Пайдаланылған әдебиеттер тізімі

1. Кубесов А.К. Математическое наследие аль-Фараби. Алма-Ата, «Наука», 1974. – 246 с.

2. Аль-Фараби, Математические трактаты. – Алма-Ата, 1972. -318 с.

3. Бидайбеков Е.Ы., Бостанов Б.Г., Камалова Г.Б. The mathematical heritage of Al-Farabi by A.Kubesov in modern conditions of educations // Матер. IX Межд. конгресса ISAAC. 5–9 августа 2013 г. Краков, 2013. -С. 33–34.

4. Carry J. Tee (University of Aucland), Kubesov A.K. The Mathematical Heritage of al-Farabi // Journal for the history of Arabic science. -1978. -№ 1. -P. 150–153 (in Russian).

5. И.И.Ильясов, Ш.Г.Мулдашев. Әл-фарабидің кітабынан алынған кейбір есептерге түсініктеме./«Математикалық білім: жағдайы, мәселелері, болашағы» атты халықаралық ғылыми – практикалық конференция материалдары. – Ақтөбе, 2019. – Б.71-76.

МРНТИ 20.51.23

МЕТОДЫ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

Ж.А.ТАСКАЛИЕВА, Л.Е.КАПАРОВА

Актюбинский государственный университет им.К.Жубанова, Актобе, Казахстан

Аннотация. С развитием современных информационных технологий и всемирная компьютеризация привели к тому, что безопасность информации не только становится обязательной, она еще и одна из характеристик информационной системе.

Проектный метод получил в настоящее время очень широкое распространение в обучении. Его можно использовать в любой дисциплине, где решаются большие по объему задачи, желательно для заинтересованных исследователей.

Главной целью проекта является формирование творческого мышления. Существует множество классификаций методов обучения, но почти в каждой в них присутствует исследовательский метод, когда дается познавательная задача, которую они решают самостоятельно, подбирают для этого необходимые методы.

Ключевые слова: Шифрование, методами шифрования, криптографическая система, проектный метод, защита информации.

Аннотация. Қазіргі заманғы ақпараттық технологиялардың дамуы дүниежүзілік компьютерлендіруге әкелді және ақпараттың қауіпсіздік бұл ақпараттық жүйенің міндетті сипаттамаларының бірі болып табылады.

Жобалық әдіс қазіргі уақытта оқытуда өте кең таралған. Оны көлемі жағынан үлкен міндеттер шешілетін кез келген пәнде қолдануға болады.

Жобаның басты мақсаты-шығармашылық ойлауды қалыптастыру. Оқыту әдістерінің көптеген тәсілдері бар, бірақ олардың әрқайсысында да зерттеу әдістері бар, онда зерттеушіге өздері шешетін танымдық тапсырма беріледі, ол үшін қажетті әдістерді таңдалады

Кілттік сөздер: Шифрлау, шифрлау әдістері, криптографиялық жүйе, жобалық әдіс, ақпаратты қорғау.

Abstract. The development of modern information technologies has led to the worldwide information system mandatory computerization and this is one of the characteristics of information security.

The project method is currently very common in training. It can be used in any subject where large tasks are solved in terms of volume.

The main goal of the project is to form creative thinking. There are many ways of teaching, but each of them has research methods, in which the researcher is given a cognitive task, which they decide on, for which the necessary methods are chosen.

Keywords: encryption, encryption methods, cryptographic system, project method, information security.

В данное время существует очень обширный класс систем обработки информации, при разработке которых фактор безопасности играет первостепенную роль (к примеру - банковские информационные системы).

Шифрование в целом появилось примерно четыре тысячи лет тому назад.Самым первым известным применением шифра (кода) считается египетский текст, датированный примерно 1900 г. до н. э., автор которого использовал вместо обычных (для египтян) иероглифов не совпадающие с ними знаки.[1]

В давние времена шифрование называлось *тайнописью*.

Шифрование представляет собой процесс превращения открытого текста в зашифрованный, а дешифрование - процесс обратного преобразования, при котором восстанавливается исходный текст.

Шифрование — это тоже кодирование, но с засекреченным методом, известным только источнику и адресату. [2]

Методами шифрования занимается наука под названием криптография.

Криптографическая система представляет собой семейство T преобразований открытого текста. члены этого семейства индексируются, или обозначаются символом k; параметр k является ключом. Пространство ключей K - это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита. [3]

На данное время можно сказать что рождается новая актуальная, технология –Кибер защита (Cyber security) защиты информации в компьютерных информационных системах и в сетях передачи данных. Для реализации этой технологии требуется увеличивающихся расходов и усилий. Однако все это позволяет избежать значительно превосходящих потерь и ущерба, которые могут возникнуть при реальном осуществлении угроз ИС и ИТ.

Проектный метод можно отнести к исследовательскому типу, при котором исследователи индивидуально занимаются какой-либо поставленной проблемой.

В основе учебного процесса оказывается сотрудничество и продуктивное общение студентов, направленное на совместное разрешение проблемс преподавателями, формирование способности выделять важное, ставить цели, планировать деятельность, распределять функции и ответственность, критически мыслить, достигать значимые результаты.

В рамках реализации созданного проекта исследователи приобретут навыки самостоятельной исследовательской деятельности, понимание необходимости ответственного отношения к информации, избирательного отношения к полученной информации.

Работа над проектом стимулирует их познавательную активность и большую мотивацию.

Переднами были поставлены задачи добавить к имеющим методам защиты от несанкционированного доступа к информации что то новое и составить проект.

В шифрование использовалось:

- Таблица кодов ASCII
- Генератор случайных чисел RANDOM
- Время компьютера
- Функция MOD

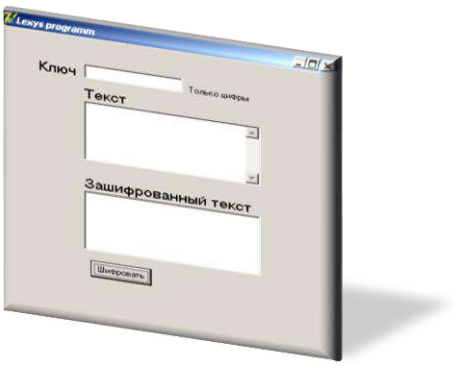

Рисунок 1. Вид программы

В данном методе шифрования используется ключ состоящий из набора цифр который пользователь вводит при шифровании данных. Так же учитывается в какое время время был зашифрован текст, можно сказать что время это второй ключ для шифрования текста.

Принцип работы шифрования данных: пользователь вводит ключ, набирает текст который нужно зашифровать и программа шифрует данные. Сначала она переводит каждый символ текста в числовое значение используя таблицу ANSI символов, после чего программа считывает время с компьютера и преобразует его в четырехзначное число.

Первоначальный ключ служит для размера выбора случайных чисел из функции random.

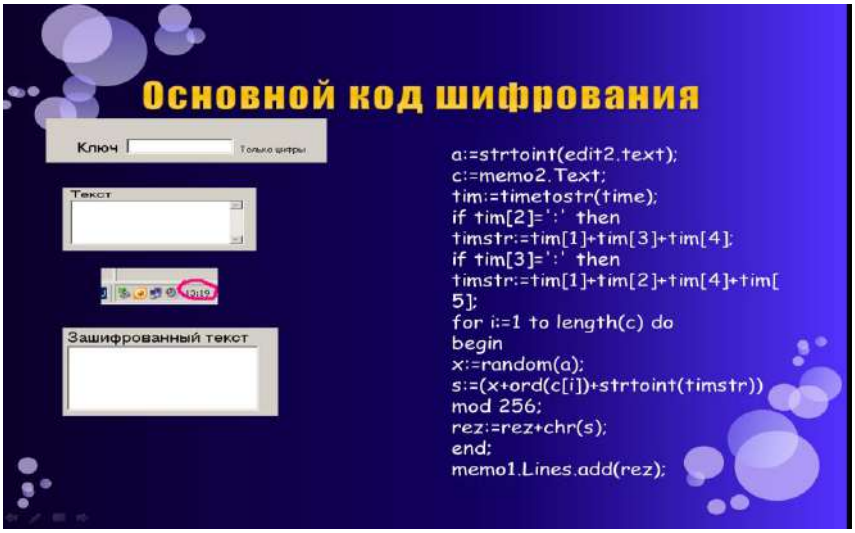

Рисунок 2. Основной код шифрования

По статистике, что во всех странах убытки от злонамеренных действий непрерывно возрастают. Причем, основные причины убытков связаны не столько с недостаточностью средств безопасности как таковых, сколько с отсутствием взаимосвязи между ними, т.е. с нереализованностью системного подхода.

Поэтому необходимо опережающими темпами совершенствовать комплексные средства защиты. Исходя из всего сказанного выше, какие бы методы шифрования не были, методы должны сочетать в себе как удобство, гибкость и оперативность использования, так и надежную защиту от злоумышленников циркулирующей в системе информации.

Список использованной литературы

1. Коростовцев М. А. Развитие иероглифической системы. Письмо греко-римского времени. Криптография /Введение в египетскую филологию. — М., 1963.

2. Семакин И. Г. Информатика и ИКТ. Базовый уровень/ И. Г. Семакин, Е. К. Хеннер. - 8-е изд. - М.: БИНОМ. Лаборатория знаний, 2012, стр. 13-15

3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.

4. Крысин А.В. Информационная безопасность. Практическое руководство — М.: СПАРРК, К.:ВЕК+,2003.

5. Титоренко Г.А. Информационные технологии управления. М., Юнити: 2002.

6. Тарасюк М.В. Защищенные информационные технологии. Проектирование и применение — М.: СОЛОН-Пресс, 2004.