

Государственное бюджетное профессиональное образовательное учреждение
«Краснодарский краевой базовый медицинский колледж»
министерства здравоохранения Краснодарского края

Цикловая комиссия Общеобразовательных дисциплин

Проект

ШИФРОВАНИЕ ИНФОРМАЦИИ

Студентов Крюковой Екатерины Сергеевны, Герасимовой Виктории
Александровны
специальности 34.02.01 Сестринское дело
1 курса, группы Е-11

Руководитель проекта: Гришай Вероника Сергеевна, преподаватель
Рецензент: Иванова Елена Ивановна, преподаватель

Проект допущен к защите.

Заместитель директора по учебной работе _____ И.В. Ротаренко
(подпись)

" ____ " _____ 20__ г.

Дата защиты: « ____ » _____ 20__ г.

Оценка _____

Краснодар 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	3
СВЕДЕНИЯ О ПРОЕКТЕ	4
ГЛАВА 1. ШИФРОВАНИЕ. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ	6
1.1. Что такое шифр, криптограмма, криптография.....	6
1.2. Типы шифров.....	8
1.3. Наиболее известные и значимые шифры	13
ГЛАВА 2. ПРИМЕНЕНИЕ ШИФРОВ.....	16
2.1. Кодировка и шифры в повседневной жизни	16
2.2. Обеспечение безопасности информации.....	23
ВЫВОДЫ И ЗАКЛЮЧЕНИЕ	29
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	Ошибка! Закладка не определена.

ВВЕДЕНИЕ

Актуальность темы. Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. Среди всего спектра методов защиты данных от нежелательного доступа особое место занимают криптографические методы. 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.

С широким распространением письменности криптография стала формироваться как самостоятельная наука.

Актуальность темы очевидна, т.к. информация в современном обществе – одна из самых ценных вещей в жизни, требующая защиты от несанкционированного проникновения лиц, не имеющих к ней доступа.

Цель проекта: ознакомление с многообразием видов шифрования, ролью и определением области практического применения кодирования информации.

Задачи проекта:

1. Выполнить анализ литературных источников и Интернет-ресурсов по теме проекта.
2. Систематизировать, углубить и расширить знания о кодировании информации.
3. Написать реферат по теме проекта.
4. Подготовить мультимедийную презентацию для защиты проекта.

СВЕДЕНИЯ О ПРОЕКТЕ

Участники проекта.

1. Студентка 1 курса группы 11 специальности "Сестринское дело"
Крюкова Екатерина Сергеевна.

2. Студентка 1 курса группы 11 специальности "Сестринское дело"
Герасимова Виктория Александровна.

Сроки реализации проекта: октябрь 2018 г. – май 2019 г.

Этапы реализации проекта.

№	Этап выполнения проекта	Сроки выполнения
1.	Разработка и утверждение темы проекта.	Октябрь 2018 г.
2.	Формулировка цели, постановка задач проекта.	Ноябрь 2018 г.
3.	Распределение задач между участниками проекта.	Ноябрь 2018 г.
4.	Анализ литературных источников и Интернет-ресурсов по теме проекта.	Декабрь 2018 г. - Январь 2019 г.
5.	Написание реферата: введения, основной части, выводов и заключения.	Февраль - Март 2019 г.
6.	Корректировка реферата, внесение дополнений и изменений.	Апрель 2019 г.
7.	Оформление списка литературы и документации по проекту.	Апрель 2019 г.
8.	Подготовка мультимедийной презентации для защиты проекта.	Апрель - Май 2019 г.
9.	Защита (презентация) проекта.	Май 2019 г.

Место проведения презентации проекта: ГБПОУ «Краснодарский краевой базовый медицинский колледж», актовый зал.

Оснащение для реализации и презентации проекта:

- Интернет-ресурсы;
- справочная и электронная литература;
- мультимедийный проектор (или интерактивная доска);
- персональный компьютер (или ноутбук).

ГЛАВА 1. ШИФРОВАНИЕ. ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

1.1. Что такое шифр, криптограмма, криптография

Для любой операции над информацией (даже такой простой, как сохранение) она должна быть как-то представлена. Этот процесс имеет специальное название – кодирование информации. Мы знаем, насколько огромны возможности компьютеров, и широк спектр их применения сегодня и можем только догадываться, какие задачи смогут решать они в ближайшем будущем. Поэтому особенно остро встает вопрос о знании и понимании способов представления информации в компьютере. Нужно, чтобы люди имели понятие о кодировании информации и о возможных способах кодирования разных видов информации. Кодирование информации — одна из базовых тем курса теоретических основ информатики, отражающая фундаментальную необходимость представления информации в какой-либо форме. При этом слово «кодирование» понимается не в узком смысле — кодирование как способ сделать сообщение непонятным для всех, кто не владеет ключом кода, а в широком — как представление информации в виде сообщения на каком-либо языке.

Главной целью шифрования является хранения важной информации в ненадёжных источниках и передачи её по незащищённым каналам связи.

Если разобрать шифрование по этапам, то сначала идет шифрование информации, затем передача ее от одного лица другому, после чего последний дешифрует эту информацию.

Шифрование – это преобразование (кодирование) открытой информации в зашифрованную, недоступную для понимания посторонних.

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования расшифрования.

Криптографические преобразования обеспечивают решение двух главных проблем: проблемы секретности (лишение противника возможности извлечь информацию из канала связи) и проблемы имитостойкости (лишение противника возможности ввести ложную информацию в канал связи или изменить сообщение так, чтобы изменился его смысл).

Шифр — система условных знаков для секретного письма, читаемого с помощью ключа.

Основной характеристикой шифра является криптостойкость, которая определяет его стойкость к раскрытию методами криптоанализа. Обычно эта характеристика определяется интервалом времени, необходимым для раскрытия шифра.

Ключ - это конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Вскрытие шифра — процесс получения защищаемой информации (открытого текста) из зашифрованного сообщения (шифртекста) без знания примененного шифра.

Дешифрирование — процесс, обратный шифрованию, и заключающийся в преобразовании зашифрованного сообщения в защищаемую информацию с помощью определенных правил, содержащихся в шифре.

Окончательно обработанное и отосланное секретное сообщение называется **криптограммой**.

То, что изучает все вышеперечисленное, это **криптография** — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства.

Криптография — одна из старейших наук, её история насчитывает несколько тысяч лет.

Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в зашифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифровывание и расшифровывание проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Криптография не занимается защитой от обмана, подкупа или шантажа законных абонентов, кражи ключей и других угроз информации, возникающих в защищённых системах передачи данных.

1.2. Типы шифров

Как было сказано ранее, **шифр** — система условных знаков для секретного письма, читаемого с помощью ключа. Существует огромное количество шифров, которые можно разбить на несколько типов:

- Симметричные шифры;
- Ассиметричные шифры;
- Блочные шифры;
- Поточные шифры.

Симметричные криптосистемы (также симметричное шифрование, симметричные шифры) — способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. До изобретения схемы асимметричного шифрования единственным существовавшим способом являлось симметричное шифрование. Ключ алгоритма должен сохраняться в тайне обеими сторонами, осуществляться меры по защите доступа к каналу, на всем пути следования криптограммы, или сторонами взаимодействия посредством криптообъектов, сообщений,

если данный канал взаимодействия под грифом "Не для использования третьими лицами". Алгоритм шифрования выбирается сторонами до начала обмена сообщениями.

Алгоритмы шифрования данных широко применяются в компьютерной технике в системах сокрытия конфиденциальной и коммерческой информации от злонамеренного использования сторонними лицами. Главным принципом в них является условие, что передатчик и приемник заранее знают алгоритм шифрования, а также ключ к сообщению, без которых информация представляет собой всего лишь набор символов, не имеющих смысла.

Классическими примерами таких алгоритмов являются симметричные криптографические алгоритмы, перечисленные ниже:

- Простая перестановка
- Одиночная перестановка по ключу
- Двойная перестановка
- Перестановка «Магический квадрат»

Простая перестановка без ключа — один из самых простых методов шифрования. Сообщение записывается в таблицу по столбцам. После того, как открытый текст записан колонками, для образования шифртекста он считывается по строкам. Для использования этого шифра отправителю и получателю нужно договориться об общем ключе в виде размера таблицы. Объединение букв в группы не входит в ключ шифра и используется лишь для удобства записи несмыслового текста.

Одиночная перестановка по ключу - более практический метод шифрования, называемый одиночной перестановкой по ключу, очень похож на предыдущий. Он отличается лишь тем, что колонки таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

Двойная перестановка используется для дополнительной скрытности; можно повторно шифровать сообщение, которое уже было зашифровано.

Этот способ известен под названием двойная перестановка. Для этого размер второй таблицы подбирают так, чтобы длины её строк и столбцов отличались от длин в первой таблице. Лучше всего, если они будут взаимно простыми. Кроме того, в первой таблице можно переставлять столбцы, а во второй строки. Наконец, можно заполнять таблицу зигзагом, змейкой, по спирали или каким-то другим способом. Такие способы заполнения таблицы если и не усиливают стойкость шифра, то делают процесс шифрования гораздо более занимательным.

Магическими квадратами называются квадратные таблицы со вписанными в их клетки последовательными натуральными числами от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Подобные квадраты широко применялись для вписывания шифруемого текста по приведенной в них нумерации. Если потом выписать содержимое таблицы по строкам, то получалась шифровка перестановкой букв. На первый взгляд кажется, будто магических квадратов очень мало. Тем не менее, их число очень быстро возрастает с увеличением размера квадрата. Так, существует лишь один магический квадрат размером 3×3 , если не принимать во внимание его повороты. Магических квадратов 4×4 насчитывается уже 880, а число магических квадратов размером 5×5 около 250000. Поэтому магические квадраты больших размеров могли быть хорошей основой для надежной системы шифрования того времени, потому что ручной перебор всех вариантов ключа для этого шифра был невыносим.

Криптографическая система с открытым ключом (разновидность асимметричного шифрования, асимметричного шифра) — система шифрования и/или электронной подписи (ЭП), при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения. Для генерации ЭП и для расшифровки сообщения используется закрытый ключ.

Асимметричное шифрование с открытым ключом базируется на следующих принципах:

- Можно сгенерировать пару очень больших чисел (открытый ключ и закрытый ключ) так, чтобы, зная открытый ключ, нельзя было вычислить закрытый ключ за разумный срок. При этом механизм генерации является общеизвестным.
- Имеются надёжные методы шифрования, позволяющие зашифровать сообщение открытым ключом так, чтобы расшифровать его можно было только закрытым ключом. Механизм шифрования является общеизвестным.
- Владелец двух ключей никому не сообщает закрытый ключ, но передает открытый ключ контрагентам или делает его общеизвестным.

Если необходимо передать зашифрованное сообщение владельцу ключей, то отправитель должен получить открытый ключ. Отправитель шифрует свое сообщение открытым ключом и передает его получателю (владельцу ключей) по открытым каналам. При этом расшифровать сообщение не может никто, кроме владельца закрытого ключа.

В результате можно обеспечить надёжное шифрование сообщений, сохраняя ключ расшифровки секретным для всех - даже для отправителей сообщений.

Блочный шифр — разновидность симметричного шифра^[1], оперирующего группами бит фиксированной длины — блоками, характерный размер которых меняется в пределах 64–256 бит. Если исходный текст (или его остаток) меньше размера блока, перед шифрованием его дополняют. Фактически, блочный шифр представляет собой подстановку на алфавите блоков, которая, как следствие, может быть моно- или полиалфавитной. Блочный шифр является важной компонентой многих криптографических протоколов и широко используется для защиты данных, передаваемых по сети.

В отличие от шифроблокнота, где длина ключа равна длине сообщения, блочный шифр способен зашифровать одним ключом одно или несколько сообщений суммарной длиной больше, чем длина ключа. Передача малого по сравнению с сообщением ключа по зашифрованному каналу — задача значительно более простая и быстрая, чем передача самого сообщения или ключа такой же длины, что делает возможным его повседневное использование. Однако, при этом шифр перестает быть невзламываемым. От поточных шифров работа блочного отличается обработкой бит группами, а не потоком.

При этом блочные шифры надёжней, но медленнее поточных. Симметричные системы обладают преимуществом над асимметричными в скорости шифрования, что позволяет им оставаться актуальными, несмотря на более слабый механизм передачи ключа (получатель должен знать секретный ключ, который необходимо передать по уже налаженному зашифрованному каналу. В то же время, в асимметричных шифрах открытый ключ, необходимый для шифрования, могут знать все, и нет необходимости в передаче ключа шифрования).

К достоинствам блочных шифров относят сходство процедур шифрования и расшифрования, которые, как правило, отличаются лишь порядком действий. Это упрощает создание устройств шифрования, так как позволяет использовать одни и те же блоки в цепях шифрования и расшифрования. Гибкость блочных шифров позволяет использовать их для построения других криптографических примитивов: генератора псевдослучайной последовательности, поточного шифра, имитовставки и криптографических хешей.

Пото́чный или **Пото́ковый шифр** — это симметричный шифр, в котором каждый символ открытого текста преобразуется в символ шифрованного текста в зависимости не только от используемого ключа, но и от его расположения в потоке открытого текста. Поточный шифр реализует другой подход к симметричному шифрованию, нежели блочные шифры.

1.3. Наиболее известные и значимые шифры

Необходимость засекречивать важные послания возникла еще в древности. Со временем люди находили новые, все более сложные способы делать послания недоступными чужим глазам. Древние рукописи и языки были поняты с помощью техник декодирования и дешифрования. Фактически коды и шифры определяли исход многих войн и политических интриг на протяжении всей истории человечества. Существуют тысячи типов шифрования сообщений и вот некоторые из них.

В транспозирующих шифрах буквы переставляются по заранее определенному правилу. Например, если каждое слово пишется задом наперед, то из «all the better to see you with» получается «lla eht retteb ot ees joY htiw». Другой пример — менять местами каждые две буквы. Таким образом, предыдущее сообщение станет «la tl eh eb tt re ot es ye uo iw ht». Подобные шифры использовались в Первую Мировую и Американскую Гражданскую Войну, чтобы посылать важные сообщения. Сложные ключи могут сделать такой шифр довольно сложным на первый взгляд, но многие сообщения, закодированные подобным образом, могут быть расшифрованы простым перебором ключей на компьютере.

Шифр ROT1 известен многим детям. Ключ прост: каждая буква заменяется на следующую за ней в алфавите. Так, А заменяется на В, В на С, и т.д. «ROT1» значит «ROTate 1 letter forward through the alphabet» (*англ.* «сдвиньте алфавит на одну букву вперед»). Сообщение «I know what you did last summer» станет «J lopx xibu zpv eje mbtu tvnnfs». Этот шифр весело использовать, потому что его легко понять и применять, но его так же легко и расшифровать. Из-за этого его нельзя использовать для серьезных нужд, но дети с радостью «играют» с его помощью.

В азбуке Морзе каждая буква алфавита, все цифры и наиболее важные знаки препинания имеют свой код, состоящий из череды коротких и длинных сигналов, часто называемых «точками и тире». Так, А — это «•—», В — «—

...», и т.д. В отличие от большинства шифров, азбука Морзе используется не для затруднения чтения сообщений, а наоборот, для облегчения их передачи (с помощью телеграфа). Длинные и короткие сигналы посылаются с помощью включения и выключения электрического тока. Телеграф и азбука Морзе навсегда изменили мир, сделав возможной молниеносную передачу информации между разными странами, а также сильно повлияли на стратегию ведения войны, ведь теперь можно было осуществлять почти мгновенную коммуникацию между войсками.

Шифр Цезаря называется так, как ни странно, потому что его использовал сам Юлий Цезарь. На самом деле шифр Цезаря — это не один шифр, а целых двадцать шесть, использующих один и тот же принцип! Так, ROT1 — всего один из них. Получателю нужно сказать, какой из шифров используется. Если используется шифр «G», тогда А заменяется на G, В на H, С на I и т.д. Если используется шифр «Y», тогда А заменяется на Y, В на Z, С на A и т.д. На шифре Цезаря базируется огромное число других, более сложных шифров, но сам по себе он не представляет из себя интереса из-за легкости дешифровки. Перебор 26 возможных ключей не займет много времени. Li bra ghflskhu wklv dqg bra nqrz lw, fods brxu kdqgv.

ROT1, азбука Морзе, шифр(ы) Цезаря относятся к одному и тому же типу шифров — моноалфавитной замене. Это значит, что каждая буква заменяется на одну и только одну другую букву или символ. Такие шифры очень легко расшифровать даже без знания ключа. Делается это при помощи частотного анализа. Например, наиболее часто встречающаяся буква в английском алфавите — «Е». Таким образом, в тексте, зашифрованном моноалфавитным шрифтом, наиболее часто встречающейся буквой будет буква, соответствующая «Е». Вторая наиболее часто встречающаяся буква — это «Т», а третья — «А». Человек, расшифровывающий моноалфавитный шифр, может смотреть на частоту встречающихся букв и почти законченные слова. Так, «Т_Е» с большой долей вероятности окажется «THE». К сожалению, этот принцип работает только для длинных сообщений.

Короткие просто не содержат в себе достаточно слов, чтобы с достаточной достоверностью выявить соответствие наиболее часто встречающихся символов буквам из обычного алфавита. Мария Стюарт использовала невероятно сложный моноалфавитный шифр с несколькими вариациями, но когда его наконец-то взломали, прочитанные сообщения дали ее врагам достаточно поводов, чтобы приговорить ее к смерти.

ГЛАВА 2. ПРИМЕНЕНИЕ ШИФРОВ

2.1. Кодировка и шифры в повседневной жизни

В мире существует множество видов информации, которая передается нашему сознанию через слух, обоняние, осязание. Существует текстовая информация, слуховая, зрительная, и не все можно представить в виде кода. Информация, в целом, крайне абстрактное понятие, вызывающее большое количество дискуссий в науке. Информация является сведениями, воспринимаемыми человеком, как факт отражения духовного и материального мира. Поскольку кодирование является преобразованием информации в формы, доступные для передачи, обработки и хранения её на компьютере и других электронных и технических устройствах, не все виды информации, которые способен воспринять человек, могут быть преобразованы в код, доступный для понимания операционной системой. К примеру, код для информации, дошедшей для человека путем вкуса или обоняния, составить невозможно, поскольку они не являются объектами материального мира и не имеют эквивалента в электронном виде. Кроме того, кодирование - представление информации при использовании определенной шкалы измерения степени проявления какого-либо явления. Если звук может быть громче и тише, мы можем представить его в виде кода, то для запаха не существует такой шкалы, степени его измерения связаны с индивидуальными ассоциациями каждого человека. Разные виды информации каждым человеком воспринимаются по-разному, а кодирование - это приведение определенной информации в стандарты, установленные операционной системой. Кодирование - это перевод информации с одного языка на другой, но не всю информацию можно так "перевести".

В современной жизни со всевозможными системами кодирования информации, использующими самые разнообразные способы преобразования каких-либо сведений с помощью кодов, мы встречаемся каждый день.

Следует признать, что с некоторыми кодами мы, скорее всего не знакомы, хотя слышали о них и видели их. К их числу можно отнести, например, штриховой код в магазинах.

С развитием информационной техники, широким внедрением средств вычислительной техники во многие сферы деятельности все острее встает вопрос быстрого и надежного ввода информации. Ручной ввод кода изделия требуют больших затрат ручного труда, времени, часто приводит к ошибкам. К машиночитаемым относятся сопроводительные документы, ярлыки и упаковки товаров, чековые книжки и пластиковые карточки для оплаты услуг, магнитные носители. Наиболее перспективным и быстроразвивающимся направлением автоматизации процесса ввода информации в ЭВМ является применение штриховых кодов. Штриховой код представляет собой чередование темных и светлых полос разной ширины. По мнению специалистов, системы штрихового кодирования имеют перспективу и дают возможность решить одну из самых сложных компьютерных проблем - ввод данных. В настоящее время штриховые коды широко используются не только при производстве и в торговле товарами, но и во многих отраслях промышленного производства. Товарный штриховой код присваивается продукции (товару) на этапе запуска его в производство. Таким образом штрих-коды получили широкое практическое применение почти во всех сферах деятельности человека.

Чаще всего, конечно, мы встречаемся с закодированной информацией в компьютерах или телефонах, ведь элементарное сообщение, написанное собеседнику, кодируется устройством.

Различают кодирование подобной информации следующих видов:

- кодирование текстовой информации;
- кодирование цвета;
- кодирование графической информации;
- кодирование числовой информации;
- кодирование звуковой информации;

- кодирование видеозаписи.

Кодирование текстовой информации. Любой текст состоит из последовательности символов. Символами могут быть буквы, цифры, знаки препинания, знаки математических действий, круглые и квадратные скобки и т.д. Текстовая информация, как и любая другая, хранится в памяти компьютера в двоичном виде. Для этого каждому ставится в соответствии некоторое неотрицательное число, называемое кодом символа, и это число записывается в память ЭВМ в двоичном виде. Конкретное соотношение между символами и их кодами называется системой кодировки. В персональных компьютерах обычно используется система кодировки ASCII (American Standard Code for Informational Interchange – Американский стандартный код для информационного обмена).

Кодирование цвета. Чтобы сохранить в двоичном коде фотографию, ее сначала виртуально разделяют на множество мелких цветных точек, называемых пикселями (что-то на подобии мозаики). После разбивки на точки цвет каждого пикселя кодируется в бинарный код и записывается на запоминающем устройстве.

Однако качество кодирования фотографий в бинарный код зависит не только от количества пикселей, но также и от их цветового разнообразия. Алгоритмов записи цвета в двоичном коде существует несколько. Самым распространенным из них является RGB. Эта аббревиатура – первые буквы названий трех основных цветов: красного – англ. Red, зеленого – англ. Green, синего – англ. Blue. Смешивая эти три цвета в разных пропорциях, можно получить любой другой цвет или оттенок. На этом и построен алгоритм RGB. Каждый пиксель записывается в двоичном коде путем указания количества красного, зеленого и синего цвета, участвующего в его формировании. Чем больше битов выделяется для кодирования пикселя, тем больше вариантов смешивания этих трех каналов можно использовать и тем значительнее будет цветовая насыщенность изображения.

Сокращение от Cyan-Magenta-Yellow-Black - голубой-пурпурный-желтый-черный. **СМΥК** - это цветовая модель, в которой все цвета описываются как смесь этих четырех обрабатываемых цветов. СМΥК - стандартная цветовая модель, используемая в цветной печати. Т.к. здесь используются чернила четырех основных цветов, ее еще называют четырехцветной печатью.

Цветовая модель СМΥК в отличие от RGB описывает поглощаемые цвета. Цвета, которые используют белый свет, вычитая из него определённые участки спектра, называются субтрактивными (вычитательными). Именно такие цвета и используются в модели СМΥК. Они получаются путём вычитания из белого аддитивных цветов модели RGB.

Основными цветами в СМΥК являются голубой (Cyan), пурпурный (Magenta) и жёлтый (Yellow). Голубой цвет получается путём вычитания из белого красного цвета, пурпурный - зелёного, жёлтый - синего.

При смешении всех трёх цветов получается чёрный цвет, т.е. сложение цветов в СМΥК аддитивно.

Цветовая модель СМΥК является основной для печати. В цветных принтерах также применяется данная модель. Получается, что для того, чтобы распечатать чёрный цвет, необходимо большое количество краски. Кроме того смешение всех цветов модели СМΥК на самом деле даёт не чёрный, а грязно-коричневый цвет. Поэтому, для усовершенствования модели СМΥК, в неё был введён один дополнительный цвет - чёрный. Он является ключевым цветом при печати, поэтому последняя буква в названии модели - К, а не В. Таким образом, модель СМΥК является четырёхканальной.

Дело в том, что у СМΥК цветовой охват более узкий, чем у RGB. Поэтому, при конвертации из RGB в СМΥК часть цветов теряется. Это необходимо учитывать, если Вы работаете в графических редакторах. С другой стороны Вы можете использовать конвертацию для того, чтобы

посмотреть, какой приблизительно вид будет иметь RGB-рисунок распечатанный на принтере.

Как же осуществляется печать при помощи модели СМΥК? Изображение растрируется, то есть представляется в виде совокупности точек цветов С, М, Υ и К. На расстоянии точки, расположенные близко друг к другу, сливаются, и создаётся ощущение, что цвета накладываются друг на друга. Глаз смешивает их и таким образом получает необходимый оттенок. Растрирование выделяют амплитудное (наиболее часто используемое, при котором, количество точек неизменно, но различается их размер), частотное (изменяется количество точек, при одинаковом размере) и стохастическое, при котором не наблюдается регулярной структуры расположения точек.

Числовые значения в СМΥК и их преобразование. Каждое из чисел, определяющее цвет в СМΥК, представляет собой процент краски данного цвета, составляющей цветовую комбинацию, а точнее, размер точки растра, выводимой на фотонаборном аппарате на пленке данного цвета (или прямо на печатной форме в случае с СТР). Например, для получения тёмно-оранжевого цвета следует смешать 30 % голубой краски, 45 % пурпурной краски, 80 % желтой краски и 5 % черной краски. Это можно обозначить следующим образом: (30,45,80,5). Иногда пользуются таким обозначением: C30M45Y80K5.

Важно отметить, что числовое значение краски в СМΥК не может само по себе описать цвет. Цифры - лишь набор аппаратных данных, используемых в печатном процессе для формирования изображения. На практике реальный цвет будет обусловлен не только размером точки растра на фотовыводе, соответствующем числам в подготовленном к печати файле, но и реалиями конкретного печатного процесса: растискиванием, на которое могут влиять такие факторы, как состояние печатной машины, качество бумаги, влажность в цеху; условиями просмотра отпечатка (спектральными характеристиками источника освещения) и другими.

Для получения представления о цвете, заданном в цветовой модели CMYK, применяют цветовые профили, которые связывают значения аппаратных данных с реальным цветом, выраженным, как правило, в цветовых моделях XYZ или LAB. Наибольшее применение в наши дни нашли ICC-профили.

Кодирование графической информации. Описанная выше техника формирования изображений из мелких точек является наиболее распространенной и называется растровой. Но кроме растровой графики, в компьютерах используется еще и так называемая векторная графика. Векторные изображения создаются только при помощи компьютера и формируются не из пикселей, а из графических примитивов (линий, многоугольников, окружностей и др.). Векторная графика - это чертежная графика. Она очень удобна для компьютерного «рисования» и широко используется дизайнерами при графическом оформлении печатной продукции, в том числе создании огромных рекламных плакатов, а также в других подобных ситуациях. Векторное изображение в двоичном коде записывается как совокупность примитивов с указанием их размеров, цвета заливки, места расположения на холсте и некоторых других свойств.

Кодирование числовой информации. При кодировании чисел учитывается цель, с которой цифра была введена в систему: для арифметических вычислений или просто для вывода. Все данные, кодируемые в двоичной системе, шифруются с помощью единиц и нулей. Эти символы еще называют битами. Этот метод кодировки является наиболее популярным, ведь его легче всего организовать в технологическом плане: присутствие сигнала – 1, отсутствие – 0. У двоичного шифрования есть лишь один недостаток – это длина комбинаций из символов. Но с технической точки зрения легче орудовать кучей простых, однотипных компонентов, чем малым числом более сложных.

Кодирование звуковой информации. Схему работы компьютера со звуком в общих чертах можно описать так. Микрофон превращает колебания

воздуха в аналогичные по характеристикам электрических колебаний. Звуковая карта компьютера преобразовывает электрические колебания в двоичный код, который записывается на запоминающем устройстве. При воспроизведении такой записи происходит обратный процесс (декодирование) - двоичный код преобразуется в электрические колебания, которые поступают в аудиосистему или наушники. Динамики акустической системы или наушников имеют противоположное микрофону действие. Они превращают электрические колебания в колебания воздуха. Принцип разделения звуковой волны на мелкие участки лежит в основе двоичного кодирования звука. Аудиокарта компьютера разделяет звук на очень мелкие временные участки и кодирует степень интенсивности каждого из них в двоичный код. Такое дробление звука на части называется дискретизацией. Чем выше частота дискретизации, тем точнее фиксируется геометрия звуковой волны и тем качественней получается запись.

Кодирование видеозаписи. Видеозапись состоит из двух компонентов: звукового и графического. Кодирование звуковой дорожки видеофайла в двоичный код осуществляется по тем же алгоритмам, что и кодирование обычных звуковых данных. Принципы кодирования видеоизображения схожи с кодированием растровой графики (рассмотрено выше), хотя и имеют некоторые особенности. Как известно, видеозапись - это последовательность быстро меняющихся статических изображений (кадров). Одна секунда видео может состоять из 25 и больше картинок. При этом, каждый следующий кадр лишь незначительно отличается от предыдущего. Учитывая эту особенность, алгоритмы кодирования видео, как правило, предусматривают запись лишь первого (базового) кадра. Каждый же последующий кадр формируются путем записи его отличий от предыдущего.

2.2. Обеспечение безопасности информации

Под **информационной безопасностью** понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации.

На практике важнейшими являются три аспекта информационной безопасности:

- **доступность** (возможность за разумное время получить требуемую информационную услугу);
- **целостность** (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- **конфиденциальность** (защита от несанкционированного прочтения).

Нарушения этих аспектов могут быть вызваны различными опасными воздействиями на информационные компьютерные системы.

Современная информационная система представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя.

Опасные воздействия на компьютерную информационную систему можно подразделить на случайные и преднамеренные. **Преднамеренные воздействия** - это целенаправленные действия нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник. Наиболее распространенным и многообразным видом компьютерных нарушений является **несанкционированный доступ (НСД)**.

Особо следует остановиться на угрозах, которым могут подвергаться компьютерные сети. Основная особенность любой компьютерной сети состоит в том, что ее компоненты распределены в пространстве. Связь между

узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Компьютерные сети характерны тем, что против них предпринимают так называемые *удаленные атаки*. Нарушитель может находиться за тысячи километров от атакуемого объекта, при этом нападению может подвергаться не только конкретный компьютер, но и информация, передающаяся по сетевым каналам связи.

Несмотря на то, что современные ОС для персональных компьютеров имеют собственные подсистемы защиты, актуальность создания дополнительных средств защиты сохраняется. Дело в том, что большинство систем не способны защитить данные, находящиеся за их пределами, например при сетевом информационном обмене.

Аппаратно-программные средства защиты информации можно разбить на пять групп:

- системы идентификации (распознавания) и аутентификации (проверки подлинности) пользователей.
- системы шифрования дисковых данных.
- системы шифрования данных, передаваемых по сетям.
- системы аутентификации электронных данных.
- средства управления криптографическими ключами.

Системы идентификации и аутентификации пользователей применяются для ограничения доступа случайных и незаконных пользователей к ресурсам компьютерной системы. Общий алгоритм работы таких систем заключается в том, чтобы получить от пользователя информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.

При построении этих систем возникает проблема выбора информации, на основе которой осуществляются процедуры идентификации и аутентификации пользователя. Можно выделить следующие типы:

- секретная информация, которой обладает пользователь (пароль, секретный ключ, персональный идентификатор и т.п.); пользователь должен запомнить эту информацию или же для нее могут быть применены специальные средства хранения;
- физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза и т.п.) или особенности поведения (особенности работы на клавиатуре и т.п.).

Системы, основанные на первом типе информации, считаются **традиционными**. Системы, использующие второй тип информации, называют **биометрическими**. Следует отметить наметившуюся тенденцию опережающего развития биометрических систем идентификации.

Чтобы сделать информацию бесполезной для противника, используется совокупность методов преобразования данных, называемая **криптографией**.

Системы шифрования могут осуществлять криптографические преобразования данных на уровне файлов или на уровне дисков. К программам первого типа можно отнести архиваторы типа ARJ и RAR, которые позволяют использовать криптографические методы для защиты архивных файлов. Примером систем второго типа может служить программа шифрования Diskreet, входящая в состав популярного программного пакета Norton Utilities, Best Crypt.

Другим классификационным признаком систем шифрования дисковых данных является способ их функционирования. По способу функционирования системы шифрования дисковых данных делят на два класса:

- системы "прозрачного" шифрования;
- системы, специально вызываемые для осуществления шифрования.

В системах прозрачного шифрования (шифрования "на лету") криптографические преобразования осуществляются в режиме реального времени, незаметно для пользователя. Например, пользователь записывает подготовленный в текстовом редакторе документ на защищаемый диск, а система защиты в процессе записи выполняет его шифрование.

Системы второго класса обычно представляют собой утилиты, которые необходимо специально вызывать для выполнения шифрования. К ним относятся, например, архиваторы со встроенными средствами парольной защиты.

Большинство систем, предлагающих установить пароль на документ, не шифрует информацию, а только обеспечивает запрос пароля при доступе к документу. К таким системам относятся MS Office, 1С и многие другие.

Различают два основных способа шифрования: канальное шифрование и оконечное (абонентское) шифрование.

В случае **канального шифрования** защищается вся информация, передаваемая по каналу связи, включая служебную. Этот способ шифрования обладает следующим достоинством - встраивание процедур шифрования на канальный уровень позволяет использовать аппаратные средства, что способствует повышению производительности системы. Однако у данного подхода имеются и существенные недостатки:

- шифрование служебных данных осложняет механизм маршрутизации сетевых пакетов и требует расшифрования данных в устройствах промежуточной коммуникации (шлюзах, ретрансляторах и т.п.);
- шифрование служебной информации может привести к появлению статистических закономерностей в зашифрованных данных, что влияет на надежность защиты и накладывает ограничения на использование криптографических алгоритмов.

Оконечное (абонентское) шифрование позволяет обеспечить конфиденциальность данных, передаваемых между двумя абонентами. В этом случае защищается только содержание сообщений, вся служебная

информация остается открытой. Недостатком является возможность анализировать информацию о структуре обмена сообщениями, например об отправителе и получателе, о времени и условиях передачи данных, а также об объеме передаваемых данных.

Системы аутентификации электронных данных

При обмене данными по сетям возникает проблема аутентификации автора документа и самого документа, т.е. установление подлинности автора и проверка отсутствия изменений в полученном документе. Для аутентификации данных применяют код аутентификации сообщения (имитовставку) или электронную подпись.

Имитовставка вырабатывается из открытых данных посредством специального преобразования шифрования с использованием секретного ключа и передается по каналу связи в конце зашифрованных данных. Имитовставка проверяется получателем, владеющим секретным ключом, путем повторения процедуры, выполненной ранее отправителем, над полученными открытыми данными.

Электронная цифровая подпись представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом. Отправитель формирует цифровую подпись, используя секретный ключ отправителя. Получатель проверяет подпись, используя открытый ключ отправителя.

Таким образом, для реализации имитовставки используются принципы симметричного шифрования, а для реализации электронной подписи - асимметричного. Подробнее эти две системы шифрования будем изучать позже.

Средства управления криптографическими ключами

Безопасность любой криптосистемы определяется используемыми криптографическими ключами. В случае ненадежного управления ключами злоумышленник может завладеть ключевой информацией и получить полный доступ ко всей информации в системе или сети.

Различают следующие виды функций управления ключами: генерация, хранение, и распределение ключей.

Способы **генерации ключей** для симметричных и асимметричных криптосистем различны. Для генерации ключей симметричных криптосистем используются аппаратные и программные средства генерации случайных чисел. Генерация ключей для асимметричных криптосистем более сложна, так как ключи должны обладать определенными математическими свойствами. Подробнее на этом вопросе остановимся при изучении симметричных и асимметричных криптосистем.

Функция **хранения** предполагает организацию безопасного хранения, учета и удаления ключевой информации. Для обеспечения безопасного хранения ключей применяют их шифрование с помощью других ключей. Такой подход приводит к концепции иерархии ключей. В иерархию ключей обычно входит главный ключ (т.е. мастер-ключ), ключ шифрования ключей и ключ шифрования данных. Следует отметить, что генерация и хранение мастер-ключа является критическим вопросом криптозащиты.

Распределение - самый ответственный процесс в управлении ключами. Этот процесс должен гарантировать скрытность распределяемых ключей, а также быть оперативным и точным. Между пользователями сети ключи распределяют двумя способами:

- с помощью прямого обмена сеансовыми ключами;
- используя один или несколько центров распределения ключей.

ВЫВОДЫ И ЗАКЛЮЧЕНИЕ

1. Можно сделать вывод, что шифрование - это преобразование открытой информации в зашифрованную, недоступную для понимания посторонних, которое появилось в древности для защиты информации. Большинство людей знают такие шифры, как азбука Морзе или шифр Цезаря, шифры встречаются им ежедневно.

2. Кодирование является преобразованием информации в формы, доступные для передачи, обработки и хранения её на компьютере и других электронных и технических устройствах, не все виды информации, которые способен воспринять человек, могут быть преобразованы в код, доступный для понимания операционной системой.

3. В современном мире шифрование продолжает оставаться одним из инструментов защиты информации и персональных данных на устройствах и в сети.

4. Чтобы создать определенный шифр и пользоваться им на постоянной или нет основе, мало иметь фантазию для того, чтобы зашифровать тот или иной знак, нужно сделать свой шифр актуальным, целостным и конфиденциальным одновременно.

Практической значимостью проекта является систематизация, углубление и расширение знаний по разделу "Информация. Подходы к понятию информации. Информационные процессы. Принципы обработки информации. Арифметические и логические основы работы компьютера" общеобразовательной учебной дисциплины "Информатика", а также выявление внутрипредметных и межпредметных связей, что позволит более осознанно подойти к изучению общепрофессиональных дисциплин.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Литературные источники:

1. Адаменко М.В., Основы классической криптологии, 2016 г.
2. Гохберг Г.С., Зафиевский А.В. и др. Информационные технологии. (СПО)и 2014 г.
3. Камский В.А., Защита личной информации в интернете, смартфоне и компьютере, 2017 г.
4. Тайлаков Н.И., Ахмедов А.Б., Пардаева М.Д., Информатика и информационные технологии, 11 класс, 2018 г.
5. Хлебников А.А., Информационные технологии, 2016 г.

Интернет ресурсы :

6. <http://calutcaia-com.blogspot.ru>
7. <http://informatikaiikt.narod.ru>
8. <http://psinovo.ru>
9. <https://ru.wikipedia.ru>
10. <https://www.polygraphcity.ru/stati/dizajn-i-reklama/chto-takoe-cmyk-kak-osushchestvlyaetsya-tsvetnaya-pechat-pri-pomoshchi-modeli-cmyk.html>
11. <http://www.redov.ru>