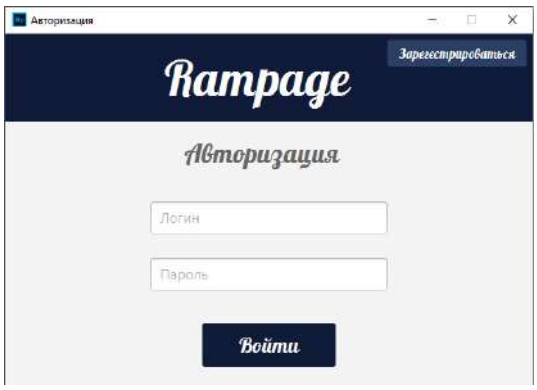

Рисунок 4 — Авторизация

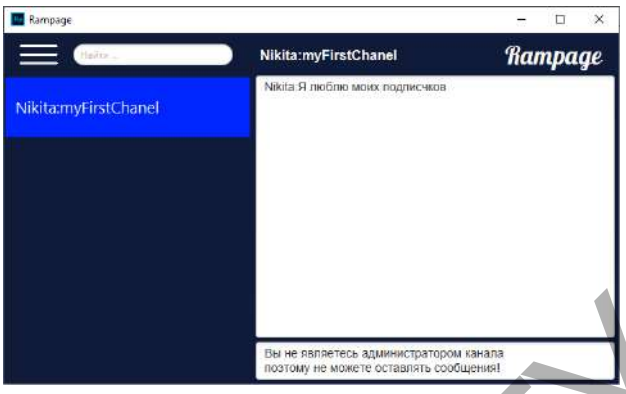

Рисунок 5— Главное окно

После успешного входа в систему перед пользователем открывает главное окно приложения, на котором расположен список чатов пользователя, их поиск, меню, поле ввода и просмотра текста (рисунок 5).

Заключение. Программа Чат-Микроблог была написана на строго типизированном объектно-ориентированном языке программирования Java с использованием всех возможностей данного языка. Было проведено тестирование программы, позволяющее увидеть весь ее функционал, преимущества и недостатки. Данное приложение показало важность таких составляющих разработки как frondend и backend (клиентской и серверной части).

Список цитируемых источников

1. Объектно-ориентированный подход [Электронный ресурс]. — Режим доступа: http://opensourcerules.net/java/gl3_2.html. Дата доступа: 13.12.2018

2. Евсеева, О. Н. Работа с базами данных на языке JAVA. / О. Н. Евсеева, А. Б. Шамшев. — Ульяновск: УлГТУ, 2009. — 170 с.

3. Сокеты — сетевое программирование [Электронный ресурс]. — 2016. — Режим доступа: http://lecturesnet.readthedocs.io/net/low-level/ipc/socket/intro.html. — Дата доступа 22.12.2018.

4. Обзор JSON — сетевое работает с JSON Java [Электронный ресурс]. — 2016. — Режим доступа: http://www.javenue.info/post/gson-json-api — Дата доступа 27.12.2018.

5. Объектно-ориентированное программирование [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/Объектно-ориентированное_программирование. Дата доступа: 24.12.2018.

УДК 519.1

В. С. Бурмако, Д. С. Кислый

Учреждение образования «Барановичский государственный университет», Барановичи

ШИФРОВАНИЕ КАК МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ

Введение. Необходимость засекречивать важные послания возникла еще в древние времена. Со временем люди находили все более сложные способы делать послания недоступными чужим глазам. Древние рукописи и языки были поняты с помощью техник декодирования и дешифрования. Самый известный пример — Розеттский камень Древнего Египта. Фактически коды и шифры определяли исход многих войн и политических интриг на протяжении всей истории человечества [1].

Актуальность темы очевидна, так как информация в современном обществе — одна из самых ценных вещей в жизни, требующая защиты от проникновения лиц, не имеющих к ней доступа. Что такое шифрование? Шифрование — это способ преобразования пригодного для чтения текста, делающий невозможным его прочтение третьими лицами, причем текст снова становится пригодным для чтения после верификации ключа. Таким образом, суть шифрования заключается в том, что зашифрованная информация не представляет никакой ценности без знания ключа доступа. Криптография — наука о шифрах. Сообщения шифруются и расшифровываются с помощью алгоритмов, созданных комбинацией информатики и математики. С развитием технологий человечество старается находить все более надежные способы защиты информации. Но для того, чтобы понять более сложные методы шифрования, необходимо знать и понимать, как работают шифры, изобретенные еще до появления компьютеров. Хотя растущая производительность компьютеров позволяет

создавать более совершенные и надежные шифры, а криптография стала неразрывно связана с информационными технологиями, история шифровального дела насчитывает не одну тысячу лет.

Основная часть. Существуют тысячи типов шифрования сообщений, но в этой статье мы рассмотрим лишь некоторые наиболее известные и значимые из них:

ROT13. Применение алгоритма ROT13 к части текста требует простой замены каждого буквенного символа на соответствующий ему со сдвигом на 13 позиций в алфавите A становится N, B становится O, и т. д. до M, которое становится Z, а затем последовательно применяются буквы из начала алфавита: N становится A, O становится B, и так далее до Z, которая становится M. Затронуты лишь те буквы, которые используются в английском алфавите; цифры, символы, пробелы и все остальные символы остаются без изменений. Поскольку в английском алфавите всего 26 букв, а 26 = 2 × 13, то функция ROT13 является обратной для самой себя [2].

Приведем пример: необходимо зашифровать предложение «Hello world», используя шифр ROT13. Для удобства составим таблицу английского алфавита и добавим строку, в которой сдвинем алфавит на 13 позиций.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
X	Y	Z																				
K	L	M																				

Используя данную таблицу, мы можем легко зашифровать наше предложение. Получится: «Uryyb jbeyq».

Транспозиция. В транспонирующих шифрах буквы переставляются по заранее определенному правилу. Например, если «зеркально отразить» предложение, то из «the more you know, the less is known» получается «nwonk si ssel eht wonk uoy erom eht». Или же можно разделить предложение на группы по несколько символов, например, по 7, а затем каждую из таких групп зеркально отразить. Таким образом, предыдущее сообщение станет «eromeht wonkuoy sseleht nwonksi». Подобные шифры использовались в Первую Мировую и Американскую Гражданскую Войну, для отправки важных сообщений.

Азбука Морзе. 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». 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 можно осуществлять почти мгновенную коммуникацию между войсками [1].

Шифр Цезаря. Шифр Цезаря назван в честь Юлия Цезаря, использовавшего его для особо важных переписок. На самом деле, шифр Цезаря — это название не конкретного шифра, а любого, с использованием следующего принципа: каждая буква заменяется другой, определяемой по алфавиту, с определенным сдвигом. Если получатель знает значение сдвига, он без труда восстановит сообщение. Например, если используется шифр «D», тогда A заменяется на D, B на E, C на F и т.д. Если используется шифр «Z», тогда A заменяется на Z, B на A, C на B и т.д. На шифре Цезаря базируется огромное число других, более сложных шифров, но сам по себе он не представляет из себя интереса, так как его легко дешифровать вручную, ведь перебор ключей по количеству букв в данном алфавите не займет много времени.

Моноалфавитная замена. Шифр Цезаря и азбука Морзе относятся к одному и тому же типу шифров — моноалфавитной замене. Это значит, что каждая буква однозначно заменятся на одну другую букву или символ. Эти шифры легко подвергаются дешифровке, даже без знания ключа, при помощи частотного анализа. Например, наиболее часто встречающаяся буква в английском алфавите — «E». Таким образом, в тексте, зашифрованном моноалфавитным шифром, наиболее часто встречающейся буквой будет та, что соответствует «E». За ней по частоте следуют «T» и «A». Основываясь на уже расшифрованных символах, возможно дополнить имеющиеся слова так, чтобы они обрели смысл, например, «T_E» с большой долей вероятности окажется «THE». Однако это выполнимо лишь для длинных сообщений, так как в коротких недостаточно слов чтобы достоверно утверждать о частоте встречаемости букв.

Шифр Виженера. Этот метод шифровки использует шифры Цезаря с различными сдвигом, причём для различных букв в шифруемом тексте выбираются различные сдвиги по некоторому правилу. В качестве такого правила можно сформировать ключевой текст, такого же размера как исходный, и каждой букве поставить в соответствие шифр Цезаря с таким сдвигом, чтобы первая буква алфавита заменялась этой буквой из ключевого текста. После этого, буквы исходного текста шифруются с помощью шифра Цезаря, соответствующего букве в той же позиции в ключевом тексте. Для упрощения шифрования применяется таблица Виженера, представляющая собой строчки, состоящие из букв алфавита, где каждая следующая является предыдущей со сдвигом на один.

Шифрование публичным ключом. Этот метод заключается в использовании двух ключей: публичного (открытого) и приватного (закрытого). Публичный ключ - это достаточно большое число, имеющее только два делителя, помимо самого себя и единицы. Эти два делителя составляют секретный ключ. При помощи открытого ключа сообщение шифруется, а при помощи секретного расшифровывается. Криптостойкость обеспечивается отсутствием быстрых алгоритмов нахождения таких делителей для достаточно больших чисел. Например, публичный ключ — это 2059, а секретный — 71 и 29.

Заключение. Шифрование изначально использовалось только для передачи конфиденциальной информации. Однако впоследствии шифровать информацию начали с целью её хранения в ненадёжных источниках. Шифрование информации с целью её хранения применяется и сейчас, это позволяет избежать необходимости в физически защищённом хранилище. С помощью шифрования обеспечиваются три состояния безопасности информации: конфиденциальность, целостность, идентифицируемость [3].

На данный момент в мире не существует абсолютно безопасного способа передачи и хранения информации. Но с развитием науки и технологий, мы можем создавать и применять все более надежные способы защиты.

Изучение основ криптографии способствует повышению интереса к математике и информатике, раскрывает перед учащимися один из аспектов практического применения математических знаний в практической жизни людей, благоприятствует развитию логического мышления, формированию исследовательских навыков.

Список цитируемых источников

1. 10 популярных кодов и шифров [Электронный ресурс]. — Режим доступа: https://tproger.ru/translations/10-codes-and-ciphers. — Дата доступа: 24.02.2019

2. ROT13 [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/ROT13. — Дата доступа: 24.02.2019.

3. Шифрование [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/Шифрование. — Дата доступа: 24.02.2019.

УДК 330

Д. С. Войтушевская, Ю. В. Корчиц
Учреждение образования «Барановичский государственный университет», Барановичи

ВЛИЯНИЕ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ НА ПРОЦЕСС ПРИНЯТИЯ РЕШЕНИЙ ОРГАНИЗАЦИОННОГО ПЛАНА В БИЗНЕСЕ И ПРЕДПРИНИМАТЕЛЬСТВЕ

Введение. Организация деятельности любого предприятия предполагает эффективную работу взаимосвязанных структур системы. Для достижения поставленных целей и задач необходимо оперативно принимать верные решения, которые зависят от выбора необходимых данных из огромного потока информации. В данной статье рассматриваются системы поддержки принятия решений (СППР), виды и подвиды СППР, преимущества использования систем в деятельности предприятия.

Основная часть. В последнее время наблюдается увеличение информации, которую следует систематически обрабатывать. В результате роста объемов неструктурированных данных и быстроты в принятии решений предъявляются новые требования, как к руководителям организаций, так и к бизнес-аналитикам. Также наблюдается стремительный рост интереса компаний к созданию программных продуктов, которые позволяют работать с большими объемами информации, накопленными в учетных системах и хранилищах данных.

На стадиях и этапах процесса принятия решений существует множество методов решения возникающих проблем. Эти методы в виде соответствующего математического аппарата реализованы в информационных системах — системах поддержки принятия решений (СППР).

Система поддержки принятия решений (Decision Support Systems) — это компьютерная система, которая при помощи сбора и анализа информации может влиять на процесс принятия решений организационного плана в бизнесе. Имеющиеся автоматизированные системы помогают получить необходимые данные из первоисточников, осуществить их анализ. С помощью таких систем можно получить сравнительные значения объемов продаж, наблюдать все доступные информационные активы, рассматривать альтернативные решения, спрогнозировать доход организации при предполагаемом внедрении новой технологии и т.д. [1].

Системы поддержки принятия решений появились в результате объединения систем: управления базами данных, управленческих и информационных. Всё чаще системы поддержки принятия решений стали применяться на практике, а не в теории. Для того чтобы определить тип системы поддержки принятия решений, нужно сначала понять к какому из методов классификации подходит решаемая задача [2].

Примером СППР может выступать Assistant Choice. Данная система помогает решать частично структурированные и не структурированные задачи, в большинстве из которых известна лишь часть их связей и элементов. К особенностям СППР можно отнести то, что для решения задачи пользователь должен описать проблему путем создания дерева критериев, оценить все критерии и альтернативы по их значимости, и описанным критериям. Более того, система Assistant Choice позволяет упростить принятие решения для лиц, принимающих данное решение.

Информационные системы поддержки принятия решений могут использоваться на любом уровне управления предприятием, которые позволяют руководителю усилить свои аналитические возможности в многочисленных процессах принятия решений в комплексе с методами разработки и анализа альтернатив [3].