатах большинство проблем, связанных с использованием шифром, стали очевидны. Это было связано с тем, что огромное количество зашифрованных депеш передавались между действующими армиями, столицей, различными штабами генералов, различными подразделениями. Кроме того, это была одна из первых войн, в которой активно использовалось телеграфная связь. Например, Север даже снабжал полевые штабы своих генералов отдельными линиями телеграфной связи.

Проблемы, которые при этом возникали, были следующие. Во-первых, противник мог перехватывать большой объем сообщений и активно проводить их анализ. Кроме того, в это время уже был известен способ подключения к телеграфным проводам и перехвата сообщений, передаваемых по телеграфу. Значит, для сохранения секретности требовалось передавать информацию по телеграфным проводам в зашифрованном виде. Непременно иначе они могли бы быть без проблем читаемы противником. Преобразование шифра, то есть EK и DK, то есть преобразование зашифрования и расшифрования, рано или поздно становится общеизвестными, становятся известны противнику. Полагаться на надежность шифра из-за того, что противнику не известны именно эти преобразования, неразумно, поскольку он достаточно быстро об этом узнает. И если весь секрет состоит только в них, сможет читать переписку без особого труда. Требуется использование значительного числа ключей, а многократно используемые ключи также становятся известными противнику. Например, южане использовали для шифров инженеров всего три, хотя и очень длинных, ключа. Достаточно быстро они стали известны разведчикам северян. И, соответственно, шифрованная переписка Юга уже не была надежно скрыта от командования северных войск, который могли таким образом принимать верные тактические решения, зная о планах своего противника. Кроме того, очень часто сталкивались абоненты с тем, что отправители сообщений, которые они получали, допускали ошибки в зашифровании сообщения, а это в свою

очередь приводило к тому, что сообщение вовсе невозможно прочесть. Известен случай, когда один из генералов запрашивал подкрепление, отправил гонца с зашифрованной депешей. Несколько часов ушло в бесплодных попытках эту депешу расшифровать и прочесть, после чего был отправлен обратно к отправителю гонец, для того чтобы запросить уже открытое сообщение в явном виде. Но к этому времени подкрепление уже не требовалось, к этому времени тот, кто запрашивал подкрепление, уже потерпел поражение и отступил.

В ответ на эти проблемы голландский автор Огюст Керхгоффс опубликовал в журнале военных наук, французском журнале, свой труд под названием «Военная криптография», или по-французски Cryptographie militaire. Данная работа состояла из четырех частей, описывавших современное на тот момент состояние криптографии, и, в частности, формулировала требование к шифрам, которое следовало предъявлять для того, чтобы эти шифры можно было бы комфортно и надежно использовать в военных условиях.

Требования, которые сформулировал Огюст Керхгоффс в своей работе, следующие:

- Система должна быть физически, если не математически невзламываемой. Это означает, что даже если шифр теоретически можно взломать, например перебрать все его ключи, или подобрать каким-то образом к нему атаку, которая позволит прочесть открытый текст, это должно быть либо физически нереализуемо, либо очень сложно, трудозатратно, то есть на самом деле неосуществимо.
- Сама система при этом не должна секретной, а ее попадание в руки противника не должно вызывать никаких неудобств. То есть секретность должна основываться только на неизвестном ключе.
- Ключ должен быть пригодным для передачи и хранения без каких-либо записей, а также для изменений и модификации по желанию корреспондентов. Это означает, что ключ должен легко меняться и никаким образом не влиять на работу системы.
- Система должна быть пригодна для передачи сообщений по телеграфу — это отвечает современному на тот момент уровню развития технологий. Передовым методом связи был телеграф, и система должна была выдавать такой шифр-текст, который можно было бы передавать по телеграфу. Можно сказать, что этому требованию как раз соответствует разработка шифров Плейфера и двух квадратов в противовес таблице де ла Порта.
- Система должна быть портативной и не требовать дополнительного персонала для ее обслуживания. Данное требование означает то, что как можно меньше людей должны быть посвящены в работу шифровальной системы, шифровального устройства. Не должно быть никаких помощников,

дополнительных ассистентов, которые могли бы знать секреты и таким образом стать целью, например, вражеской разведки.

- Система должна быть простой и не требовать от пользователя ни существенных умственных усилий, ни знания большого перечня правил использования.

Здесь Керхгоффс стремился максимально оградить от ошибок пользователя шифровальных устройств, поскольку в полевых условиях офицерам службы связи, которые зашифровывают и расшифровывают депеши, приходилось обрабатывать большое количество данных в, можно сказать, экстремальных условиях — в условиях военных действий. Поэтому вероятность ошибок тут была максимальная, и именно в упрощении системы Керхгоффс видел защиту от этого. Два из этих требований до сих пор считаются актуальными и именуются принципом Керхгоффса, двумя как бы его составляющими.

Первое требование: сама система не должна быть секретной, а ее попадание в руки противника не должно вызывать никаких неудобств. Это означает — на современном языке, с современной точки зрения, — что все элементы шифра, кроме конкретного выбранного ключа, и, конечно же, конкретного открытого текста, не являются секретными. Анализ надежности шифра происходит в предположении, что противник знает о шифре абсолютно все: оба преобразования (зашифрование и расшифрование), множество открытых и шифр текстов, множество ключей, принцип выработки ключей и его использование, то есть конкретно выбранного ключа. И факт того, что противник это знает, никаких неудобств вызывать не должен. Стойкость системы должна быть основана исключительно на секретности ключа.

И вторая часть принципа Керхгоффса: ключ должен быть пригодным для передачи и хранения без каких-либо записей. Как правило, это требование уже опускается, а также для изменений и модификаций по желанию корреспондентов. Это означает, что корреспонденты должны быть способны в любой момент менять ключ так часто, как им это требуется. Если существует подозрение о том, что ключ был перехвачен противником, он должен быть легко заменен. Не должно быть никаких с этим проблем. Например, если мы вспомним диск Альберти, в нем ключ был настоящим устройство, то есть внутренним диском с расположенными на нем символам, и заменить его было, наверное, нетривиально. Требовалось, чтобы его изготовили, чтобы его каким-то образом доставили абонентам. И после этого они достаточное время должны им пользоваться, до тех пор пока не будет изготовлен новый ключ. Вот в соответствии с принципом Керхгоффса это недостаток — ключ должен легко изменяться. Любый ключ из как бы множества ключей должен быт доступен для выбора абонентом в любой момент.

На основе принципов Керхгоффса разрабатывались новые шифры в конце XIX и начале XX века, но затем они столкнулись с новым испытанием в уже

новом уровне развития технологий, а именно с Первой мировой войной, где помимо телеграфа активно вышло на передний план как средство связи радио. А радио, как известно, может быть легко перехвачено противником, поэтому уровень противодействия между противоборствующими сторонами еще более усилился.

Идеальный шифр и классы стойкости шифров

После того, как во Вторую мировую войну и даже еще на начальном ее этапе было показано, что шифровальные машины тоже не обеспечивают надежного уровня секретности, то есть могут быть подвержены успешным атакам по криптоанализу, по взлому, идеи того, можно ли в принципе построить идеальный, то есть совершенно невзламываемый шифр, витала в воздухе, и желательно было получить на нее ответ. Ответ на этот вопрос приписывается чаще всего американскому математику Клоду Шеннону, автору фундаментальных трудов по теории информации, который в опубликованном в 1945 году и рассекреченном в 1949 году труде "Теория связи в секретных системах" ответ на этот вопрос дал. В русской историографии также указывается, что схожие результаты получил отечественный ученый по фамилии Котельников. Указывается также, что буквально накануне начала Великой отечественной войны, в 1941 году, рукопись с аналогичными результатами он сдал на хранение в Наркомат связи, ну а в самое ближайшее врея началась война, и рукопись до послевоенного времени оказалась невостребованной. К тому моменту труд Клода Шеннона уже был опубликован. Результат, который, предлагает Шеннон, заключается в следующем. Во-первых, что такое идеальный шифр Как его описывал Шеннон? Это такой шифр, который противник не может взломать даже за неограниченное время. Это базируется на том, что даже перехватив шифр-текст, противник не получает никакой информации об открытом тексте или выбранном ключе.

Стойкость шифра – это способность шифра противостоять атакам на него. Стойким считается алгоритм, который для успешной атаки требует от противника недостижимых вычислительных ресурсов, недостижимого объёма перехваченных открытых и зашифрованных сообщений или же такого времени раскрытия, что по его истечению защищенная информация будет уже не актуальна, и т. д.

В криптографии различают три типа стойкости:

- **вычислительная стойкость** – когда имеется потенциальная возможность вскрыть шифр, но при выбранных в шифры параметрах и ключах на современном этапе розвития криптоанализа у противника не хватит вычислительных ресурсов и времени для вскрытия. Если алгоритм вскрытия

шифра на современных мощных компьютерах должен выполнить $\approx 2^{80}$ операций, то шифр называют вычислительно стойким. Никакой реальный шифр нельзя обоснованно считать вычислительно защищенным, поскольку мы не знаем, как доказать оптимальность найденного метода взлома. Не являются вычислительно стойкими: шифры сдвига, замены, Виженера. К вычислительно стойким шифрам относятся DES, AES, RSA, шифр Эль-Гамаля.

- **информационно-теоретическая стойкость** (или абсолютную стойкость), когда криптоаналитик не может раскрыть криптосистему ни теоретически, ни практически, даже имея бесконечно большие вычислительные ресурсы. Доказательства стойкости в такой модели выводятся из теории информации;
- **доказуемая стойкость,** при которой доказательство стойкости криптосистеми сводят к решению определенной трудно решаемой математической проблемы, положенной в основу алгоритму. Например, криптосистема RSA стойка, если модуль алгоритму n нельзя факторизовать.

Большинство современных шифров, входящих в государственные стандарты различных стран, а также стойкие коммерческие шифры являются именно шифрами практической стойкости. Эта теория разделения шифров на классы стойкости, как мы видим, основаны на теории Шеннона о абсолютной стойкости. Собственно, опять же, как видно из примеров, сами по себе абсолютно стойкие шифры не получили повсеместного арспространения, а распространенными стали шифры практической стойкости, которые и составляют основную часть используемых в современном мире шифров.

Список использованной литературы

1. Adam Shostack. “Threat Modeling: Designing for Security”. Published by John Wiley & Sons, Inc., Canada 2014.- 626 p.
2. Richard Bejtlich. “The Practice of Network Security Monitoring”. Published by No Starch Press, Inc., USA 2013. – 380 p.
3. Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams and Abdul Aslam. “Enterprise Cybersecurity: how to build a successful Cyberdefense program against advanced threats”. Published by Apress, 2015. – 508 p.
4. Хорев А. А. Организация защиты конфиденциальной информации в коммерческой структуре // Защита информации. Инсайд : журнал. — 2015. — № 1. — С. 14—17. — ISSN 2413-3582
5. Фред Б. Риксон. Коды, шифры, сигналы и тайная передача информации. — Астрель, 2011. — ISBN 978-5-17-074391-9.