2. Шутько, Н. П. Математическая модель системы текстовой стеганографии на основе модификации пространственных и цветовых параметров символов текста / Н. П. Шутько, Д. М. Романенко, П. П. Урбанович // Труды БГТУ. Сер. VI: Физ.-мат. науки и информатика. – 2015. – № 6. — С. 152–156.

УДК 003.26+347.78

Студ. А. Н. Щербакова
Науч. рук. проф. П. П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

КЛОД ШЕННОН – ОСНОВОПОЛОЖНИК ЦИФРОВЫХ ТЕХНОЛОГИЙ И ТЕОРИИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ

Клод Элвуд Шеннон (1916-2001 гг.) – американский инженер и математик. Человек, которого называют отцом современных теорий информации и связи.

Теория информации неразрывно связана с опубликованной в 1948 году статьей К. Шеннона «Математическая теория связи». Фактически данная работа предопределила путь, по которому с тех пор развивается теория информации. В своей книге Шеннон изложил способ, как количественно характеризовать сигнал. Для этого он использовал величину, которая называется количеством информации, или энтропией.

Энтропия означает мера неопределённости или непредсказуемости информации. Это количество информации, которое приходится на одно элементарное сообщение источника. Энтропия применяется во многих системах. Рассмотрим применение энтропии для анализа сложности пароля. Энтропия пароля (сложность пароля, измеряемая в битах), сгенерированного случайным образом, находится по следующей формуле:

$$H = L\frac{lnN}{ln2}, \quad (1)$$

где L – набор символов в пароле, N – количество символов в используемом алфавите.

Вывод состоит в том, что чем меньше сложность пароля, измеренная в битах, тем легче его взломать методом полного перебора.

Множество работ Шеннона связаны с секретностью и стойкостью пароля. Рассмотрим понятие «расстояние единственности». Если криптографическая система не является совершенно секретной, то зашифрованное сообщение может дать криптоаналитику некоторую информацию об исходном сообщении. Существует некоторая длина перехваченного сообщения, после которой сообщение может быть дешифровано с вероятностью, близкой к единице. Шеннон ввел понятие расстояния единственности шифра (или расстояния уникальности) *U*, которое показывает, сколько букв зашифрованного сообщения необходимо перехватить для однозначного восстановления ключа. Для вычисления расстояния единственности необходимо знать энтропию ключа *H(K)*. Если известна энтропия ключа *H(K*) для некоторого шифра, то расстояние единственности U для него вычисляется по формуле:

$$U = \frac{H(K)}{D}, \quad (2)$$

где *D* – избыточность шифруемого сообщения (бит).

К. Шеннон был одним из первых, кто развеял миф о «безопасности через сокрытие». До этого пытались сохранить в тайне именно алгоритмы шифрования в надежде на то, что не зная деталей реализации, враг не сможет перехватывать шифрованные сообщения.

Шеннон сформулировал принцип «враг знает систему». Это значит, что нет смысла прятать алгоритм, а даже наоборот, следует открыть его для всех желающих. Но что-то скрываемое все равно должно быть, ведь шифр по определению – это сообщение, прочитать которое в идеале может лишь один человек – обладатель секрета шифра. При подходе «враг знает систему» подобным секретом стал так называемый ключ.

В своей исторической работе «Теория связи в секретных системах» К.Шеннон доказал, что одноразовый гамма-блокнот является «невскрываемой» шифрсистемой. Фактически Шеннон представил эту криптосистему как совершенную.

«Одноразовый блокнот» использует длинную шифрующую последовательность, которая состоит из случайно выбираемых бит или наборов бит (символов). Шифрующая последовательность побитно или посимвольно накладывается на открытый текст, имеет ту же самую длину, что и открытое сообщение, и может использоваться только один раз. Открытый текст сообщения m записывают как последовательность бит или символов:

$$m = m_1, m_2, m_3, \dots, m_{n-1}. \quad (3)$$

Шифрующая последовательность k той же самой длины:

$$k = k_5 \text{ÆG}_6 \text{ÆG}_7 \text{Æ} \quad \text{ÆG}_{\text{Æ}?5} \tag{4}$$

Шифртекст определяется следующим образом:

$$? \; \text{L} \; \text{I}\bigcirc\text{Æ} \; \text{G} \tag{5}$$

Чтобы получить шифртекст, необходимо выполнить операцию сложения по модулю 2 (XOR) над первым битом сообщения и первым битом в одноразовом блокноте, что дает первое значение шифртекста. Затем выполняется XOR над следующим битом сообщения и следующим битом в блокноте, что дает второе значение шифртекста. Этот процесс продолжается до тех пор, пока все сообщение не будет зашифровано.

Схема шифрования с использованием одноразового шифровального блокнота считается не взламываемой только в том случае, если в процессе ее реализации выполнены следующие условия:

1. Блокнот должен использоваться только один раз.

2. Блокнот должен существовать ровно столько же времени, что и само сообщение.

3. Блокнот должен распространяться безопасным образом и защищаться получателем.

4. Блокнот должен быть заполнен действительно случайными значениями.

К известным теоремам Шеннона можно отнести:

1. Прямая и обратная теоремы Шеннона для источника общего вида – о связи энтропии источника и средней длины сообщений.

2. Прямая и обратная теоремы Шеннона для источника без памяти.

3. Прямая и обратная теоремы Шеннона для канала с шумами – о связи пропускной способности канала и существования кода, который возможно использовать для передачи с ошибкой, стремящейся к нулю.

4. Теорема Найквиста-Шеннона об однозначном восстановлении сигнала по его дискретным отсчётам.

6. Теорема Шеннона об источнике шифрования (или теорема бесшумного шифрования).

7. Теорема Шеннона — Хартли.

Рассмотренные работы и теоремы К. Шеннона – лишь малая часть того, какой вклад он внес в развитие теории информации, криптографии и других сфер.

ЛИТЕРАТУРА

1. Совершенно секретные системы [Электронный ресурс]. Режим доступа: http://www.intuit.ru/studies/courses/691/547/lecture/12395. – Дата доступа: 11.04.2017

2. Информационная безопасность [Электронный ресурс]. Режим доступа: http://dorlov.blogspot.com.by/2010/08/issp-06-1.html. – Дата доступа: 10.04.2017

УДК 378.147

Студ. П. А. Короткая
Науч.рук.: доц., к.т.н. Н. Н. Пустовалова
доц., к.п.н. Н. П. Коровкина
(кафедра информационных систем и технологий,
кафедра автоматизации производственных процессов и электротехники БГТУ)

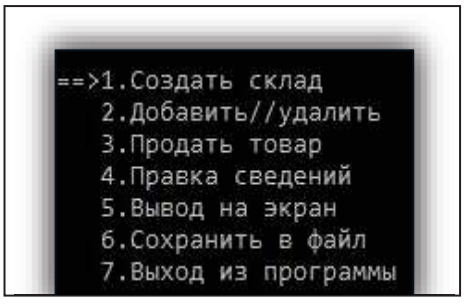
ПРОГРАММНОЕ СРЕДСТВО ДЛЯ УЧЕТА ТОВАРОВ НА ПРЕДПРИЯТИИ

В данной работе представлена программа, которая может найти практическое применение в области менеджмента и бухгалтерии, что поможет развить коммерческий потенциал организации, использующей программный продукт.

Программа написана на языке C++, что обуславливает потенциальную кроссплатформенность и расширяет круг устройств и операционных систем, поддерживающих данный программный продукт, а значит и целевую аудиторию, готовую приобрести его. Также с переносом программы на мобильные устройства увеличиваются возможности использования программы.

Рассмотрим работу программы на примере. Пусть необходимо создать склад для некоторого товара и управлять движением товара. Основное меню появляется сразу после открытия программы. Навигация по пунктам меню осуществляется при помощи клавиатурных стрелок, ввод – стандартный с клавиатуры. В первую очередь надо создать новый склад для товаров, нажав на выбранном пункте меню клавишу Enter.

После создания нового склада следует нажать клавишу «стрелка вниз» и каретка оказывается напротив пункта «Добавить//удалить».



Клавиша Enter служит для перехода в подменю добавления и удаления.