СибАК
www.sibac.info

ISSN 2310-4066

XXXII СТУДЕНЧЕСКАЯ МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

№ 5(31)

# НАУЧНОЕ СООБЩЕСТВО СТУДЕНТОВ XXI СТОЛЕТИЯ. ТЕХНИЧЕСКИЕ НАУКИ

г. НОВОСИБИРСК, 2015


# НАУЧНОЕ СООБЩЕСТВО СТУДЕНТОВ XXI СТОЛЕТИЯ. ТЕХНИЧЕСКИЕ НАУКИ

*Электронный сборник статей по материалам XXXII студенческой международной заочной научно-практической конференции*

№ 5 (31)
Май 2015 г.

Издается с Октября 2012 года

Новосибирск
2015

УДК 62
ББК 30
Н 34



**Н 34** **«Научное сообщество студентов XXI столетия. Технические науки»:** Электронный сборник статей по материалам XXXII студенческой международной научно-практической конференции. — Новосибирск: Изд. «СибАК». — 2015. — № 5 (31)/ [Электронный ресурс] — Режим доступа. — URL: http://www.sibac.info/archive/Technic/5(31).pdf.

Электронный сборник статей по материалам XXXII студенческой международной научно-практической конференции «Научное сообщество студентов XXI столетия. Технические науки» отражает результаты научных исследований, проведенных представителями различных школ и направлений современной науки.

Данное издание будет полезно магистрам, студентам, исследователям и всем интересующимся актуальным состоянием и тенденциями развития современной науки.

ББК 30
ISSN 2310-4066

**Оглавление**

# СЕКЦИЯ 1.

# ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

## ЗНАНИЯ И СИСТЕМЫ НА ОСНОВЕ ЗНАНИЙ

***Алханов Асет Адылович***
*магистрант 1 курса кафедры «Информатика и информационная безопасность» ЕНУ им. Л.Н. Гумилева,*
*Республика Казахстан, г. Астана*
*E-mail: assetalkhanov@gmail.com*

***Омарбекова Асель Сайлаубековна***
*научный руководитель, канд. техн. наук, и. о. доцента кафедры «Информатика и информационная безопасность» ФИТ ЕНУ,*
*Республика Казахстан, г. Астана*

Вероятно, вопрос о том, какое определение должно быть для термина «знание» является самым важным и сложным. Он состоит из следующих пунктов: 1) определение знания, 2) данные, 3) методы вывода, с которыми мы будем иметь дело. Может появиться мысль, что знание может быть определено как убеждение, которое находится в согласии с фактами. Проблема в том, что никто не знает, что такое убеждение, что такое факт, какого рода согласие между ними сделало бы убеждение правдой.

Знания необходимы для интеллектуального поведения. Без знаний, интеллектуальный агент не может делать обоснованные решения, и вместо этого должен полагаться на использование некоторой формы поискового поведения, включающего исследование или коммуникацию для того, чтобы получить недостающие знания. В жизни люди всегда полагаются на знания — знания о том, как общаться с другими людьми, где другие люди живут и работают, где находятся те или иные вещи, как вести себя в различных ситуациях, как выполнить различные задачи, и так далее. Без умения хранить и обрабатывать знания, познавательные способности человека сильно ограничиваются. Например, болезнь Альцгеймера может ослаблять познавательные

способности человека, когда появляется потеря памяти, усложненностью запоминания только что выученных фактов.

Мы все знаем (или думаем, что знаем), что мы имеем в виду, когда мы используем термин «знание». Но что же на самом деле знание? Бертранд Рассел(1926) осознавал сложный вопрос, как определить значение «знания» [1]:

«Вероятно, не мудро будет начать с определения предмета, так как, как и везде в философских суждениях, определения спорны, и будут неизбежно отличаться в различных школах».

Определение знания, это объект непрерывных философских дебатов и в настоящее время очень много конкурирующих теории, у которых нет простого универсально-согласованного определения. Следовательно, обработка знаний с точки зрения искусственного интеллекта часто сознательно избегала определения, что есть знание. Тем не менее, это уклонение от предоставления определения знанию является результатом нехватки точности в литературе и исследованиях. Следующий аргумент продемонстрирует, почему система, основанная на знаниях — это термин, используемый в искусственном интеллекте который, относиться к системе обрабатывающей знания каким — либо образом. Система, основанная на знаниях, является хранилищем для знаний (подобно людям хранящим знания в своей голове), в то время как база данных является хранилищем для данных. Тем не менее, термин «знание» очень часто упускается из виду и остается неясным его значение и отличие от данных.

Общепринятое понятие о системах основанных на базе знаний это то, что они могут рассуждать основываясь на логические выводы (основанные на правилах, установленных рамках). Современные системы управления базами данных также включают в себя стандартные техники «баз знаний». Очевидно, что применение логического предположения недостаточно, чтобы дать определение системе на основе знаний. Тем не менее, большинство литературы по искусственному интеллекту допускает такое мнение [2].

Избегая определения что такое знание, появляется проблема, является ли система основанная на знаниях, которую мы собираемся разрабатывать действительно основанной на знаниях. Было отмечено, что в начале появления систем искусственного интеллекта, этим системам не хватало оценки — был большой всплеск для разработки таких систем, но было приложено мало усилий, чтобы проверить насколько правильно система работала. То же самое может произойти и с системой на основе знаний, если не знать и не понимать то, как эта система должна работать или делать.

Тем не менее, можно избежать подводных камней определяя термин «знание», вместо того, чтобы заявлять, что то или иное определение верно, можно начать с разработки принципов для системы на основе знаний. Следовательно, разработчик может сам решать, каких принципов система будет придерживаться, чтобы она подходила требованиям системы на основе знаний, также имея возможность добавления новых принципов или изменять их. Таким образом, нет острой необходимости для предоставления одного точного определения для термина «знание», но, есть и должна быть критика относительно правильности принципов с точки зрения инженерий. Оценивание системы будет легче, если знать, отвечают ли принципы системы требованиям. Существуют некоторые принципы для системы на основе знаний [3].

1. Система на основе знаний должна быть системой ориентированной на агента.

Система, ориентированная на агента придерживается следующих принципов — она автономна, она реагирующая, она активная.

Суть системы ориентированной на агента в том, что знания не могут существовать сами по себе, они могут существовать только в агентах, которые являются транспортировщиками знании. Например, птица — агент, так как она знает, где находится ее гнездо. Дерево — не может быть агентом, так как у него не может быть знания, поэтому дерево — это объект.

2. Система на основе знании должна отвечать на вопросы или выполнять задачу, для решения которой у системы предполагаются знания;

3. Система на основе знании должна быть четкой;

4. Система на основе знании должна быть не двусмысленной;

5. Система на основе знании должна быть обновленной;

6. Система на основе знании по мере возможности должна быть корректной;

7. Система на основе знании по возможности должна быть завершенной.

Поведенческий подход к знанию обращает особое внимание не на построение специфичных независимых систем, а на построение агентов показывающих поведение, демонстрирующих знание об их окружающей среде и об агентах. В этом подходе действие «знания» появляется, когда у агента есть информация, которая может способствовать выполнению мер предпринятых самим агентом или другим агентом. Кроме того, агент может считаться «знающим» если он знает вероятный результат действия, которое он может выполнить, или действие, которое выполняет другой агент, или что может произойти с объектом в окружающей среде [4]. По данному определению, агенту нет необходимости выполнять поведение-поиск, чтобы найти вероятный ответ или то, что может произойти, так как у него уже есть знания о том, что может произойти или какой будет ответ.

Вместо попыток определить знание мы можем определить виды знании. К примеру, шимпанзе и тигр два примера животных, у которых есть свои отличительные черты и которым легче дать определение, чем определение животному. Определение разных видов знании может помочь нам понять как можно построить агентов, которые будут показывать знание.

Мы можем определить, что агент владеет декларативным знанием, если он утверждает что утверждение истинно. Чтобы определить является ли знание декларативным или нет, агент может задать следующий вопрос, «Это правда, что …?», так как агент может ответить на этот вопрос да или нет, можно определить, что это декларативное знание агента.

Относительно, правды и лжи нужно отметить, что в реальности абсолютные ответы встречаются редко, то есть не всегда все бывает только правдой и не всегда все бывает только ложью.

В случае, когда агент не может определить является ли утверждение правдой или ложью, агенту необходимо обратиться к другому агенту или исследовать и провести наблюдения окружающей среды, чтобы получить информацию. В этом случае агенту необходимо выполнить два действия, получить знания об утверждении и затем, сделать выводы, основываясь на полученном знании. Данное знание агента является процедурным, если агент знает выполнение последовательности действии, чтобы убедиться что утверждение будет истинным. Чтобы определить является ли знание процедурным или нет, агент может задать следующий вопрос: «Какие действия мне нужно выполнить, чтобы я мог заявить, что утверждение истинно?» В этом случае если вопрос имеет смысл, его можно считать процедурным знанием.

**Список литературы:**


1. Негневитский М. Искусственный Интеллект Руководство к Интеллектуальным системам. Эдисон Уэсли, Эдинбург, 2002.
2. Нильсон, Нилс Дж. Искусственный Интеллект: Новый Синтез. Выпуск Моргана Кауфмана по Искусственному Интеллекту, 1998
3. Уиллиам Дж.Т. Искусственный Интеллект Поведение агента, 2010, — 138 стр.
4. OSTIS (Открытая семантическая технология для интеллектуальных систем) — [Электронный ресурс] — Режим доступа. — URL: www.ostis.net

# ИССЛЕДОВАНИЕ ПРОГРАММ-ШИФРОВАЛЬЩИКОВ

***Борисов Владислав Игоревич***
*студент 3 курса, кафедра автоматики и телемеханики ПНИПУ,*
*РФ, г. Пермь*
*E-mail: borisovvi94@yandex.ru*

***Хлебников Максим Валерьевич***
*студент 3 курса, кафедра автоматики и телемеханики ПНИПУ,*
*РФ, г. Пермь*
*E-mail: permcityvillain@yandex.ru*

***Кротова Елена Львовна***
*научный руководитель, канд. физ.-мат. наук, доцент ПНИПУ,*
*РФ, г. Пермь*

Компьютерный вирус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведения в негодность аппаратных комплексов компьютера.

Создателем теории самовоспроизводящихся механизмов считается Джон фон Нейман. Первые вирусы появились в 1981 году. Это были вирусы Virus1,2,3 и Elk cloner. Данные вирусы не наносили особый урон.

Сегодня же каждый из нас имеет не по одному компьютеру или смартфону, на котором располагаются много файлов, содержащих важную информацию. Потеря которой станет для вас большой проблемой, чаще всего финансовой. Поэтому в последнее время все большее распространение стали получать вирусы-вымогатели.

Почти все вирусы вымогатели создаются для извлечения из них коммерческой выгоды. Рассмотрим основные ограничение, вызываемые данными программами(ransomeware).

Ограниченный доступ к веб-сайтам. В данном случае после запуска вредоносного кода изменяется файл HOSTS, который содержит базу

домменных имен. После выполнения вредоносного кода при вводе в адресной строке браузера мы попадаем на сайт злоумышленников. На данном сайте находится информационное сообщение об необходимости перечисления денежных средств на счет злоумышленников. Избавиться от последствий данного кода не составляет сложности. Достаточно удалить все лишние строки из файла HOSTS. Часто это строки отделены множеством пробелов или пропуском строк. Также необходимо удалить сам исполняемый файл, содержащий вирус.

Ограничение работы с браузером. В данном случае после запуска вредоносного кода в окне браузера появляется окно, которое невозможно закрыть. Обычно такие окна используют механизм надстроек BHO(browser helper object) или расширения для браузера. Избавиться от последствий данных программ не составляет сложности. Необходимо отключить все подозрительные расширения в браузере. В некоторых случаях необходимо пересоздать ярлык браузера.

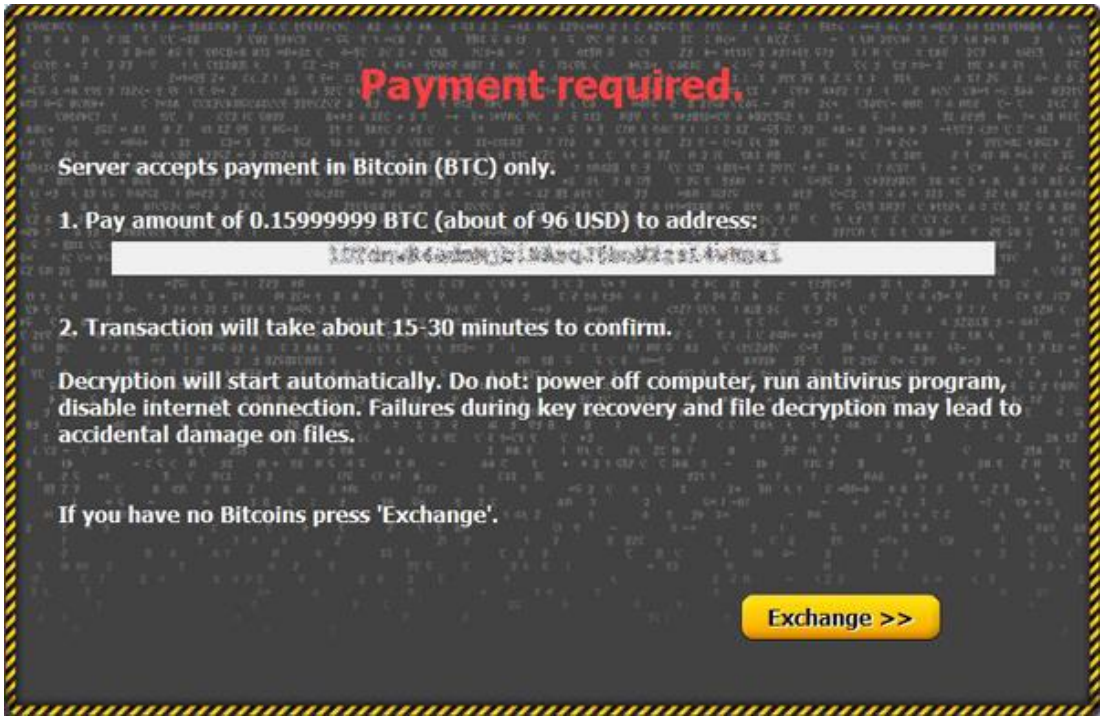



***Рисунок 1. Пример Окна-вымогателя***

Блокирование доступа к операционной системе. Если в двух предыдущих случаях операционная система оставалась полностью рабочей, то в данном

случае на этапе загрузки операционной системы появляется информационное окно, с требованием перевести денежные средства на указанный номер телефона. Для решения данной проблемы необходимо применять специализированные утилиты.

Шифрование данных пользователя. Данный вид программ начал применяться не так давно. При запуске этих программ происходит шифрование данных пользователя. Часто данные программы шифруют файлы определенного формата, с использованием секретного ключа, которые могут содержать важную информацию. Каждая программа нацелена на определенного пользователя. Один из вирусов кодировал профили, сохранения игр. Эти файлы невозможно восстановить, поэтому геймеры соглашались на любые условия злоумышленников. Чаще всего данные программы называют Cryptolocker. Одни из версий Cryptolocker могут шифровать и съемные хранилища информации(такие как usbflash, облачные хранилища, съемные жесткие диски). После заражения на дисплее компьютера появляется информационное окно, с требованием перевести денежные средства на указанный кошелек. Самое главное отличие от других программ-вымогателей заключается в том, что без секретного ключа(находится у злоумышленников) невозможно расшифровать закодированные данные.

Обычно для шифрования используется алгоритм ассиметричного шифрования RSA в связке с алгоритмом AES. Смысл этой связки заключается в следующем. На сервере злоумышленников генерируется пара ключей по алгоритму RSA: публичный ключ(public) и секретный ключ(private). Публичный ключ отправляется вредоносному коду, а секретный ключ всегда находится на сервере злоумышленников. Файлы на компьютеры жертвы шифруются с помощью алгоритма AES. На каждый файл генерируется новый ключ(aes-key), который после зашифровки файла шифруется с помощью открытого ключа RSA-public. Такой алгоритм применялся в такий вирусах, как Cryptolocker 1.0, 2.0, Teslacrypt, CoinVault. На данный момент ведущие

антивирусные компании перехватили базы данных с ключами дешифровки и создали утилиты, способные расшифровать зараженные файлы.

Но разработчики вредоносного ПО не стоят на месте. В конце июня 2014 года был обнаружен новый шифровальщик, получивший название CTB-Locker. В отличии от предыдущих версий, сервер с секретными ключами располагается в анонимной сети Tor, что затрудняет поиск злоумышленников. Если раньше злоумышленники пользовались легальным ПО от разработчиков Tor для включения компьютера в эту сеть, то в данном случае код взаимодействия реализован внутри вредоносной программы. Это позволяет ей пользоваться сетью Tor без использования сторонних исполняемых файлов и запуска дополнительных процессов. Но самое главное отличие от предыдущих версий — это использование протокола Диффи-Хеллмана на эллиптической кривой. Генерируется два ключа: открытый и секретный. Абоненты обмениваются открытыми ключами. Зная чужой открытый ключ и свой секретный, генерируется разделяемый секрет (shared secret). У обоих должно получиться один и тот же ключ. С помощью этого ключа можно зашифровать файл, используя любой алгоритм симметричного шифрования [1].

Session-shared = ECDH(master-private, session-public)= ECDH(master-public, session-private) (ФОРМУЛА 1).

Рассмотрим алгоритм шифрования CTB-Locker. Вредоносное ПО генерирует пару ключей: секретный ключ(master-private) и открытый ключ(master-public). Секретный ключ отсылается на сервер. На каждый файл генерируется пара сессионных ключей(session-public, session-private) и вычисляется разделяемый секрет(session-shared). После сжатия файла библиотекой Zlib, он шифруется алгоритмом AES. В качестве ключа берется хэш от разделяемого секрета SHA256. После шифрования ключ session-public сохраняется в файл, а session-private не сохраняется. Следовательно остается один вариант расшифровки: необходимо найти ECDH (master-private,session-public). А master-private храниться на сервере злоумышленников [2].

Вирус CTB-Locker распространяется в сети при помощи двух других вирусов, а именно Andromeda и Joleee.

Помимо CTB-Locker стали учащаться появления вредоносных программ-шифровальщиков в сети Tor. Не удивительно , ведь хакеры всегда находят средства усовершенствовать вирус. Совершенствуются средства защиты — совершенствуются средства нападения.

Как же обезопасить себя от данных программ-вымогателей?

Одним из самых эффективных методов — создание резервных копий важных для вас файлов. Только резервные копии необходимо делать на носители, отключаемые от компьютеров после копирования. Так же не стоит пренебрегать антивирусными продуктами крупных компаний.

Если ваш компьютер заражен, то стоит обратится в службу поддержки вашего антивируса, приложив несколько зашифрованных файлов.

**Список литературы:**


1. Сергей Николенко. Эллиптическая криптография // Опубликовано в журнале "Компьютерра" № 31 от 31 августа 2006 года [Электронный ресурс] — Режим доступа. — URL: http://old.computerra.ru/2006/651/283929/
2. Федор Синицын. Новое поколение вымогателей // SecureList июль 24,2014 [Электронный ресурс] — Режим доступа. — URL: https://securelist.ru/analysis/obzor/21090/novoe-pokolenie-vymogatelej

# СРАВНЕНИЕ СТАНДАРТОВ ШИФРОВАНИЯ США И РФ

***Брагина Виктория Германовна***
*студент 3 курса, Электротехнический факультет, ПНИПУ,*
*РФ, г. Пермь*
*Email: bragina951993@yandex.ru*

***Кротова Елена Львовна***
*научный руководитель, канд. физ.-мат. наук, доцент ПНИПУ,*
*РФ, г. Пермь*

В 1990 году был введен в действие отечественный стандарт шифрования ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» [1].

Стандарт был разработан действующей в то время спецслужбой. Является обязательным для применения в организациях, осуществляющих криптографическую защиту данных для передачи ее по сетям ЭВМ.

Через 12 лет, в 2002 году в США был принят новый стандарт шифрования взамен старому (DES). Стандарт носит название Advanced Encryption Standard (AES). В отличие от отечественного, избирался на конкурсной основе. В данный момент является одним из самых распространенных алгоритмов симметричного шифрования [4].

Далее рассмотрены основные характеристики стандартов в попытке выяснить: уступает ли отечественный стандарт зарубежному.

**Описание архитектур.**

Алгоритм AES основан на архитектуре “Square”, что в переводе означает «Квадрат», которая представляет собой прямые преобразования шифруемого блока, который представлен в виде двумерного байтового массива размером 4x4 [2, с. 84].

За один раунд шифруемый блок преобразуется целиком, таким образом, необходимую сложность преобразований можно получить за меньшее число раундов.

Каждый раунд заключается в сложении по модулю два начального блока данных и ключевого элемента, далее следуют три операции, рассмотренные в следующей части.

Алгоритм ГОСТ 28147-89 базируется на архитектуре «сеть Файстеля». Данная архитектура подразумевает разбиение исходного блока данных на две части. Одна из частей изменяется с помощью функции шифрования в зависимости от ключа раунда и далее складывается по модулю 2 с другой частью. После каждого раунда части меняются местами, т. е. на следующем раунде текущий измененный блок становится неизменным [2, с. 73].

Недостатком данной архитектуры, по сравнению с используемой в алгоритме AES является то, что за один раунд шифруется только половина блока.

**Описание раундов шифрования.**

В алгоритме AES шифруемый блок представлен в виде матрицы 4x4. Все операции производятся над отдельными байтами матрицы, а так же над ее строками и столбцами [2, с. 85].

В каждом раунде происходят следующие преобразования:

- Операция SubBytes представляет собой замену каждого байта массива данных новым значением, используя таблицу замены. Такая подстановка обеспечивает нелинейность алгоритма шифрования [2, с. 85].
- Операция ShiftRows выполняет циклический сдвиг влево всех строк массива данных, кроме нулевой. Шаг смещения байтов зависит от номера строки [2, с. 85].
- Операция MixColumns выполняет умножение каждого столбца массива данных, которые принимаются за многочлены над полем $GF(2^8)$, на фиксированный полином [2, с. 85].

$$a(x) = 3x^2 + x^2 + x + 2. \quad (1)$$

умножение по модулю $x^4 + 1$. (2)

- Операция AddRoundKey выполняет сложение по модулю два массива данных с ключом.

Алгоритм ГОСТ 28147-89 шифрует информацию блоками по 64 бита, которые разбиваются на подблоки по 32 бита (N1 и N2) [3]. Состоит из следующих шагов:

- Сложение по модулю $2^{32}$ ключевого элемента и подблока N1 [3].
- Табличная замена. Далее подблок разбивается на восемь 4-битовых частей, значения каждой из которых заменяются в соответствии с таблицей замены, называемой S-блоком. Количество S-блоков адекватно 4-битовым частям и представляют собой перестановку чисел от 0 до 15 [3].
- Выходы S-блоков объединяются в 32-битную последовательность и циклически сдвигаются влево на 11 битов к старшему разряду [3].

Очевидно, что в каждом стандарте раунды шифрования аналогичны друг другу. Что значительно упрощает их аппаратную и программную реализацию. Последний раунд AES не содержит операции MixColumns, в последнем раунде ГОСТа отсутствует перестановка подблоков, в данном случает это сделано, чтобы обеспечить возможность расшифровки блока данных.

Учитывая, что в стандарте 28147-89 используется 32 раунда шифрования, это позволяет противостоять существующим методам криптоанализа. Так при, примерно, 24 раундах атака становится абсолютно непрактичной.

В алгоритме шифрования стандарта AES предусмотрено 10—14 раундов. Но достаточная криптостойкость алгоритма достигается уже при 6—8 раундах.

Таким образом, оба алгоритма обладают достаточной стойкостью к методам криптоанализа с некоторым запасом [2, с. 86].

**Обратное преобразование**

В соответствии с тем, что архитектура стандарта 28147-89 основана на сети Файстеля, процедура расшифрования данных идентична прямому преобразованию, с тем исключением, что порядок использования ключевых элементов — обратный [3].

В стандарте AES расшифрование происходит путем применения обратных операций в обратной последовательности. При сопоставлении алгоритмов прямого и обратного преобразований можно заметить, что они практически одинаковы, за исключением того, что все ключевые моменты выполняются в обратном порядке.

Таким образом, процедуры шифрования и расшифрования в обоих стандартах могут быть совмещены при их реализации.

**Ключи шифрования**

В отечественном стандарте используется 256-битный ключ, который разбивается на восемь 32-битовых подключей (k1..k8). Ключи k9..k24 являются повторением ключей k1..k8, ключи с k29 по k32 повторяют ключи k8..k1. Следовательно, каждый подключ используется ровно четыре раза. Порядок их использования зависит от номера раунда [3].

Благодаря достаточно большой длине ключа сохраняется высокая криптостойкость алгоритма [3].

В стандарте AES ключ для каждого раунда вырабатывается с помощью операции расширения. Длина каждого ключа составляет 128, 192 или 256 бит. Алгоритмы определения ключа шифрования различаются незначительно. Рассмотрим на примере 128-битного ключа или четырех 4-байтовых слов $w_i$, $w_{i+1}$, $w_{i+2}$, $w_{i+3}$. Все ключи — 44-байтовых слова. Первые четыре слова заполняются ключом шифра, а из остальных 40 слов выбираются 4 слова для ключа раунда. Слова выбираются следующим образом: четыре первых слова являются ключом с номером 0, следующие четыре слова — ключом для первого раунда и т. д. [3].

Формирование последующих раундовых ключей происходит в соответствии с формулами:

$$w_{i+5} = w_{i+4} \oplus w_{i+1} \quad (3)$$

$$w_{i+6} = w_{i+5} \oplus w_{i+2} \text{ и т. д.} \quad (4)$$

Изменение первых слов в каждом ключе раунда происходит по следующей формуле:

$$w_{i+4} = w_i \oplus g(w_{i+3}) \quad (5)$$

Функция g выполняется в виде последовательных шагов:

1. Rotword — сдвиг влево на один байт

2. SubBytes — замена каждого байта

3. Суммирование по модулю два байтов с раундовой константой, с целью избежания симметрии и появления слабых ключей.

Несмотря на сложность выбора ключей шифрования в AES, метод остается достаточно простым и эффективным. В данном случае атака с перебором ключей не имеет практического значения.

Рассмотрев некоторые параметры стандартов, можно прийти к выводу, что их основные рабочие моменты вполне сопоставимы, несмотря на использование разных архитектур. Основные параметры криптостойкости ни одного из стандартов не имеют преимуществ перед другим. Недостатком отечественного стандарта будет являться его более медленная аппаратная реализация.

Таким образом, можно сказать, что отечественный стандарт не уступает современным требования к шифрованию данных, несмотря на то, что разница в годах разработки между ним и AES достаточно большая с точки зрения развития технологий.

**Список литературы:**


1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М.: ИПК Изд-во стандартов, 1990. — 26 с.
2. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. СПб.: БХВ-Петербург, 2009. — 576 с.
3. Стандарт шифрования ГОСТ 28147-89// http:// computerra.ru : [Электронный ресурс] — Режим доступа. — URL: http://www.computerra.ru/cio/old/it-expert/328198/ (дата обращения 02.05.14).
4. Advanced encryption standard: [Электронный ресурс] — Режим доступа. — URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (дата обращения 05.05.14).

# ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ЛОГИСТИКЕ

***Гуанова Сатаней Хазритовна***
*студент 3 курса, кафедра информационных систем и технологий СКФУ, РФ, г. Пятигорск*
*E-mail: guanova2014@yandex.ru*

***Коломенская Валерия Юрьевна***
*студент 3 курса, кафедра информационных систем и технологий СКФУ, РФ, г. Пятигорск*
*E-mail: lera_numb1@mail.ru*

***Битюцкая Наталья Ивановна***
*научный руководитель, канд. физ.-мат. наук, доцент СКФУ, РФ, г. Пятигорск*

Системы поддержки принятия решений (СППР)позволяют человеку управлять процессом принятия решений с помощью компьютераи становятся в последнее время все более актуальными и популярными.

Увеличение объема информации и необходимость интенсивного и оперативного ее обмена, усложнение задач управления, необходимость учета большого количества взаимосвязанных факторов приводят к необходимости использования вычислительной техники в процессе принятия решений.СППР применяют в таких областях, как телекоммуникации, банковское дело, страхование, логистика и др. [2].

Целью данного исследования является сравнительный анализ информационных систем поддержки принятия решений в сфере логистики.

Сегодня логистика стала неотъемлемой частью любого бизнеса. Логистикой называется многоступенчатый процесс, который управляет материальными и информационными потоками в сферах производства и обращения [1]. Она необходима для грамотного распределения сырья и готового товара. Под логистикой подразумевается организация и координация процессов закупок, транспортировки и хранения продукции, оптимизация издержек всех функциональных областей предприятия, которые

неизбежны на любом производстве. Логистика позволяет рассмотреть совокупность всех звеньев производственного процесса как единую систему.

Различают следующие виды логистики: закупочная, производственная, сбытовая, транспортная и складская логистика.

В настоящее время на российском рынке программных продуктов, предусматривающих автоматизацию управления логистическими процессами, представлено огромное количество систем и пакетов прикладных программ.

Для проведения сравнительного анализа информационных систем, применяемых в логистике, были выбраны наиболее известные программные продукты отечественных и зарубежных производителей, представленные на российском рынке:

- «1С-Логистика: Управление складом 3.0» — «1С:Предприятие 8» для автоматизации управления складским хозяйством предприятия;
- web-сервис «Департамент логистики» — новый облачный сервис для автоматического планирования маршрутов, который помогает сократить транспортные расходы за счет использования математических алгоритмов при формировании маршрутов, распределения заказов по транспортным средствам и загрузке кузова;
- "Roadnet Transportation Suite" — пакет программных продуктов для управления транспортной логистикой, предназначенный для планирования оптимальных маршрутов доставки;
- «1С-Рарус:Транспортная логистика и экспедирование» — программный продукт, который предназначен для автоматизации управления процессом перевозки в компаниях, занимающихся оказанием услуг по доставке и экспедированию грузов различными видами транспорта: автомобильным, железнодорожным, авиационным, морским [3];
- "Solvo.WMS " — программный продукт для автоматизации складских комплексов, портов и контейнерных терминалов, для управления цепочками поставок;

- «Ингит. Деловая карта» — программный комплекс, предназначенный для представления на электронных картах размещения клиентов и решения задач транспортной логистики в целях оптимизации грузотранспортных потоков и использования транспорта при доставке заказов;
- «ФОЛИО Купец» — современный программный комплекс для автоматизации учета на складах ответственного хранения, в торговле и производстве;
- "iSolutions-Логистика" — решение, расширяющее возможности модуля «Управление складом» Microsoft Dynamics AX, который позволяет комплексно автоматизировать процессы управления складом;
- программы для логистики компании «Первый БИТ» — транспортная и складская логистика;
- "E-SKLAD" — программное обеспечение для решения задач складской логистики;
- "TopRouteToplogistic" — система, предназначенная для автоматизации процесса планирования доставки грузов автотранспортом.

В таблицах 1 и 2 представлены результаты сравнения наиболее популярных программных продуктов в сфере транспортной и складской логистики.

***Таблица 1.***

**Сравнение ПОв сфере транспортной логистики**

| **Критерий сравнения** | **Департа-ментлогисти-ки** | **Roadnet Transportation Suite** | **1С-Рарус: Транспортная логистика и экспедирова-ние** | **Ингит. Дело-вая карта** | **Первый БИТ** | **TopRoute Toplogistic** |
|---|---|---|---|---|---|---|
| Стоимость (руб.) | От 3200 до 28800 | – | От 24000 до 40000 | 14000 | – | От 50000 до 1180000 |
| Маршрутизация перевозок, планирование | Да | Да | Да | Да | Да | Да |
| Отслеживание статуса груза | Нет | Да | Да | Да | Нет | Да |
| Контроль передвижения транспортного средства и персонала | Нет | Да | Да | Нет | Да | Да |

| | | | | | | |
|---|---|---|---|---|---|---|
| On-line взаимодействие водителя с логистом | Нет | Да | Да | Нет | Да | Да |
| Формирование оптимальных схем загрузки товара в ТС | Нет | Да | Да | Нет | Нет | Да |
| WEB-отчетность | Да | Да | Да | Да | Нет | Да |

***Таблица 2.***

**Сравнение ПОв сфере складской логистики**

| **Критерий сравнения** | **1С-Логистика: Управление складом 3.0** | **Solvo.WMS** | **ФОЛИО Купец** | **iSolutions-Логистика** | **Первый БИТ** | **E-SKLAD** |
|---|---|---|---|---|---|---|
| Стоимость (руб.) | 37800 | – | От 500000 до 1200000 | 900000 | – | – |
| Учет серий и сроков годности при размещении | Да | Да | Да | Да | Да | Нет |
| Формирование правил размещения товара на складе | Да | Да | Нет | Да | Да | Нет |
| Оптимизация складских запасов за счёт перераспределения товара | Нет | Да | Да | Да | Да | Да |
| Контроль качества товара | Да | Да | Нет | Да | Да | Да |
| Получение актуальной информации об остатках товара на складе | Да | Да | Да | Да | Да | Да |
| Оптимизация маршрутов отбора товара по разным критериям | Нет | Да | Нет | Да | Нет | Нет |

Таким образом, можно заметить, что по основополагающим функциям данные программы очень схожи между собой, за исключением их стоимости. Такое большое отличие в стоимости объясняется дополнительными функциями программ и предоставляемыми ими услугами.

Важно отметить, что рассмотренные программные продукты улучшаются под изменяющиеся требования клиентов, посредством постоянного обновления и выпуска дополнений к предыдущим версиям.

Использование данных программных продуктов на предприятиях значительно упрощает процессы доставки грузов и управления складами ответственного хранения, а также позволяет значительно сократить логистические затраты.

Для автоматизации складской логистики крупным компаниям лучше всего подойдет система управления складом последнего поколения"Solvo.WMS". А для решения задач транспортной логистики как для крупных компаний, так и для небольших организаций можно порекомендовать программный продукт «1С-Рарус: Транспортная логистика и экспедирование», так как у него большие функциональные возможности и невысокая стоимость.

Транспортная и складская логистика играют большую роль, независимо от стратегической цели компании. Компания должна действовать таким образом, чтобы обеспечить наиболее оптимальный результат при имеющихся ограниченных ресурсах. Компания может решить данную задачу, если она будет обеспечивать себя современными аналитическими информационными системами, некоторые из которых были приведены в этой статье. Необходимо соответствовать требованиям современного общества, чтобы, во-первых, не допустить того, чтобы клиенты уходили к конкурентам, а во-вторых — создать такие условия, при которых логистическая система компании будет максимально эффективной.

**Список литературы:**


1. Официальный сайт «1С-Рарус» [Электронный ресурс] — Режим доступа. — URL: http://rarus.ru (дата обращения 04.05.2015).
2. Сергеев В.И. Логистика: Информационные системы и технологии: учебно-практическое пособие. М.: Издательство «Альфа-Пресс», 2012. — 608 с.
3. Советов Б.Я., Цехановский В.В., Чертовской В.Д. Интеллектуальные системы и технологии. М.: Издательский центр «Академия», 2013. — 320 с.

# РАЗРАБОТКА АЛГОРИТМА ПРОТОКОЛА АУТЕНТИФИКАЦИИ В КЛИЕНТ-СЕРВЕРНОЙ МОДЕЛИ

***Дубман Станислав Эдуардович***
*магистрант 2 курса, кафедра «ИБ», НИУ «МИЭТ», РФ, г. Зеленоград*
*E-mail: feyde87@gmail.com*

***Смык Сергей Владимирович***
*научный руководитель, канд. техн. наук, доцент, Научно-исследовательский университет «МИЭТ», РФ, г. Зеленоград*

Целью работы является разработка алгоритма протокола аутентификации на базе криптоалгоритмов *RSA* и Диффи-Хэллмана, позволяющего без установки дополнительного программного обеспечения на клиентской рабочей станции безопасно передавать информацию, требующую защиты.

В настоящий момент самым распространенным способом аутентификации, при доступе к сетевым ресурсам является ввод логина и пароля. Для большей защищенности, можно использовать многофакторную аутентификацию, однако введение её в клиент-серверную модель небольших организаций не всегда целесообразно.

Для решения проблемы обмена данными были разработаны различные протоколы, например протокол взаимоблокировки (рисунок 1) Основная идея которого заключается в том, что при передаче данных по незащищенной сети сообщения делятся на две части, каждая из которых в отдельности бесполезна. Сам протокол можно записать в следующем виде [1]:

1. первый участник протокола (далее Алиса) отправляет второму участнику (далее Боб) свой открытый ключ;

2. Боб отправляет Алисе свой открытый ключ; Алиса шифрует свое сообщение с помощью открытого ключа Боба.

3. Половину зашифрованного сообщения она отсылает Бобу;

4. Боб шифрует свое сообщение с помощью открытого ключа Алисы. Половину зашифрованного сообщения он отсылает Алисе;

5. Алиса отправляет оставшуюся половину зашифрованного сообщения;

6. Боб складывает обе половины сообщений Алисы и расшифровывает его своим закрытым ключом. Затем Боб посылает Алисе оставшуюся половину своего шифрованного сообщения;

7. Алиса складывает обе половины сообщений Боба и расшифровывает его своим закрытым ключом.

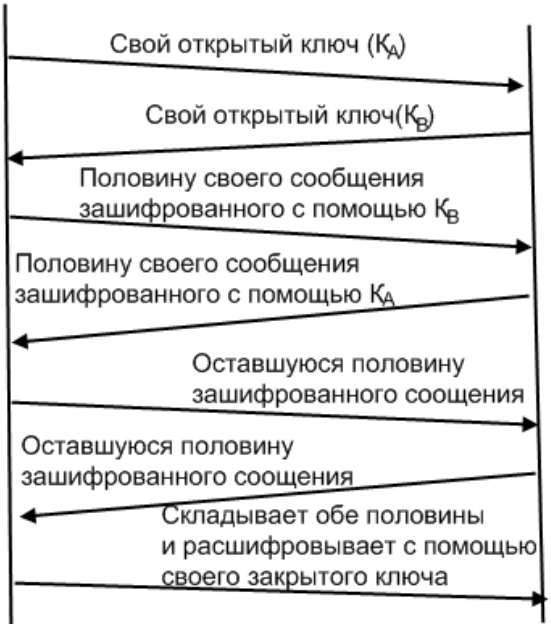



***Рисунок 1. Протокол взаимоблокировки***

Данный протокол помогает предотвратить атаку «человека посередине» при передаче сообщений, но не удобен при практической реализации, так как приходится передавать сообщения не целиком, а по частям, в связи с чем возникают дополнительные «расходы» на передаваемый трафик.

Добавив в эту схему такие дополнительные модули, такие как хэш-функцию, функцию генерации случайного числа и криптоалгоритм с отрытым ключом, можно провести аутентификацию пользователя. Последовательность реализации алгоритма выглядит следующим образом:

1) сервер генерирует случайное число *R_B*, вычисляет хэш-функцию:

$$P = H(H(\text{логин, пароль}), R\_B) \qquad (1)$$

и отправляет половину значения *P*;

2) клиент генерирует случайное число *R_A*, вычисляет хэш-функцию:

$$N = H(H\ (\text{логин, пароль}), R\_A) \quad (2)$$

и так же отправляет половину значения *N*;

3) сервер получив «первую половину значения» *N* отправляет «вторую часть» *P* и *R_B* клиенту;

4) клиент вычисляет:

$$P' = H(H(\text{логин, пароль}), R\_B) \quad (3)$$

сравнивает *P* и *P'*, если равенство *P = P'* выполняется, то посылается серверу «вторая часть» *N* и *R_A*;

5) сервер вычисляет значение:

$$N' = H(H\ (\text{логин, пароль}), R\_A) \quad (4)$$

а так же сравнивает получившееся значение и *N*. В случае верного равенства, считаем аутентификацию пройденной.

Данная схема (рисунок 2) позволяет, подтвердить взаимную подлинность участников протокола. Для возможности установки защищенного канала связи необходимо передать сеансовые ключи. Для этого необходимо включить в вычисление хэш-функции, происходящее на первом и втором шаге, открытые ключи сервера и клиента соответственно [2]. После чего устанавливаем сеансовый ключ, который будет использован для шифрования передаваемых данных. Для увеличения надежности протокола, можно предоставить пользователю выбор криптоалгоритма, поддерживаемого сервером.

Таким образом, одновременно проходит аутентификация клиента и сервера, а так же устанавливаются сеансовые ключи.

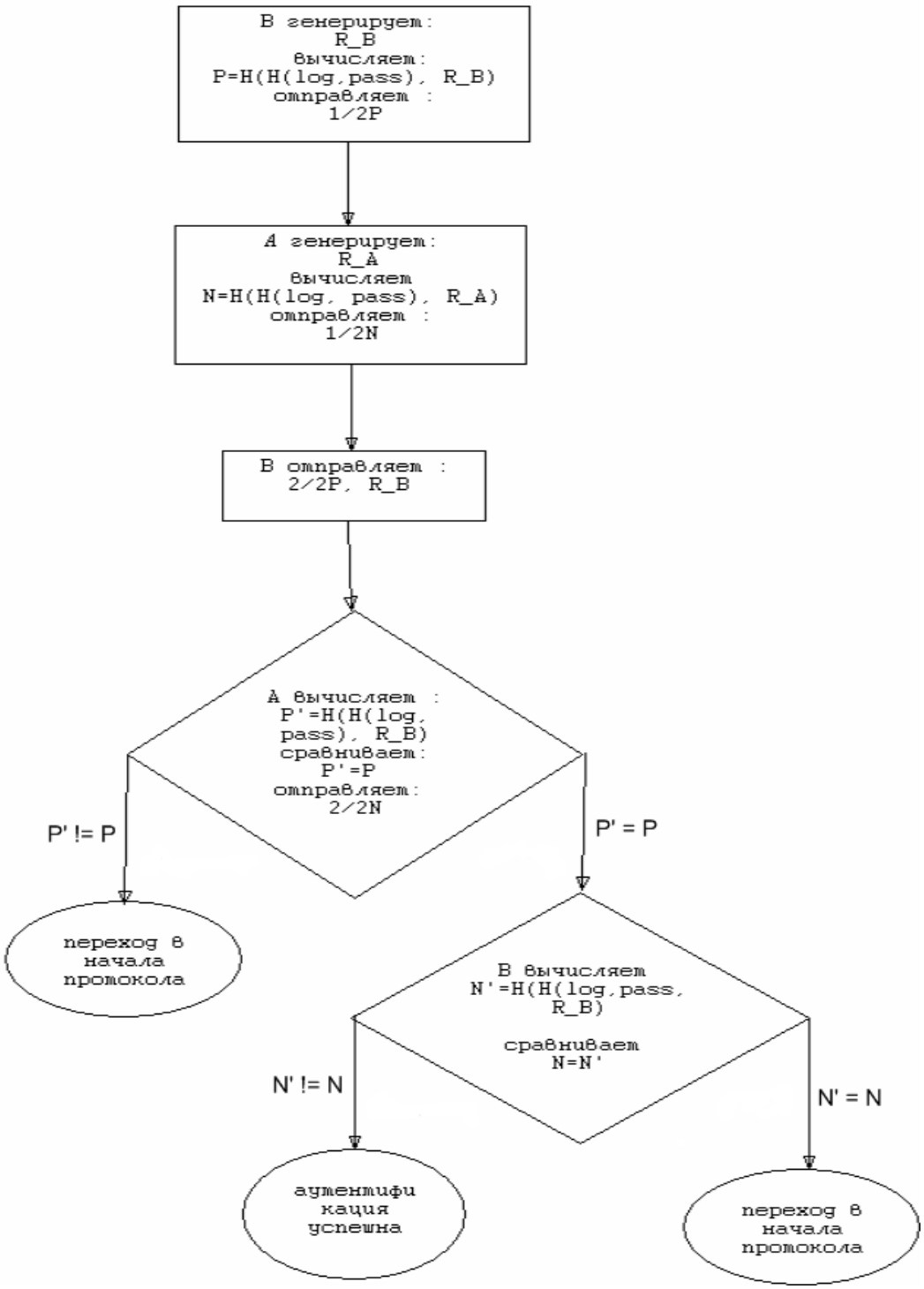



***Рисунок 2. Алгоритм аутентификации пользователя***

В таком виде протокол не будет подвержен пассивным атакам в виду того, что информация не передается в открытом виде по каналу связи. Однако, учитывая возможность того, что злоумышленник может использовать данные предыдущих сеансов, нельзя быть полностью уверенным в невозможности реализации атаки «человек посередине». Для устранения данной уязвимости

предлагается проведение между клиентом и сервером синхронизации по времени, а так же установка «метки времени». Протокол предполагает, что пользователь уже зарегистрирован на сервере.

Для предоставления регистрационных данных серверу, возможно, использовать следующий алгоритм (рисунок 3):

1) сервер (далее *B*) генерирует случайное число *R_B*, вычисляет:

$$P = H(OK_B, Ser, R\_B), \quad (5)$$

делит *P* на две части и отправляет «первую половину» *P* клиенту, где *H* это функция хеширования, $OK_B$ открытый ключ *B*, *Set* сертификат сервера;

2) клиент генерирует *R_A*, вычисляет:

$$N = H(login, password, R\_A, 1/2P), \quad (6)$$

так же делит полученное *N* на две половины и отправляет «первую половину» *N* серверу;

3) *B* отправляет клиенту «вторую часть» *P*, *R_B*, *Ser*, $OK_B$;

4) *A* проверяет равенство $P = P'$, где

$$P' = H(OK_B, Ser, R\_B), \quad (7)$$

шифрует с помощью $OK_B$ и ассиметричного алгоритм следующие данные $E_B(login, password, R\_A, P)$, далее вычисленное значение отправляет серверу, где $E_B$ — функция шифрования с помощью открытого ключа *B*;

5) сервер, используя свой закрытый ключ, расшифровывает сообщение клиента. Если значения *P* и *P'* совпадают, то записываем регистрационные данные в базу данных, если нет, то пробуем еще *n* раз.

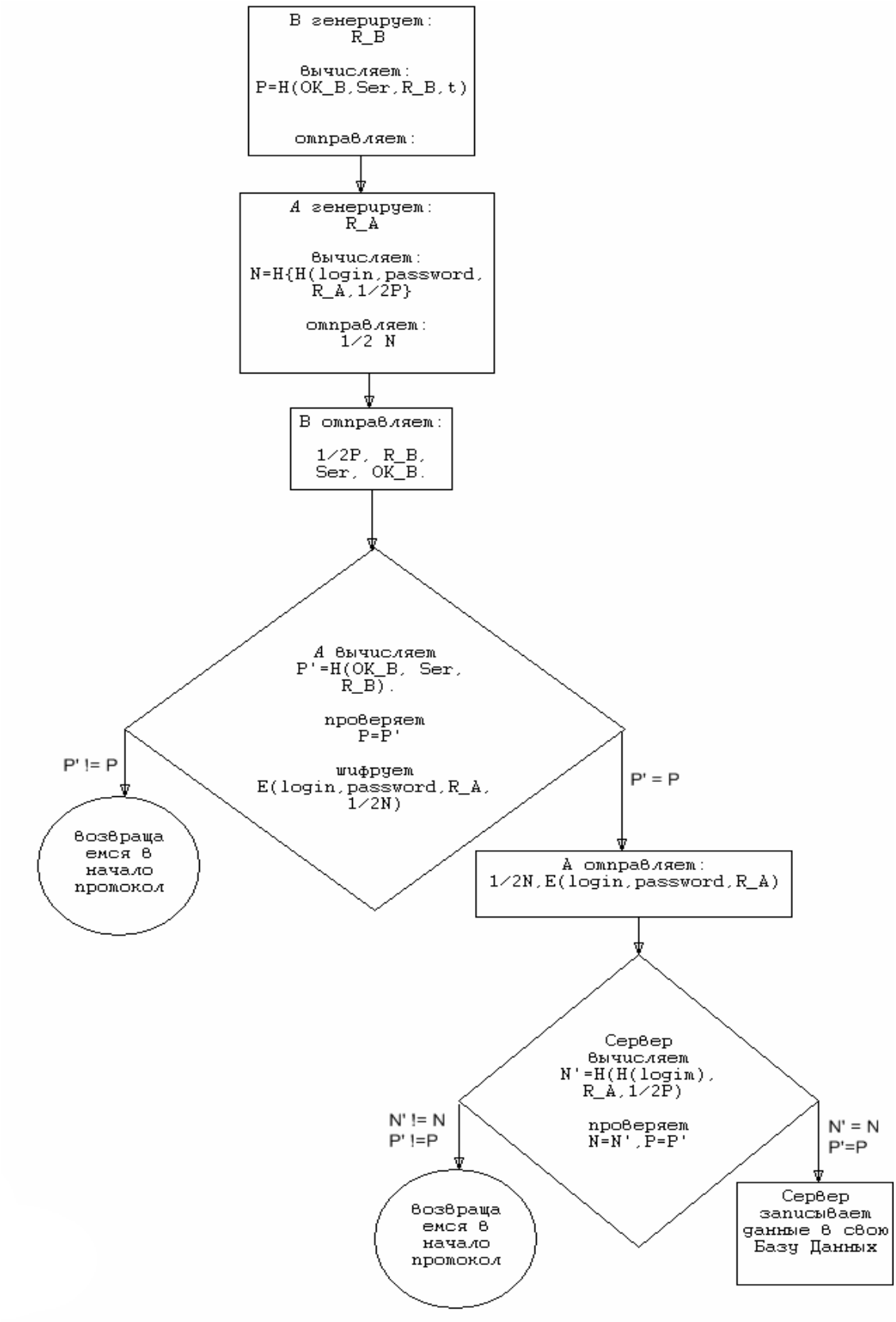



***Рисунок 3. Алгоритм передачи регистрационных данных***

Достоверность в данном протоколе, подтверждает только сервер. Для клиент-серверных систем эта особенность считается оправданной, однако может негативно повлиять на защищенность используемых схем.

При организации передачи данных, можно использовать протокол Диффи-Хэллмана для генерации сеансового ключа и передачи информации. В результате получим следующий алгоритм:

1) сервер генерирует случайное число *R_B*, вычисляет

$$P = H(DH\_B, Ser, R\_B), \quad (8)$$

где *H* это функция хеширования, $OK_B$ открытый ключ *B, Set* сертификат сервера.

Сервер делит *P* на две части и отправляет «первую половину» *P* клиенту;

2) клиент генерирует *R_A*, вычисляет

$$N = H(H(login), DH\_A, R\_A, 1/2P), \quad (9)$$

так же делит полученное *N* на две половины и отправляет «первую половину»*N* серверу;

3) *B* отправляет клиенту «вторую часть» *P, R_B, Ser, DH_B*;

4) *A* проверяет равенство $P = P'$, где

$$P' = H(DH\_B, Ser, R\_B), \quad (10)$$

если равенство верное, то отправляется «вторая половина» *N*, *H*(*login*), *R_A, DH_A;*

5) сервер вычисляет

$$N' = H(H(login), R\_A, DH\_A, 1/2P); \quad (11)$$

6) на основе сеансового ключа, полученного с помощью алгоритма Диффи-Хэлмана, устанавливаем защищенный канал связи и передаем регистрационную информацию;

7) сервер проверяет верность равенства $H(login)=H(login')$. Если оно верно, то считаем регистрационные данные верными и при необходимости продолжаем передачу данных.

К недостаткам, данного алгоритма можно отнести следующие моменты:

1. в протоколе узкой частью является знание таких данных как логин и пароль пользователя. Если злоумышленнику станут известны эти значения, он сможет выдавать себя за регистрированного пользователя;

2. пользователю необходимо каждый раз при аутентификации, генерировать пару ключи шифрования.

Приведенная схема аутентификации была разработана специально для клиент-серверной модели, где предполагалось взаимное доверие между его участниками.

Данная схема позволяет без установки дополнительного программного обеспечения на клиентской рабочей станции безопасно передавать информацию, требующую защиты, в тот момент, когда это требуется, при этом проводится проверку аутентичности.

**Список литературы:**


1. Смит Р.Э., Аутентификация: от паролей до открытых ключей: пер. с англ. М.: Издательский дом «Вильямс», 2002. — 432 с.
2. Шнайер Б., Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си: Пер. с англ. М.: Триумф, 2003. — 816 с.

# МУЛЬТИМЕДИЙНЫЕ ТЕХНОЛОГИИ — КАК ЭФФЕКТИВНЫЙ МЕТОД ИЗУЧЕНИЯ ГРАФИЧЕСКИХ ДИСЦИПЛИН

***Кисельман Татьяна Сергеевна***
*студент 1курса кафедры стандартизации и управления качеством, ПИ СФУ, РФ, г. Красноярск*
*E-mail: tanya.kiselman@mail.ru*

***Борисенко Ирина Геннадьевна***
*научный руководитель, доцент кафедры, НГ и Ч, ПИ СФУ, РФ, г. Красноярск*

В современном обществе, как никогда возросла социальная потребность в нестандартно мыслящих творческих личностях, потребность в творческой активности специалиста и развитом мышлении [3], в умении конструировать и создавать отвечающую запросам современного общества технику.

Инженерная графика изучается студентами высших учебных заведений с целью освоения ими понятия чертежа, как средства графического представления информации о каком-либо процессе или изделии. Чертеж является одним из главных носителей технической информации, без которой не обходится ни одно производство [4]. Но сегодня мы не можем себе представить процесс обучения графическим дисциплинам без использования современных обучающих мультимедийных средств. Принципиальное новшество, вносимое компьютером в образовательный процесс — интерактивность, позволяющая развивать активно-деятельностные формы обучения. Именно это новое качество позволяет надеяться на эффективное, реально полезное расширение интереса к изучаемой дисциплине.

«Мультимедиа» — сравнительно молодая отрасль новых информационных технологий, которая так стремительно и широко стала использоваться во всех сферах учебной деятельности, в том числе и в процессе обучения инженерной графики. Мультимедиа — это интерактивные (диалоговые) системы, обеспечивающие одновременную работу со звуком, анимированной компьютерной графикой, видеокадрами [6], изображениями и текстами.

Как известно, дисциплина начертательная геометрия и инженерная графика включает в себя огромный объем трудного в понимании и усвоении лекционного материала, она сопровождается сложными графическими построениями, требующими определенной логической последовательности и четкости выполнения алгоритмов решения метрических и позиционных задач. Выполнение большого количества сложных построений на доске традиционным способом с помощью мела, линейки и циркуля мало эффективно, занимает много времени, не являются наглядными, а так же не является привлекательным для студентов, уже со школьной скамьи приученных к получению материала с помощью современных средств обучения. Да и к тому же у многих студентов слабо развито пространственное мышление.


***Рисунок 1. Пример страницы электронных слайдов***

Мультимедийные лекции позволяют передать студентам содержательную часть дисциплины в более доступной, наглядной форме с использованием трехмерных чертежей, Flash-технологий, видеофрагментов, анимации и цветных эффектов. Также они помогают студентам понять и сложный материал. Лекции проходят более разнообразно, вызывая интерес аудитории,

что формирует повышение познавательной активности студентов [5]. Использование анимации и электронных слайдов (***рисунок 1***) создают у студентов осознание отображения различных пространственных объектов на плоскости, что способствует развитию пространственного мышления и повышению уровня усвоения рассматриваемого материала [1].

Рассмотрим некоторые примеры представления инженерной графики с помощью мультимедиа. Например, в таких программах как Компас-3D, SolidWorks, AutoCAD можно с легкостью сделать чертеж, создать 3D-деталь, осуществить сборку деталей (***рисунок 2***) и многое другое. Но для того чтобы это сделать потребуется изучить программу, что тоже требует немало усилий. Зато это очень интересно, удобно, наглядно и легко в понимании, развивает пространственное мышление и облегчает жизнь студентам, так как если бы все чертежи чертились вручную — это бы занимало большое количество времени. А время дорого стоит.

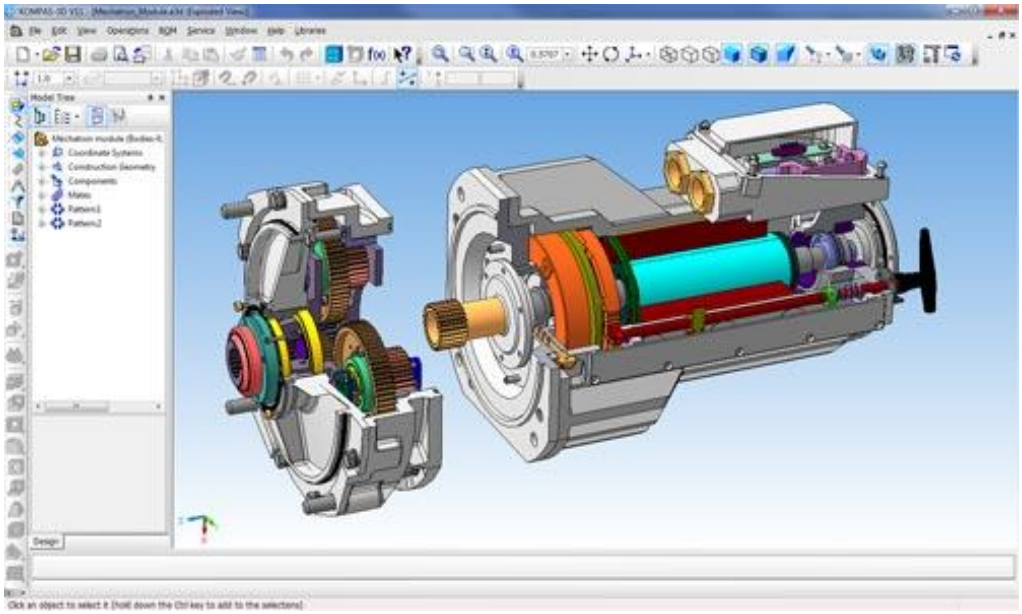


***Рисунок 2. Трехмерная модель сборки выполненная в КОМПАС-3D***

Работая в графических программах над построением трехмерных моделей, у студента создается иллюзия реальности. Поэтому представление результатов компьютерного моделирования в мультимедийной форме дает очень сильный

эффект [6]. Но есть и минусы — может возникнуть проблема с установкой той или иной программы, которая может повлечь за собой сбои и ошибки, что очень мешает при выполнении чертежа в данной программе.

Другой пример — представление теоретической информации с помощью слайдов, Flash-анимаций и объяснений преподавателя с наглядными изображениями, которые пошагово объясняют как решать ту или иную задачу. Это позволяет сократить время при изложении нового материала. Использование Flash-анимаций позволяет моделировать различные детали и узлы, демонстрировать их. Демонстрируемые слайды могут служить образцами для правильного графического исполнения работы. Этот метод представления информации удобен и интересен, а также прост для восприятия, так как людям проще усваивать информацию не сплошным текстом, а с помощью изображений. Картинка быстрее запоминается, чем большие тексты.

Следующий пример — это представление информации с помощью видеороликов и изображений с использованием звукового сопровождения. Это тоже своеобразный очень эффективный метод, но он редко используется при изучении материала, так создание подобных ресурсов очень трудозатратно. С помощью видеоуроков можно самостоятельно изучить программу для построения чертежей, разобраться с материалом, который ты не усвоил на занятии.

Заключительный пример — это представление информации с помощью электронных курсов, которые создают преподаватели на платформах своих вузов [7]. В электронных курсах широко используются все перечисленные медийные технологии. Основным преимуществом которых является доступность и возможность, если появляется необходимость, многократно просматривать при изучении теоретического материала и выполнении самостоятельной работы [2]. К тому же, самоконтроль и проверка знаний, что немало важно для подготовки к зачету или экзамену. Несомненно, это позволяет приобрести больше теоретических навыков, а также этот метод может служить для проверки самого себя.

Таким образом, мультимедийные технологии являются эффективным методом изучения начертательной геометрии и инженерной графики, они играют важную роль в понимании, запоминании и освоении информации. А правильное усвоение информации и применение ее на практике — неотъемлемая часть инженерного образования.

**Список литературы:**


1. Борисенко И.Г. Компетентностный подход в преподавании начертательной геометрии и инженерной графики // Вестник Красноярского государственного аграрного университета. — 2011. — № 12. — С. 302—304.
2. Борисенко И.Г. Организация учебного процесса в интерактивной электронной образовательной среде // Профессиональное образование в России и за рубежом. — 2014. — № 2 (14). — С. 119—123.
3. Крюкова Н. В. Инновационные методы обучения инженерной графики [Электронный ресурс]. – Режим доступа: http://festival.1september.ru/articles/504765/ (дата обращения 22.04.2015).
4. Куликов В.П. Информационные технологии в профессиональной подготовке инженеров по направлению «Информатика и вычислительная техника» [Электронный ресурс]. — Режим доступа. — URL: http://dlib.rsl.ru/01002633254 (дата обращения 20.04.2015).
5. Мачехина Д.В. Современные информационные технологии при изучении графических дисциплин на примере темы «эскизирование». [Электронный ресурс]. — Режим доступа. — URL: http://sibac.info/index.php/2009-07-01-10-21-16/3858 (дата обращения 25.04.2015).
6. Что такое мультимедиа. [Электронный ресурс]. — Режим доступа. — URL: http://school.xvatit.com/index.php (дата обращения 22.04.2015).
7. Borisenko I.G., Volodina D.N. EDUCATIONAL SMART TECHNOLOGIES IN THE EDUCATIONAL PROCESS // Журнал Сибирского федерального университета. Серия: Гуманитарные науки. — 2015. — Т. 8. — № 3. — С. 489—493.

# МЕТОДЫ ОБРАБОТКИ И СЖАТИЯ АУДИОСИГНАЛА С ПОМОЩЬЮ ВЕЙВЛЕТ АНАЛИЗА И БЫСТРОГО ПРЕОБРАЗОВАНИЯ ФУРЬЕ

***Кондыбаева Алмагуль Бауржановна***
*студент 3 курса, кафедра инженерной кибернетики, НИТУ МИСиС, РФ, г. Москва*
*E-mail: almakonde18@gmail.com*

***Шихеева Валерия Владимировна***
*научный руководитель, доцент. физ.-мат. наук, доцент НИТУ МИСиС, РФ, г. Москва*

**Введение**

В данной работе рассматриваются методы обработки аудио сигналов. Целью данного исследования является поиск и исследование методов обработки сигналов.

Главной целью работы является изучение методов представления звука в цифровой системе. Это можно трактовать так, что это изучение возможностей математики получать звук таким образом, чтобы уничтожить искажения, недостатки качества, шумы, помехи и т. д., т. е. получение звука наиболее приближенному естественному живому настоящему звучанию, получение качественного, красивого звука.

Существует множество способов очистки от шумов, множество способов представления звука (окрас отдельных инструментов, работа с тембром), наложение отдельных эффектов реверберации и прочих различных трансформаций звука. И для того, чтобы поподробнее изучить вопрос методов и возможностей обработки звука исследуются этапы поиска, выбора подходящего базиса, отвечающий определенным критериям и требованиям, а также подбор подходящих преобразований. Также очень сильно накладывается требование быстродействия алгоритмов обработки. Это обеспечит повсеместное использование алгоритмов преобразований звука.

В данной работе описывается работа с аудио сигналом и представление его в цифровой системе, а также попытка, с помощью ряда экспериментов найти

новые базисы наилучшим образом отвечающим решению обработки аудио сигнала.

**Список сокращений:**

1. АЦП — аналогово-цифровой преобразователь (analogue-to-digital converter as known as ADC)
2. ЦАП — Цифро-аналоговый преобразователь (digital-to analogue converter, DAC)
3. НЧ фильтры — низкочастотные фильтры
4. ВЧ фильтры — высокочастотные фильтры
5. ДПФ, DFT — Дискретное преобразование Фурье
6. БПФ, FFT — Быстрое преобразование Фурье

***Сигнал. Дискретные и непрерывные сигналы.***

Сигнал — зависимость одной величины от другой (функция).

С нашей точки зрения «сигнал» будет трактоваться как функция. Наша функция может трактоваться, как функция на интервале вещественных чисел R (непрерывный или аналоговый сигнал) или трактоваться, как функция на конечном множестве точек или как функция на бесконечном дискретном множестве точек (например Z дискретный или цифровой сигнал).

*Дискретные и непрерывные аудио сигналы на множестве* $Z_N$.

Большинство реальных звуковых сигналов являются непрерывными функциями (здесь мы пренебрегаем квантовыми эффектами).

Для обработки и работы с сигналом требуется перевести его в дискретную цифровую форму. Для этого как один из способов применяется равномерное по времени измерение значения сигнала на определенном промежутке времени и вводить полученные значения амплитуд в виде цифровой информации на компьютер. Измерения нужно делать часто, для того чтобы по полученному дискретному сигналу можно было бы восстановить исходный непрерывный аналоговый сигнал.

*Такой процесс замеров сигналов и перевод в цифровой формат называется процессом дискретизации [2, с. 6].*

Многие устройства проводят дискретизацию. Например, звуковая карта дискретизирует сигнал с микрофона. В результате таких операций (дискретизации) непрерывный (аналоговый) сигнал переводится в цифровой (дискретный).

*Устройство, которое производит замеры аналогового сигнала называется аналогово-цифровым преобразователем (АЦП, analogue-to-digital converter as known as ADC) [2, с. 14].*

*Частота, с которой АЦП производит замеры называется частотой дискретизации [2, с. 12].*

Важный вопрос:

С какой точностью можно восстановить исходный сигнал по его дискретным значениям и какие необходимы условия, действующие на частоту и исходный сигнал?

Читатель наверняка знаком с тем, что любую непрерывную функцию можно представить в виде ряда Фурье, разложенном на некотором отрезке.

Смысл разложения представляется в том, чтобы представить функцию в виде периодического ряда синусоид с различными амплитудами и фазами с кратными частотами. Амплитуды (коэффициенты) при синусоидах называются **спектром** функции.

Говорят, что сигнал имеет ограниченный спектр, если после определённого номера, все коэффициенты спектра равны 0.

Важное применение находит фундаментальная теорема Котельникова. Ответ мы ищем применяя ее.

*Теорема 1.1 Котельникова-Найквиста-Шеннона (или теорема отсчетов):*

*Если аналоговый сигнал имеет конечный (финитный), ограниченный по ширине спектр, то он может быть однозначно без потерь восстановлен по своим замерам, взятыми с частотой, большей или равной удвоенной верхней частоте:* $f \geq 2f_c$

*Тогда исходный аналоговый сигнал x(t) можно точно восстановить из его цифровых отсчетов x(nT), пользуясь интерполяционной формулой*

$$x(t) = \sum_{n=-\infty}^{+\infty} x(nT) \cdot Sinc(t - nT)$$

$$Sinc(t) = \frac{\sin \pi F_s t}{\pi F_s t}$$

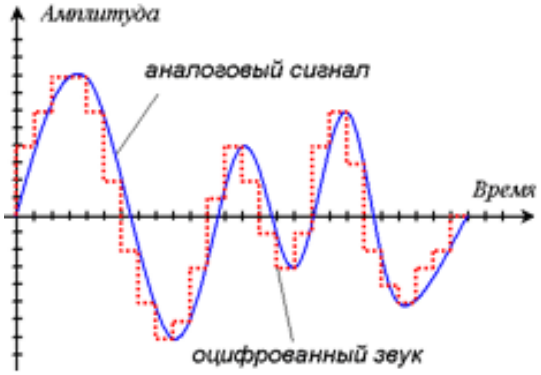



***Рисунок .1 Оцифрованный звук***

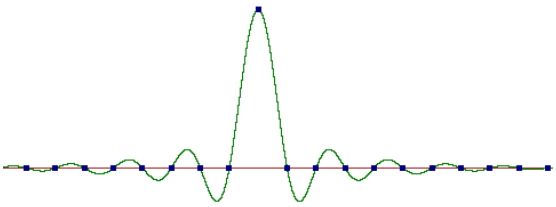


***Рисунок 2. Бесконечно затухающие колебания***

*Устройство, которое интерполирует дискретный сигнал до непрерывного, называется цифрово-аналоговым преобразователем (ЦАП, digital-to analogue converter, DAC) [2, с. 15].*

Например, в проигрывателях компакт-дисков для восстановления звука по цифровому звуковому сигналу, записанному на компакт-диск.

*Наложение спектров (алиасинг)*

Если попытаться оцифровать сигнал с недостаточной для него частотой дискретизации (или если спектр неограничен) по полученной цифровой выборке нельзя будет восстановить сигнал. Восстановленный сигнал будет выглядеть таким образом, как если бы, частоты лежащие выше половины частоты дискретизации, отразились от половины частоты дискретизации и перешли в нижнюю часть спектра.

Например, мы попытались оцифровать музыку, спектр которой лежит внутри частоты 20000 Гц, но при записи один из электроприборов сгенерировал помеху (например, дисплей) с ультразвуковой частотой в 40000 Гц, которая проникла в наш аналоговый звуковой сигнал. Мы производим оцифровку с частотой в 41000 Гц, при этом мы рассчитываем по т. Котельникова, что звук ниже 41000/2 Гц будет записан, верно. Но! Так как помеха лежит выше этой частоты, возникнет алиасинг. Потом помеха отразится в нижнею часть спектра на частоту около 5000 Гц. Затем мы пытаемся восстановить сигнал и пропускаем через ЦАП и слышим помеху на частоте 5000 Гц. Это шум. Таким образом помеха из неслышимой части ультразвуковой части переместилась в слышимую и появился шум на записи.

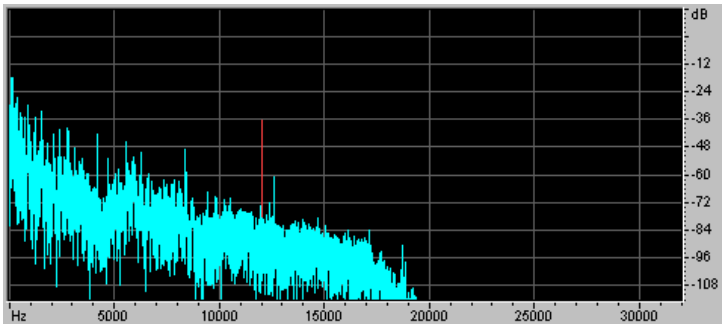



***Рисунок 3 Помеха отразилась от половины частоты дискретизации в нижнюю часть спектра и наложилась на звук. Помеха переместилась в слышимый диапазон***

*Алиасинг.(на рисунке 3)*

*Как можно его избежать?*

Существует 2 способа:

Использовать более высокую частоту дискретизации. Чтобы весть спектр уместился ниже половины частоты дискретизации

Второй способ: искусственно ограничить спектр сигнала перед оцифровкой.

Существуют устройства, называемые фильтрами для изменения спектра сигнала. Например, фильтры низких частот (НЧ- фильтры, low-pass filters),

которые пропускают, не изменяя все частоты ниже заданной, и удаляет все частоты выше заданной.

Такие частоты называются частотами среза (cutoff frequency filters) фильтра.

Одно из важных применений НЧ фильтров является искусственное ограничение спектра сигнала перед оцифровкой. В этом случае фильтры называются анти-алиасинговыми. Так как они предотвращают возникновение алиасинга при оцифровке сигнала. Часто среза обычно равняется половине частоте дискретизации.

***Импульсная Характеристика. Линейность. Инвариантность относительно сдвига.***

Мы рассматриваем дискретные линейные системы. На вход подается последовательность чисел x[n] (дискретный сигнал). И на выходе получается последовательность числе y[n]. Как и для непрерывных систем свойства линейности формулируем также.

Для того, чтобы рассмотреть каким образом линейная система может преобразовать входной сигнал в выходной рассмотрим реакцию системы на цифровую дельта-функцию (функция Кронекера). Получаем сигнал вида $\delta_{ij} = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}$ т.е. короткий единичный импульс.

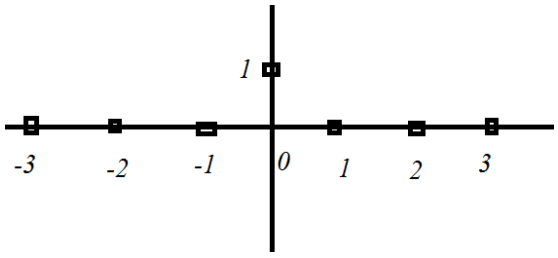



***Рисунок 4. Цифровая дельта функция (на рисунке)***

Очевидно, что любой дискретный сигнал можно разложить в сумму таких функций, сдвинутых по времени. Например, бесконечный сигнал x[n] можно представить в виде x[n] $\sum_0^{N-1} x[i]\delta[in]$.

Здесь дельта-функция — это базисные функции. x[i]-коэффициенты в линейной комбинации.

Далее, существует еще одно предположение, которое разумно наложить на нашу систему: в идеальном случае преобразователи должны быть линейными.

*Линейность.*

1. T(u + v)=T(u)+T(v);

2. T($\propto u$)=$\propto$T(u);

Линейность-это разумное предположение, которое мы накладываем на нашу математическую модель системы.

Во-первых: эффект действия системы на два сигнала должен быть суммой эффектов действия на каждый из сигналов в отдельности. Во-вторых, если мы умножаем входную систему на некоторую величину, то и входной сигнал должен быть умножен на нее.

*Инвариантность относительно сдвига.*

Еще одно предположение для системы — это инвариантность. Это означает, что в различные моменты времени если мы задерживаем сигнал на некоторое время, то единственным эффектом на выходе будет задержка сигнала на то же время. Такое предположение называется инвариантным во времени или инвариантным относительно сдвига.

Введем оператор сдвига: $(R_k z)(n) = z(n-k)$;

Инвариантность относительно сдвига представляем в виде:

T($R_k z$)=$R_k T(z)$;

Наиболее важным фактом, связанным с базисом Фурье F, является тот факт, что все линейные преобразования, инвариантные относительно сдвига диагонализируются базисом Фурье.

*Лемма 1.1. Линейные преобразования, инвариантные относительно сдвига* $l^2(Z_N) \to l^2(Z_N)$*, все диагонолизируются фактически одним базисом, более того, он ортогональный [1, с. 231].*

*Теорема 1.2.Пусть T:* $l^2(Z_N) \to l^2(Z_N)$ *линейное преобразование, инвариантное относительно сдвига. Тогда каждый элемент базиса Фурье F является собственным вектором преобразования T. Где T — диагонализируемое преобразование [1, с. 235].*

Доказательство:

Зафиксируем m $\epsilon \{0,1,2,\dots,N-1\}$

Пусть $F_m$-есть элемент базиса Фурье.

Тогда существуют комплексные скаляры такие, что

$$T(F_m)(n) = \sum_0^{N-1} a_k F_k(n) = \frac{1}{N}\sum_0^{N-1} a_k e^{2\pi ikn/N} \quad (1.0)$$

Для всех n потому, что F есть базис в $l^2(Z_N)$.

Применим действия оператора сдвига на единицу:

$$(R_1 F_m)(n)=$$

$$F_m(n-1) = \frac{1}{N} e^{2\pi i(n-1)m/N} = \frac{1}{N} e^{-2\pi im/N} e^{2\pi imn/N} = e^{-2\pi im/N} F_m(n); \quad (1.1)$$

$e^{-2\pi im/N} F_m$ не зависит от $n$ , то из линейности следует, что:

$$T(R_1 F_m)(n)=$$

$$e^{-2\pi im/N}(F_m)(n) = e^{-\frac{2\pi im}{N}} \sum_0^{N-1} a_k F_k(n) = \sum_0^{N-1} a_k e^{-2\pi im/N} F_k(n);$$

С другой стороны из равенства (1.1) вытекает также, что

$$(R_1 T(F_m))(n) = (T(F_m))(n-1) = \frac{1}{N}\sum_0^{N-1} a_k e^{\frac{2\pi ik(n-1)}{N}} =$$

$$\frac{1}{N}\sum_0^{N-1} a_k e^{-2\pi k/N} e^{2\pi kn/N} = \sum_0^{N-1} a_k e^{-\frac{2\pi ik}{N}} F_k(n)$$

Но для всех n по предположению T есть преобразование, инвариантное относительно сдвига. Сравнивая полученные выше выражения для этих 2 величин и используя единственность разложения вектора по элементам базиса, получаем, что для каждого k=0,1,…,N-1 справедливо равенство:

$$a_k e^{-2\pi i m/N} = a_k e^{-2\pi i k/N} \quad (1.2)$$

Если k≠m , то $a_k e^{-2\pi i m/N} \neq a_k e^{-2\pi i k/N}$, так как $0 \leq k, m \leq N-1$.

Поэтому равенство 1.2 может выполняться, если только $a_k = 0$.

Следовательно, мы доказали, что $a_k = 0$, только когда k≠m. Поэтому в равенстве 1.0 все слагаемые пропадают, за исключением членов с номерами k =m, получается

$$T(F_m)(n) = a_m F_m(n)$$

Следовательно, $F_m$ есть собственный вектор преобразования T с собственным значением $a_m$.

Так как m выбрано произвольно, это показывает, что каждый элемент базиса Фурье есть собственный вектор преобразования T \. Отсюда следует, что T диагонализируемо.

Сформулируем еще одну очень важную теорему:

*Теорема 1.3 Пусть T: $l^2(Z_N)$-> $(Z_N)$ есть линейное преобразовании. Тогда следующие утверждения верны:*

*1. T есть преобразование инвариантное относительно сдвига.*

*2. Матрица $A_{T,E}$ представляющая T в стандартном базисе E, есть циркулянтная матрица.*

*3. T есть оператор свертки*

*4. T есть мультипликаторный оператор Фурье.*

*5. Матрица $A_{T,F}$, представляющая T в базисе Фурье F, есть диагональная матрица.*

Утверждение о диагональной матрице (утв. 5) другими словами сформированное утверждение о том, что T диагонализируется базисом Фурье.

Стратегия доказательств этой теоремы состоит в последовательном доказательстве 1->2->3->1,3<->4 & 4<->5.

Заметим, что теорема дает и обратную ей теорему, которая утверждает, что линейное преобразование, которое диагонализируется базисом Фурье, есть преобразование инвариантное относительно сдвига.

Индексы для матриц будут изменятся от 0 до N-1 так же, как и в обозначении векторов, т.е. записываем матрицу A размера n$\times n$ как

$$[a_{mn}]_0 \leq m, n \leq N-1$$

Мы также распространим соглашение о периодичности для наших матрице, которое мы установили для наших векторов.

***Дискретное преобразование Фурье***

Представим векторы, которые мы рассматриваем в пространстве $C^N$, т. е. последовательности N комплексных чисел. Сейчас мы введем несколько обозначений: сначала пронумеруем эти N чисел индексами j $\subset \{0,1,\dots,N-1\}$ и вместо записи компонент вектора z в виде $z_j$ мы будем записывать их, как z(j). Это определяет новую точку зрения: мы рассматриваем z как функцию, определённую на конечном множестве.

$$Z_N = \{0,1,\dots,N-1\}$$

(*и это соответствует формальному определению Последовательности, Как функции на множестве индексов*)

Вектор в $C^N$ можно считать функцией, заданной в N точках, следовательно сигналом. Физически мы можем представить себе звуковой сигнал, например музыкальный фрагмент.

Система — это нечто, преобразующее входной сигнал в выходной. С нашей точки зрения система — это преобразование.

Z вектор столбец

$$\begin{pmatrix} z(0) \\ z(1) \\ z(2) \\ \dots \\ \dots \\ z(N-1) \\ \end{pmatrix}$$

Примем $l^2(Z_N)$ вместо $C^N$ для того, чтобы рассматривать функции для бесконемерного случая и применять в нашей работе.

$$l^2(Z_N) = \{z = (z(0), z(1), \dots, z(N-1)) : z(j) \epsilon C, 0 \leq j \leq N-1\}$$

С обычным покомпонентным сложением и скалярным умножением $l^2(Z_N)$. Поэтому $l^2(Z_N)$ есть N-мерное векторное пространство над полем C. Где одним из стандартных базисов является эвклидов базис $E=\{e_1, e_2, e_3, \dots, e_{N-1}\}$.

Здесь $e_j(n) = 1$, j=n, $e_j(n) = 0$ если n$\neq j$.

В этом обозначении комплексное скалярное произведение в $l^2(Z_N)$ определяется так: $\langle z, w \rangle = \sum_{k=0}^{N-1} z(k)\overline{w(k)}$

С нормой:$\|z\| = (\sum_{k=0}^{N-1} |z(k)|^2)^{1/2}$

Мы сохраняем понятие ортогональности при условии равенства нулю: $\langle z, w \rangle = 0$

z$\perp w$ тогда и только тогда, когда $\langle z, w \rangle = 0$.

Также вектор z должен быть периодическим с периодом N:

$$z(j+N)=z(j)\ \forall j \epsilon Z$$

Представим $E_0, E_1, E_3, \ldots, E_{N-1} \epsilon l^2(Z_N)$

$$E_0 = \frac{1}{\sqrt{N}}$$

$$E_1 = \frac{1}{\sqrt{N}} e^{2\pi i n/N} E_2 = \frac{1}{\sqrt{N}} e^{2\pi i 2n/N} E_3 = \frac{1}{\sqrt{N}} e^{2\pi i 3n/N} E_{N-1} = \frac{1}{\sqrt{N}} e^{2\pi i (N-1)n/N} E_m(n) = \frac{1}{\sqrt{N}} e^{2\pi i (m)n/N}$$

В $l^2(Z_N)$ воспользуемся Леммой 1.3: Множество $E_0, E_1, E_3, \ldots, E_{N-1}$ есть ортонормированный базис пространства $l^2(Z_N)$. (М.Фрейзер, 1999)

Доказательство: Пусть j,k $\in \{0,1,2,\ldots,N-1\}$

$$\langle E_j, E_k \rangle = \sum_{n=0}^{N-1} E_j(n)\overline{E_k(n)} = \sum_{n=0}^{N-1} \frac{1}{\sqrt{N}} e^{2\pi i (j)n/N} \overline{\frac{1}{\sqrt{N}} e^{2\pi i (k)n/N}} =$$

$$\sum_{n=0}^{N-1} \frac{1}{\sqrt{N}} e^{2\pi i (j)n/N} \frac{1}{\sqrt{N}} e^{-2\pi i (k)n/N} = \frac{1}{N} \sum_{n=0}^{N-1} e^{2\pi i (j-k)n/N} = \frac{1}{N} \sum_{n=0}^{N-1} (e^{2\pi i (j-k)/N})^2$$

Если j=k , то все члены внутри группы в последней сумме равны 1.

$$\langle E_j, E_k \rangle = N^{-1} \sum_{n=0}^{N-1} 1 = 1$$

Следовательно, норма тождественно равна единице.

$$\|E_j\|^2 = 1$$

Для каждого j. Т. е. все $E_j$ имеют норму 1.

Так как –N<=j-k<=N

Поэтому сумма есть частичная сумма геометрической прогрессии и

$$\sum_0^{N-1} (e^{2\pi i (j-k)/N})^2 = \frac{1-(e^{2\pi i (j-k)/N})^N}{1-(e^{2\pi i (j-k)/N})^N}$$

Сократив степени N при правых слагаемых:

$$(e^{2\pi i(j-k)/N})^N=(e^{2\pi i(j-k)})=1$$

j-k есть целое число, поэтому для каждых j k не равных друг другу выполняется :

$$\langle E_j, E_k\rangle \neq 1$$

$\langle E_j, E_k\rangle$=0

Таким образом, мы получаем ортонормированные элементы $E_j, \perp E_k$

Поэтому $\{E_0, E_1, E_3, \ldots., E_{N-1}\}$ есть ортонормированное множество. Следовательно мы получили ортогональное множество векторов $\{E_0, E_1, E_3, \ldots., E_{N-1}\}$ в непрерывном пространстве $l^2(Z_N)$ , где определено комплексное скалярное произведение . и пользуясь Леммой 1.3 наше множество Линейно Независимое множество.

Лемма 1.4: Пусть V — пространство с комплексным скалярным произведением, а B — ортогональное множество векторов в этом пространстве и 0 не принадлежит этому множеству. Тогда B есть линейно независимое множество.

Поэтому множество $\{E_0, E_1, E_3, \ldots., E_{N-1}\}$ есть базис пространства $l^2(Z_N)$.

Определение 1.1. Пусть z = $\{0,1,2,\ldots, N-1\} \in l^2(Z_N)$/ Для m=0,1,….,N-1 определим

$$\hat{z}(m) = \sum_{0}^{N-1} z(n)e^{-2\pi imn/N}$$

Пусть

$$\hat{z} = \{\hat{z}\,(0), \hat{z}(1), \hat{z}(3), \ldots, \hat{z}(N-1)\}$$

Отображение $l^2(Z_N)$в $l^2(Z_N)$, котрое связывает z и $\hat{z}$ называется Дискретным Преобразованием Фурье (ДПФ для него обычно используется аббревиатура DFT).

***Спектральный анализ.***

Часто ДПФ применяется для наблюдения и анализа спектра сигнала. При этом обычно наиболее интересными являются лишь амплитуд $C_к$ отдельных гармоник, а не их фазы. В этом случае спектр обычно отображается в виде графика зависимости амплитуды от частоты.

Перед вычислением спектра сигнала нужно выбрать отрезок сигнала, на котором будет вычисляться спектр. Длина отрезка должна быть степенью двойки (для работы БПФ). Иначе сигнал надо дополнить нулями до нужной длины. После этого к выбранному участку сигнала применяют БПФ. Коэффициенты амплитуд считают по формуле ДПФ. При вычислении спектра указанным образом возможен следующий нежелательный эффект. При разложении функции в ряд Фурье мы полагаем, что функция периодическая, с периодом, равным размеру БПФ. Вычисляется спектр именно такой функции (а не той, из которой мы извлекли кусок). При этом на границах периодов такая функция наверняка будет иметь разрывы (ведь исходная функция не была периодической). А разрывы в функции сильно отражаются на ее спектре, искажая его. Для устранения этого эффекта применяются так называемые взвешивающие окна. Они плавно сводят на нет функцию вблизи краев анализируемого участка. Выбранный для анализа участок сигнала домножается на весовое окно, которое устраняет разрывы функции при «зацикливании» данного участка сигнала. Зацикливание происходит при ДПФ, так как алгоритм полагает, что ДПФ периодическая.

*Свертка.*

Свертка — основной процесс в цифровой обработке звуков (сигналов). Поэтому важно уметь эффективно ее вычислять. Прямое вычисление свертки требует N*M умножений.

N — длина исходного сигнала,

M — длина ядра свертки.

Часто длина ядра свертки достигает несколько тысяч точек, и число умножений становится огромным.

*Теорема Свертки 1.4. Свертка во временной области эквивалентна умножению частотных областей. Свертка в частотной области эквивалентна умножению во временной области* [2, с. 15].

Это очень важная теорема, которая позволяет нам понять, что возможна свертка двух сигналов, для этого необходимо перевести сигналы в частотную область, умножит спектры сигналов в частотной области, а затем перевести их обратно во временную область.

Часто возникает потребность произвести сверку очень длинного сигнала, не помещающегося в памяти компьютера, тогда применяется так называемая секвенционная свертка.

Суть ее в том, что длинный сигнал разбивается на более короткие части и каждая эта часть сворачивается с ядром отдельно.

*Фильтрация.*

Эффект от умножения спектров сигналов при свертке называется фильтрацией. Когда спектры умножаются друг на друга как комплексные числа, происходит умножение амплитуд гармоник исходного сигнала и ядра свертки (а фазы складываются).

В звукозаписи изменение спектра позволит очищать запись от шумов, компенсировать искажения сигнала, менять тембры инструментов, акцентировать внимание слушателей на отдельных партиях.

Ядро свертки при фильтрации называют фильтром. Часто так называют все устройство, осуществляющее процесс фильтрации. Длина (размер) фильтра — это длина ядра свертки.

***Вейвлеты.***

К настоящему времени известно свыше 4300 вейвлетов, однако, лишь простейшие вейвлеты — Вейвлеты Хаара удовлетворяют нужным условиям (1,5,6,7 требования см. ниже).

Требования к вейвлетам:

1. Вычислительная простота

2. Хорошие качества приближения

3. Вычислительная устойчивость

4. Гладкость

5. Компактность носителя у базисных вейвлетов (или быстрое убывание на бесконечность, при отсутствии такой компактности)

6. Симметричность базисных вейвлетов

7. Ортогональность вейвлетного разложения

Вейвлеты на множестве $Z_N$.

Продолжаем рассматривать дискретные сигналы. Мы рассмотрели способ построения базиса Фурье для анализа сигналов, но следует отметить его недостатки: это не локализованность в пространстве. Это означает, что векторы базиса Фурье распределены настолько «равномерно» насколько это возможно.

Мы говорим, что вектор z $\epsilon\ l^2(Z_N)$ локализован в пространстве около $n_0$, если большинство компонент z(n) вектора z равны нулю или по крайней мере относительно малы всюду, за исключением нескольких значений n, близких к $n_0$.

Элемент $F_m$ базиса Фурье не локализован в пространстве около $n_0$, потому что его компоненты $F_m(n) = \frac{1}{N} e^{2\pi imn/N}$ имеют одинаковую амплитуду. Эта ситуация противоположна локализации.

В более общем случае пространственно локализованный базис полезен потому, что он гарантирует локальный анализ сигнала. Если, допустим, что некоторый коэффициент велик, то мы можем идентифицировать ту локальную область, с которой коэффициент связан.

У нас уже есть один пример локализованного базиса — это евклидов базис или так называемый, стандартный базис. Он локализован наилучшим образом, каждый базисный вектор имеет только одну ненулевую компоненту. Однако очень хотелось бы достигнуть частотной локализации, как в базисе Фурье.

Т. е. линейности и инвариантности. Поэтому базисные векторы должны состоять из очень малых групп частот.

Использование частотно-локализованных базисов позволяет нам также имитировать общую технику фильтрования.

Таким образом, наша конечная цель — это получить базис, элементы которого пространственно и частотно локализованы. Тогда коэффициенты разложения векторов в этом базисе будут давать пространственную и частотную информацию.

Поэтому мы сможем совершить одновременно: частотный и временной анализ такого вектора и вейвлеты дадут нам такой базис!

Когда мы говорим об аудио сигнале, мы имеем ввиду, что вектор — функция зависит от времени. Таким образом, вектор z(t) зависит от t, где t — это время.

Также хотелось бы, чтобы переход от стандартного эвклидова базиса к новому базису B был быстрым, вычислялся с помощью быстрого алгоритма, так как от этого зависит качество решения задачи в реальном размере.

Можем использовать формулу свертки Быстрого Преобразования Фурье для быстрого изменения базиса. Возможно, это поможет.

$$z * w = \widetilde{(\hat{z}\hat{w})}$$

Но существует одно наблюдение, которое нам препятствует: если новый базис ортонормированный, то мы не можем получить частотно-локализованный ортонормированный базис, т. к. его векторы будут с равными амплитудами.

Это наблюдение не настолько обескураживающее, как кажется, т. к. из него следует незначительная модификация исходной идеи и приводит к основополагающим результатам.

Для того, чтобы рассматривать один вектор, множество полных сдвигов, которого образует ортонормированный базис, мы рассмотрим два вектора

со множеством сдвигов по четным периодам. Один из будет называться отцовским. Второй, материнским вейвлетом.

Лемма 1.5.Множество $\{R_n u\}_{k=0}^{M-1}$ортонормировано тогда и только тогда, когда выполняется равенство

$$|\hat{u}(n)|^2 + |\hat{u}(n+M)|^2 = 2 \text{ [1, с. 158]}$$

Определение 1.2. Предположим, что M$\epsilon$N,N=2M, u,v $\epsilon\, l^2(Z_N)$

A(n) — это система матриц из u,v:

$$\frac{1}{\sqrt{2}}\begin{bmatrix} \hat{u}(t) & \hat{v}(t) \\ \hat{u}(t+M) & \hat{v}(t+M) \end{bmatrix}$$

*Теорема 1.4. Предположим, что M$\epsilon$N,N=2M, u,v* $\epsilon\ l^2(Z_N)$*. Тогда,* $B = \{R_{2k}v\}_{k=0}^{M-1} \cup \{R_{2k}u\}_{k=0}^{M-1}$=$\{v, R_1 v, R_2 v, \dots, R_{N-2}v, u, R_1 u, R_2 u, \dots, R_{N-2}u\}$*;*
*Есть ортонормированный базис* $l^2(Z_N)$*тогда и только тогда, когда система матриц A(n) унитарна для каждого n=0,1,2,…M-1.*

*Эквивалентно,*

*B есть вейвлет первого порядка тогда и только тогда, когда*

$$|\hat{u}(n)|^2 + |\hat{u}(n+M)|^2 = 2$$
$$|\hat{v}(n)|^2 + |\hat{v}(n+M)|^2 = 2$$
$$\& \ \hat{u}(n)\overline{\hat{v}(n)} + \hat{u}(n+M)\overline{\hat{v}(n+M)} = 0 \text{ [1, с. 162]}$$

Доказательство.

Матрица унитарна тогда и только тогда, когда ее столбцы образуют ортонормированный базис в $C^2$.

По лемме 1.5 множество $\{R_n u\}_{k=0}^{M-1}$ортонормировано тогда и только тогда, когда выполняется равенство

$$|\hat{u}(n)|^2 + |\hat{u}(n+M)|^2 = 2$$

Это означает, что первый столбец матрицы A(n) имеет длину равную 1 для n=0,1,…M-1; Далее утверждается что, $\langle R_{2k}u, R_{2j}u\rangle$=0 для всех j,k=0,1,…,M-1;

когда выполняется равенство $\hat{u}(n)\overline{\hat{v}(n)} + \hat{u}(n+M)\overline{\hat{v}(n+M)} = 0$.

Это означает, что столбцы матрицы A(n) ортогональны, следовательно, B есть ортонормированный базис $l^2(Z_N)$.

В общем случае показать, что отцовский и материнский базисы являются ортонормированными не очень легко. Однако нетрудно построить их таким образом, чтобы матрицы A(n) были унитарными для всех n=0,1,…M-1;

Мы можем вычислить обратное Дискретно преобразование Фурье и получить пример вейвлет базиса первого этапа.

На $|\hat{u}(n)|^2$ и $|\hat{u}(n+M)|^2$ наложено условие, что их среднее равно 1. Это означает, что одно из слагаемых может быть равно 0. Таким образом, в один из векторов не будет иметь компоненты в направлении $F_N$ ($v = \sum_{n=0}^{N-1} \hat{v}(n)F_n, u = \sum_{n=0}^{N-1} \hat{u}(n)F_n$).

Это позволяет нам выделить низкие и высокие частоты. Поэтому u-это вектор, содержащий низкие частоты (низкочастотный фильтр), а v-это вектор, содержащий высокие частоты (высокочастотный фильтр).

Такое представление ведет к очень неожиданным и разнообразным результатам.

**Выводы**

Таким образом, мы только прикоснулись к возможностям обработки аудио сигнала.

Как мы видим Преобразование Фурье хорошо тем, что требует малых вычислительных ресурсов (речь идет об алгоритме БПФ), но его главным недостатком всегда будет нелокализованность и возникающие трудности для локального анализа сигнала. Таким образом, амплитуды всегда будут равны 1 и не будет возможности скорректировать сигнал более тщательно. Поэтому вейвлеты интересны тем, что могут создать такой базис, который будет частотно-локализован, ортонормирован, периодичен, который позволит

корректировать и приближать сигнал к более качественному, более идентичному аналоговому, живому звуку. Этот раздел математики относительно новый в мире и поэтому полностью не изучен. Но природа самих вейвлетов естественным образом подталкивает и интуитивно дает понять, что у них есть большой прикладной потенциал и поэтому они требуют исследований.

**Список литературы:**


1. Введение в вейвлеты в свете линейной алгебры. М. Фрейзер. Издательство: Бином. Лаборатория знаний. ISBN 978-5-94774-557-3, 0-387-98639-1; 2008 г. / An Introduction to Wavelets Through Linear Algebra ISBN 978-5-94774-557-3, 0-387-98639-1; 2008 г.
2. Введение в цифровую обработку сигналов (математические основы). А. Лукин (2002 г). Издательство: Лаборатория компьютерной графики и мультимедиа, МГУ.
3. Введение в теорию вейвлетов. Ю.К. Демьянович, В.А. Ходаковский. СПб., 2007.

# СОЗДАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ КАК СПОСОБ УПРОЩЕНИЯ ПРОЦЕССА ОФОРМЛЕНИЯ ЗАКАЗ-ПОДРЯДА В СТРОИТЕЛЬНОЙ ОРГАНИЗАЦИИ

***Легошина Виктория Александровна***
*студент 4 курса кафедра математических методов в экономике*
*Набережночелнинский институт КФУ (филиал),*
*РФ, г. Набережные Челны*

***Фрикк Валерий Сергеевич***
*научный руководитель, старший преподаватель*
*Набережночелнинский институт КФУ (филиал),*
*РФ, г. Набережные Челны*

На данный момент процесс оформления заказ-подрядов в строительных фирмах достаточно трудоемкий, и на это затрачивается много времени. Огромные трудозатраты в большинстве случаев являются следствием отсутствия опыта автоматизации во многих компаниях строительной индустрии.

Для упрощения задачи оформления заказ-подрядов необходимо создание соответствующей информационной системы [2, с. 44]. Поскольку большинство фирм на данный момент имеют успешный опыт внедрения различных конфигураций на базе 1с, была выбрана именно эта платформа для автоматизации и совершенствования данной бизнес-задачи.

Задача оформления заказ-подрядов является частью бизнес-процесса «Подготовка оказания услуг» [1, с. 229]. Для быстрого оформления заказ-подряда необходимо затронуть следующие учетные задачи:

1. Учет заявок на проектные работы
2. Учет расчетов с контрагентами [5, с. 7].

Проектирование информационной системы состоит из трех основных этапов:

1. Проектирование информационной системы
2. Разработка информационной системы
3. Внедрение информационной системы

Также имеется процесс сопровождения информационной системы, который включает регулярные обновления и техническое сопровождение.

На сегодняшний день для моделирования и прогнозирования аналитических, технических и др. работ, имеется ряд программных продуктов и один из них это Microsoft Project.

Microsoft Project создан, чтобы помочь менеджеру проекта в разработке планов, распределении ресурсов по задачам, отслеживании прогресса и анализе объёмов работ. Microsoft Project создаёт расписания критического пути. Расписания могут быть составлены с учётом используемых ресурсов. Цепочка визуализируется в диаграмме Ганта [4].

Рассмотрим проектирование создания информационной системы на примере «Информационная система «Учет заявок на работы» для фирмы ООО «Юнипроф-16»»

Первый этап это проектирование информационной системы. Он включает следующие этапы:

1. Сбор информации о компании ООО «Юнипроф-16»

2. Анализ собранных данных о компании ООО «Юнипроф-16»

2.1.Анализ экономических отчетов компании ООО «Юнипроф-16» за прошедшие отчетные периоды

2.1 Анализ технических показателей компании ООО «Юнипроф-16» за прошедшие отчетные периоды

3. Анализ бизнес-процессов и бизнес-задач предприятия (реинжиниринг) предприятия ООО «Юнипроф-16»

3.1 Анализ имеющейся компьютерной сети ООО «Юнипроф-16»

3.2 Анализ имеющегося программного обеспечения на организации ООО «Юнипроф-16»

3.3 Анализ степени автоматизации бизнес процессов и компании ООО «Юнипроф-16»

3.4 Разработка таблицы потоков создания бизнес продуктов

3.5 Выявление информационных массивов

4. Обоснование среды разработки бизнес-задачи 1с.

5. Проектирование макета разрабатываемой информационной системы «Учет заявок на работы» (проработка атрибутов, сущностей, связей базы данных)

5.1 Проектирование атрибутов сущности документа «Заказ на подряд»

5.2 Проектирование атрибутов сущности документа «Оплата заказа»

5.3 Проектирование атрибутов сущности документа «Выполнение подряда»

5.4 Проектирование атрибутов отчета «Расчеты с контрагентами»

5.5 Проектирование атрибутов отчета «Заказы на подряд»

5.6 Задание ключевых полей сущностей.

Второй этап это разработка информационной системы, включает следующие этапы:

1.1 Создание формы справочника «Контрагенты»

1.2 Создание формы справочника «Номенклатура»

1.3 Создание формы документа «Заказ на подряд»

1.4 Создание формы документа «Оплата заказа»

1.5 Создание формы документа «Выполнение подряда»

1.6 Создание отчета «Расчеты с контрагентами»

1.7 Создание отчета «Заказы на подряд»

2 Создание диаграммы UML

3 Тестирование и выявление недочетов конфигурации информационной системы «Учет заявок на работы».

3.1 Проверка правильности связей

3.2 Проверка удобства форм документов

3.3 Тестирование верности отчетов

4 Исправление недоработок конфигурации информационной системы «Учет заявок на работы». (В случае их наличия)

5 Создание удобного пользовательского интерфейса информационной системы «Учет заявок на работы».

5.1 Объединение форм документов в одну категорию «Документы»

5.2 Объединение отчетов в одну категорию «Отчеты»

5.3 Объединение справочников в одну категорию «Справочники»

5.4 Создание отдельного столбца с возможностью прямого создания нового документа

Внедрение информационной системы:

1. Предварительное тестирование информационной системы «Учет заявок на работы» ООО «Юнипроф-16»

2 Обучение персонала компании ООО «Юнипроф-16»

3 Создание учетных записей пользователей информационной системы «Учет заявок на работы»

3.1 Создание учетной записи Менеджер информационной системы «Учет заявок на работы»

3.2 Создание учетной записи Директор информационной системы «Учет заявок на работы»

3.3 Создание учетной записи Системный Администратор информационной системы «Учет заявок на работы»

3.4 Создание учетной записи Бухгалтер информационной системы «Учет заявок на работы»

4 Обозначение прав доступа пользователей к информационной системе «Учет заявок на работы»

4.1 Обозначение прав доступа учетной записи Оператор информационной системы «Учет заявок на работы»

4.2 Обозначение прав доступа учетной записи Директор информационной системы «Учет заявок на работы»

4.3 Обозначение прав доступа учетной записи Системный Администратор информационной системы «Учет заявок на работы»

4.4 Обозначение прав доступа учетной записи Бухгалтер информационной системы «Учет заявок на работы»

5 Загрузка конфигурации информационной системы «Учет заявок на работы» на компьютеры сети ООО «Юнипроф-16»

По окончанию работ по проектированию информационной системы получаем программный продукт выходом которого будут являться два отчета:

1. Учет заявок на работы
2. Учет расчетов с контрагентами

Эти отчеты потребуются при анализе загруженности трудовых мощностей, а так же задолженности заказчика, если таковая имеется. Данные действия выполняются перед оформлением заказ-подряда для избегания накладок заказа на заказ, и оказания услуг должникам фирмы.

По окончанию моделирования проектирования информационной системы мы получаем готовый проект с диаграммой Ганта. Программный продукт Microsoft Project дает возможность визуализировать диаграмму Ганта с отслеживанием критических путей и без отслеживания. В первом случае удастся сразу увидеть критический путь и критические задачи, которые не имеют временного запаса. Скорее всего при реализации проектирования на них нужно будет обратить особое внимание.

После окончания работ по планированию, получаем готовый проект, который отображает стоимость разработки программного продукта, трудозатраты, а так же можем оценить нагрузку на трудовые и материальные ресурсы.

По плану, составленному в Microsoft Project, выполняется проектирование информационной системы. Результатом становиться документ «Заказ на подряд», функционал полей которого позволяет автоматически выполнять анализ загруженности трудовых мощностей и задолженности контрагентов. Т.е если выбранная бригада на данный промежуток времени уже обозначена в одном из подрядов, если некорректно указан временной промежуток для выполнения подряда, то документ провести не удастся. Так же если имеется задолженность контрагента, то данная информация отобразиться при оформлении документа [3].

Форма документа выглядит следующим образом:

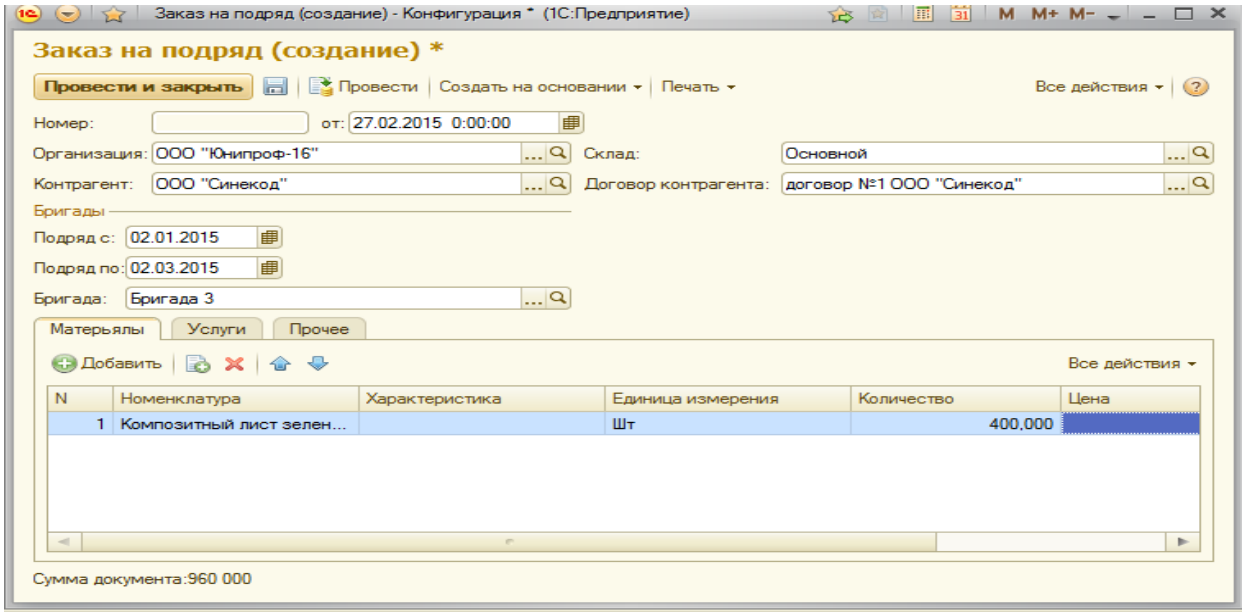



***Рисунок 1. Документ «Заказ на подряд»***

А так же позволяет выполнять учетные задачи за счет возможности вывода отчетов по необходимым промежуткам времени.

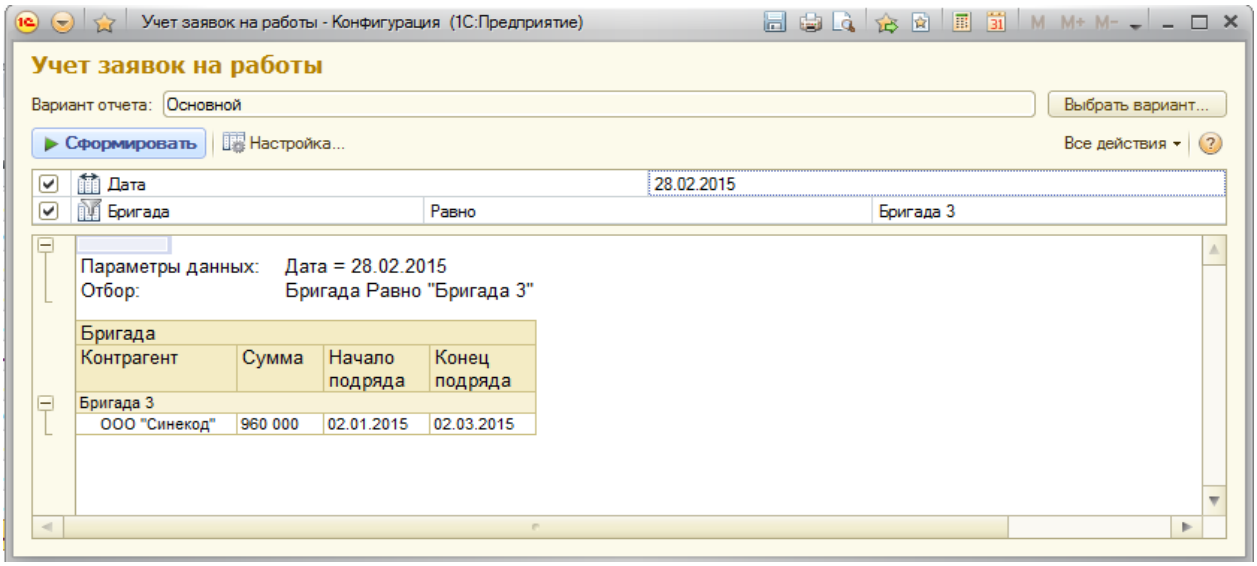



***Рисунок 2. Отчет «Учет заявок на работы»***

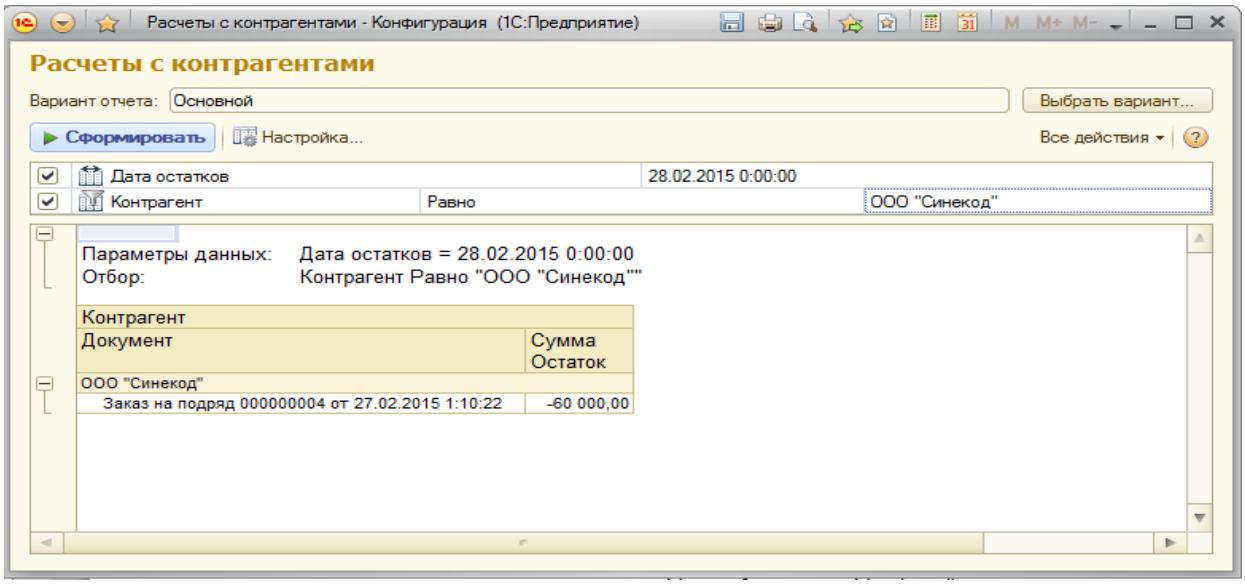



***Рисунок 3. Отчет «Расчеты с контрагентами»***

В результате внедрения конфигурации 1С разработанной для целей автоматизации бизнес-задачи «Оформление заказ подряда» количество, затрачиваемое на оформление договоров, сократилось на 10 трудочасов в неделю.

**Список литературы:**


1. Абдакиев Н.М. Реинжиниринг бизнес-процессов / Н.М. Абдакиев. М.: Эксмо, 2009. — 229 с.
2. Ойхман Е.Г. Реинжиниринг бизнеса: Реинжиниринг организации и информационные технологии / Е.Г. Ойхман, Э.В. Попов М.: Финансы и статистика, 1997. — 44 с.
3. Официальный сайт 1С [Электронный ресурс] — Режим доступа. — URL: http://v8.1c.ru/. (Дата обращения: 15.04.2015).
4. Официальный сайт Microsoft [Электронный ресурс] — Режим доступа. — URL: http://www.microsoft.com > ru-ru. (Дата обращения: 13.04.2015).
5. Устав ООО «Юнипроф-16» от 2011 г. — 7 с.

# АНАЛИЗ МЕТОДОВ ОЦЕНКИ ВЕРОЯТНОСТИ РИСКА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

***Любичев Андрей Максивович***
*студент, кафедра «Информационная безопасность», НИУ «МИЭТ», РФ, г. Москва, г. Зеленоград*
*E-mail: andreymelaman@gmail.com*

***Малёжин*** Олег Борисович
*научный руководитель, канд. техн. наук, доцент, кафедра «Информационная безопасность», НИУ «МИЭТ», РФ, г. Москва, г. Зеленоград*

В современном мире в сфере информационной безопасности очень велико многообразие определений слова «риск». Но практически во всех дефинициях слова «риск» ключевыми являются слова «вероятность» и «последствия» (или «ущерб»). Например, ГОСТ Р 51901.1-2002 «Менеджмент риска. Анализ риска технологических систем» даёт определение риска как «сочетание вероятности события и его последствий» [2]. Ещё один пример — в стандарте ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» приводится вот такая дефиниция — «риск (risk): потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей актива или группы активов» [3]. Таким образом, хоть все трактовки и отличаются между собой, но, при этом, имеют практически одинаковый смысл. Если попробовать обобщить и объединить все существующие определения, то получается, что «риск — это сочетание вероятности осуществления определённого события и негативных последствий (то есть нанесение потенциального или реального ущерба активу или группе активов), связанных с этим событием».

Если разложить риск на компоненты, то основными его составляющими будут являться тяжесть возможного ущерба (последствия) и вероятность нанесения ущерба (которая состоит из частоты и продолжительности воздействия угрозы, вероятности возникновения угрозы и возможности

избегания угрозы или ограничения ущерба от неё). Стоит отметить, что эффективность управления рисками напрямую зависит от того, насколько правильно и корректно будут оценены эти элементы.

Необходимо правильно оценивать вероятность того или иного риска, чтобы грамотно и эффективно управлять рисками. Существует несколько подходов измерения вероятности риска. Первый из них — это собственная статистика того, кто оценивает вероятность риска. Это один из самых эффективных методов, где главным условием является постоянность (неизменность) среды оценки. Статистическая (историческая) оценка позволяет прогнозировать будущее на основании информации, полученной за прошлые (прошедшие) периоды времени. Для успешной реализации данного метода требуется мониторинг и сбор данных на протяжении определённого периода времени (срок каждый раз варьируется в зависимости от конкретной ситуации). Стоит отметить, что при отсутствии адекватных инструментальных средств данный процесс является довольно ресурсоёмким — необходим сбор, нормализация, хранение и анализ данных.

Ко второму способу измерения вероятности риска можно отнести анализ отчётов и использование статистики сторонних организаций (которые специализируются в данной сфере). Например, при таком подходе можно анализировать и извлекать полезную информацию из отчётов таких организаций как Computer Security Institute (CSI), Federal Bureau of Investigation (FBI), KPMG, PricewaterhouseCoopers (PwC), Ernst & Young (EY), МВД, Perimetrix, Infowatch и других. Но при использовании данного метода стоит отметить, что не всегда можно полагаться на такую статистику. Во многих случаях специалисты, использующие такой подход для измерения вероятности риска, не знают всех условий, при которых была реализована та или иная угроза информационной безопасности, представленная в отчёте, или то каким образом произошёл определённый инцидент, приведённый в статистике. Также обычно неизвестны все детали и методы сбора, нормализации, анализа и обработки данных, которые применяет организация в своих исследованиях.

Собираемая статистика во многом зависит от применяемых способов опроса, аудитории, желания респондентов сообщать точные данные, а также от масштаба опроса. Не стоит забывать, что следует делать поправку на тип организации для которой применяется данная статистика — это тоже немаловажный аспект при измерении вероятности риска.

К третьему способу относят самостоятельный подсчёт вероятности риска. Схематично данный метод представлен ниже (рис. 1).

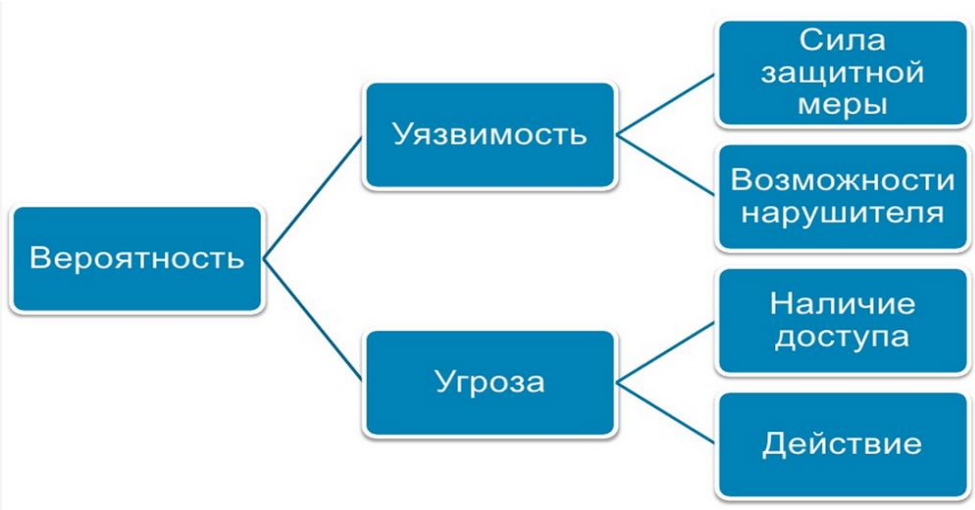



***Рисунок 1. Самостоятельный подсчёт вероятности риска***

Здесь следует отметить, что для подсчёта вероятности риска следует произвести оценку вероятности эксплуатации той или иной уязвимости (вероятность определяется силой защитной меры, направленной на защиту того или иного актива, и возможностями, которыми обладает нарушитель), а также подсчёт вероятности реализации какой-либо угрозы (которая зависит от наличия или отсутствия доступа у атакующего, а также от действий, которые нарушитель предпринимает).

К четвёртому способу относят сравнение (сопоставление) риска с другими аналогичными рисками. При сравнении рисков следует учитывать несколько факторов. Такой метод возможен только на аналогичных решениях по информационной безопасности и когда:

- установлены аналогичные средства безопасности;
- назначение систем и технологии у двух сторон сравнимы;

- угрозы и компоненты риска могут быть сопоставимы;
- технические условия сравнимы;
- условия использования сравнимы.

Также при таком подходе необходимо иметь в виду вспомогательные условия (например, потенциал нарушителя и вид защищаемой информации) [4].

Пятый способ представляет собой прогнозирование, которое можно осуществлять с помощью аналитических методов, таких как:

- «Дерево неисправностей» (Fault Tree Analysis) — диаграмма всех возможных последствий инцидента в системе;
- «Дерево событий» (Event Tree Analysis) — диаграмма всех возможных последствий данного события;
- имитационное моделирование отказов или инцидентов.

Данный подход в сфере информационной безопасности не используется или практически не используется (применяется только в критических областях).

Шестой способ — подсчёт бинарной вероятности риска. В данном случае вероятность считается равной 1 в том случае, если угроза реализуема, и 0 — если нет (при отсутствии средств защиты). Данный подход можно рассматривать при оценке вероятности только для узкого круга систем (так как он весьма ресурсоёмкий) или для очень распространённых угроз. Этот метод используется в методиках ФСТЭК и ФСБ.

Для определения риска информационной безопасности различные методы могут использовать количественные или качественные шкалы. В первом варианте все компоненты риска и сам риск измеряются в числовых значениях. При применении количественных шкал вероятность атаки может измеряться числом в интервале, ущерб — в виде денежного эквивалента материальных потерь, которые возникают у организации, если атака успешно реализована. При использовании качественных шкал числовые значения меняются на эквивалентные им понятийные уровни. В этом случае каждому понятийному уровню будет соответствовать определённый интервал количественной шкалы

оценки. Число уровней может быть различным в зависимости от используемых методик оценки вероятности риска [1].

При этом стоит отметить, что количественная оценка не всегда применима из-за:

- ехватки данных о системе;
- ехватки данных о деятельности, которая подвергается оценке;
- тсутствия или недостатка информации об инциденте (инцидентах);
- ависимости от человеческого фактора;
- ого, что зачастую такие измерения риска требуют значительных затрат ресурсов.

Также стоит уточнить, что для качественной оценки необходимо:

- чёткое объяснение всех терминов, которые используются (должна быть определена дефиниционная база);
- обоснование всех классификаций частот и последствий;
- понимание всех преимуществ и недостатков качественной (или экспертной) оценки и психологии восприятия риска.

Последний рассматриваемый (и наиболее распространённый) способ измерения вероятности риска в данной статье — это экспертная оценка. Частично она была описана выше. Стоит отметить, что при отсутствии статистических (исторических) данных экспертная оценка является единственным методом определения частоты (вероятности) реализации угрозы (или угроз). При данном подходе эксперты ранжируют вероятность возникновения того или иного события, опираясь на свой опыт и знание анализируемой системы. К достоинствам такого метода стоит отнести простоту его реализации, а к недостаткам (ограничениям) — возможность воздействия заинтересованных лиц на экспертное мнение, невозможность применения общих моделей для оценки всех рисков (всегда существуют случайные события, которые невозможно предугадать с помощью экспертной оценки), необходимость наличия достаточного количества экспертов, а также

соответствующей квалификации каждого эксперта, психология восприятия риска [5].

Все способы и методы, рассмотренные в этой статье, применимы для различных частных случаев подсчёта вероятности риска. Специалист, занимающийся построением системы управления рисками информационной безопасности, должен чётко осознавать, когда следует использовать тот или иной способ. При этом стоит отметить, что построение системы управления рисками информационной безопасностью — это более сложная задача, чем выбор способа подсчёта вероятности риска и требует хорошей теоретической подготовки, а также опыта проектирования и внедрения таких систем.

**Список литературы**:


1. Аудит информационной безопасности — основа эффективной защиты предприятия [Электронный ресурс]. — Режим доступа. — URL: http://www.dialognauka.ru/press-center/article/4753/
2. ГОСТ Р 51901.1-2002 Менеджмент риска. Анализ риска технологических систем [Электронный ресурс]. — Режим доступа. — URL: http://vsegost.com/Catalog/62/6283.shtml
3. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий [Электронный ресурс]. — Режим доступа. — URL: http://vsegost.com/Catalog/27/271.shtml
4. ГОСТ Р 51901.13-2005 (МЭК 61025:1990) Менеджмент риска. Анализ дерева неисправностей [Электронный ресурс]. — Режим доступа. — URL: http://docs.pravo.ru/document/view/20841595/19930857/
5. Как считать риски? Личный блог Лукацкого А.В. [Электронный ресурс]. — Режим доступа. — URL: http://lukatsky.blogspot.ru/2012/04/blog-post_18.html

# ГЕНЕРАТОРЫ СЛУЧАЙНЫХ ЧИСЕЛ

***Малышев Максим Вадимович***
*студент 3 курса, кафедра АТ ПНИПУ,*
*РФ, г. Пермь*
*E-mail: ckdeliverance@gmail.ru*

Как известно, ключ — одна из важнейших частей криптографии, ни один процесс шифрования или дешифрования не обходится без ключа. Некоторые ключи присылаются от доверенного источника, например, сервера криптографических ключей, большинство — создаются с помощью генератора случайных чисел. При этом генерация качественной случайной последовательности является неотъемлемой и самой важной частью многих криптографических операций. Для создания криптостойкого ключа с помощью генератора необходимо учитывать множество факторов, таких как длина ключа, его энтропия, использование истинно случайных и псевдослучайных чисел, а также предусматривать возможные атаки на генератор. Эти моменты делают вопрос исследования и создания безопасного генератора случайных чисел довольно важной темой в области криптографии.

Мера случайности называется энтропией — мерой неопределённости источника сообщения, определяемой вероятностями появления тех или иных символов при их передаче. В наборе символов из n битов энтропия m — число битов, в значении которых нельзя быть уверенным. Это значит, что чем больше энтропия в генерируемой последовательности, тем эта последовательность устойчивей к взлому. Полностью случайная последовательность называется истинно случайным числом и определить её злоумышленник может только перебором.

Энтропия числа происходит от источников неопределенности, которые находит генератор. Подобными источниками могут быть интервал между нажатием клавиш, перемещение мыши, текущие время и дата и физические процессы, ведущие себя случайным образом: шумы токов и звуковой карты, отклики жестких дисков, подсчёт тактов процессора. Проблема истинно

случайных чисел в том, что целеустремленный злоумышленник может определить так или иначе большинство этих процессов и они перестанут быть случайными. Также может отказать или уменьшить свою неопределенность один из источников случайно истинных данных, например, пользователь перестанет двигать мышкой. Данные сложности вызывают ограничения для применения истинно случайных чисел и вместо них в большей мере используются псевдослучайные числа.

Псевдослучайные числа не являются случайными, они вычисляются с помощью детерминированного алгоритма на основе некоторого начального числа. Большинство подобных генераторов используются в статистических целях и не являются криптостойкими, потому что злоумышленник, зная алгоритм генерации, может по нескольким сгенерированным числам предугадать некоторые биты других случайных значений. Криптографически сильный генератор использует в качестве начального числа истинно случайное число и на его основе создает псевдослучайные, а также может изменять начальное число с сохранением энтропии, что гарантирует непредсказуемость выходных данных, даже если злоумышленник знает начальное число.

Взломать подобный генератор можно с трех направлений. Отслеживание выходных данных и исследование их закономерности называется прямой криптоаналитической атакой. Этот вид атаки распространяется на большинство алгоритмов, использующих генерацию, но если выходы генератора не видны, как в 3DES, то он неуязвим к подобным атакам.

Атака, основанная на входных данных возможна, когда злоумышленник может использовать знания о входных сигналах ГПСЧ или контролировать их. В зависимости от доступной информации меняется тип атак — они могут строиться на угадывании данных по типу или принципу формирования, либо пытаться ввести систему в такое частное состояние, в котором точно известны генерируемые значения. Особенно стоит обозначить атаку на избранные входные данные, которая опасна при использовании в системе сигналов

от смарт-карт, токенов, а также легкодоступных данных вроде сетевых параметров, вводимой пользователем информации, времени и даты.

При проведении атак, основанных на вскрытии внутреннего состояния, злоумышленник пытается использовать ранее успешные атаки на генератор случайных последовательностей, вскрывшие его внутреннее состояние, с целью предсказания состояния дальнейших или предыдущих состояний. Такого рода атаки могут быть успешны в том случае, когда генератор начинает свою работу с известного или предсказуемого состояния. На практике очень сложно определить тот факт, что внутреннее состояние было скомпрометировано, поэтому противодействие этим атакам имеет особый приоритет. В таких атаках используется состояние генератора S в момент времени $t_0$, в зависимости от собранных данных и уязвимости генератора злоумышленник может восстановить предыдущие состояния, угадать с помощью промежуточных выходов будущее состояние или вычислить данные из середины временного отрезка с помощью крайних значений. Худшим исходом является полное компроментирование генератора, когда однажды раскрытое S создает угрозу нахождения всех прошлых и будущих состояний генератора.

Исходя из вышесказанного, идеальный генератор случайных чисел должен обладать несколькими признаками.

Во-первых, он должен быть специализированным продуктом для криптографических преобразований, а не стандартным инструментом из набора программной библиотеки или операционной системы. Впрочем, в настоящее время в крупных операционных системах есть готовые варианты криптостойких ГПСЧ, способные обеспечить хороший уровень безопасности.

Во-вторых, нужно оптимально использовать источники энтропии, отдавая предпочтение надежным элементам с высоким показателем неопределенности — различным шумам, случайным колебаниям в дисковых накопителях, времени и величинам внешних событий. Источники с низким качеством случайных данных могут навредить системе большинства генераторов, и поэтому от их использования стоит воздерживаться.

В-третьих, необходимо удовлетворять «тесту на следующий бит». Смысл теста в следующем: не должно существовать полиномиального алгоритма, способного при знании первых $k$ битов случайной последовательности предсказать ($k$+1)-ый бит с вероятностью более 50 %.

В-четвертых, стоит использовать хэш-функции, чтобы скрыть реальные выходные значения генератора, как и стоит хэшировать входные данные с постоянно меняющимся значением, чтобы защитить систему от основанных на них атак.

В-пятых, внутреннее состояние генератора должно периодически полностью меняться. Это поможет защититься от атак, основанных на вскрытии внутреннего состояния, или, по крайней мере, уменьшит урон, нанесённый успешной атакой.

Примеры успешных генераторов:

- ГПСЧ стандарта ANSI X9.17 — используется в PGP, работает на тройном DES, энтропия - текущие дата и время;
- Fortuna Брюса Шнайера — гибкая настройка источников энтропии;
- Функция CryptGenRandom в Microsoft CryptoAPI — встроена в Windows, является стандартным генератором подобного рода для среды разработки под Win32:
- Специальный файл ОС UNIX /dev/random, в частности, /dev/urandom. Есть во всех Unix, надёжный источник энтропии.

Генераторы случайных последовательностей — очень важный элемент шифрования, достаточно уязвимый и критичный. Случайность собираемых данных делает малопредсказуемыми планирование и моделирование состояний подобного генератора, затрудняет предсказание и обнаружение атак на него. Поэтому криптостойкий генератор требует тщательного выбора источников энтропии, алгоритмов хеширования и шифрования входов и выходов. Особым уязвимым местом генератора является его внутреннее состояние, успешная атака на воссоздание которого может обрушить всю схему криптографического преобразования данных.

При этом криптостойкий генератор практически невозможно взломать и он, работая с неплохой скоростью, обеспечивает вашу криптографическую систему надежными и стойкими ключами. На сегодняшний день генерация чисел используется в любом стандарте шифрования и может быть как самым слабым его звеном, так и самым сильным.

**Список литературы:**


1. Атака на ГПСЧ // Википедия — свободная энциклопедия. [Электронный ресурс] — Режим доступа. — URL: https://ru.wikipedia.org/wiki/Атака_на_ГПСЧ (дата обращения: 12.05.2015).
2. Фергюсон Н., Шнайер Б. [Ferguson N., Schneier B.] Практическая криптография: пер. с англ. М.: Вильямс, 2005.

# РЕАЛИЗАЦИЯ ПРОТОКОЛОВ ТАЙНОГО ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ

***Мешкова Елена Владимировна***
*студент 3 курса, кафедра автоматики и телемеханики ПНИПУ,*
*РФ, г. Пермь*
*E-mail: lenchik447@yandex.ru*

***Митрошина Екатерина Валерьевна***
*студент 3 курса, кафедра автоматики и телемеханики ПНИПУ,*
*РФ, г. Пермь*
*E-mail: mitroshina.katya@inbox.ru*

***Кротова Елена Львовна***
*научный руководитель, канд. физ.-мат. наук, доцент ПНИПУ,*
*РФ, г. Пермь*

Несомненно, голосование является неотъемлемым атрибутом современного мира. Мы постоянно встречаемся с выборами, которые играют важную роль в нашей жизни. Нам предоставляется возможность сделать выбор, начиная от голосования на каком-нибудь сайте с фильмами или за любимый трек на радио и заканчивая довольно-таки серьезным делом, выбором президента или выбором депутатов в государственную думу.

Совсем не так давно, выборы президента или депутатов проводились для народа привычным способом. Посредством заполнения бумажного бюллетеня на избирательном участке человек делал выбор, голосуя за того или иного претендента. Следует отметить, что с голосованием на сайте, которое является одной из разновидностей электронного голосования, встречались не многие.

В настоящее время, в связи с интенсивным развитием сетевых технологий, стало возможным задуматься о реализации подобных выборов в глобальном масштабе. Но голосование в Internet за любимый фильм и за президента — это совершенно разные вещи. Требования к безопасности и защите информации при выборе президента значительно больше, чем при выборе фильма. Как с точки зрения защиты информации, так и в физическом плане, реализация подобного проекта является делом чрезвычайно сложным и дорогим, поскольку далеко не все люди имеют возможность голосовать через Internet. Вследствие

этого возникает вопрос: повысит ли явку избирателей голосование через Internet? Иначе выборы с помощью электронного голосования окажутся бессмысленными.

В ходе реализации выборов через Internet необходимо решить ряд не менее важных технологические проблем и проблем безопасности информации. Для этого важно разработать надежные системы защиты от атак хакеров. Также должны быть изобретены способы, обеспечивающие в полном объеме секретность, которая поддается проверке. При этом нельзя исключить из внимания то, что избиратель должен полностью доверять системе.

Помимо этого существует проблема при подведении итогов выборов. Необходимо, чтобы система голосования имела высокую точность при сборе и подсчете голосов.

В конце концов, нужно решить проблему идентификации и проверки избирателя. Избиратель должен голосовать один раз, поэтому важно разработать системы, которые могли бы гарантировать то, что именно тот избиратель голосует, и что он делает выбор единожды.

Реализацию безопасного электронного голосования выполняют протоколы обмена данными, такие как: простой протокол тайного цифрового голосования, протокол двух агенств, протокол Фудзиока-Окамото-Охта, протокол Не-Su, протокол на основе ANDOS и другие протоколы, которые не так широко известны. Рассмотрим теперь некоторые из них.

**Простой протокол тайного цифрового голосования**

Данный протокол имеет совсем не сложный алгоритм электронного голосования, который представляет собой переписку с электронными подписями между избирательным советом и множеством избирателей. Данные, сообщающие о выборе избирателя, содержатся в цифровой бюллетене, которая также содержит в себе число и имя кандидата.

В данном алгоритме необходимо, чтобы избиратель послал на рассмотрение агентству, проводящему электронное голосование, цифровую бюллетень с приложенным номером идентификации избирателя. Номер идентификации

выдается избирателю при регистрации, которая проводится на кануне выборов. Агентство, в свою очередь, проверяет избирателя в списке зарегистрированных избирателей с помощью номера идентификации. Дальнейшим действием агентства является снятие номера идентификации и послание цифровой бюллетени электронному счетчику, который производит запись результата голосования и добавляет его к общему числу.

Несмотря на простоту алгоритма электронного голосования, данного протокола достаточно для защиты от внешнего вмешательства, подделки голосов и дискредитации законных избирателей. При всем удобстве алгоритма, существует несколько недостатков. Голосующим приходится полностью доверять агентству, так как его работа никем не контролируется и тем самым, может нарушить секретность избирателей. Также нет возможности убедиться, что агентство не изменяет цифровую бюллетень перед отправкой электронному счетчику.

Следует сделать вывод, что простой протокол тайного цифрового голосования может применяться только в тех сообществах, где все находятся на полном доверии друг друга.

**Протоколы слепой подписи**

В 1982 году Дэвид Чаум, представивший концепцию слепых подписей, предложил то, что эти подписи могли бы использоваться в ходе секретных выборов. Слепые подписи — это класс цифровых подписей, которые позволяют документу быть подписанными без того, чтобы показать его содержание.

Затем, в 1992 году. была разработана схема Фудзиока-Окамото-Охта, названная в честь своих разработчиков. Данная схема базируется на крипто-графической подписи вслепую и протоколе двух агентств. Главной идеей протокола двух агентств является замена одного избирательного агентства двумя для полного контроля друг друга. Схема Фудзиока-Окамото-Охта частично решает проблему сговора двух агентств, при этом сам алгоритм протокола усложняется несильно. Для работы протокола необходим заранее выбранный способ маскирующего шифрования, то есть такой способ

шифрования, который позволяет убедиться в том, что документ подлинный и подписанный авторизованным пользователем.

В протоколе Фуджиока-Окамото-Охта избиратель делает свой выбор и отражает его в избирательном бюллетене, далее производит шифрование с помощью секретного ключа, после чего маскирует бюллетень. Следующим шагом избирателя является отправка бюллетеня, с собственной подписью, некому электронному прибору. Электронный прибор проверяет действительно ли избирательный бюллетень подписан зарегистрированным пользователем, который еще не сделал свой выбор. Если на данном бюллетене подпись является подписью зарегистрированного пользователя, то электронный прибор подписывает избирательный бюллетень и отсылает его обратно избирателю. При получении бюллетеня обратно, избиратель убирает маскировку, тем самым раскрывает зашифрованный избирательный бюллетень. Далее избиратель отправляет зашифрованный бюллетень счетчику, который, в свою очередь, проверяет подпись на бюллетене с подписью электронного прибора. При совпадении подписей, счетчик помещает бюллетень в перечень, издание которого произойдет только после окончания голосования. Как только перечень бюллетеней издан, избиратель проверяет, что его бюллетень находится в списке и отправляет счетчику свой секретный ключ для дешифрования. Счетчик раскрывает бюллетень с помощью ключа, высланного избирателем, и добавляет результат голосования к общему числу голосов. После всех выборов счётчик издает ключ дешифрования наравне с зашифрованным избирательным бюллетенем для того, чтобы избиратель мог независимо проверить выбор.

К недостаткам данного протокола относится возможность не принимать бюллетени агентством, которое проводит электронное голосование. Но при этом агентство может игнорировать сообщения лишь в случайном порядке, не зная от кого именно он не принял бюллетень. Поэтому учитывать сообщения от конкретных нежелательных избирателей невозможно, что можно отнести к достоинству данного протокола. Остается нерешенной проблема отдачи голосов за избирателей, которые не явились на выборы. Кроме того, если

произойдет техническая ошибка, то для переголосования потребуется дополнительный модуль. На данный момент протокол Фудзиока-Окамото-Охта (а также его модификации) является одним из самых проверенных протоколов дистанционного электронного голосования.

В заключении хочется сказать, что ни один из протоколов, описанных здесь, не удовлетворяет аспекту верифицируемости полностью потому, что ни один из них не имеет возможности быть проверенным какой-либо стороной, заинтересованной в этом. Агентства, который проводят электронные голосования и в последующем позволяют избирателям проверять, что их личные голоса были подсчитаны верно, удовлетворяют аспекту в значительной степени. Но, система проверки, которая надеется на избирателей, берущих на себя какие-то действия после выборов, навряд ли имеет возможность существовать полностью реализованной. Важно, что безопасность должна быть принята во внимание при конструировании электронных систем голосования.

К обычным способам защиты безопасности, которые обязаны быть, добавляются и другие, связанные с тем, что система электронного голосования обладает уникальными чертами, проявляющимися в результате поддержки секретности избирателя. Однако ни один из протоколов тайного электронного голосования, которые представлены в данной работе, не удовлетворяет всем желаемым свойствам полностью.

Совсем не скоро электронные выборы в правительственные органы будут реализованы, но уже многие организации, занимающиеся общественной деятельностью, начали осуществлять выборы, используя электронику.

**Список литературы:**


1. Лифшиц Ю.А. Электронные выборы — 2005. — [Электронный ресурс] — Режим доступа. — URL: http://yury.name/crypto/03cryptonote.pdf (дата обращения 15.05.2015).
2. Шнайер Б. Прикладная криптография. 2-е изд. М: Триумф, 2002. — 610 с.
3. Ященко В.В. Введение в криптографию. 3-е изд., доп. М.: МЦНМО: «ЧеРо», 2000. — 288 с.

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ПОИСКА ГРАНИЦ

***Овцынова Виктория Валерьевна***
*магистрант группы 13ИВТ-1мг,*
*ФБГОУ ВПО «Брянский государственный технический университет»,*
*РФ, г. Брянск*
*E-mail: vovcynova@gmail.com*

***Буйвал Александр Константинович***
*научный руководитель, канд. техн. наук, доц.,*
*ФБГОУ ВПО «Брянский государственный технический университет»,*
*РФ, г. Брянск*

С развитием науки и техники все больше технических устройств ввода графической информации (фото- и видеокамеры) используют автоматическое наведение и распознавание различных объектов, в первую очередь лиц людей. Но немаловажным является и определение местоположения различных статических объектов, связанное с определением границ этих объектов. Для решения задачи определения границ объектов существует множество различных алгоритмов, применимость которых напрямую зависит от конкретной прикладной задачи.

Определение объектов и их границ широко используется в робототехнике для навигации роботов. При этом используется информация не только с камеры, но и с других датчиков.

Существует достаточно много определений понятия контур изображения. В общем случае, под контуром понимают внешнее очертание объекта на изображении, вдоль которого происходит резкое изменение яркости. При обнаружении контура объекта необходимо руководствоваться основными свойствами, присущими любому контуру: кривизна и компонент. Первое частично определяется процессом формирования изображения и может варьироваться. Наличие второго — компонент — неизбежно, так как большинство объектов в природе не имеют идеально прямые края, в следствие чего возникает проблема «разбиения» контура на составляющие компоненты. Сам компонент представляет собой некоторую часть контура, чьи точки полностью соединены друг с другом отдельными сегментами общего контура.

Каждый компонент, в свою очередь, характеризуется замкнутостью, которая определяет является ли последняя точка компонента его первой точкой. Наиболее сложными в обнаружении являются контуры, состоящие из множества компонент открытого типа.

Немаловажную роль при определение контура объекта играет цвет самого объекта, а так же цвета окружающей среды. В случае, если перепады яркости и цвета будут незначительными, обнаружение границ объекта на изображении будет затруднено. Так же свою лепту вносят помехи на самом изображении, которые так же затрудняют процесс обнаружения краев объекта на изображении. Поэтому перед непосредственным поиском границ объектов необходимо провести некоторые подготовительные действия по улучшению качества изображения.

На данный момент разработано множество методов улучшения изображений. При рассмотрении этого процесса в контексте его использования в сфере робототехники, стоит отметить применимость специализированных программных библиотек реализующих алгоритмы улучшения изображений. Эти библиотеки, как и методы которые они реализуют, описаны в различных источниках. Наиболее эффективным методом является метод улучшения гистограммы изображения с помощью эквализации (автоматический метод поиска функции преобразования, которая сформирует изображение с равномерной гистограммой) [1]. Сама гистограмма рассматривается как функция яркости пикселей изображения.

Обнаружение границ объектов в робототехнике начинается с построения модели, на которую накладывается изображение полученное с камер. После чего происходит рендеринг модели для построения списка видимых линий с помощью их координат. Поиск края наложенного изображения происходит с помощью выделения нормалей от линий модели, при этом необходимо сузить угол поиска примерно до 45о.

Обнаружение самих краев объекта можно произвести по одному из ниже представленных алгоритмов.

Операторы Собеля и Лапласа

Оператор Собеля используется для вычисления приближения градиента яркости изображения. Он вычисляет градиент яркости изображения в каждой точке. Таким образом можно получить направление наибольшего изменения яркости и величину ее изменения по этому направлению, а следовательно определить как меняется яркость изображения в каждом пиксиле, вероятность нахождения точки на границе объекта и ее ориентацию. Таким образом применяя оператор Собеля можно получить вектор, пересекающий границу областей различной яркости в направлении ее увеличения (точка на границе объекта). Оператор Собеля основан на свертке изображения небольшими целочисленными фильтрами в вертикальном и горизонтальном направлениях, поэтому его относительно легко вычислять. Оператор использует наложение на каждую точку изображения двух масок вращения. Эти маски представляют собой две ортогональные матрицы размерностью $3 \times 3$, представленные на рис. 1.

| | | |
|---|---|---|
| -1 | 0 | +1 |
| -2 | 0 | +2 |
| -1 | 0 | +1 |

$G_x$

| | | |
|---|---|---|
| +1 | +2 | +1 |
| 0 | 0 | 0 |
| -1 | -2 | -1 |

$G_y$

***Рисунок 1. Маски Собеля***

Эти маски выявляют границы, расположенные вертикально и горизонтально на изображении. При раздельном наложении этих масок на изображение можно получить оценку градиента по каждому из направлений $G_x$, $G_y$. Конечное значение градиента определяется по формуле

$$G = \sqrt{G_x^2 + G_y^2}$$

Оператор Лапласа позволяет, в свою очередь вычислить лапласиан изображения (сумма производных второго порядка) путем умножения каждого элемента двумерной апертуры $3 \times 3$ на соответствующий элемент так называемой матрицы Лапласа, представленной на рис. 2.

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | | 0 | -1 | 0 | | -1 | 1 | 1 | | 1 | 1 | 1 |
| 1 | -2 | 1 | | -1 | 4 | -1 | | -1 | -2 | 1 | | -1 | -2 | 1 |
| -1 | -1 | -1 | | 0 | -1 | 0 | | -1 | 1 | 1 | | -1 | -1 | 1 |

***Рисунок 2. Матрицы Лапласа***

*Детектор границ Canny*

Этот метод является самым популярным в использовании для реализации в компьютерном зрении. Сам алгоритм выполняется в несколько шагов:

1. устранение шума и лишних деталей;
2. подсчет градиента изображения;
3. уменьшение толщины краев (edge thinning);
4. связывание отдельных краев в контур (edge linking).

Детектор границ так же использует вышеописанный оператор Собеля для получения первой производной в горизонтальном ($G_y$) и вертикальном ($G_x$) направлениях. Через вычисление этого градиента можно найти угол направления всей границы.

$$Q = arctan G_x G_y$$

После чего вычисленный угол округляется до одного из четырех углов, представляющих вертикаль, горизонталь, а так же две диагонали (как уже было описано выше, под углом $45^o$).

В результате применения этого метода получаются двоичное изображение, содержащие границы.

*Преобразование Хафа*

Этот метод используется для поиска линий и других простых форм на изображении. Преобразование Хафа используется для поиска объектов, принадлежащих отдельному классу фигур (например, прямая или окружность) с использованием процедур голосования.

Для поиска линий в основу берется утверждение, что абсолютно любая точка изображения может являться частью некоторого набора линий. Сам алгоритм использует представление линий в полярной системе координат, которое имеет следующий вид

$$R = x * cos(f) + y * sin(f),$$

где: x и y — координаты;

f — угол между перпендикуляром к прямой и осью OX;

R — длина нормали к прямой из начала координат.

Через каждую точку с координатами (x, y) на изображении можно провести несколько прямых с разными значениями R и f, таким образом каждой точке (x, y) изображения соответствует набор точек (R, f) в пространстве, образующий синусоиду.

***Таблица 1.***

**Сравнительная характеристика алгоритмов на опытных примерах с изображением куба**

| **Алгоритм** | **Количество распознанных граней из 5 опытов (max/min)** | **Количество распознанных граней из 15 опытов (max/min)** | **Количество распознанных граней из 25 опытов (max/min)** |
|---|---|---|---|
| Детектор Canny, преобразование Хафа (при настройке угла в 270$^{o}$) | 9 / 7 | 9 / 6 | 10 / 7 |
| Операторы Собеля и Лапласа (с порядком производной 1) | 7 / 6 | 7 / 6 | 7 / 6 |

**Список литературы:**


1. Вудс Р. Цифровая обработка изображений. Издание 3-е, исправленное и дополненное. / Р. Вудс, Р. Гонсалес. М.: Техносфера, 2012. — 1104 с.
2. Senthilkumaran N.A. Study on Edge Detection Methods for Image Segmentation / N. Senthilkumaran, R. Rajesh / Proceedings of the International Conference on Mathematics and Computer Science (ICMCS-2009). — 2009. — Vol. 1. — P. 255—259.
3. Яне Б. Цифровая обработка изображений. М.: Техносфера, 2007. — 584 с.
4. Yusef Shafi S. Designing Node and Edge Weights of a Graph to Meet Laplacian Eigenvalue Constraints / S. Yusef Shafi, Murat Arcak, Laurent El Ghaoui / University of California, Berkeley.

# ПРИМЕНЕНИЕ МЕТОДОВ ТЕОРИИ ГРАФОВ ПРИ ОЦЕНКЕ ЭФФЕКТИВНОСТИ БИЗНЕС-ПРОЦЕССОВ

***Петрова Марина Александровна***
*студент 2 курса магистратуры, кафедра УИТЭС*
*ВлГУ им. А.Г. и Н.Г. Столетовых,*
*РФ, г. Владимир*
*E-mail: pma-33@yandex.ru*

***Шутов Антон Владимирович***
*научный руководитель, канд. физ.-мат. наук, доцент кафедры УИТЭС*
*ВлГУ им. А.Г. и Н.Г. Столетовых,*
*РФ, г. Владимир*

В теории графов существует огромное множество видов задач, которые можно использовать при оценке эффективности бизнес-процессов и их сравнения. В нашем случае разберем задачу нахождения пути максимальной эффективности.

Допустим, что задан определенный граф, в котором для каждой дуги (i; j) указаны два числа $(Э_{ij}, S_{ij})$, которые можно определить как эффект при выполнении конкретной операции — $Э_{ij}$ и затраты на эту операцию — $S_{ij}$. Эффективность $K(\mu)$ пути $\mu$ определяется как отношение его эффекта $Э(\mu) = \sum Э_{ij}$ к затратам $S(\mu) = \sum S_{ij}$, то есть $K(\mu) = Э(\mu)/S(\mu)$. Сама задача подразумевает поиск пути $\mu*$ максимальной эффективности: $K(\mu) \to \max$.

Допустим, что решение $K* = K(\mu*)$ поставленной задачи уже известно, то по факту $K*$ в данном случае выполнено:

$$Э(\mu) - K* S(\mu) \le 0 \quad \forall \mu \qquad (1)$$

Соответственно, задача сводится к поиску минимального значения $K*$, для которого выполняется (1). Иначе говоря, необходимо выполнить поиск минимального $K*$, такого, чтобы все пути (длина которых равна $l_{ij}(K*) = Э_{ij} - K* S_{ij}$) в графе имели неположительную длину (неравенство (1) должно быть соблюдено также и для пути максимальной длины).

Алгоритм решения:

1. Допустим, что $K^* = 0$. Ищем путь $m_1$ максимальной длины. Допускаем, что $K_1(\mu) = Э\ (\mu_1) / S(\mu_1)$ (при $K^* = K_1$ длина пути $\mu(K_1)$ равна нулю).

2. Найдем максимальный путь $\mu_2$ при $K = K_1$. Если длина пути $\mu_2$, обозначаемая как $L(K_1)$, равна нулю, то рассматриваемая задача уже решена. Если $L(K_1) > 0$, то считаем $K_2(\mu) = Э\ (\mu_2) / S(\mu_2)$ и отсюда можно найти максимальный путь $\mu_2$ при $K = K_1$ и т. д.

Далее необходимо рассмотреть путь максимальной эффективности с учетом штрафов. Допустим, что для каждой дуги $(n+1)$ — вершинного графа задаются два показателя: эффект $Э_{ij}$ и время $t_{ij}$. Каждый путь $\mu$ из начальной вершины в конечную вершину определяет некоторый процесс. Продолжительность пути в данном случае — это сумма времен его дуг. Если длительность (продолжительность) рассматриваемого процесса отлична от заданного изначально времени T, то налагаются штрафы $\chi(\mu)$, которые пропорциональны отклонению, т. е.:

$$\chi(\mu) = \begin{cases} \alpha(T - T(\mu)), T(\mu) \le T \\ \beta(T(\mu) - T), T \le T(\mu) \end{cases}$$

где коэффициенты $\alpha$ и $\beta$ могут быть и отрицательными, и положительными.

В конечном итоге задача подразумевает, что необходимо найти путь μ*, который представляет собой максимизацию разности между эффектом и штрафами, т.е.:

$$\mu^* = \arg\max[\ Э\ (\mu) - \chi(\mu)]$$

Определим, что $l_{ij}(\lambda) = Э_{ij} - \lambda t_{ij}$, где $l$ — некоторый параметр, $T(\lambda)$ — длительность (продолжительность) наиболее оптимального пути при

параметре λ, т.е. пути, который имеет максимальную длину, при этом подразумевая, что длина измеряется в $l_{ij}(\lambda)$ [1] .

Из рассмотренного видно, что при увеличении λ величина $T(\lambda)$ не возрастает. Определим $T(\alpha)$ и $T(\beta)$ как длительности (продолжительности) наиболее оптимального пути при условии, что λ равна α и, соответственно, β; $\mu(\alpha), \mu(\beta)$ — сами пути (для того, чтобы их найти, нужно решить 2 задачи, каждая из которых задача на поиск пути максимальной длины). Рассмотрим 6 случаев (первоначальную задачу можно разделить на 2 подзадачи — поиска максимума $Э(\mu) - \chi(\mu)$ при $T(\mu) \le T$ и при $T(\mu) \ge T$ ).

Допустим, что $\alpha \ge \beta$ в этом случае $T(\alpha) \ge T(\beta)$ и:

1) если $T(\beta) \ge T$ , то $\mu(\beta)$ — оптимальное решение;

2) если $T \ge T(\beta) \ge T(\alpha)$ , то $\mu(\alpha)$ — оптимальное решение;

3) если $T(\beta) \ge T \ge T(\alpha)$ , то, при сравнении по длинам $\mu(\alpha)$ и $\mu(\beta)$ $l = Э - \chi$ , выбирать необходимо именно путь максимальной длины.

Допустим, что $\alpha \le \beta$ тогда в этом случае $T(\alpha) \le T(\beta)$ и:

4) если $T(\alpha) \ge T(\beta) \ge T$ , то $\mu(\beta)$ — оптимальное решение;

5) если $T \ge T(\alpha) \ge T(\beta)$ , то $\mu(\alpha)$ — оптимальное решение;

6) если $T(\alpha) \ge T \ge T(\beta)$ , то данная задача вообще не имеет рациональных методов решения.

Для обеспечения возможности применения данного алгоритма для задачи оценки эффективности бизнес-процессов (БП) нужно найти отображение множества БП в множество элементов графа [1].

Ориентированный граф включает три множества: множество вершин (V), множество дуг графа (E) и множество весов графа (L).

Бизнес-процесс можно описать следующими множествами: множество участников бизнес-процесса (S), множество документов, сообщений, файлов (D), множество трудоемкостей выполнения функций бизнес-процесса ($T_O$), множество функций бизнес-процесса (O).

В данном случае возможны различные варианты отображения. Рассмотрим только некоторые из них.

1. D→V, S→E — данное отображение определяет состояния БП и участников БП на каждом этапе обработки информации.

Рассмотрим пример.

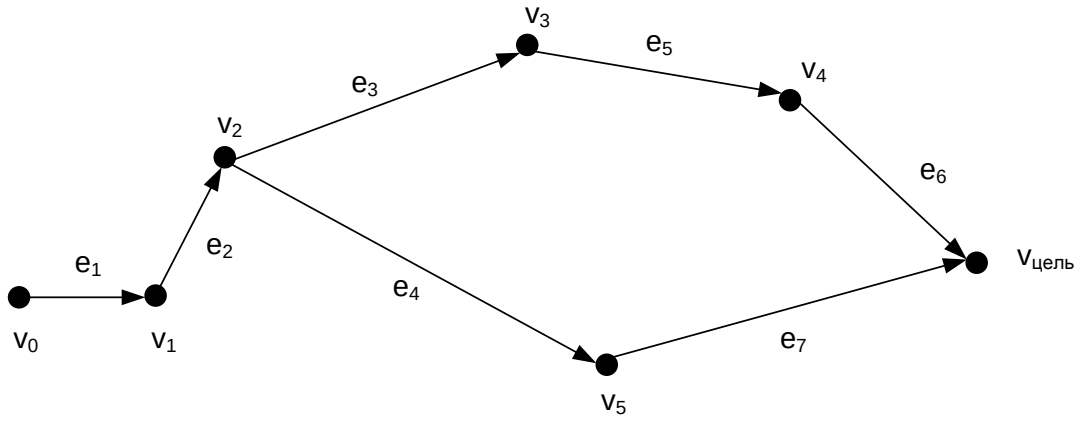



***Рисунок 1 – Граф отображения D→V, S→E***

***Таблица 1.***

**Множество E — множество участников БП (Пример)**

| Обозначения | Описание |
|---|---|
| $e_1$ | Консультант |
| $e_2$ | Сметчик |
| $e_3$ | Старший специалист отдела водных коммуникаций |
| $e_4$ | Старший специалист отдела систем освещения |
| $e_5$ | Специалист отдела водных коммуникаций |
| $e_6$ | Специалист отдела систем освещения |
| $e_7$ | Специалист отдела согласования |

***Таблица 2.***

**Множество V — элементов множество документов, сообщений, файлов**

| Обозначения | Описание |
|---|---|
| $V_0$ | Заказ клиента |
| $v_1$ | Техническое задание |
| $v_2$ | Смета проекта |
| $v_3$ | План-график выполнения проекта водных коммуникаций |
| $v_4$ | Проект водных коммуникаций |
| $v_5$ | План-график выполнения проекта системы освещения |
| $V_{цель}$ | Проектная документация для клиента |

2. D→V, O→E — данное отображение показывает состояния БД и функций БП. Рассмотрим пример.

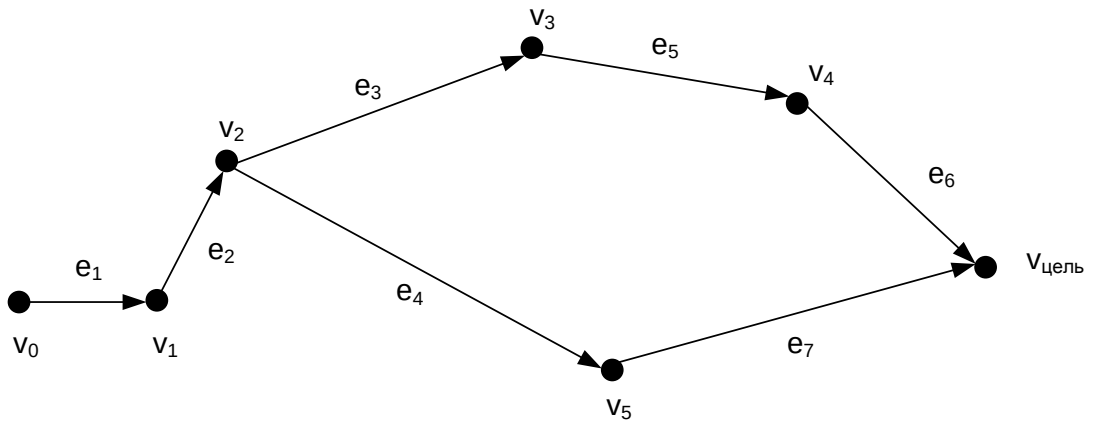



***Рисунок 2. Граф отображения D→V, O→E***

***Таблица 3.***

**Множество E — множество функций БП**

| Обозначения | Описание |
|---|---|
| $e_1$ | Подготовка ТЗ исходя из заказа клиента |
| $e_2$ | Расчет сметы проекта |
| $e_3$ | Разработка план-графика подготовки проекта водных коммуникаций |
| $e_4$ | Разработка план-графика подготовки проекта системы освещения |
| $e_5$ | Подготовки проекта водных коммуникаций |
| $e_6$ | Согласование проекта с водоканалом |
| $e_7$ | Подготовки проекта системы освещения |

***Таблица 4.***

**Множество V — множество документов, сообщений, файлов**

| Обозначения | Описание |
|---|---|
| $V_0$ | Заказ клиента |
| $v_1$ | Техническое задание |
| $v_2$ | Смета проекта |
| $v_3$ | План-график выполнения проекта водных коммуникаций |
| $v_4$ | Проект водных коммуникаций |
| $v_5$ | План-график выполнения проекта системы освещения |
| $V_{цель}$ | Проектная документация для клиента |

3. D→V, O→E, T→L — данное отображение показывает состояния БП и функций БП, а также трудоемкость их выполнения. Рассмотрим пример.

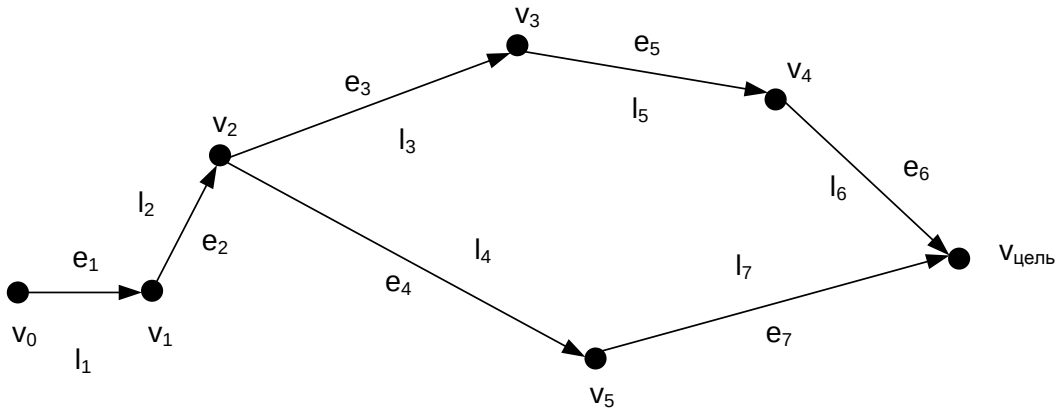



***Рисунок 3. Граф отображения D→V, O→E, T→L***

***Таблица 5.***

**Множество E — множество функций БП**

| Обозначения | Описание |
|---|---|
| $e_1$ | Подготовка ТЗ исходя из заказа клиента |
| $e_2$ | Расчет сметы проекта |
| $e_3$ | Разработка план-графика подготовки проекта водных коммуникаций |
| $e_4$ | Разработка план-графика подготовки проекта системы освещения |
| $e_5$ | Подготовки проекта водных коммуникаций |
| $e_6$ | Согласование проекта с водоканалом |
| $e_7$ | Подготовки проекта системы освещения |

***Таблица 6.***

**Множество V — множество документов, сообщений, файлов**

| Обозначения | Описание |
|---|---|
| $V_0$ | Заказ клиента |
| $v_1$ | Техническое задание |
| $v_2$ | Смета проекта |
| $v_3$ | План-график выполнения проекта водных коммуникаций |
| $v_4$ | Проект водных коммуникаций |
| $v_5$ | План-график выполнения проекта системы освещения |
| $V_{цель}$ | Проектная документация для клиента |

***Таблица 7.***

**Множество L — множество трудоемкостей выполнения функций БП**

| Обозначения | Описание |
|---|---|
| $l_0$ | 8 чел/часов |
| $l_1$ | 10 чел/часов |
| $l_2$ | 6 чел/часов |
| $l_3$ | 8 чел/часов |
| $l_4$ | 8 чел/часов |
| $l_5$ | 56 чел/часов |
| $L_7$ | 48 чел/часов |
| $L_6$ | 24 чел/часов |

Рассмотренные нами примеры представляют собой отдельные бизнес-процессы. С помощью графов можно строить модели разных уровней детализации — от элементарной функции до целого этапа обработки информации.

**Список литературы:**


1. Альпин Ю.А., Ильин С.Н. Дискретная математика: графы и автоматы. Учебное пособие. Казань: Казанский государственный университет им. В.И. Ульянова-Ленина, 2006. — 78 с
2. Cardoso J., «How to measure the control-flow complexity of web processes and workflows» in The Workflow Handbook, pp. 199—212, 2005.
3. Rol´on E., Ruiz F., Garc´ıa F., and Piattini M., «Towards a suite of metrics for business process models in BPMN» in 8th International Conference on Enterprise Information Systems, Paphos, Cyprus, 2006.

# ВИРУСЫ-ШИФРОВАЛЬЩИКИ

***Рангулов Артур Вильнурович***
*студент 3 курса, кафедра автоматики и телемеханики ПНИПУ,*
*РФ, г. Пермь*
*E-mail: rangulov.artur@mail.ru*

***Еременко Николай Николаевич***
*студент 3 курса, кафедра автоматики и телемеханики ПНИПУ,*
*РФ, г. Пермь*
*E-mail: eremenko.nick@gmail.com*

***Кротова Елена Львовна***
*научный руководитель, канд. физ.-мат. наук, доцент ПНИПУ,*
*РФ, г. Пермь*

В настоящее время, троянцы-шифровальщики являются одной из самых актуальных угроз безопасности. По информации производителя антивирусных средств «Доктор Веб», количество разновидностей подобных вирусов, появившихся в 2006—2007 годах, увеличилось на 1900 % всего за два-три года [5]. Эти вредоносные программы сначала выполняют криптографическое преобразование пользовательских файлов на жестком диске определенных форматов, например таких как *.doc, *.docx, *.pdf, *.jpg, *.rar, после чего размещают требования для расшифровки файлов в текстовом документе и/или на новом изображении рабочего стола. Сумма, запрашиваемая злоумышленниками, может достигать десятки тысяч долларов. Этому семейству вирусов были даны следующие названия Trojan-Ransom в классификации «Лаборатории Касперского» и Trojan.encoder в "DrWeb" [1].

Для шифрования данных вирусы используют различные алгоритмы от самых простых булевых функции "XOR" до методов симметричного шифрования (DES, AES, Blowfish и другие) и для криптостойких алгоритмов расшифровка данных без ключа практически невозможна.

В большинстве случаев пользователь конечного устройства сам является виновником запуска (активации) шифровальщика. Одним из способов заражения является попадание троянца в систему через спам-рассылки на элект-

ронную почту [5]. К примеру, попадание Trojan.Encoder.225 в систему возможно с письма, который будет содержать вложенный текстовой документ расширения ".doc", содержащий эксплойт к уязвимости CVE2012-0158, позволяющая удаленному пользователю выполнить произвольный код на целевой системе [2]. Вирус проникает в систему пользователя при помощи уязвимости Microsoft Office. Троянец Trojan.Encoder.94 нередко скачивается на компьютер жертвы с использованием бэкдора BackDoor.Poison, который, в свою очередь, массово рассылается в письмах с вложенными файлами [3].

Новые модификации вирусов-шифровальщиков могут быть не распознаны ни одним из антивирусов, из-за того, что при создании вредоносного кода злоумышленники используют различные методы сокрытия вредоносных намерений, и выдать вирус может только его поведение. Таким образом, используя только антивирусное ПО, которое не содержит хотя бы превентивную защиту, родительский контроль, а также иные средства ограничения возможности проникновения и запуска еще неизвестных антивирусной базе вредоносных программ, пользователь подвергается повышенной опасности заражения троянцем-шифровальщиком.

В настоящее время наиболее совершенным вирусом является Trojan.Encoder.686, альтернативное названием которого CTB-Locker. Особенность данного троянца состоит в том, что его управление происходит через гибридную анонимную сеть Tor, в которой сложно найти следы злоумышленников. Данный шифровальщик использует алгоритм Диффи-Хеллмана на эллиптических кривых (Elliptic Curve Diffie-Hellman). Вирусописатели дают заразившемуся пользователю всего 96 часов на оплату, а в случае отказа все файлы, которые были зашифрованы, будут потеряны навсегда. На сегодняшний день, расшифровка зашифрованных данных не возможна [5].

Другой опасный вирус — CryptoLocker. Особенность данного шифровальщика так же состоит в конечном времени (72 часа) возможности оплаты выкупа и расшифровки данных, в противном случае, ключ шифрования удаляется, после чего становится невозможным расшифровать файлы. Данный

вирус использует для шифрования RSA и AES алгоритмы вместе. На данный момент все ещё не существует эффективного метода расшифровать свои данные, кроме как заплатить выкуп злоумышленникам и получить ключ. Но необходимо уточнить, что выполнение условий злоумышленников не всегда позволяет вернуть свои файлы, так как злоумышленники могут просто не открыть ключ шифрования.

К необходимым рекомендациям по противодействию можно отнести следующие пункты:

1. Ограничивать привилегии пользователей. Если пользователь не имеет определенных прав на запуск новых приложений, вирус не сможет выполнить свои действия, но так же необходимо обновлять систему, так как не обновленная версия может содержать уязвимости, с помощью которых, вирус сможет повысить свои привилегии.

2. Внимательно относиться к файлам, полученным из неизвестных источников.

3. Своевременно обновлять базы данных сигнатур вирусов и антивирусное ПО. Это позволит уменьшить вероятность заражения уже известными вредоносными программами.

4. Создавать резервные копий важных данных с регулярной периодичностью. Причем, необходимо хранить эти копии вне устройства. Это дает возможность просто восстановить данные любой экстренной ситуации и обойтись без серьезных потерь.

Если система все же подверглась заражению, необходимо обратиться в полицию, есть вероятность найти злоумышленников и получить ключ для расшифровки. Не нужно удалять тело вируса, возможно, оно поможет в расшифровке файлов, так же не нужно изменять расширения файлов, удалять их. Далее необходимо определить версию вредоносной программы. Для этого нужно обратить внимание на расширение зашифрованных файлов, адрес для связи со злоумышленниками, по этой информации можно идентифицировать версию вируса. Если данный вирус уже был анализирован и был создан

дешифратор — есть возможность восстановить зашифрованные файлы. Например, компанией «Лаборатория Касперского» был создан дешифратор XoristDecryptor для противодействия вирусам семейств Trojan-Ransom.Win32.Xorist, Trojan-Ransom.MSIL.Vandev. Но не следует восстанавливать информацию с помощью сторонних программ, не предназначенных для этой версии вируса. Так же разработчики антивирусных программ нередко помогают в восстановлении данных своим клиентам, для этого нужно обратиться к специалистам в службу поддержки.

Несомненно, вирусы-шифровальщики являются одной из серьезных угроз для пользователей и нельзя недооценивать их способности, ведь в результате заражения рядовые пользователи могут потерять важные для себя файлы, а компании — огромные средства, в связи с шифрованием необходимых для работы данных. Поэтому мошенники постоянно будут получать прибыль, ведь для кого-то проще заплатить несколько тысяч долларов, чем потерять гораздо большие суммы в результате простоя. К тому же, бесспорно, что алгоритмы, по которым работают шифровальщики, будут становиться все более совершенными, делая восстановление файлов без оплаты гораздо сложнее. Одним из способов улучшения являются средства анонимизации, которые будут мешать обнаруживать источники распространение вирусов по сети.

Следуя приведенным в статье простым рекомендациям, будет возможным снизить вероятность заражения системы, так как инфицирование, в основном, происходит из-за недостаточной осведомленности и внимательности пользователя и/или неправильной настройки системы.

**Список литературы:**


1. Вирусная библиотека Dr.Web / [Электронный ресурс] — Режим доступа. — URL: http://vms.drweb.ru/search/?q=Trojan.Encoder (дата обращения 12.05. 2015).
2. Выполнение произвольного кода в Microsoft Windows // Информационный портал, оперативно и ежедневно рассказывающий о событиях в области защиты информации, интернет права и новых технологиях. — 01.05.2014. / [Электронный ресурс] — Режим доступа. — URL: http://www.securitylab.ru/vulnerability/422990.php (дата обращения 18.05. 2015).

3. Очередная волна троянцев-шифровальщиков / / Новостная лента компании «Доктор Веб». — 20.06.2013 / [Электронный ресурс] — Режим доступа. — URL:http://www.freedrweb.com/show/?i=3633&c=19&lng=ru (дата обращения 05.05. 2015).
4. Синицын Ф. Новое поколение вымогателей // Вирусная энциклопедия. — 24.07.2014 / [Электронный ресурс] — Режим доступа. — URL: https://securelist.ru/analysis/obzor/21090/novoe-pokolenie-vymogatelej/ (дата обращения 05.05. 2015)
5. Троянцы-шифровальщики. Угроза № 1 / [Электронный ресурс] — Режим доступа. — URL: http://antifraud.drweb.ru/encryption_trojs/?lng=ru (дата обращения 13.05.2015).

# ОБЗОР ПРАВОВЫХ МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ И ПЕРСПЕКТИВ ИХ РАЗВИТИЯ

***Рожкова Екатерина Олеговна***
*студент 4 курса, кафедра судовой автоматики и измерений СПбГМТУ,*
*РФ, г. Санкт-Петербург*
*E-mail: rina1242.ro@gmail.com*

***Ткачёв Павел Сергеевич***
*студент 4 курса, кафедра судовой автоматики и измерений СПбГМТУ,*
*РФ, г. Санкт-Петербург*
*E-mail: P.S.Tkachev@gmail.com*

***Шавинская Сания Караматовна***
*научный руководитель, доцент*
*Санкт-Петербургского Морского Технического Университета,*
*РФ, г. Санкт-Петербург*

Характеристика подсистемы правовых мер защиты государственных секретов является важной научной задачей, поскольку её совершенствование является необходимым условием обеспечения безопасности государственных секретов (и, как следствие, национальной безопасности) и соблюдения баланса прав и интересов субъектов данных отношений.

В 2000г. Президентом Российской Федерации была утверждена Доктрина информационной безопасности, которая определяет способы, цели и методы обеспечения информационной безопасности Российской Федерации. Согласно этой доктрине: «информационная безопасность (ИБ) есть состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства». Можно сказать, что Доктрина непосредственно продолжает развитие Концепции национальной безопасности Российской Федерации в информационной сфере.

Четыре основные составляющие национальных интересов РФ в информационной сфере выделенных в доктрине:

1. Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею;

2. Информационное обеспечение государственной политики РФ, связанное с доведением до российской и международной общественности достоверной информации;

3. Развитие современных информационных технологий, отечественной индустрии информации, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов;

4. Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем [2].

Защита национальных интересов реализуется организационно-техническими, экономическими и правовыми методами; особенности последних и будут рассмотрены в данной статье. Правовые методы включают в себя разработку правовых актов и законодательства, регламентирующего отношения в информационной сфере, и методических документов в вопросах обеспечения информационной безопасности Российской Федерации.

Следует отметить, что правовое регулирование защиты государственных секретов имеет конституционно-правовую основу. Таким образом, защита атрибутов государственности осуществляется в рамках обеспечения национальной безопасности. Кроме этого, осуществляя регулирование оборота государственных секретов, государство реализует установленные в Конституции исключительные права на обладание отдельными объектами и на осуществление отдельных видов деятельности. Если говорить о тенденциях развития специальной терминологии обеспечения информационной безопасности, то оно во многом определяется развитием соответствующих аппаратно-программных средств и технологии систем обработки информации, а также движется в направлении наращивания практических аспектов в сравнении с теоретико-информационными. Кроме того, динамика развития терминологии характеризуется устареванием ряда терминов, которые, в свою очередь, взаимосвязаны с устареванием программно-аппаратных средств и технологий [1]. Нельзя также не отметить тенденцию заимствования терминов из традиционных стран-

изготовителей систем обработки информации, а также англоязычные заимствования.

Эти суждения дают право сделать вывод: одним из важнейших условий развития правовых методов защиты информации является строгость и однозначность формулирования и корректность использования принятых терминов. В частности, многими специалистами используется термин «конфиденциальная информация», при этом на данный момент в законодательстве Российской Федерации нет такого понятия; данный термин был отражен в ФЗ № 24 «Об информации, информатизации и защите информации», который утратил силу 27.07.2006 года, в связи с вступлением в силу ФЗ № 149 «Об информации, информационных технологиях и защите информации». Согласно этому закону: «конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации».

Первой крупной составляющей правовых мер обеспечения информационной безопасности является составление перечня сведений, который разделяет сведения на строго конфиденциальные, конфиденциальные и для служебного пользования; определяет и утверждает списки доступа; исключает сведения, не относящиеся к коммерческой тайне и т. д. Вторая составляющая — развитие нормативно-правовой базы, которая определяет экономическую безопасность, а также устанавливает административную и уголовную ответственность. Существенное значение будет иметь вопрос введения изменений и дополнений, вносимых в нормативно-правовые документы в связи с задачами по обеспечению информационной безопасности.

Безусловно, для совершенствования правовых методов необходимы грамотные специалисты, которые ведут активную профессиональную деятельность, а также могут оценить средства и методы информационного противоборства в условиях современной информационной войны. На рисунке 1 приведена схема классификации информации по категориям доступа, из которой видно, насколько широкий диапазон законов охватывает обеспечение информационной безопасности.

Вопросы правового регулирования в сфере защиты информации Российской Федерации отражены в следующих нормативно-правовых актах законодательства федерального уровня: Гражданский кодекс РФ, Уголовный кодекс РФ, Бюджетный кодекс РФ, а также федеральные законы: «О правовой охране программ для ЭВМ и баз данных»; «Об авторском праве и смежных правах»; «О государственной тайне»; «Об информации, информационных технологиях и защите информации»; «Об электронной цифровой подписи» и т. д.

Ограничение в доступе к информации состоит в установлении федеральным законом условий отнесения этой информации к коммерческой и иной тайне, обязательности соблюдения конфиденциальности такой информации и ответственности за разглашение такой информации.


***Рисунок 1. Схема классификации информации по категориям доступа***

Основа правовой базы для обеспечения информационной безопасности в РФ отображена в таблице 1.

*Таблица 1.*

**Основа правовой базы для обеспечения ИБ РФ**

| Вид информации | Составляющая | Правовое регулирование |
|---|---|---|
| Открытая информация, доступ к которой запрещено ограничивать | • О ЧП и катастрофах, угрожающих здоровью и безопасности граждан, и их последствиях, а также о стихийных бедствиях и их официальных прогнозах и последствиях;<br>• О состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, с\х, о состоянии преступности, о чрезвычайных ситуациях; об информации, необходимой для обеспечения безопасности функционирования населенных пунктов, производственных объектов и населения в целом;<br>• О привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, учреждениям и организациям;<br>• О случаях нарушения прав и свобод человека и гражданина;<br>• О случаях нарушения законодательства органами государственной власти и их должностными лицами;<br>• Нормативные акты, устанавливающие правовой статус органов власти, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;<br>• Документы, с информацией о деятельности органов власти, об использовании бюджетных средств, других ресурсов, про состояние экономики и потребностях населения, кроме тех сведений, составляющих государственную тайну. | • Статья 7. Закона о гос. тайне Сведения, не подлежащие отнесению к государственной тайне и засекречиванию.<br>• Статья 10. ФЗ № 149 «Об информации…» Распространение информации или предоставление информации. |
| Открытая информация, которая должна быть беспрепятственно предоставлена | • Информация о санитарно-эпидемиологической обстановке, состоянии среды обитания, качестве и составе продукции производственно-технического назначения, пищевых продуктов, товаров для личных и бытовых нужд, потенциальной опасности для здоровья человека выполняемых работ и оказываемых услуг; | • Ст. 8 ФЗ «О банках и банковской деятельности»;<br>• Ст. 23, 30 ФЗ «О рынке ценных бумаг»;<br>• Ст. 237 УК РФ. Сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей |

| | | |
|---|---|---|
| | • Лицензия на осуществление финансовых операций, бухгалтерский баланс и отчет о прибыли и убытках, аудиторское заключение за предыдущий год, а также ежемесячные бухгалтерские балансы за текущий год — для коммерческих организаций;<br>• В определенных случаях информация, схожая с той, которую обязаны предоставить банки, должна быть предоставлена эмитентами ценных бумаг;<br>• Лица, располагающие информацией о фактах и обстоятельствах, создающих угрозу для жизни людей, за сокрытие, а также за требование оплаты таковой, несут уголовную ответственность. | |
| Государственная тайна | Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.<br><br>Существует три степени классификации секретности данных, признанных как государственная тайна и соответствующих степеням грифы секретности для материальных носителей: "особой важности", "совершенно секретно" и "секретно". | • Федеральный закон РФ "О безопасности" от 28 12 2010 года № 390-ФЗ;<br>• ФЗ РФ "О государственной тайне" от 21 07 1993 года № 5485-1;<br>• Перечень сведений, отнесенных к государственной тайне, утвержден Указом Президента РФ от 30. ноября 1995 г. № 1203;<br>• Федеральный закон РФ "О техническом регулировании" от 27 декабря 2002 года № 184-ФЗ;<br>• Статья 275 УК РФ. Государственная измена;<br>• Статья 276 УК РФ. Шпионаж;<br>• Статья 283 УК РФ. Разглашение государственной тайны;<br>• Статья 284 УК РФ. Утрата документов, содержащих государственную тайну; |

| | | |
|---|---|---|
| Персональные данные | Любая информация, которую можно сопоставить с определенным или определяемому на основании такой информации лицу, в том числе: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация. | • ФЗ 152 «О персональных данных» от 27 июля 2006 г;<br>• указ Президента РФ от 6.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;<br>• Постановление Правительства РФ от 01.11.2012 г. № 1119 г. "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";<br>• Приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;<br>• ТК РФ Глава 14. Защита персональных данных работника;<br>• "Кодекс РФ об административных правонарушениях" Статья 13.14. Разглашение информации с ограниченным доступом. |
| Коммерческая тайна | Информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам; информация, к которой нет свободного доступа на законном основании; информация, в отношении которой обладатель такой информации введен режим коммерческой тайны.<br>Сюда относятся сведения научно-технического, производственного, финансового и делового характера. | • ФЗ № 98 «О коммерческой тайне» от 15.07.2004;<br>• ГК РФ ст. 139 Служебная и коммерческая тайна;<br>• Статья 183 УК РФ Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну. |
| Служебная тайна | Сведения ограниченного распространения (не являющиеся секретная информация), касающаяся деятельности организаций, прекращение свободного распространения которой диктуется служебной необходимостью. Перечень этих сведений предусматривается в ведомственных инструкциях и наставлениях. | • Постановление Правительства РФ от 03.11.1993 № 1233 «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»<br>• Статья 1470 ГК РФ Служебный секрет производства;<br>• п. 7 ст. 243 ТК РФ Случаи полной материальной ответственности; |

| | | |
|---|---|---|
| | | • ТК РФ Статья 232. Обязанность стороны трудового договора возместить ущерб, причиненный ею другой стороне этого договора. |
| Профессиональная тайна | Отдельно охраняемые законом тайны, необходимость соблюдения которых вытекает из специфически доверительного характера отдельных профессий. | • Адвокатская тайна: ФЗ «об адвокатской деятельности и адвокатуре в РФ» Статья 8. Адвокатская тайна;<br>• Нотариальная тайна: Основы законодательства РФ о нотариате" (от 11.02.1993 № 4462-1)Статья 16. Обязанности нотариуса;<br>• Банковская тайна: ФЗ "О банках и банковской деятельности" от 02.12.1990 № 395 Статья 26. Банковская тайна;<br>• Журналистская тайна: Закон РФ от 27.12.1991 № 2124-1 "О средствах массовой информации" Статья 41. Обеспечение конфиденциальности информации. |
| (Сведения о сущности изобретения) Патентное право | Патентное право регулирует имущественные и личные неимущественные отношения, возникающие в связи с признанием авторства и охраной изобретений, установлением режима их использования и защитой права их авторов и патентообладателей. | • Глава 72 ГК РФ — (ст. 1345-1407). Патентное право;<br>• «Кодекс РФ об административных правонарушениях»; Статья 7.12: «Нарушение авторских и смежных прав, изобретательских и патентных прав»;<br>• УК РФ Глава 19.Статья 147.Нарушение изобретательских и патентных прав. |

Конфиденциальность это отражение ограничений, которых наложил собственник информации на доступ к ней третьих лиц, т. е. собственник устанавливил правовой режим этой информации в соответствии с законом.

Если говорить о режиме коммерческой тайне, то он начинает действовать после того, как обладатель информации установил данный режим; определил перечень информации, составляющей коммерческую тайну; определил порядок ограничения доступа к информации, составляющей коммерческую тайну. Следует учитывать тот факт, что эти действия не должны противоречить

ФЗ «О коммерческой тайне», а также Гражданскому кодексу РФ. В частности, коммерческую тайну не могут составлять учредительные документы, лицензии, патенты, финансово-хозяйственные документы, документы о платежеспособности, численности, зарплата, налоги и платежи, экология, антимонопольные сведения, безопасность труда, участие должностных лиц в бизнесе.

Режим конфиденциальности информации позволяет ее собственнику при существующих или возможных обстоятельствах увеличить доходы или избежать расходов, сохранив положение на рынке услуг, товаров, работ, или получить иную коммерческую выгоду. Носителями коммерческой информации являются руководители предприятий или организаций, а также другие служащие, допущенные к коммерческим секретам.

К сведениям научно-технического характера, которые составляют коммерческую тайну, относятся: идеи, открытия, ноу-хау, патенты, лицензии, новые методы организации производства; содержание рационализаторских предложений, планы внедрения новых технологий и новых видов продукции; анализ конкурентоспособности; ПО, коды, пароли доступа к конфиденциальной информации.

К сведениям производственного (технологического) характера, которые составляют коммерческую тайну, относятся: способы производства и технология; конструкторская документация, чертежи и схемы; сведения о материалах; рецептура товаров; система организации труда, время выхода на рынок и планы выпуска продукции; планы инвестиций в производство.

К сведениям финансового характера, которые составляют коммерческую тайну, относятся: размер прибыли и уровень себестоимости продукции; механизм формирования цен; банковский и торговые операции; уровень платежеспособности фирмы.

К сведениям делового характера, которые составляют коммерческую тайну, относятся: характер и условия заключенных контрактов; система организации труда; планы рекламных акций; сведения о поставщиках, посред-

никах, конкурентах, контрагентах; о персонале фирмы; о деловых переговорах; о коммерческой переписке.

Следует также упомянуть Федеральный закон Российской Федерации № 1 от 10 января 2002 года «Об электронной цифровой подписи», который обеспечивает конфиденциальность информации в электронном виде — подпись, рассматривается как личная подпись субъекта.

Помимо перечисленных существуют и иные законодательные акты, в той или иной степени регулирующие отношения в области конфиденциальных данных, информации и защиты информации.

С учетом вышеизложенной в работе информации можно придти к следующим выводам: учитывая сложность законодательства Российской Федерации, а также очевидную необходимость защиты информации, правовая сторона информационной безопасности требует постоянного совершенствования, корректировки на предмет противоречий и исключения двусмысленности формулировок, поскольку исследование существующего законодательства в области обеспечения информационной безопасности подтвердило его принципиальные недостатки — противоречивость, декларативность, наличие «белых пятен» [3]. Изменения в сфере правового регулирования информационной безопасности являются сигналом для продолжения исследований этой области. Учитывая современные тенденции глобализации информационного общества, национальное законодательство нуждается в уточнении направления развития; кроме того, на международной арене также происходят изменения, требующие адекватного правового вмешательства. Опираясь на опыт зарубежных коллег, на международные документы по защите информации, а также внося свои индивидуальные особенности в составление правовой базы, Российская Федерация продолжает активно участвовать в процессе формирования глобального информационного общества не только на национальном уровне, но и в рамках международных процессов. Это показывает востребованность в совершенствовании правового регулирования в сфере

противодействия новым вызовам и угрозам национальной безопасности, их особенности, и проблемы борьбы с терроризмом и кибертерроризмом [4].

Таким образом, стратегия развития информационного общества в РФ при правовом обеспечении информационной безопасности должна основываться на демократизме, законности, научности, учитывая принципы правового регулирования в области защиты информации, определенных законодательством РФ, законодательно закрепить принципы обеспечения единого информационного пространства, и сбалансировать интересы личности, общества и государства и их общей ответственности.

**Список литературы:**


1. Алексеев А.Ф. Сертификация систем обработки информации. Учебное пособие/Санкт-Петербург, 2010. — С. 12—13.
2. Доктрина информационной безопасности Российской Федерации (от 9 сентября 2000 г. № пр. 1895).
3. Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство: Монография / Санкт-Петербург, ун-т МВД России. СПб.: Фонд «Университет», 2000. — С. 354—360.;
4. Патрушев Н.П. Особенности современных вызовов и угроз национальной безопасности России // Журнал рос. права. — 2007. — № 7 (127). — С. 3—12.

# ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ИЗДАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ ВУЗА

***Сухотина Мария Константиновна***
*студент 4 курса, кафедра информационных технологий и компьютерного дизайна МГУДТ,*
*РФ, г. Москва*
*E-mail: mksukhotina@list.ru*

***Фирсов Андрей Валентинович***
*научный руководитель, проф., д-р. техн. наук. МГУДТ,*
*РФ, г. Москва*

Тема моего проекта связана с издательской деятельностью Московского государственного университета дизайна и технологии.

Издательские функции вуза осуществляет редакционно-издательский отдел МГУДТ, который является структурным подразделением университета.

Основной задачей редакционно-издательского отдела (РИО) является Обеспечение нужд университета в редакционно-издательских и полиграфических работах, формирование издательской политики в целях обеспечения вуза научной, справочной и иной литературой, организация редактирования и выпуска литературы (научной, учебной и методической, а также информационных и нормативных материалов), необходимой для деятельности МГУДТ, практических пособий и руководств; учебных программ, монографий, учебников, материалов конференций, учебно-методических пособий; рекламных проспектов МГУДТ [1].

Тематика издаваемой литературы многообразна: экономика, юриспруденция, вычислительная техника, машиностроение, текстильное дело, философия и социология и др.

Содержание учебной литературы соответствует государственным образовательным стандартам. Обновление вузовской учебной литературы идет синхронно с изменением учебных программ. Расширение доли факультативных занятий, появление новых форм обучения предопределило издание более

широкого ассортимента тематической литературы и изданий для разных форм обучения студентов.

Литература представляет интерес не только для студентов, аспирантов и преподавателей, но и для широкого круга читателей.

Сейчас отдел РИО активно развивается. И целью моего проекта является создание информационной системы, которая помогла бы оптимизации производящей деятельности отдела.

Мой программный продукт призван не только облегчить работу сотрудникам отдела РИО, но и помочь клиентам типографии, экономя свои нервы и время, узнать во сколько им обойдется та или иная услуга или товар.

Данный программный продукт не является первопроходцем. Он имеет множество аналогов. Но уникальность моего продукта состоит в том, что он будет создан и настроен под издательство университета. В это понятие входит красивый, функциональный, а главное удобный интерфейс.

Продукт, а именно «онлайн-калькулятор», который будет встроен в сайт, должен будет отвечать всем потребностям производителя печатной продукции. А, поскольку, данный программный продукт будет ориентирован на выполнения только определенных задач, которые исполняет конкретная типография — это и делает его уникальным.

Онлайн-калькулятор — это программный модуль, встраиваемый в сайт, позволяющий посетителям сайта оперативно вычислить стоимость предлагаемых на сайте услуг, продаваемых товаров и т. д. В онлайн-калькуляторе, в отличие от традиционных программ все изменения происходят на сервере, а пользователь рассчитывает через обычный браузер [2].

В основе построения программы - база данных (хранятся все настройки калькулятора), форма отображения, логика работы, собственная административная часть для управления калькулятором.

Для системы может быть разработана уникальная структура базы данных (MySQL), которая расширяема и взаимозаменяема. Серверным языком расчетов является PHP.

**Структура сайта**

Стартовая страница состоит из пяти блоков (см. рис. 1):

1. Шапка с логотипом ***РИО***
2. Кнопка ***«Каталог»***
3. Кнопка ***«Инфо»***
4. Кнопка ***«Расчет услуг»***
5. ***Текстовое поле***.

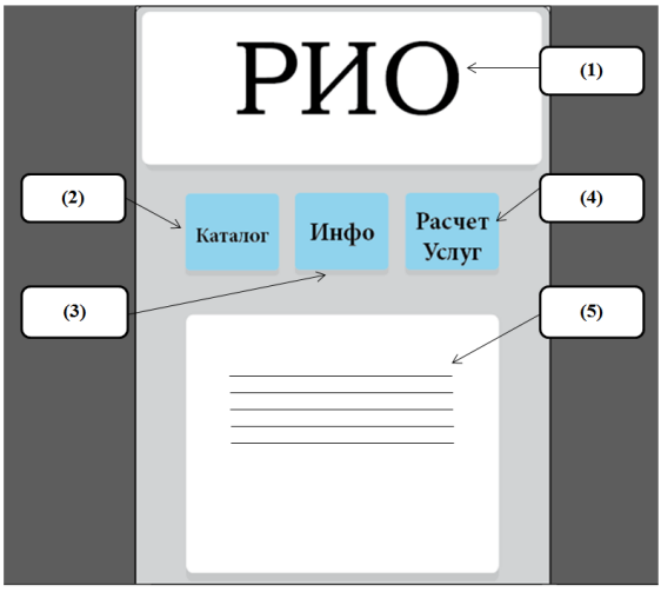



***Рисунок 1. Стартовая страница: 1 — шапка с логотипом РИО, 2 — кнопка «Каталог», 3 — кнопка «Инфо», 4 — кнопка «Расчет услуг», 5 — текстовое поле***

Шапка с логотипом ***РИО*** является ссылкой на главную страницу сайта.

Кнопка «***Каталог***» на рис. 1 является ссылкой на страницу основных услуг и товаров (см. рис. 2).

При нажатии на одну из кнопок на странице, отображенную на рис. 2, посетитель может получить информацию о данном товаре.

Кнопка «***Инфо***» на рис. 1 является ссылкой на страницу с контактами и основной информацией, которая отображена на рис. 3.

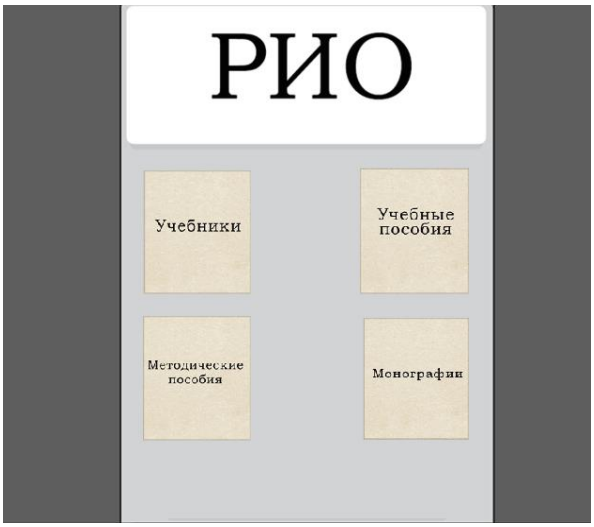



***Рисунок 2. Страница «Каталог»***

Кнопка ***«Расчет услуг»*** на рис. 1 является ссылкой на страницу «Онлайн-калькулятора» (см. рис. 4).

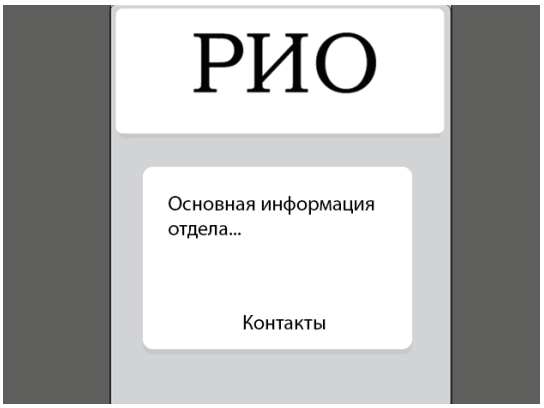



***Рисунок 3. Страница «Инфо» для заказчиков***

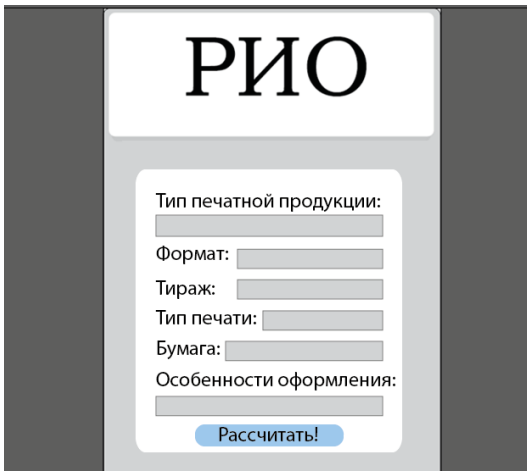



***Рисунок 4. Страница «Расчет услуг»***

При заполнении указанных полей пользователь получит цену товара или услуги.

Если на сайт заходит администратор, набрав соответствующий пароль, то вместо кнопки ***«Рассчитать!»*** на странице **«Расчет услуг»**, показанную на рис. 4 — высвечивается кнопка ***«Заказы»*** (см. рис. 5).


***Рисунок 5. Страница «Расчет услуг» для администратора***

При нажатии на нее администратор видит сведения о заказах (см. рис. 6).


***Рисунок 6. Страница «Заказы»***

Мною будет созданы 2 базы данных:

1. хранение наименования товаров и услуг;
2. хранение информации о ресурсах.

Открывая заказ, администратор получит информацию из базы № 2, о том, если ли ресурсы для выполнения заказа. Если есть — заказ идет в работу и происходит перерасчет ресурсов. Таким образом, отпадает надобность постоянно обновлять расходные материалы вручную.

***Текстовое поле***

На данном текстовом поле отображаются новости сайта.

С появлением цифровых информационных систем и Интернета масштабы издательской деятельности расширились и теперь включают электронные ресурсы.

Если грамотно воспользоваться новыми возможностями можно существенно повысить качественный уровень производства и сбыта печатной продукции редакционно-издательской деятельности МГУДТ.

И особенно важно, развивать данную отрасль в университете, ведь поставляя качественный печатный материал для изучения, университет помогает студентам получать знания, делает инвестиции в чье-то будущее.

**Список литературы:**


1. Сборник нормативных документов Московского государственного университета дизайна и технологии в 4-х частях. Управление университетом и обеспечение его деятельности / Сост. Белгородский В.С. [и др.]. М. : МГУДТ, 2014. — Ч. 1. — Т. 2. — 177 с.
2. Создание онлайн-калькулятора для вашего сайта: сайт разработка онлайн-калькуляторов любой сложности. — 2015 [Электронный ресурс]. — Режим доступа. — URL: http://calc.by/calculator-for-your-site.html (дата обращения: 22.05.2015).

# ПРОВЕРКА НАДЕЖНОСТИ ПАРОЛЯ

***Фомина Анна Александровна***
*студент 3 курса, кафедра автоматики и телемеханики ПНИПУ,*
*РФ, г. Пермь*
*E-mail: ankadom@yandex.ru*

***Макарютин Михаил Михайлович***
*студент 3 курса, кафедра автоматики и телемеханики ПНИПУ,*
*РФ, г. Пермь*
*E-mail: mishka_94_2008@mail.ru*

***Кротова Елена Львовна***
*научный руководитель, канд. физ.-мат. наук, доцент ПНИПУ,*
*РФ, г. Пермь*

Современную жизнь сложно представить без сети Интернет. Миллиарды людей по всему миру ищут различную информацию в интернете, проверяют электронную почту, оплачивают услуги с помощью интернет-банкинга или просто общаются. Ежесекундно около десяти человек на планете регистрируются в той или иной социальной сети. Безусловно, далеко немаловажную роль при этом играет безопасность персональных данных, размещаемых в Интернете.

При регистрации на любом Интернет-ресурсе, требуется ввести некий набор сведений, идентифицирующий пользователя в компьютерной системе. Один из наиболее важных атрибутов любой учетной записи — это, конечно, пароль. Именно от его надежности зависит сохранность вашей личной информации на просторах глобальной сети. Когда Вы заполняете поле «Password» при регистрации аккаунта, система автоматически проверяет и выдает информацию, насколько введенный Вами пароль удовлетворяет критериям безопасности. Проблема состоит лишь в том, что каждый отдельный сайт определяет адекватность пароля по-разному. При этом ни один из них не может дать стопроцентной гарантии, что Ваш аккаунт не взломает какой-нибудь продвинутый хакер.

В большинстве случаев пользователи сети в качестве пароля используют свою фамилию, дату рождения, кличку любимого питомца, ввиду того, что его очень просто запомнить. Конечно, такой пароль не обладает высокой надеж-

ностью, особенно когда ваша фамилия упоминается не только в составе пароля, но и, например, в адресе электронной почты, используемой в качестве логина.

К другим неудачным, но по каким-то причинам самым распространенным, относятся такие пароли как: 12345678 и qwerty. Естественно, человеку намного проще ввести буквы или цифры, находящиеся на расположенных подряд кнопках клавиатуры, чем запоминать сложную комбинацию цифр, букв, символов, перемешанных между собой, да еще и с разным регистром. Несмотря на то, что такие пароли давно находятся в пятерке самых распространённых, далеко не все сайты определяют их как ненадежные, в силу того, что он удовлетворяют одному из первостепенных критериев — количество символов должно быть не менее 6 (8) штук.

Мы решили проверить, как разные сайты определяют процент надежности паролей. Для этого будем использовать наиболее распространённый пользовательский пароль, составленный из фамилии и даты рождения. Для сравнения будем использовать следующие комбинации:

1. Fomina1994
2. foMina1994
3. f1o9M9i4na
4. FominaFominaFo
5. fominafominafo

Для начала мы воспользовались услугой проверки надежности пароля, которую можно найти на официальном сайте компании Microsoft [1]. Первые три варианта нам определили как пароли средней надежности, два последних как хорошо защищенные. Закрадывается подозрение, что данный сайт проверяет надежность пароля только по одному критерию — количество символов. Так, пароль длиной более 8 символов «высвечивается» как medium, а более 14 — strong, при этом абсолютно не имеет значение, какие именно символы были использованы. Также нами был проверен пароль «12345678», который тоже, по мнению разработчиков данного ресурса, оказался средне

защищённым. Самое интересное, что на этом же сайте представлены распространенные ошибки при создании паролей, среди которых упоминается последний.

Следующим на очереди оказался блог Лаборатории Касперского [2], где тоже можно протестировать свой пароль на уровень надежности. Результаты представлены в таблице 1. Надежность пароля на данном ресурсе определяется временем подбора пароля на обычном компьютере.

***Таблица 1.***

**Сравнение надежности паролей**

| № | Пароль | Надежность |
|---|---|---|
| 1 | Fomina1994 | 28 минут |
| 2 | foMina1994 | 2часа |
| 3 | f1o9M9i4na | 5 месяцев |
| 4 | FominaFominaFo | 4 века |
| 5 | fominafominafo | 21 год |
| 6 | 12345678 | 1 секунда |
| 7 | F1o9M9I4Na | 400 веков |
| 8 | Ащьштф1994 | 4 века |

Как мы видим, в отличие от сайта Microsoft, на данном ресурсе все сгенерированные нами пароли имеют разную степень надежности. Как и ожидалось, пароль «12345678» имеет самую низкую надежность. Наибольшую надежность имеет пароль под номером 7, имеющий кроме английских заглавных букв и цифр, строчные русские буквы «а» и «о». Также хорошую надежность показал пароль под номером 8, где фамилия «Фомина» написана английскими буквами на русской раскладке.

На каждом из вышеперечисленных сайтов пользователей заверяют, что данные сайты предназначены исключительно в ознакомительных целях, носят справочный характер, не являются при этом гарантией безопасности, а также не хранят введенные Вами данные. Но кто знает, может быть в поисках online-программы по проверке надежности пароля, Вы случайным образом наткнетесь на сайт, где злоумышленники не только не выдадут Вам адекватный результат, но и составят из введенных паролей базу данных, для последующих взломов. Конечно, существуют и другие способы проверки надежности. Так, в Интернете можно найти множество различных примеров, как простой скрипт

может быть написан с использованием JavaScript и jQuery для соблюдения требований комплексного пароля.

На основе всего вышеизложенного, мы пришли к выводу, что проверка своих паролей на надежность с помощью различных сайтов является не только бессмысленной тратой времени, но и далеко небезопасным занятием. Самым верным способом создания надежного пароля является использование следующих рекомендаций:

1. При создании пароля включайте в него не только цифры и буквы разных регистров, но и символы, а также знаки препинания. Как показала практика, чередование строчных и заглавных букв, разных языков вперемешку с цифрами, обеспечивает высокую надежность Вашему паролю.

2. Создавайте пароль, состоящий более чем из 8 символов. Чем больше количество символов, тем сложнее взломать данный пароль.

3. Если вам трудно запомнить обычный набор букв и цифр, создавайте пароли из нескольких коротких, но несвязных слов, разбавляя их при этом цифрами и знаками препинания.

4. Старайтесь не включать в состав пароля личную информацию: имя, фамилию, дату рождения и т. п.

5. Не используйте в качестве пароля повторяющиеся наборы символов 12345678, 222222 или смежных символов на клавиатуре (qwerty).

6. Не используйте один пароль для всех учетных записей. Для простоты запоминания можно к Вашему паролю прибавить первую букву названия сайта.

7. Регулярно меняйте свои пароли для всех аккаунтов.

Придерживаясь данным правилам создания пароля, Вы будете на 100 % уверены, что ни один хакер не взломает ваши личные данные, если, конечно, Вы не упустите еще одно важное правило — никогда и никому не показывать Ваш пароль.

**Список литературы:**


1. Проверка надежности пароля // Microsoft: [Офиц.сайт]. [Электронный ресурс] — Режим доступа. — URL:https://www.microsoft.com/ru-ru/security/pc-security/password-checker.aspx (дата обращения 23.05.2015).
2. Спасаем мир словом [Электронный ресурс] // Официальный русский блог лаборатории Касперского: [Офиц.сайт]. [Электронный ресурс] — Режим доступа. — URL: https://blog.kaspersky.ru/password-check/ (дата обращения 23.05.2015).

# ВСТРАИВАНИЕ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ВИДЕОПОТОКИ, СЖАТЫЕ С ИСПОЛЬЗОВАНИЕМ ДРЕВОВИДНЫХ СТРУКТУР КОДИРОВАНИЯ

***Шипицин Сергей Павлович***
*студент 3 курса, кафедра Автоматика и телемеханика,*
*Электротехнический факультет,*
*Пермский национальный исследовательский политехнический университет,*
*РФ, г. Пермь*
*E-mail: shipitsyn_sp@mail.ru*

***Кротова Елена Львовна***
*научный руководитель, канд. физ.-мат. наук, доцент*
*(кафедра Высшая математика), ПНИПУ,*
*РФ, г. Пермь*

В статье затрагивается тема встраивания цифровых водяных знаков (ЦВЗ) и т. н. «отпечатков пальцев» в видеопотоки, подвергнутые сжатию с потерями. Рассматриваются форматы сжатия последнего поколения (HEVC, VP9), предлагается метод встраивания ЦВЗ, базирующийся на особенностях их реализации.

Кинематограф зародился в конце XIX века, Интернет — во второй половине XX. Тем не менее, до сих пор эти сферы массовой культуры соприкасаются довольно опосредованно, в основном, из-за вполне обоснованных опасений правообладателей за свой контент и, соответственно, прибыли. Законодательство в области обеспечения авторских прав достаточно проработано, однако на практике цифровая дистрибуция осложнена в связи с повсеместным несанкционированным копированием и распространением. Наименее защищённым ввиду сложности обнаружения конкретного злоумышленника остаётся медиаконтент, в том числе видео [2].

Исторически от несжатого видео в цифровом пространстве было решено отказаться сразу из-за чрезвычайно большого информационного объёма и избыточности, поэтому стали развиваться технологии цифровой компрессии видеосигнала. Последней на сегодняшний день ступенью развития технологий сжатия стал формат H.265 или HEVC (High Efficiency Video Coding), разработанный ITU-T Video Coding Experts Group (VCEG) совместно с ISO/IEC Moving Picture Experts Group (MPEG), а также открытый кодек VP9 от компании Google.

Одним из наиболее перспективных методов защиты медиаконтента является встраивание цифровых водяных знаков (ЦВЗ) — видоизменение контейнера таким образом, чтобы встроенное сообщение не было заметно визуально, однако обнаруживалось специальными детекторами. ЦВЗ обычно представляет собой текст или логотип, идентифицирующий автора. В данной работе рассматривается другое применение ЦВЗ —– так называемые «цифровые отпечатки пальцев», которые позволяют либо локализовать точку утечки информации, либо однозначно определить злоумышленника [3].

Важной характеристикой ЦВЗ является робастность (устойчивость) — способность ЦВЗ быть зафиксированным детекторами при различных искажениях контейнера. Ниже перечислены основные атаки на системы с ЦВЗ, направленные на сокрытие встроенного сообщения:

- атаки, направленные на удаление ЦВЗ;
- геометрические атаки, направленные на искажение контейнера;
- криптографические атаки;
- атаки против протокола встраивания и проверки ЦВЗ [1].

Основой реализации алгоритмов сжатия HEVC и VP9 является применение блоков с древовидной структурой кодирования (рис. 1) вместо макроблоков в алгоритмах предыдущего поколения [5; 6].

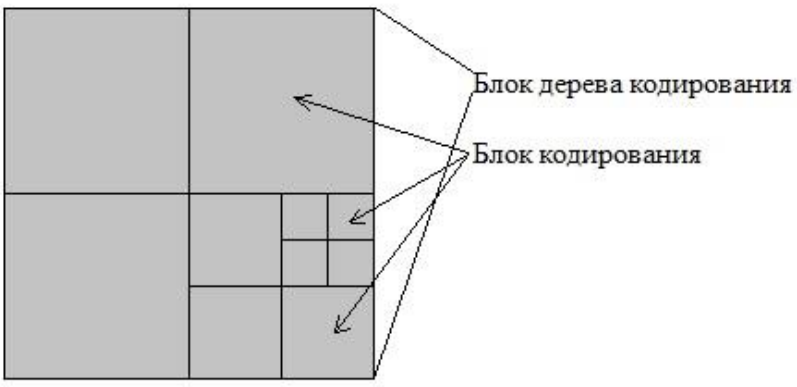



***Рисунок 1. Древовидная структура кодирования***

В данной работе предлагается использовать блоки кодирования в качестве своеобразных пикселей, из которых будет формироваться изображение,

составляющее ЦВЗ. Возможные размеры блока: 4x4 (только в VP9), 8x8, 16x16, 32x32, 64x64. Будем выбирать максимальную величину блока встраивания исходя из разрешения видеопотока, а также из необходимости сохранения ЦВЗ при сжатии его до 240p (некое минимальное разрешение, воспринимаемое человеком как достаточное для просмотра). Допустим, имеем видео с разрешением 1080p. Чтобы усилить устойчивость ЦВЗ к аффинным преобразованиям, увеличим размер блока вдвое. Получаем 1080*2/240 = 9 и округляем в большую сторону. Таким образом, максимальный размер блоков кодирования, используемых для встраивания, составит 16x16 пикселей. Блоки меньшего размера будем использовать аналогичным образом.

И в HEVC, и в VP9 используется цветовая модель, в которой цвет представляется как компонента яркости и две цветоразностных компоненты. Мы будем встраивать ЦВЗ в компоненту яркости, поскольку она ввиду особенностей использования не подвергается сжатию [4]. Необходимо учитывать, что изменения яркости визуально заметны сильнее, чем изменения цветности. Встраивание будем производить следующим образом: накладываем чёрно-белое изображение — ЦВЗ на кадр из видеопотока, а затем заполняем контейнер, уменьшая на шаг дискретизации компоненту яркости в блоках, соответствующих контуру объекта, и увеличивая в соседних блоках (рис. 2). Таким образом, формируем детектируемые локальные экстремумы трёхмерной функции яркости конкретного кадра при отсутствии визуальной заметности.

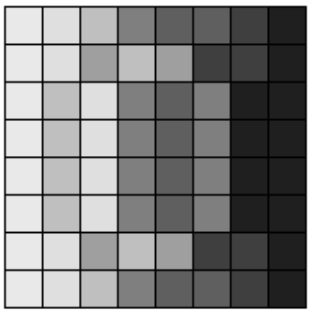


***Рисунок 2. Пример встраивания в градациях серого***

Поскольку мы ограничиваем максимальный размер применяемых блоков, неизбежно приходится сталкиваться с ситуацией, когда полной отрисовке ЦВЗ

в одном кадре мешает большое количество крупных блоков. В этом случае предлагается использовать в детекторе наложение функций яркости нескольких кадров друг на друга, чтобы полностью сформировать ЦВЗ (рис. 3) либо удостовериться в его наличии (рис. 4).

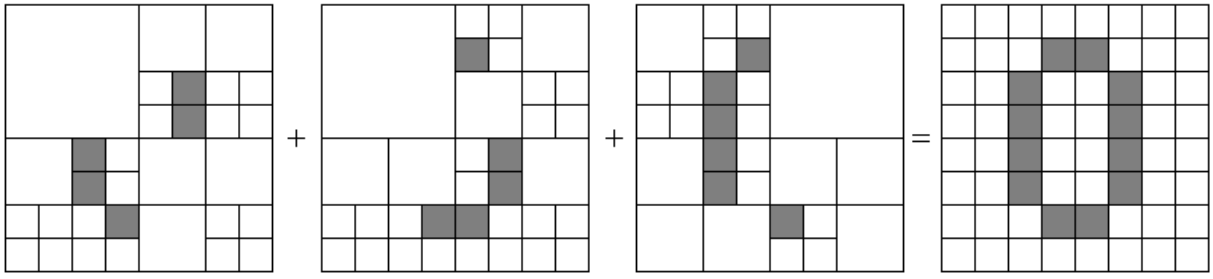


***Рисунок 3. Окончательное формирование ЦВЗ***

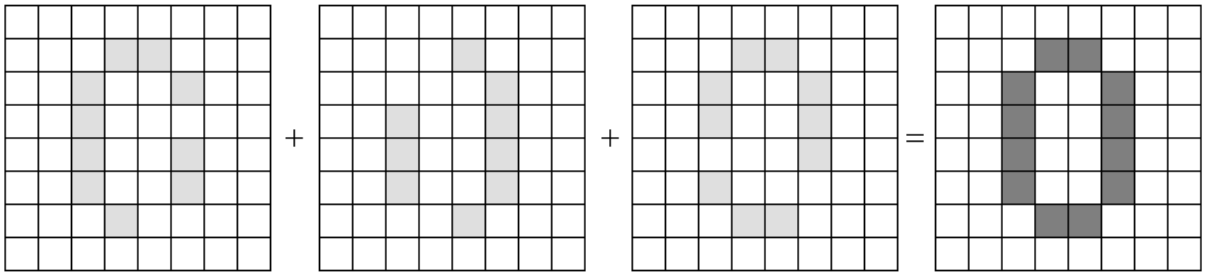


***Рисунок 4. Проверка наличия ЦВЗ***

Несомненным преимуществом предложенного метода является высокая робастность к большинству атак на ЦВЗ. Так, например, внесение шума в высокочастотные составляющие яркости не принесёт ощутимых результатов, поскольку на этапе встраивания в половине случаев изменение яркости влечёт за собой изменение не только нулевого, но и первого разряда. За счёт запаса по выбору размера блока даже при сжатии до 240p блок кодирования, содержащий фрагмент ЦВЗ, не вырождается в пиксель. Таким образом, аффинные преобразования также бесполезны, так как небольшие искажения не повлияют на многопиксельные структуры (минимум 2x2), а существенные преобразования не позволят человеку нормально воспринимать видео. Менее очевидна устойчивость к созданию в контейнере ложных ЦВЗ, однако эта проблема решается с помощью кодирования и шифрования информации, использующейся во встраиваемом сообщении.

Важно, что данный метод позволит внедрять ЦВЗ на этапе предоставления видео конкретному пользователю, поскольку встраивание возможно с помощью модификации уже готового битового потока. Рассмотрим простейший пример. Правообладатель предоставляет контент, используя онлайн-трансляции. Пользователь, желающий посмотреть какое-либо видео, авторизуется под своим именем, вносит плату за просмотр и получает доступ к контенту. С этого момента в каждый видеофайл, предоставляемый этому пользователю, встраивается ЦВЗ, содержащий ссылку на соответствующую строку в базе данных клиентов, дату и время предоставления. Таким образом, в случае несанкционированного распространения правообладатель получает возможность легко вычислить злоумышленника и привлечь его к ответственности.

В настоящее время не существует алгоритмов встраивания ЦВЗ, предназначенных для видеопотоков, сжатых с использованием технологий последнего поколения. Практическая реализация предложенного в данной работе метода встраивания позволит закрыть «дыру» в защите, мешающую правообладателям и распространителям видеоконтента переходить на новые, более эффективные стандарты сжатия, а также в полной мере реализовывать авторские права, увеличив тем самым удобство использования своих сервисов для потребителя.

**Список литературы:**


1. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. М.: СОЛОН-ПРЕСС, 2009. — 272 с.
2. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. К.: МК-ПРЕСС, 2006. — 288 с., ил.
3. Covert and robust mark for media identification: patent 7430302 United States. US 20070019836 A1; filed July, 19, 2006; published Jan, 25, 2007.
4. ITU-T. Recommendation H.265. [Geneva], 2014. — 518 p.
5. Richardson I.E. An introduction to High Efficiency Video Coding (FULL) [electronic resource] / I.E. Richardson. — Electronic data. — Aberdeen: Vcodex Ltd, 2013. — Mode of access: https://www.vcodex.com/press.asp. — Title screen.
6. Sukumaran S. Intra Prediction Efficiency and Performance Comparison of HEVC and VP9: Interim Report / S. Sukumaran. — Electronic data. — Arlington: Univercity of Texas Arlington, 2014. — Mode of access: http://www.slideserve.com/halee-dickson/intra-prediction-efficiency-and-performance-comparison-of-hevc-and-vp9-interim-report. — Title screen.

# МЕТОД ИЗОМОРФИЗМА ГРАФОВ КАК МЕТОД АУТЕНТИФИКАЦИИ В БАНКОВСКИХ СИСТЕМАХ

***Ширинкина Виктория Андреевна***
*студент 3 курса, Электротехнический факультет, ПНИПУ, РФ, г. Пермь*
*Email: shirinkinav@bk.ru*

***Бондаренко Евгения Сергеевна***
*студент 3 курса, Электротехнический факультет, ПНИПУ, РФ, г. Пермь*
*Email: evgeni.zv@gmail.com*

***Кротова Елена Львовна***
*научный руководитель, канд. физ.-мат. наук, доцент ПНИПУ, РФ, г. Пермь*

На сегодняшний день тема обеспечения полной аутентификации в банковских системах является очень актуальной. В наш век глобальной информатизации информация имеет наибольшее значение, чем когда-либо. Система платежей, без которой уже невозможно представить современное общество, по существу является механизмом, через который обязательства, возникающие вследствие связанной с финансами деятельности, исполняются путем перевода денежных средств. Однако, необходимо отметить, что с увеличением ценности информации возникает все больше угроз: ее утраты, нарушения конфиденциальности, целостности и др.

В настоящее время очень развиты банковские системы. Многие утверждают, что гораздо удобнее совершить покупку в интернете, заполнив при этом некоторые реквизиты, чем ездить по городу, или даже по странам, в поисках необходимой вещи и расплачиваться наличными деньгами. Если на мгновение представить, что банковские системы будут легко уязвимы, то все счета, все вклады могут обнулиться, произойдут безвозвратные потери. Очевидно, что очень важны методы и качество защиты этих банковских систем.

Для начала рассмотрим структуру платежной системы. В ней можно выделить трех участников: пользователи (предприятия и частные лица),

посредники (коммерческие банки, осуществляют перевод финансовых средств) и Центральный банк (придает финансовым процедурам завершенность).

В процессе обработки и хранения банковских данных практически не применяются *криптографические методы* для защиты от различных угроз, а так же на всех этапах ее обработки, хранения и передачи. Однако, активное использование этих методов могло бы значительно повысить эффективность банковских систем.

Основная задача криптографии — защитить и сохранить в тайне требуемую информацию (в переводе с греческого языка слово криптография означает *тайнопись*).

Технологии в области криптографии предлагают четыре основных вида услуг в банковской сфере: *аутентификацию*, *целостность*, *конфиденциальность* и *контроль участников взаимодействия*.

Криптография превращает сообщения в недоступный для понимания противником (персоной, не имеющей прав на ознакомление с содержанием передаваемой информации) вид. При этом обычно считается, что злоумышленник может не только перехватывать передаваемые по каналу связи сообщения для последующего их использования, но и нарочно изменять их, а также отправлять подменные сообщения от имени одного из пользователей.

*Аутентификация пользователя* — это процесс проверки, на самом деле ли проверяемый пользователь является тем, за кого он себя хочет выдать. Для правильной аутентификации пользователя необходимо, чтобы пользователь предоставил аутентификационную информацию — некоторую единственную в своем роде информацию, обладателем которой должен быть только он и никто другой [2].

На данный момент существует множество способов аутентификации пользователей. Вот некоторые из них:

- пароли;
- специфические механизмы привязки к мобильным устройствам;
- механизм «запрос-ответ» и др.;

Выбор аутентификационного метода определяется тремя основными условиями: требованием к защищенности системы, простоте в использовании и ресурсоемкостью.

Существует так же еще один метод аутентификации пользователей в банковской системе, а именно — ***метод изоморфизмов графов***. Рассмотрим этот метод более подробно. Он основан на множестве *изоморфных графов* и *доказательстве с нулевым разглашением*, который заключается в следующем: проверяющий не получает в результате выполнения протокола никакой полезной для себя дополнительной информации, за исключением единственного факта, что утверждение истинно (свойство нулевого разглашения).

Рассмотрим определение свойства изоморфизма графов. Графы $G=(V,U)$ и $G'=(V',U')$ изоморфны, если существует такое взаимно однозначное соответствие между множествами их вершин $V$ и $V'$, что вершины соединены ребрами в одном из графов только тогда, когда соответствующие им вершины соединены в другом графе.

Если графы $G$ и $H$ изоморфны, то пишут $G$ р $H$ (тогда и $H$ р $G$). Изоморфные графы обычно принимают подобными и их можно изображать одним и тем же рисунком. Они могут различаться только обозначениями вершин и ребер, и так как их число должно быть одинаковым, соответствующие друг другу вершины обязаны иметь одинаковое количество входящих в них ребер. Следует заметить, что совершенно не имеет значения, какой именно графической реализацией отображать граф [1].

На основании свойства изоморфности графов существует криптографический протокол аутентификации — ***протокол IG*** *(Isomorphism Graph)*.

Опишем его суть:

Допустим, что $\varphi$ — это изоморфизм между двумя графами $G_1$ и $G_0$. Выберем двух участников процесса — *претендент* $P$ и *верификатор* $V$. Претендент — тот, кто хочет пройти аутентификацию, а верификатор — тот, кто проверяет подлинность претендента. Следующие четыре шага выполняются в цикле $n$ раз, каждый раз с независимыми случайными величинами.

1. Претендент P выбирает случайную перестановку $\pi$ на множестве $U$, вычисляет $H=\pi G_1$ и отправляет этот граф верификатору V.

2. P генерирует случайный бит $\alpha$ и передает его V.

3. В случае, когда $\alpha=1$, P посылает V перестановку $\pi$, иначе — перестановку $\pi \cdot \varphi$.

4. В случае, когда перестановка, принятая V, не представляет собой изоморфизм между $G_\alpha$ и $H$, то V прекращает свое действие и отрицает доказательство. В другом случае выполнение этих четырех шагов продолжается еще $m$ раз. Если проверки четвертого шага дали положительный результат во всех $m$ раз, то V принимает доказательство.

Полнота протокола IG очевидна. Чтобы доказать правильность, необходимо лишь сказать, что выбираемый V на втором шаге бит, указывает P, для которого из графов — $G_0$ или $G_1$ — требуется предоставить изоморфизм с графом $H$. В случае, когда нельзя сказать, что графы $G_0$ и $G_1$ изоморфны, то граф $H$ может быть изоморфен, по крайней мере, одному из них. Поэтому проверка четвертого шага даст положительный результат с вероятностью меньше или равной 0,5 в одном цикле и с вероятностью меньше или равной единице, деленной на два в степени $m$, во всех $m$ циклах. Отметим, что основной задачей V является получение максимально возможной информации об изоморфизме между графами $G_0$ и $G_1$ [4, с. 37].

Рассмотрим практическое приложение протокола IG в качестве способа аутентификации.

Представим следующую ситуацию. Участвуют два элемента — Алиса и Боб. Алиса — это интеллектуальная банковская карточка, в ней осуществлена последовательность действий P, а Боб — это компьютер банка, выполняющий программу V. Не имеет смысла доказывать, что два графа изоморфны, важно лишь то, что и является целью Алисы — доказать, что именно она знает изоморфизм $\varphi$. До начала выполнения любых банковских операций, банк удостоверяется в действительности карточки и определяет, истинный ли ее владелец участвует в операции, или, другими словами, карточка должна

пройти аутентификацию. Один из вариантов — использование протокола IG. При данных условиях, в банковском компьютере хранятся два графа ($G_0$, $G_1$), соотнесенных Алиса, а на интеллектуальной карточке — те же графы, изоморфизм $\varphi$. Считается, что только Алиса обладает информацией об этом изоморфизме (возможно, за исключением Боб), и, следовательно, с помощью протокола IG карточка доказывает свою аутентичность банковскому компьютеру. При этом важно учесть, что свойство полноты подразумевает тот факт, что карточка определенно докажет компьютеру свою аутентичность.

Предположим, имеет место тот факт, что карточка является поддельной. Для этого случая можно сказать, что свойство правильности оберегает интересы банка от злоумышленника, который не является клиентом банка и пытается пройти аутентификацию, используя поддельную карточку. Злоумышленник, получив одно или более выполнений протокола аутентификации данной карточки, пытается пройти аутентификацию под именем Алисы. Свойство нулевого разглашения позволяет клиенту быть защищенным от противника.

Важно отметить, что в случае применения протокола IG на практике очень важным свойством является то, что алгоритм P, получивший в качестве дополнительного входа изоморфизм $\varphi$, работает за полиномиальное время. Данный протокол можно заменить, вообще говоря, любым другим протоколом с доказательством нулевого разглашения, в котором алгоритм P обладает этим свойством. Но, к сожалению, на практике этот метод не реализуется и рассматривается исключительно как теоретический. Для реальных приложений протокол IG, как и большинство подобных протоколов, не эффективен и активно подвергается угрозам: слишком большое количество циклов, очень длинные сообщения, злоумышленник может имитировать лицо, которое на самом деле обладает информацией и т. д. Таким образом, можно подытожить, что поиск более действенных и обоснованно стойких протоколов — одно из главных направлений исследовании в этой области — области аутентификации в банковских системах.

**Список литературы:**


1. Лекция 12. Графы [Электронный ресурс] — Режим доступа. — URL: http://vuz.exponenta.ru — URL: http://vuz.exponenta.ru/PDF/L12.html (дата обращения 23.05.2015)
2. Методы аутентификации [электронный ресурс] http://www.iso27000.ru — [Электронный ресурс] — Режим доступа. — URL: http://www.iso27000.ru/chitalnyi-zai/kriptografiya/metody-autentifikacii (дата обращения 13.05.2025)
3. Технологии безопасности данных в банковских сетях [электронный ресурс]http://eos.ibi.spb.ru — [Электронный ресурс] — Режим доступа. — URL: http://eos.ibi.spb.ru/umk/5_14/5/5_R0_T2.html#2_3_2 (дата обращения 13.05.2015)
4. Ященко В.В. Введение в криптографию 3-е издание., доп. М.:МЦНМО: “ЧеРо”, 2000. — 37 с.

# СЕКЦИЯ 2.

# КОСМОС, АВИАЦИЯ

## ОРБИТАЛЬНЫЙ КОМПЛЕКС ПО ОБСЛУЖИВАНИЮ ЛУННЫХ КОСМИЧЕСКИХ АППАРАТОВ НА ОКОЛОЗЕМНОЙ ОРБИТЕ

***Ли Ян Евгеньевич***
*студент 4 курса, кафедра «Конструкция и испытания летательных аппаратов» филиала «Восход» МАИ,*
*РФ, г. Байконур*
*E. mail: fan2mas@list.ru*

***Нуртаева Шынар Бахитбековна***
*студент 4 курса, кафедра «Конструкция и испытания летательных аппаратов» филиала «Восход» МАИ,*
*РФ, г. Байконур*
*E-mail: shinara.nurtaeva@mail.ru*

***Абильдаева Кенжегуль Жалгасбаевна***
*научный руководитель, старший преподаватель кафедры Б11 — «Конструкция и испытание летательных аппаратов» филиала «Восход» МАИ,*
*РФ, г. Байконур*

Основные задачи для решения, которых создается комплекс

- проведение обслуживания лунных космических аппаратов, включая орбитальный комплекс обслуживания;
- использование орбитального комплекса для монтажа и строительства на ОЗО лунных КА в беспилотном и пилотируемом вариантах;
- проведение ремонтных и регламентных работ и операций обслуживания на орбите ИСЗ крупногабаритных КА и др.;
- осуществление стартов орбитального комплекса лунных кораблей и других аппаратов и приема при возвращении космонавтов и различных грузов на Землю;
- проведение фундаментальных и прикладных исследований на борту орбитального комплекса;

• использование комплекса в различных коммерческих программах, в то числе для проведения туристических полетов на орбиты Земли и Луны;

• выполнение совместных космических программ с другими государствами.

По принятой концепции орбитальный комплекс (ОК) должен осуществлять захват и перенос специальными приспособлениями грузов, доставляемых транспортными космическими аппаратами (ТКА) к местам монтажа и сборки. При этом должен обеспечиваться комфорт для космонавтов, учитывая сложность и трудоемкость проводимых ими работ. Стандартный экипаж (сменный) ОК должен составлять 3—5 человек.

В связи с этим, мы предлагаем следующий облик орбитального комплекса.

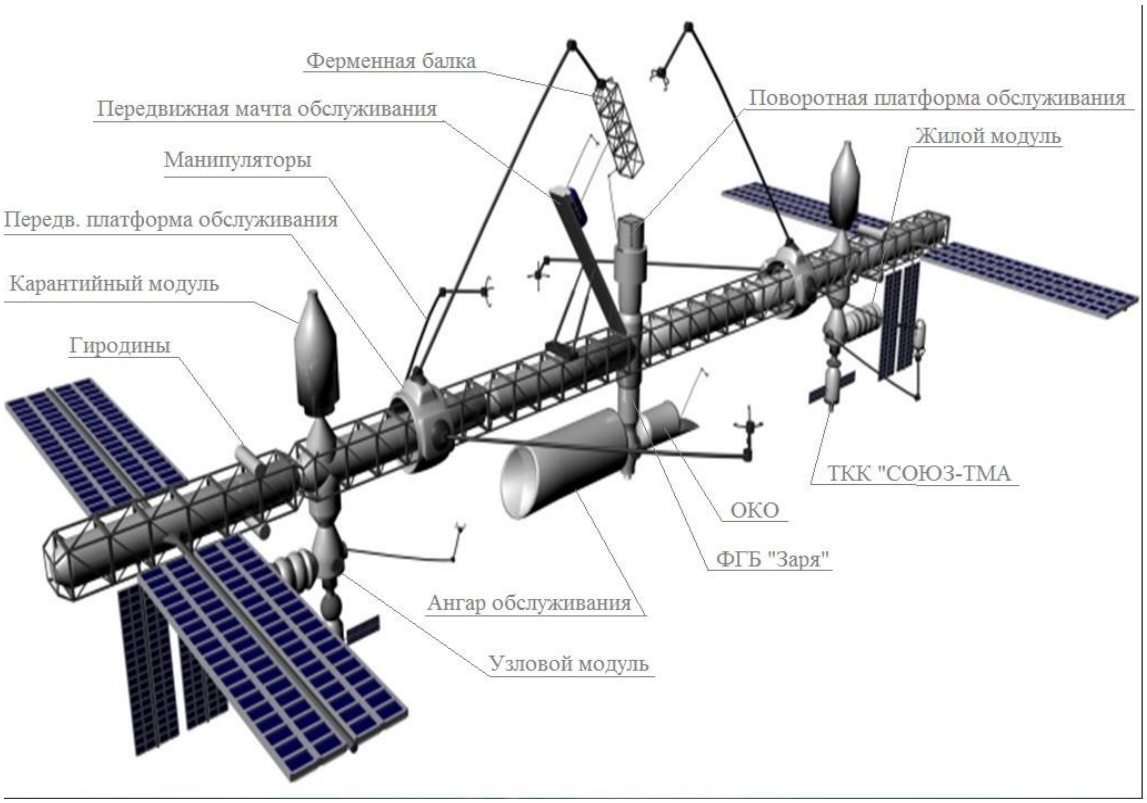



***Рисунок 1. Облик орбитального комплекса***

• **КАС** предназначен для доставки экипажей на орбитальный комплекс, возвращение их на Землю, а также покидание комплекса в аварийных ситуациях, смены экипажей космическими кораблями типа «Союз-ТМА»;

ППТС (перспективная пилотируемая транспортная система) или КК «Орион» (США) соответственно массой 7 т, 14,5 т, 15 т.

- **Жилой модуль** является тем элементом комплекса, в котором космонавты отдыхают и принимают пищу. Жилой модуль представляет собой аналог российского сегмента МКС «ФГБ» (функционально-габаритный блок) с шаровым модулем с пятью стыковочными узлами. Масса 19 т, длина 16 м.

- **Ресурсный модуль** предназначен для обеспечения ОК всеми расходными материалами и служит сегментом для стыковки и сборки, монтажа космических объектов.

- **Лабораторный модуль** (типа «МЛМ» российский сегмент МКС) со стыковочными узлами для приема транспортных космических кораблей (ТПК «Союз-ТМА; ТГК «Прогресс-М») и других модулей. Предусматривает создание в одном комплексе оборудования для проведения широкого спектра исследований. Модуль представляет аналог ФГБ-1 «Заря» длиной 13 м, массой 20 т.

- **Модуль космического мониторинга и управления (МКМУ)** служит для ориентации стабилизации и управления ОК, изучения и наблюдения за динамикой управления положением всего комплекса. Данный модуль представляет собой аналог российского сегмента МКС (служебного модуля с двумя стыковочными узлами длиной 13 м, массой 20 т.)

- **Основная монтажная ферменная конструкция** предназначена для монтажа и сборки космических объектов. Общая длина фермы 72 метра.

- **Ферменная балка с системой электропитания** служит для обеспечения электроэнергией всего комплекса. На ОК предусмотрены две ферменные балки с СЭП. Масса одной балки с СЭП — 8 т.

**Транспортное обеспечение**

Как уже было упомянуто выше, ОК представляет собой конструкцию, которую невозможно за раз вывести на орбиту. Поэтому вся конструкция разделена на блоки, которые по отдельности выводятся на ОЗО и там уже

монтируются в одну единую конструкцию. Сборка ОК начинается с выведения на ОЗО с жилого модуля ФГБ «Заря» РН «Протон» массой 19 т.

Следующим запусками РН «Ангара -5» на орбиту выводятся ресурсные модули массой по 25 т. каждый. Ферменные конструкции массой 35 т. выводятся двумя последующими пусками РН «Протон-М». Далее, предусматривается выведение на ОЗО составляющих ОК: жилые модули типа российского сегмента МКС «ФГБ» массой по 19 т и лабораторные модули типа МЛМ российского сегмента МКС по 20 тонн каждый. Кроме того, к уже собранным ферменным конструкциям пристыковываются ферменные балки с СЭП по 8 т. каждая. Последними на орбиту доставляются ОКО и МКМУ.

Таким образом, после завершения серий пусков, вся система технических средств полностью вводится в строй. Далее, орбитальный комплекс обслуживается полетами ТКА типа «Союз–ТМА, ТГК «Прогресс-М», ППТК (Россия), КК «Орион» (США) и другими средствами.

**Ферменные конструкции**

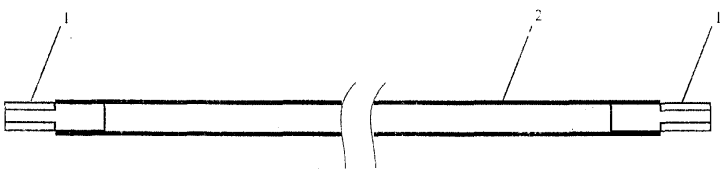



***Рисунок 2. Схема ферменной трубки: 1 — наконечник с резьбой; 2 — графитопластиковая трубка***

Исходя из массо-прочностных характеристик, в качестве материала для ферменных конструкций был выбран эпоксидный графитопластик AS-1/3501-6 ф-мы Hercules Aerospace Company.

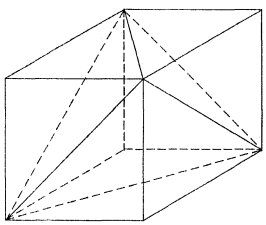


***Рисунок 3. Основа ферменной конструкции***

Основой ферменной конструкции является куб со сторонами 3 м, из труб диаметром 5 см и толщиной стенок 6 мм. На концах каждой трубки крепится наконечник (с резьбой из стали AISI-301 EH), работающий при широком диапазоне температур от 80 до 700 К и обладающий не меньшей прочностью. Наконечники крепятся в трубе на клею (FM-123-2 ф-мы American Ciamid). Они предназначены для присоединения трубок между собой путем вкручивания в специальные узловые элементы. Каждая труба выдерживает нагрузку на растяжение 1377,6 кН. Удельная масса ферменной конструкции 40,45 кг/м. Общая длина ферменной конструкции 72 метра, масса около 40 т.

Основой орбитального комплекса по сборке и обслуживанию на ОЗО лунных космических аппаратов для полетов на Луну является основная ферменная монтажная конструкция. Она предназначена для установки, монтажа и сборки космических кораблей крупных размеров.

Сама конструкция представляет собой ферменную балку в виде треугольной конструкции длиной 70 метров.

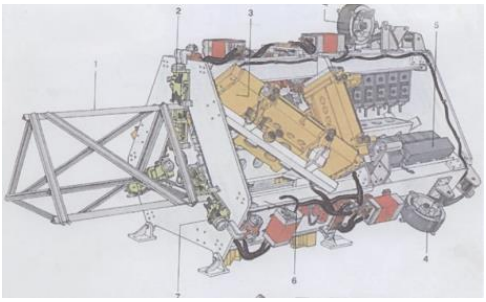


***Рисунок 4. Сборочный модуль***

На верхней поверхности ферменной балки располагается мобильный сборочный модуль. Платформа «передвигается» по рельсам ферменной балки и обслуживает строящийся космический корабль. На ней предусмотрены манипуляторы-рукава, с различной длиной: 15 м, 20 м, 30 м, со специальными захватами, приспособлениями для фиксации конструкций.

В конструктивном плане модуль представляет собой совокупность двух взаимосвязанных объектов: агрегатного и герметичного.

**Другие технические средства**

Основой комплекса обслуживания является ферменная конструкция длиной 72 метра четырехугольной конструкции. Посередине размещается стапель-конструкция захватным устройством и поворотным столом с разворотом на 360 градусов строящегося космического аппарата.

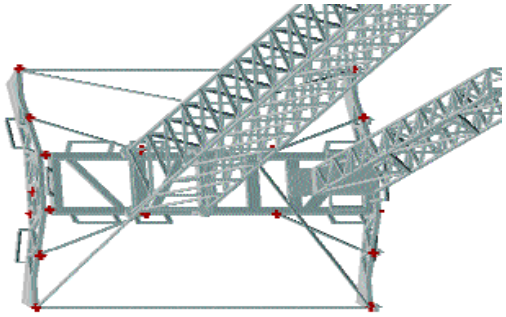


***Рисунок 5. Поворотный стол***

Снизу размещается модули обслуживания с робототехническим комплексом. Также, там же в перспективе будут размещены герметичные ангары и негерметичные платформы для обслуживания КА. Впоследствии при осуществлении миссии на другие планеты здесь же могут быть размещены карантинные модули.

На концах ферменной конструкции размещены жилые модули, предназначенные для посещения экипажами космических кораблей, для приема ПН, предназначенные для постройки межпланетных кораблей. Завершают архитектуру комплекса сегменты ферменной конструкции с СЭП.

С правой стороны, от центра по рельсам перемещаются вдоль фермы мобильные центры обслуживания. Они используются для перемещения ПН от места отправки к месту строительства КА.

С левой стороны, впервые, используются для обслуживания строящегося КА мачта обслуживания с кабинами, постами управления и мобильными системами обслуживания. Мачта обслуживания может с горизонтального положения, развёрнута вертикальное положение, т.е. этим достигается доступ обслуживающего персонала к КА. Сбоку и снизу располагаются рельсы для

мобильных средств (платформы, дистанционно-управляемые средства, робототехнические комплексы).

На стапеле, вращающемся столе планируется сборка лунных и марсианских кораблей (ЛДОС, ЛГТК, УСП, ЛЭК, МЭК, АГК).

**Телеуправляемые космические роботы (ТКР)**

Планируется использовать свободно летающий ТКР FTS (Martin Marietta), спроектированный по контракту с центром космических полетов NASA им. Годдарда, ТКР имеет антропоморфический корпус (подобный телу человека), к которому крепятся два электромеханических манипулятора, каждый имеет форму человеческой руки; третья рука используется для фиксации ТКР на рабочем месте. Система обзора ТКР включает четыре телекамеры. Концевые приспособления манипуляторов снабжены металлическими защелками, а также датчиком усилий.

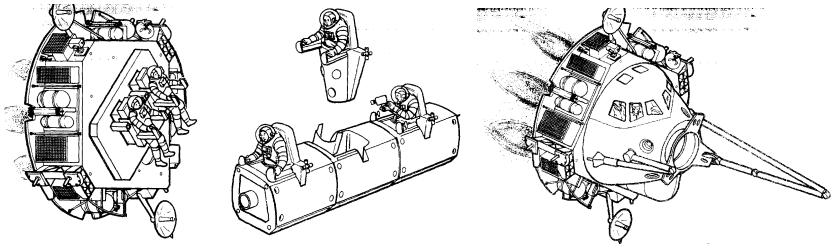


***Рисунок 6. Свободнолетающие ТКР, управляемые космонавтами***

Другой тип ТКР, представляет собой электромеханический манипулятор целевого назначения с дистанционным управлением (телеробот), по которому подразумевается либо дистанционное управление космонавтом-оператором под его непосредственным наблюдением (супервизирование), либо работа в автоматическом режиме по заданной программе.

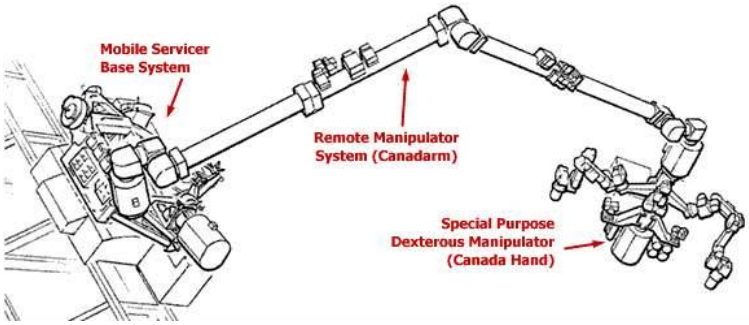



***Рисунок 7. Рука-манипулятор***

**Мобильная система обслуживания**

Разрабатываемая канадскими специалистами мобильная система обслуживания MSS. Представляет собой более сложный и многоцелевой объект.

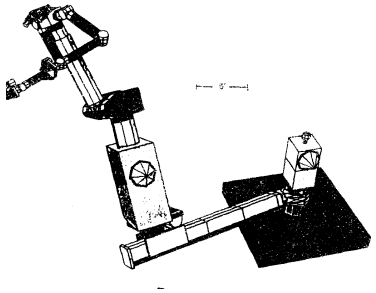


***Рисунок 8. Робот-сервисер***

Его основными компонентами являются транспортёр MT, перемещающийся вдоль несущей конструкции орбитального комплекса, соответственно центр обслуживания MSC, который может устанавливаться на транспортёре с помощью стыковочного узла, а также дистанционный манипулятор SSRMS, для повышения возможности последнего на его рабочем конце впоследствии может быть установлен дополнительный манипулятор SPDM .

**Раздвижная ферма обслуживания**

Как мы знаем, ферма обслуживания используется на стартовых комплексах (СК Бармина РН «Союз», РН «Протон» и др. РН). С помощью ферм обслуживания осуществляется доступ персонала по обслуживанию РН.

От центра, от базового блока, слева от орбитального комплекса, планируется поместить ферму обслуживания, которая в исходном положении «лежит» на ферменных конструкциях. В рабочее положение ферма обслуживания устанавливается вертикально. Для удобства и целесообразности при обслуживании персоналом и робототехническими средствами строящегося, например лунного корабля, ферма обслуживания может «находиться» от 2-х до 6 метров от ПН. Создаваемое пространство, позволяет персоналу свободно принимать решения, собирать и перемещать, перестраивать объекты (узлы, детали, блоки, конструкции). Кроме того, ферма обслуживания может

раздвигаться до нужной длины от 8 до 30 метров. Габариты в сложенном виде 8 м х 4 м х 2 м.

На ферме обслуживания планируется разместить специальные кабины обслуживания, посты обслуживания с канадскими манипуляторами, которые могут подстраиваться к любому узлу строящегося космического корабля. (Например, при установке баков с рабочим телом в районе между РММ и секцией с ПН). В рабочем порядке, по регламенту, соединение бака к космическому кораблю осуществляется космонавтом, космонавтом-оператором и телеуправляемым роботом.

Посты обслуживания и кабины обслуживания могут быть герметичными и негерметичными.

**Ангары обслуживания**

Размеры ангара обеспечивает размещение большинства существующих и проектируемых КА. Ангар присоединяется в нижней части орбитального комплекса к рабочим модулям, присоединенным к стапелю-конструкции. По всей длине негерметичного ангара имеются герметизированные проходы, проходы диаметром по 3 м, обеспечивающие переход экипажей без скафандров из обитаемых модулей в кабины КА, пристыкованных к внешним узлам. По этим проходам операторы могут переходить для работы в мобильные герметизированные кабины, пристыкованные к узлам проходов или перемещаемых с помощью ангарных манипуляторов.

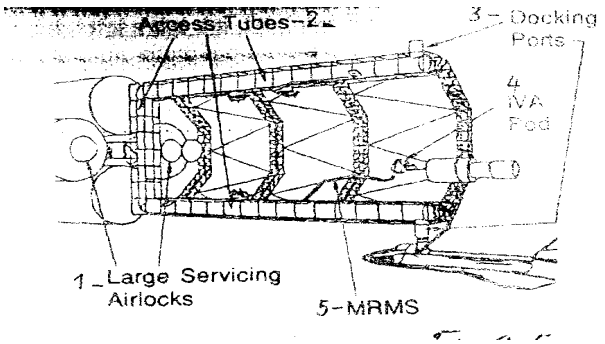



***Рисунок 9. Ангар***

Проектом предусмотрено использование четырех таких кабин, которые могут применяться в любой зоне ангара. Мобильность кабины обеспечивается

установкой ее на конце мощного манипулятора, перемещающегося по рельсам вдоль стенки ангара. Для непосредственного обслуживания объекта кабина оснащается собственными манипуляторами с набором сенсорных и эффекторных средств, управляемых оператором из кабины.

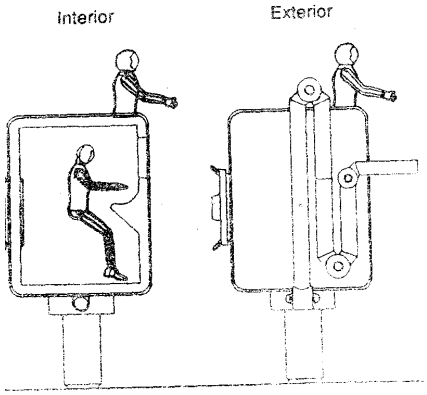



***Рисунок 10. Мобильная система обслуживания***

При этом, в отличие от процедур надевания скафандра и подготовки оператора к внекорабельной деятельности, технология использования встроенного полускафандра может быть упрощена. Предусматривается, в частности, применение автоматических привязных для надувных элементов фиксации торса оператора в полускафандре.

**Требования ДУ комплекса обслуживания**

Основной задачей ДУ является обеспечение импульса тяги для поддержания орбиты и управления пространственным положением комплекса. Среди других задач можно указать на использование ДУ для сближения и стыковки с другими космическими объектами, предотвращения столкновения с другими объектами.

Планируется использование кислородно-водородных двигателей, использующие в качестве компонентов топлива продукты электролиза воды, а также электротермические ДУ малой тяги, использующих в качестве компонентов продукты утилизации отходов других систем. Кислородно-водородные двигатели, рассчитанные на 10-летний период должны быть рассчитаны на импульс тяги $67 \cdot 10^6$ Н·с.

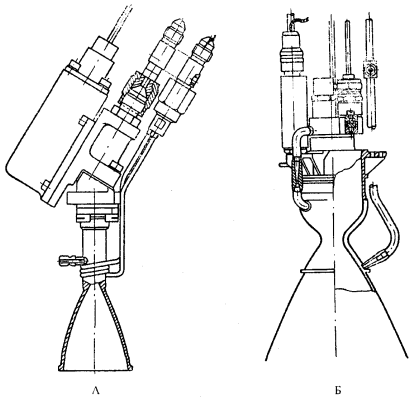


***Рисунок 11. ДУ малой тяги***

Прототип $O_2$–$H_2$ двигателя уже прошел испытания. Конструктивное исполнение базового варианта ДУ закладывается в виде четырех независимых блоков, кислородно-водородных двигателей.

Каждый блок включает в себя девять двигателей, баллоны высокого давления с газообразным $O_2$ и $H_2$ и соответствующие клапаны и устройства управление. Трубопроводы соединяют баллоны с компонентами топлива каждого блока с центральным агрегатом производства $O_2$ и $H_2$. Блоки предполагается разместить на двух противоположенных направлениях в МКМУ по два. При этом три двигателя в каждом блоке работают для обеспечения маневра по изменению высоты, а остальные – для управления положением вокруг центра масс.

**СЭП с оптимальными батареями (СБ)**

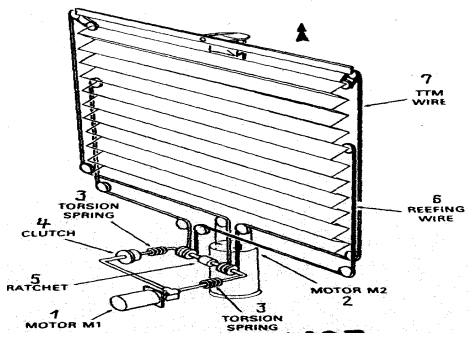



***Рисунок 12. Раздвижная мачта СБ: где, 1,2 — двигатели, 3 — пружины кручения, 4 — механизм сцепления, 5 — храповый механизм, 6 — рифовый трос, 7 — трос механизма перемещения верхней плоскости панели***

Более приемлемым для орбитального комплекса является солнечная батарея, которая в настоящее время эксплуатируется на борту МКС.

Раздвижная мачта, состоящая из трех эластичных свернутых в кольцо лонжеронов, стальных стержней и растяжек.

При выборе типа фотоэлементов (ФЭП) более подходит арсенид гелия. Для подкладки подложки из двух слоев пленки “кэптон” толщиной 25,4 мкм каждый, соединенных адгезионной пленкой из под. полиэстера такой же толщины. Между ними находится печатная схема из меди толщиной 35,4 мкм, выводы которой припаиваются к ФЭП, что обеспечивает высокую технологичность процесса сборки батарей и возможности сворачивания элементов ФЭП в трубу.

В качестве накопления электроэнергии, на борту комплекса предпочитается использовать никель-водородные аккумуляторы емкостью до 300 А·ч, числом разряд-заряд — 700—1000 циклов при глубине разряда до 80 % за суммарное время эксплуатации до 7—10 лет.

**Вывод**

На сегодняшний день одной из приоритетных задач развития космонавтики не только в России, но и ряда других стран Европы, является освоение Луны. В России, например, планируют построить обитаемую базу и постепенно разместить испытательные полигоны для накопления и передачи энергии на расстояние, для испытаний новых двигателей. Поэтому первоочередной задачей, является программа по освоению планет Солнечной системы.

Нами был представлен проект орбитального комплекса по сборке и обслуживанию на околоземной орбите космических аппаратов.

Мы считаем, что задачи для решения, которых создается комплекс, вполне адекватны и могут быть оправданы. Луна уже изученная планета. Своими имеющимися свойствами (глубокий вакуум, низкая гравитация, дешевая солнечная энергия и т. д.) она привлекает человечество для более глубоких исследований в области астрономии, металлургической промышленности, электроники.

Разрабатываемый проект является актуальным и перспективным. Ведь дальнейшее освоение и масштабное проникновение человечества на Луну, позволит глубоко изучить дальние области Вселенной.

**Список литературы:**


1. Андреянов В.В. и др. Автоматические планетные станции. М.: Наука, 1993. — 289 с.
2. Иванов Н.М. Управление движением КА к Луне. М.: Наука, 2003. — 219 с.
3. Марленский А.Д. Основы космонавтики. – М.: Просвещение, 1989. — 349 с.
4. Сердюк В.К. и др. Транспортные средства обеспечения космических программ. М.: ВИНИТИ. Итоги и науки, 1990. — 418 с.
5. Эрике-Краффт. Будущее космической индустрии. М.: Машиностроение, 1988 г. — 518 с.

# СЕКЦИЯ 3.

# МОДЕЛИРОВАНИЕ

## МОДЕЛИРОВАНИЕ ТРАЕКТОРИЙ НАВЕДЕНИЯ РАКЕТ РАЗЛИЧНЫМИ МЕТОДАМИ

***Клименко Владислав Николаевич***
*студент 3 курса, кафедра радиоэлектронных и телекоммуникационных систем ИРИТ-РТФ УрФУ, РФ, г. Екатеринбург*
*E-mail: Vlad55588@yandex.ru*

***Самусевич Галина Александровна***
*научный руководитель, доцент, канд. тех. наук, ИРИТ-РТФ УрФУ, РФ, г. Екатеринбург*

В настоящее время широкое развитие вычислительной техники позволяет производить моделирование различных процессов в режиме реального времени.

Задача наведения ракеты на цель заключается в сближении ракеты с целью, то есть в совмещении их координат. Она решается с помощью различных методов наведения, определяющих требуемый закон движения ракеты. Наведение ракеты на цель решает сложный комплекс взаимосвязанных устройств. В него входит сама ракета с ее динамическими характеристиками, устройства, которые определяют положение ракеты и цели в пространстве, системы передачи информации и другие. Имеется большое разнообразие типов ракет, обусловленное различием типов целей (воздушные, наземные, морские), диапазоном их скоростей и особенностей тех ситуаций, в которых происходит преследование цели.

Процесс наведения ракеты на цель можно разделить на три основных этапа:

- Этап доставки ракеты в район расположения цели начинается с момента старта ракеты и продолжается до достижения ракетой заранее заданного расстояния до цели

- Этап наведения ракеты на цель
- Этап поражения цели, который начинается с некоторого расстояния (радиус мертвой зоны), когда отключается система управления и ракета летит по прямой. Минимальное расстояние до цели определяет промах ракеты.

Законы наведения ракеты на цель:

- Метод погони

При этом методе ракета всегда подходит к цели с хвоста независимо от направления скоростей ракеты и цели перед пуском.

Графический метод построения траектории представлен на Рис. 1. Обозначим точками *Ц0* и *Р0* положения цели и ракеты в момент начала самонаведения. Разобьем траекторию цели на отрезки. Соединим прямой линией точки *Ц0* и *Р0*. Определив отрезок *D1* проходимый ракетой за время t, отложим его на прямой *Ц0Р0*. Положение ракеты в момент времени *t1* характеризует точка *Р1*. Соединим точки *Ц1* и *Р1*, аналогично найдем точку точки *Р2* и т. д. Соединив точки *Р0, Р1, Р2,...*получим кинематическую траекторию метода погони.

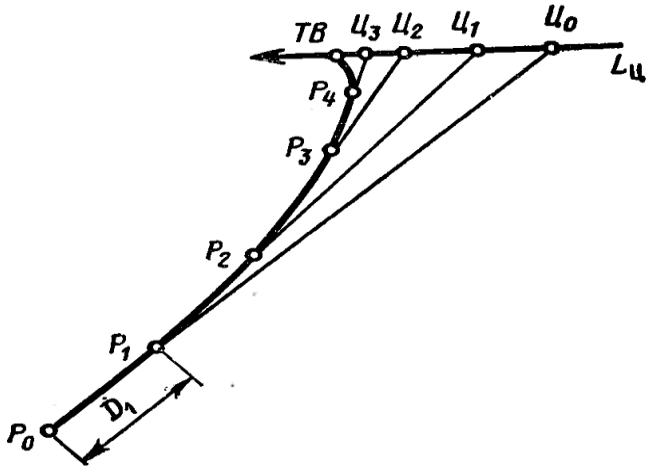



***Рисунок 1. Траектория полета ракеты при методе погони***

- Параллельное сближение

При наведении ракеты на цель по методу параллельного сближения требуемое значение угловой скорости линии ракета-цель равно нулю, т. е. φ=0.

Уравнение метода наведения выражается формулой $\varphi = \varphi_0 = const$

Графический метод построения траектории полета представлен на Рис. 2. Обозначим точками *Ц0* и *Р0* положения цели и ракеты в момент начала самонаведения. Разобьем траекторию цели на отрезки. Для построения кинематической траектории необходимо:

Из точек провести семейство прямых параллельных прямой *Ц0Р0*.

Вычислить отрезки пути, проходимые ракетой за интервалы времени

Для нахождения точки *Р1* найти точку пересечения дуги радиусом *D1* с центром в точке *Р0* с прямой, проходящей через точку *Ц1*. Аналогичным образом строятся *Р2, Р3, Р4, …*

Соединив точки *Р0, Р1, Р2…*получим кинематическую траекторию метода погони.

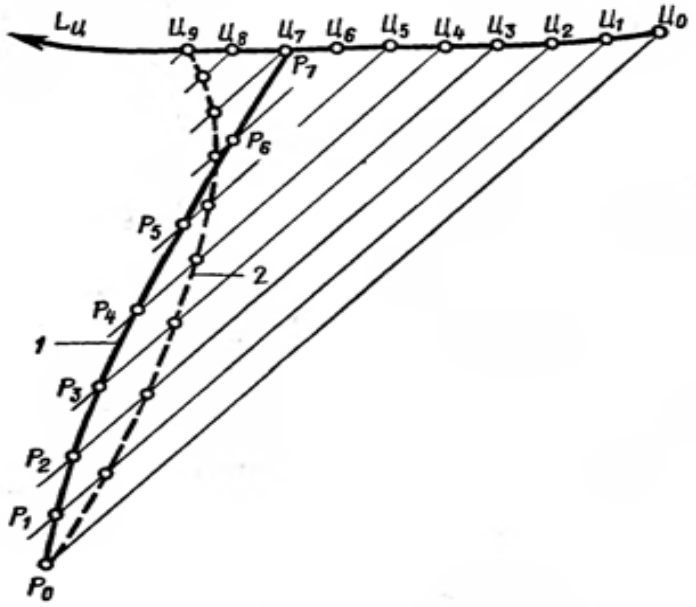



***Рисунок 2. Графическое построение траектории полета ракеты при методе параллельного сближения***

- Метод пропорционального сближения

Уравнение метода наведения выражается формулой $\dot{\theta} = k \cdot \dot{\varphi}$ (Рис. 3.), где $\dot{\theta}$ — угловая скорость поворота вектора скорости ракеты;

$\dot{\varphi}$ — угловая скорость вращения линии ракета-цель;

$k$ — коэффициент пропорциональности (навигационная постоянная);

ее величина изменяется в зависимости от направления атаки; при атаке точно навстречу цели она наибольшая, при атаке в заднюю полусферу — наименьшая; ее значение принимается равным нескольким единицам.

Для реализации метода пропорционального сближения необходимо в каждый момент времени измерять угловую скорость линии ракета-цель и сравнивать ее с угловой скоростью вращения вектора скорости ракеты.

Кинематическая траектория полета ракеты, наводимой на цель по методу пропорционального сближения, характеризуется уравнениями вида:

$$\left.\begin{aligned} \dot{D} &= -V_{Ц}\cos\varphi + V_P\cos(\theta-\varphi) \\ D_{\dot{\varphi}} &= V_{Ц}\sin\varphi - V_P\sin(\theta-\varphi) \end{aligned}\right\}$$

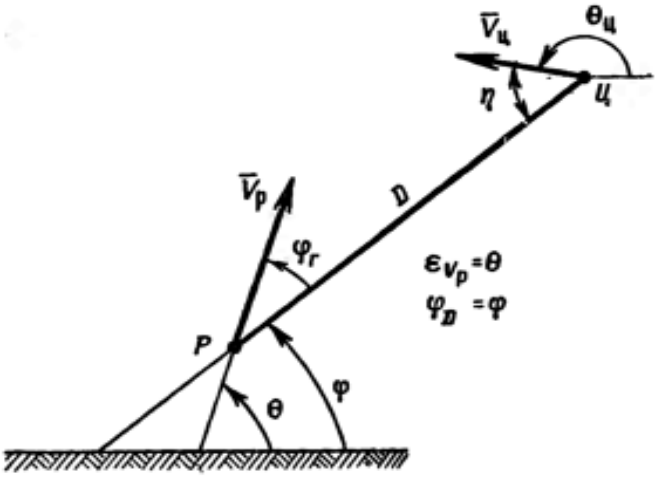



***Рисунок 3. Взаимное положение ракеты и цели***

- Метод упреждения

Этот метод позволяет уменьшить кривизну траектории и тем самым увеличить дальность и точность стрельбы.

Уравнения этого метода:

$$\left.\begin{aligned} \varepsilon_К &= \varepsilon_Ц + C_1 \cdot \Delta r \\ \beta_К &= \beta_Ц + + C_2 \cdot \Delta r \end{aligned}\right\}$$

При задании параметра метода наведения постоянным нельзя уменьшить величину нормального ускорения ракеты для всех возможных параметров движения цели и координат точки встречи.

При отклонении условий стрельбы от заданных кинематическая траектория будет искривляться. (Рис. 4).

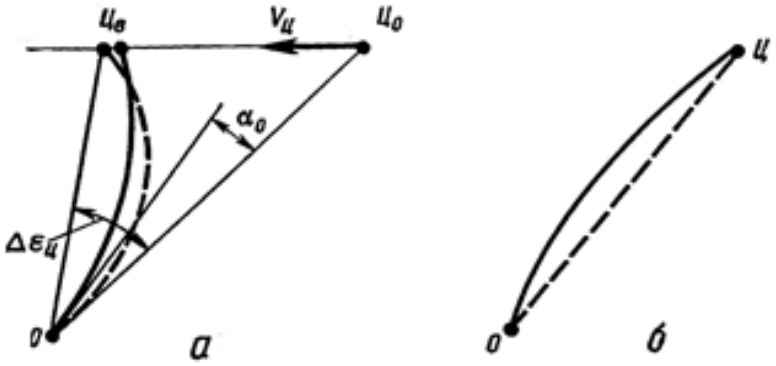



***Рисунок 4. Вид траектории метода упреждения***

Сложность исследования законов наведения заключается в наличии огромного числа параметров, которые влияют на траекторию ракеты и цели. Поэтому некоторые из них идеализируются, тем самым позволяя упростить задачу и выделить влияние оставшихся факторов на характер траектории. Далее будем считать возможным пренебречь влиянием ошибок определения ракеты и цели в пространстве, а также влиянием ошибок в каналах связи.

В данной работе была поставлена задача модернизации программного продукта, который моделирует траекторию наведения ракет на цель методами погони, постоянного угла упреждения и пропорциональной навигации, с визуальным отображением траекторий на экране монитора.

Задача модернизации заключается в следующем:

- разработать удобный для пользователя интерфейс, который поможет даже неподготовленному пользователю смоделировать наведение ракеты на цель
- Обеспечить наглядность и высокую точность расчетов
- позволить использовать программу в качестве лекционной демонстрации, пособия, или лабораторного практикума для изучения вопросов теории наведения ракет для студентов специальности «Радиоэлектронные системы и комплексы».

Программа написана на языке С с использованием алгоритмов численного интегрирования для решения дифференциальных уравнений, описывающих движение цели и ракеты для двух режимов полёта ракеты: кинематического (в соответствие с заданным законом наведения) и некинематического (движение с максимально возможной перегрузкой). Движение цели — прямолинейное, либо по окружности с постоянной нормальной перегрузкой.

Программа позволяет моделировать поведение цели и ракеты в зависимости от начальных параметров, таких как: скорость цели, скорость ракеты, расстояние по линии визирования, угол визирования, ошибка прицеливания, допустимая перегрузка ракеты, коэффициент пропорциональной навигации.

В случае, когда коэффициент пропорциональной навигации равен единице и при соответствующих начальных условиях реализуются законы наведения по кривой погони и с постоянным углом упреждения.

**Список литературы:**

1. Радиосистемы управления: учеб. для вузов / В.А. Вейцель, А.С. Волковский, С.А. Волковский и др. ; под ред. В.А. Вейцеля. М.: Дрофа, 2005. — 416 с.: ил. — (Высшее образование: Радиотехнические системы).

# ВЫПОЛНЕНИЕ ПРЕЗЕНТАЦИИ РАЗРАБОТКИ МЕТОДИКИ ПОСТРОЕНИЯ ТРЕХМЕРНЫХ КОМПЬЮТЕРНЫХ МОДЕЛЕЙ: ПОСТРОЕНИЕ ПРУЖИНЫ

***Крушинская Евгения Александровна***
*студент 1курса кафедры стандартизации и управления качеством, Политехнического института Сибирского федерального университета, РФ, г. Красноярск*
*E-mail: krushinskaya.evgenia@yandex.ru*

***Борисенко Ирина Геннадьевна***
*научный руководитель, доцент кафедры начертательной геометрии и черчения, Политехнического института Сибирского федерального университета, РФ, г. Красноярск*

Современное высокотехнологичное производство требует грамотных специалистов, владеющих современными CAD-технологиями и адаптированными к жизни в быстро меняющемся информационном обществе.

Актуальность работы определяется необходимостью совершенствования графической подготовки студентов, решающей задачи развития у обучаемых пространственного, конструктивного, геометрического, алгоритмического мышления, одновременно создавая условия для развития личности и самореализации члена общества, способного учиться всю жизнь. Инженерную подготовку студента технических специальностей невозможно представить без владения инструментами CAD-систем.

Одним из наиболее эффективных способов при обучении инженерной графике является сотрудничество, или совместная деятельность преподавателя и студента в ходе образовательного процесса, направленное на усвоение знаний, навыков и умений будущих инженеров и, несомненно, повышающее их мотивацию к обучению [3]. При таком сотрудничестве роль студента из пассивного ученика меняется на активную учебную и творческую деятельность, связанную с решением проблемных задач. Студент в результате совместной работы с преподавателем усваивает дополнительную информацию вместе с учебным материалом на качественно более высоком уровне.

Наиболее удачным примером совместной работы преподавателя и студента является создание более «продвинутыми» студентами тематических презентаций и видеоуроков, которые в последствии будут использоваться в процессе обучения при чтении лекций, проведения практических занятий, а так же как дополнительный материал в ЭОК при самостоятельной работе студентов, испытывающих затруднения в обучении. Ведь в настоящее время около 80 % поступающих в технические вузы, не изучали в школе черчение, не обладают пространственным представлением, не умеют работать самостоятельно [2—4].

Рассмотрим пример презентаций по элементу, вызывающему у студентов затруднения, это построение пружины резьбы. Методика создания моделей пружины основана на построении винтовой линии, построении образующего контура и использовании винтовой линии в качестве пространственной траектории, двигаясь по направлению которой, образующий контур формирует трехмерную твердотельную модель винтового изделия или его части. Создание методики решения подобных задач с использованием слайдов с поэтапным построением существенно облегчает задачу обучения студентов решению подобных задач.

*Построение пружины.*

1. В Дереве модели выбираем плоскость (XY,ZX,ZY), в которой будет построена спираль (рис. 1, *а*).

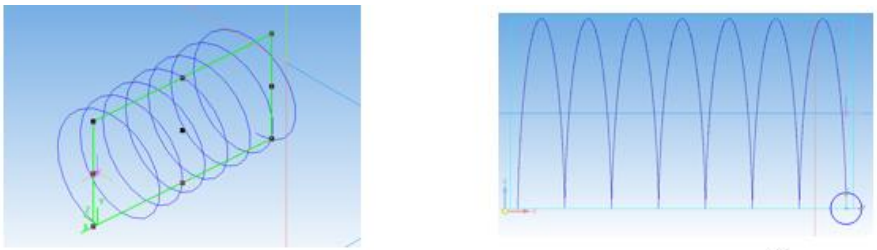
2. На панели Пространственные кривые выбираем команду «Спираль цилиндрическая» и задаем параметры спирали (рис. 1, *б*).

3. С помощью команды «Плоскость» через вершину перпендикулярно ребру на панели «Вспомогательная плоскость» проводим плоскость через конечную точку спирали (рис. 2, *а*).

*а* *б*

***Рисунок 1. Построение пружины***

4. Теперь строим эскиз сечения — например, окружность диаметром 2 мм: чтобы витки пружины не касались. Для этого выделяем плоскость ZX, строим на ней эскиз окружности с центром в начальной точке спирали (рис. 2, *б*).



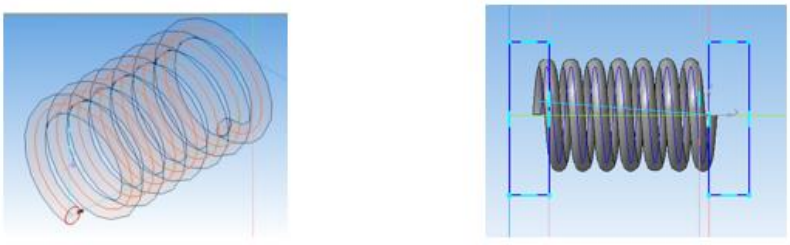
*а* *б*

***Рисунок 2. Построение пружины***

5. На панели «Редактирование детали» выбираем «Кинематическую операцию»: сечение-эскиз 2, траектория-спираль цилиндрическая (рис. 3, *а*).

6. Для среза пружины по краям выбираем плоскость XY, создаем эскиз и проводим через крайние витки пружины два прямоугольника (рис. 3, *б*).

7. Выходим из эскиза, на панели «Редактирование детали» выбираем операцию «Вырезание выдавливанием», задаем параметры Выдавливание в обоих направлениях, и срезаем витки пружины (рис. 4, *а*).



*а* *б*

***Рисунок 3 Построение пружины***

8. Пружина готова (рис. 4, *б*).

*а* *б*

***Рисунок 4. Построение пружины***

Преподаватель, в результате совместной деятельности приобретает новую роль — организатора самостоятельной, познавательной, исследовательской, творческой деятельности студентов и одновременно мотивируя студентов самостоятельно овладевать необходимыми навыками и знаниями, анализировать получаемую информацию, учиться делать выводы, аргументировать их, решать возникающие проблем.

Таким образом, в связи с изменением роли преподавателя и студента в учебном процессе при смене образовательной парадигмы, одним из важных условий современного инженерного образования становится эффективное сотрудничество преподавателя и студента. Мотивация студента активно учиться, получать знания путем совместного решения проблемных задач является подготовкой студентов к решению не только учебных проблем, но и решению сложных задач в будущей профессиональной деятельности, что способствует выработке активной жизненной позиции. Следовательно, обучение умению работать в сотрудничестве должно стать одной из стратегических целей инженерного образования.

**Список литературы:**


1. Бахвалов В.А. Развитие учащихся в процессе творчества и сотрудничества. М.: Центр «Педагогический поиск», 2000. — 144 с.
2. Борисенко И.Г. Компетентностный подход в преподавании начертательной геометрии и инженерной графики // Вестник Красноярского государственного аграрного университета. — 2011. — № 12. — С. 302—304.

3. Борисенко И.Г. Инновационные технологии в преподавании начертательной геометрии при формировании профессиональных компетенций // Вестник Иркутского государственного технического университета. — 2011. — № 12 (59). — С. 355—357.
4. Борисенко И.Г., Петровская Н.М. Информационные технологии в преподавании графических дисциплин при формировании профессиональных компетенций // Вестник ВСГУТУ. — 2012. — № 4 (39). — С. 38—42.

# ВОЗМОЖНОСТИ И ИНСТРУМЕНТЫ МОДУЛЯ GEOSTATISTICAL ANALYST

***Кынашев Санжар Кадырович***
*магистрант ГУ им. Шакарима,*
*Республика Казахстан, г. Семей*
*E-mail: kynashev89@gmail.com*

***Баранов Сергей Александрович***
*научный руководитель, канд. биол. наук, кафедра «Технической физики и теплоэнергетики» ГУ им. Шакарима,*
*Республика Казахстан, г. Семей*

Geostatistical Analyst представляет собой гибкое программное средство, предоставляющее любому пользователю, имеющему пространственно распределенные данные, широкие возможности исследования и анализа этих данных с использованием статистических инструментов и методов интерполяции оптимальных поверхностей. К некоторым из сфер эффективного применения модуля Geostatistical Analyst можно отнести такие как охрана окружающей среды, сельское хозяйство, георазведка (зондирование), геология, метеорология, гидрология, археология, лесное хозяйство, здравоохранение, горное дело, операции с недвижимостью и многие другие.

## 1. ПРЕДСТАВЛЕНИЕ ДАННЫХ И ИССЛЕДОВАНИЕ ДАННЫХ

Для визуализации данных имеется достаточно много инструментов, предоставляющих большой объем информации еще до построения самой поверхности, она также позволяет получить полезную информацию. Представление данных является очень важным этапом для оценки репрезентативности данных и идентификации внешних факторов, которые могут оказывать первостепенное значение распределение данных.

Инструменты исследовательского анализа (ESDA) предназначены специально для исследования пространственных данных, такими средствами являются: визуализация распределения данных, выявление трендов данных, показ глобальных и локальных выбросов, определение пространственной автокорреляции, осмысление ковариаций (взаимной изменчивости) между

несколькими наборами данных. ESDA представляет собой мощный набор исследовательских инструментов для выбора оптимального метода интерполяции для данных. Виды в ESDA выборочно интерактивны с ArcMap. Данные, выбранные или подсвеченные с помощью этих инструментов, будут также выбраны или подсвечены в окне отображения ArcMap. Это предоставляет пользователю уникальную возможность визуально взаимодействовать с данными для лучшего понимания взаимоотношений, представленных в разных вариантах отображения данных.

## 2. ПОДБОР МОДЕЛИ, ПОСТРОЕНИЕ ПОВЕРХНОСТИ

После тщательного исследования данных на предмет наличия аномалий, таких как глобальные и локальные выбросы и тренды в данных. Geostatistical Analyst предлагает применить Мастер, значительно облегчающий проведение процесса интерполяции. В нем имеется широкий выбор методов интерполяции для построения поверхностей.

Предлагаемые интерполяционные методы можно разделить на две основные группы, детерминированные и геостатистические. Первые используются для построения поверхностей по точечным измерениям, проведенным на основе области распространения сходства или степени сглаженности. Методы геостатистической интерполяции основаны на статистических проверках и используются для более продвинутого моделирования прогнозных поверхностей с учетом оценки достоверности или неопределенности прогнозов.

В зависимости от выбранного метода, могут быть созданы следующие виды выходных поверхностей: прогнозная, прогноза стандартной ошибки (неопределенности), квантильная, вероятностная, а также поверхность стандартной ошибки индикаторов. Geostatistical Analyst предоставляет пользователю возможность полного контроля за предлагаемыми параметрами соответствующих моделей и надежностью установок по умолчанию.

## 2.1 ДЕТЕРМИНИРОВАННЫЕ МЕТОДЫ

Методы детерминированной интерполяции используются для построения поверхностей по точечным измерениям на основе области распространения сходства или степени сглаженности.

- Обратные взвешенные расстояния
- Глобальные полиномы
- Локальные полиномы
- Радиальные функции

Методы детерминированной интерполяции можно разделить на две группы: глобальные н локальные. Глобальные методы дают прогнозную оценку с использованием всего набора данных. Локальные методы дают прогнозную оценку по точкам измерений, расположенным в заданных областях (окрестностях) — локальных зонах в пределах более обширной области исследования. Geostatistical Analyst предлагает глобальные полиномы в качестве общего (глобального) интерполятора н IDW, локальные полиномы, и радиальные функции в качестве локальных интерполяторов.

Интерполяция может привести к тому, что результирующая поверхность будет либо проходить через измеренные значения данных (исследуемой переменной), либо не будет. Метод интерполяции, дающий прогнозные значения, идентичные измеренным в соответствующих точках, называется точным (полным, строгим) интерполятором. Неточный (нестрогий) интерполятор дает прогнозное значение в точке измерений, которое отличается от реально измеренного значения, который можно использовать, с целью избавиться от резких пиков или впадин в выходной поверхности. Методы IDW н основанные на радиальных функциях являются строгими интерполяторами, а методы, основанные на глобальных или локальных полиномиальных зависимостях — нестрогими. Типичными областями применения детерминированного метода может быть анализ местоположения недвижимости с целью прогноза интенсивности ее продаж в зависимости от близости домов и земельных участков к месту, где живет покупатель. Применение весовых

показателей, используемых в методе IDW, позволяет дать эффективный прогноз оптимального расположения торговых точек.

## 2.2 ГЕОСТАТИСТИЧЕСКИЕ МЕТОДЫ

Методы геостатистической интерполяции основаны на статистических расчетах, они используются для более продвинутого прогноза н моделирования поверхности, включающего оценку ошибок или неопределенности полученного прогноза.

Предлагаются следующие варианты.

Кригинг и Кокригинг

- Обычный (Ordinary)
- Простой
- Универсальный
- Индикаторный
- Вероятностный
- Дизъюнктивный (альтернативный)

Выходные поверхности

- Прогноз или прогноз стандартной ошибки
- Квантильная
- Вероятностная и стандартная ошибки индикаторов

Геостатистические методы создают поверхности на основе статистических свойств данных измерений. Поскольку геостатистические прогнозы основаны на статистике, эти методы создают не только прогнозные поверхности, но также поверхности ошибки (достоверности) и неопределенности, являющиеся индикаторами качества прогноза. Кригинг позволяет решать два вида задач: количественная оценка пространственной структуры данных н прогнозирование. Первая задача, также называемая вариографией, заключается в подборе модели пространственной зависимости для описания данных. Для прогноза неизвестного значения исследуемой переменной в заданном местоположении кригинг будет использовать подходящую модель из вариографии, конфигурацию пространственных данных н значения,

измеренные в точках опробования вокруг местоположения, для которого выдается прогноз. Geostatistical Analyst предоставляет много инструментов, помогающих определить, какие параметры использовать, и предлагает установки по умолчанию, обеспечивающие быстрое построение поверхности. С геостатистикой ассоциируется многие методы, но все они относятся к семейству кригинговых. Geostatistical Analyst предоставляет обычный, простой, универсальный, вероятностный н дизъюнктивный кригинг. а также множественные версии кокригинга.

Кригинг представляет собой достаточно быстрый интерполятор, который может быть как строгим, так и нестрогим (сглаженным) в зависимости от используемой модели ошибок измерений. Это очень гибкий метод, и он позволяет пользователям исследовать графики пространственной автокорреляции. Кригинг использует статистические модели, обеспечивающие на выходе такие картографические представления как прогнозные поверхности, прогнозы стандартных ошибок, стандартную ошибку индикаторов н вероятностную поверхность. Гибкость метода кригинга может обусловить необходимость принятия многих предварительных решений. Кригинг подразумевает, что входные данные подчиняются требованиям стационарного стохастического процесса. Стохастический процесс является совокупностью случайных переменных значений, распределенных в пространстве и или во времени подобно измерениям высоты поверхности. Ряд методов, таких как обычный, простой н универсальный кригинг подразумевает нормальное распределение данных.

Кокригинг является множественным (многомерным) эквивалентом кригинга. Вследствие использования нескольких наборов данных он является исключительно гибким методом интерполяции, предоставляющим пользователям возможность исследования графиков взаимной корреляции и автокорреляции. С гибкостью кокригинга связана высокая потребность в принятии предварительных решений по всем аспектам его применения. В кокригинге могут использоваться как вариограммы, так и ковариации. В нем

могут применяться преобразования (трансформации) и удаляться тренды, он допускает наличие ошибок измерений в тех же случаях, что и в разных методах кригинга.

В Geostatistical Analyst доступны четыре типа интерполяционных поверхностей: прогноза, квантилей, вероятности превышения пороговых значений н ошибки прогноза. Они позволяют анализировать данные разными способами, с разных позиций.

- Прогнозная карта: Строится по интерполируемым значениям свободной переменной в местоположениях, по которым отсутствуют данные измерений.
- Карта ошибок прогноза: Строится по значениям стандартных ошибок интерполируемых значений или стандартной ошибке интерполированных значений индикатора с целью отображения неопределенности прогноза.
- Карта квантилей: Строится, когда пользователь задает вероятность и хочет получить карту прогнозных значений, превышающих (не превышающих) измеренные значения на заданной значений вероятности.
- Карта вероятности: Строится, когда пользователь задает пороговую величину и хочет получить карту вероятности того, что значения превысят (не превысят) заданную предельную величину.

## 3. АНАЛИТИЧЕСКИЕ ИНСТРУМЕНТЫ ДЛЯ ПОСТРОЕНИЯ ПОВЕРХНОСТЕЙ

Мастер в Geostatistical Analyst содержит аналитические инструменты, помогающие определить значение параметров используемых при построении поверхностей каждого из перечисленных выше типов. Часть предлагаемых диалоговых окон применима практически ко всем методам интерполяции, к ним, например, относятся диалоги задания окрестности поиска, перекрестной (взаимной) проверки достоверности и проверка достоверности. Другие, такие как моделирование вариограмм, трансформации, детрендинг, декластеринг и проверка соответствия нормальному распределению, относятся к геостатистическим методам (кригинг и кокригинг).

Функции вариограмм и ковариации помогают определить степень статистической корреляции в зависимости от расстояния. Geostatistical Analyst предлагает пользователю средство предварительного просмотра вариограммы ковариационной зависимости. Это облегчает и повышает эффективность процедуры подбора параметров модели, включая анизотропию и моделирование ошибок измерений. Вариограмма показывает статистическую корреляцию между соседними точками измерений. При росте расстояния, вероятность взаимосвязи между значениями в точках измерений уменьшается. Это значит, что дисперсия значений возрастает с ростом расстояния между точками измерений, то есть вариограмму можно рассматривать в качестве функции, представляющей несходство данных.

Взаимная (перекрестная) ковариация представляет статистическую тенденцию (тренд) переменных разного типа изменяться в зависимости от взаимосвязей друг с другом**Ошибка! Источник ссылки не найден.**. Положительная взаимная ковариация возникает, когда обе переменные имеют общую тенденцию быть больше их среднего значения, а отрицательная взаимная ковариация — в случае, когда одна из переменных стремится быть больше своего среднего, а другие — меньше их среднего значения. Моделирование на основе взаимной ковариации используется для определения локальных характеристик пространственной корреляции между двумя наборами данных и для поиска локальных сдвигов во взаимной корреляции между двумя наборами данных.

Иногда бывает полезным удалить (вычесть) поверхностный тренд из данных и применить методы кригинга или кокригинга к этим бес трендовым (оставшимся) данным. Например, если в наборе данных по содержанию озона в атмосфере отмечается подавляющее направленное влияние восточных ветров, может понадобиться удалить этот тренд, чтобы лучше понять фактические уровни содержания озона над данной территорией. Детрендинг разделяет данные на два компонента, компонент детерминированного тренда и компонент случайной автокорреляции. После удаления тренда вы сможете применить

метод кригинга к оставшимся данным**Ошибка! Источник ссылки не найден.**. А перед тем, как сделать окончательный прогноз, выделенный тренд может быть добавлен к результирующей поверхности.

По мере удаления точек с данными измерений от местоположения, где значение переменной неизвестно, они становятся все менее полезными для целей прогнозирования. На некотором расстоянии пропадает корреляция между значениями в этих точках и точке, по которой делается прогноз, и весьма вероятно, что точки измерений даже находятся в области, значительной отличающейся от той, где находится точка с неизвестным значением. Поэтому, обычной практикой является задание области поиска, которая ограничивает количество и конфигурацию расположения точек, используемых в прогнозе. Для ограничения числа используемых точек существует два механизма: задание формы области соседства (окрестности) и задание ограничений для точек в пределах и вне этой формы.

## 4. ДИАГНОСТИРОВАНИЕ

После построения прогнозной поверхности полезно проверить, является ли данная модель оптимальной для анализируемого набора данных. Geostatistical Analyst предлагает инструменты взаимной проверки (cross-validation) и проверки (validation) достоверности, обеспечивающие аналитическую оценку созданной поверхности. Эти инструменты позволяют количественно оценить «точность» модели. Вы можете либо принять модель с данными параметрами, либо изменить параметры модели и попытаться построить более подходящую поверхность.

Взаимная проверка и проверка достоверности основаны на следующей идее — изъять одно или несколько точечных измерений и затем спрогнозировать связанные с ними данные, используя данные измерений в оставшихся точках опробования. Взаимная проверка достоверности использует все данные для оценки тренда и моделей автокорреляции. Затем удаляется каждое из точечных измерений, по одному за раз, и рассчитывается связанное с ним

значение исследуемой переменной. Для всех точек взаимная проверка достоверности проводит сравнение измеренных н прогнозных значений.

Geostatistical Analyst обеспечивает построение ряда графиков и сводок сравнения измеренных н прогнозных значений.

Прогнозный график (Predicted) показан, синей линией, проходящей через поле точек, уравнение которой приведено в нижней части графика. График ошибки (Error) отличается от прогнозного графика тем, что он проводится по данным, полученным вычитанием истинных значений из прогнозных значений. Для графика стандартной ошибки (Standard Error) истинные значения вычитаются из прогнозных графиков и делятся на оцененные методом кригинга стандартные ошибки. Все эти три графика помогают понять, насколько хорош прогноз на основе кригинга.

Диалоговое окно Сравнение (Comparison) используется в методе взаимной проверки достоверности и помогает проанализировать статистические выкладки вместе с каждым из графиков. Как правило, наилучшей является модель со стандартизованным средним близким к нулю, наименьшей среднеквадратической ошибкой прогноза, средней стандартной ошибкой, наиболее близкой к среднеквадратической ошибке прогноза, и наиболее близкой к единице стандартизованной среднеквадратической ошибкой прогноза. С помощью диалогового окна Сравнение вы можете провести совместное изучение статистик и графиков по разным моделям.

**Список литературы:**

1. ArcGIS 9 Geostatistical Analyst Руководство пользователя. Издательство: Dataplus 2006, — 278 с.

# МОДЕЛИРОВАНИЕ ДВУХФАЗНОЙ СИСТЕМЫ МАССОВОГО ОБСЛУЖИВАНИЯ

***Черанёв Александр Александрович***
*студент 3 курса, кафедра радиоэлектронных и телекоммуникационных систем ИРИТ-РТФ УрФУ,*
*РФ, г. Екатеринбург*
*E-mail: kraxc@yandex.ru*

***Самусевич Галина Александровна***
*научный руководитель, доцент, канд. тех. наук, ИРИТ-РТФ УрФУ,*
*РФ, г. Екатеринбург*

Представляется стохастическая модель двухканальной системы массового обслуживания (СМО) с ограничениями на время пребывания заявки, как в очереди, так и в системе. Один поток входных заявок. Поток входных заявок и оба потока обслуживания являются простейшими. Имеется возможность задать наибольшее число входных приоритетных заявок и, следовательно, время работы модели, что позволяет изучать эффективность рассматриваемой системы, как в ходе переходного процесса, так и в установившем режиме ее работы.

Разрабатываемый программный продукт предназначен для создания двух лабораторных работ:

1. лабораторная работа для студентов бакалавриата для изучения влияния относительного приоритета на эффективность СМО. Дисциплина — «Основы теории массового обслуживания».

2. лабораторная работа для студентов магистратуры предполагает изучение принципов моделирования стохастических динамических процессов. Дисциплина — «Методы моделирования и оптимизации».

Программный продукт будет разработан на языке C++ с использованием алгоритмов для решения поставленной задачи и получения необходимых данных. В итоге, будет смоделирована двухканальная система массового обслуживания с ограничениями на время пребывания заявки, как в очереди, так и в системе.

***Описание переменных***

M — число входных заявок (j∈[1, M]);

tj = tj-1 + η — момент времени появления в системе j-ой заявки,

где η = 1/λ — среднее значение интервала времени между соседними заявками, λ — параметр показательного закона распределения вероятностей случайной величины $T$;

$t_{\text{ож}\,j}^{\,i}$ — время ожидания в очереди *j*-ой заявкой освобождения *i*-го канала;

$$t_{\text{ож}\,j}^{\,i} = \begin{cases} t_{\text{осв}}^{i} - t_j, & \text{если } t_{\text{осв}}^{j} - t_j \geq 0, \\ 0, & \text{если } t_{\text{осв}}^{j} - t_j < 0, \quad p_{\text{прос}}^{i} = t_j - t_{\text{осв}}^{j} \end{cases}$$

$t_{\text{осв}}^{i} = t_j + t_{\text{ож}\,j}^{\,i} + \mu_i$ — момент времени освобождения *i*-го канала, *i* = 1, 2,

где $\mu_i$ — средняя величина времени обслуживания заявки *i*-ым каналом. показательный закон распределения вероятностей, определяющая длительность обслуживания *j*-ой заявки *i*-ым каналом;

$t_{\text{преб}\,j}^{\,i} = t_{\text{ож}\,j}^{\,i} + \mu_i$ — время пребывания *j*-ой заявки в системе;

$t_{\text{ож max}}$ — наибольшее время пребывания заявки в очереди;

$t_{\text{преб max}}$ — наибольшее время пребывания заявки в системе.

***Текущие показатели эффективности системы***

*b* — суммарное число обслуженных заявок к моменту времени $t_j$;

*c* — число заявок, покинувших систему необслуженными из-за ограничения на время пребывания в очереди к моменту времени $t_j$;

*d* — число заявок, покинувших систему необслуженными из-за ограничения на время их пребывания в системе к моменту времени $t_j$;

$T_{\text{обс}}^{i} = T_{\text{обс}}^{i} + \mu_i$ — суммарное время обслуживания заявки ***i***-м каналом;

$T_{\text{прос}}^{i} = T_{\text{прос}}^{i} + t_{\text{прос}}^{i}$ — суммарное время простоя *i*-го канала;

$T_{\text{ож}} = T_{\text{ож}} + t_{\text{ож}\,j}^{\,1} + t_{ожj}^{\,2}$ — суммарное время пребывания заявок в очереди к моменту времени $t_j$;

$T_{\text{преб}} = T_{\text{преб}} + t_{\text{преб}}{}^{1}_{j} + t_{\text{преб}}{}^{2}_{j}$ — суммарное время пребывания заявок в системе к моменту времени $t_j$.

**Результирующие показатели эффективности системы**

Результирующие показатели эффективности, вычисляются после окончания цикла по $j$ (когда $j = M$) для момента времени $T_{\max} = t_M$.

$P_{\text{обс}} = \dfrac{b}{M}$ —— вероятность обслуживания;

$P_{\text{отк}} = \dfrac{c+d}{M}$ — вероятность отказов, вызванных ограничением на время пребывания заявки в очереди и на время пребывания заявки в системе;

$k_{\text{з}} = \dfrac{1}{2}\left[\dfrac{T^1_{\text{обс}} + T^2_{\text{обс}}}{T_{\max}}\right]$ — коэффициент загрузки системы;

$k_{\text{прос}} = \dfrac{1}{2}\left[\dfrac{T^1_{\text{прос}} + T^2_{\text{прос}}}{T_{\max}}\right]$ — коэффициент простоя системы;

$T_{\text{ож}}$ — суммарное время пребывания заявок в очереди.

$T_{\text{преб}}$ — суммарное время пребывания заявок в системе.

**Приложение**

Результаты моделирования

***Таблица 1.***

| **Входные данные** | | |
|---|---|---|
| Номер фазы системы | 1 фаза | 2 фаза |
| Число циклов итерационного процесса | | |
| Интенсивность потока обслуживания 1-го канала | | |
| Интенсивность потока обслуживания 2-го канала | | |
| Интенсивность потока входных заявок | | |
| Допустимое время пребывания заявки в очереди | | |
| Допустимое время пребывания заявки в системе | | |

***Таблица 2.***

| **Результирующие показатели эффективности системы** | | |
|---|---|---|
| Номер фазы системы | 1 фаза | 2 фаза |
| Время работы СМО | | |
| Максимальное число входных заявок | | |
| Число обслуженных заявок | | |
| Число необслуженных заявок из-за ограничения на время пребывания в очереди | | |
| Число необслуженных заявок из-за ограничения на время пребывания в системе | | |
| Суммарное время обслуживания заявок | | |

| | | |
|---|---|---|
| Суммарное время каналов обслуживания | | |
| Время пребывания заявок в очереди | | |
| Время пребывания заявок в системе | | |

## Макет разрабатываемой программы


***Рисунок 1. Главное окно со структурной схемой СМО с ограничениями. (1 — входящий поток, 2 — очередь, 3 — Количество отказов из-за превышения времени пребывания в очереди, 4 — отказ из-за превышения времени пребывания заявки в системе, 5,6 — каналы обслуживания)***

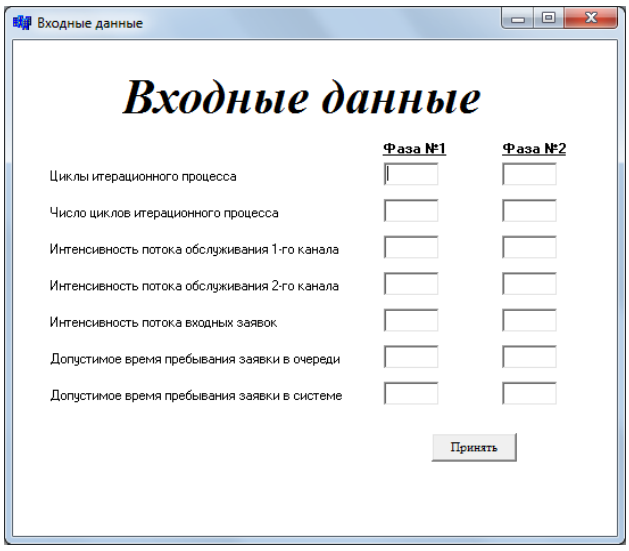



***Рисунок 2. Окно ввода данных***

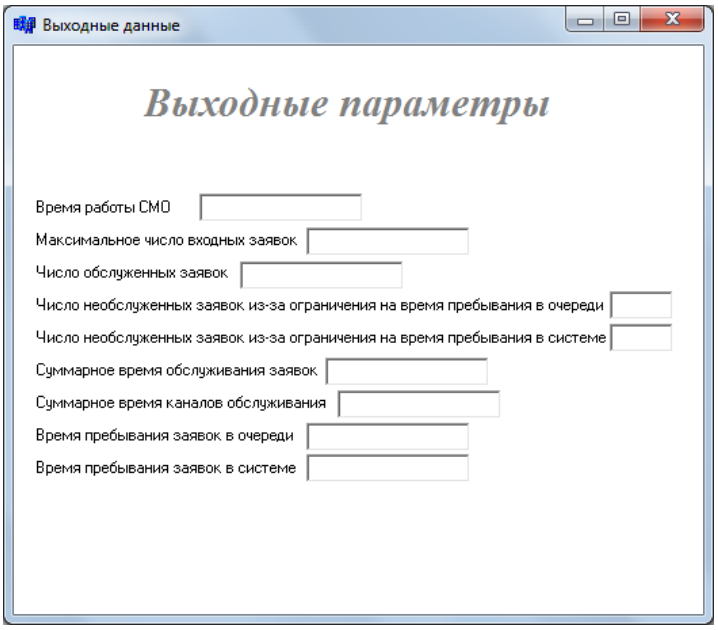



***Рисунок 3. Выходные параметры***

**Список литературы:**

1. Моделирование систем: Учебник для студентов высш. Учеб. заведений/ [С.И. Дворецкий, Ю.А. Муромцев, В.А. Погодин, А.Г. Схиртладзе]. М.: Изд. Центр «Академия», 2009. — 320 с.
2. Советов Б.Я., Яковлев С.А. С56 Моделирование систем: Учебник для вузов 3-е изд., перераб. и доп. М.: Высш.шк., 2001. — 343 с.: ил. (УДК 519.87, ББК 22.18, С56).
3. Самусевич Г.А. Основы теории массового обслуживания: Конспект лекций / Г.А. Самусевич. Екатеринбург: Изд-во ГОУ ВПО - УГТУ УПИ, 2005. — 102 с.

# СЕКЦИЯ 4.

# НАНОТЕХНОЛОГИИ

## ПРОБЛЕМЫ ОБНАРУЖЕНИЯ НАНОТРУБОК В КАУЧУКЕ

***Николаев Иван Владимирович***
*магистрант 1 курса, кафедра физики ОмГТУ,*
*РФ, г. Омск*
*E-mail: www.amicus@mail.ru*

***Даньшина Валентина Владимировна***
*научный руководитель, канд. хим. наук, доцент ОмГТУ,*
*РФ, г. Омск*
*E-mail: danshina_v@mail.ru*

Для изготовления материалов с заданными свойствами все чаще используют нанокомпозиты — это материалы, сформированные при введении наноразмерных компонентов (наполнителей) в структурообразующую твёрдую фазу (матрицу).

С целью диверсификации продукции на заводе ОАО «Омский каучук» стали изготавливать каучук, легированный многослойными углеродными нанотрубками (МУНТ). Образцы синтетического бутадиен-метилстирольного каучука марки СКМС-30АРК наполняют МУНТ по методике солевой коагуляции. После синтеза нанокомпозита важной задачей является исследование структуры и свойств нового материала. В литературных источниках не найдено информации о том насколько равномерно распределяются нанотрубки в объеме каучука или они седиментируют на дно образца.

Для исследования был изготовлен образец, состоящий из синтетического каучука с многослойными углеродными нанотрубками (МУНТ) Graphistrength™ (корпорация Arkema) диаметром 10—15 нм и длиной 1—10 мкм.

Цель работы: исследовать структуру наполнителя с помощью различных видов микроскопии. Так как синтетический каучук марки СКМС-30АРК — диэлектрический образец, то одним из способов получения изображения его легирующих компонентов является сканирующая зондовая микроскопия. Суть

метода заключается в том, что с помощью специального зонда сканируется поверхность, а затем с помощью программного обеспечения строится изображение. При работе в полуконтактном режиме возбуждаются колебания кантилевера, на конце которого находится игла (зонд). При колебаниях зонд касается поверхности образца. На рис. 1 показано изображение нанокомпозита, сделанное с помощью атомно-силового микроскопа в полуконтактом режиме.

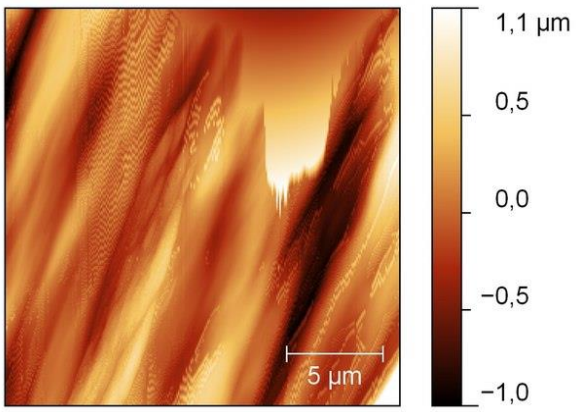



***Рисунок 1. Изображение рельефа образца с МУНТ, сделанное на атомно-силовом микроскопе***

Как видно из рисунка 1 получается размытая структура, это связано с тем, что сам образец легко подвержен упругой деформации, а рельеф имеет большую неоднородность. Перепады высот рельефа образца от впадины (-1) до пика (1,1) достигают 2,1 мкм. При таком методе визуально обнаружить МУНТ не представилось возможным.

Каучук является диэлектриком, т.е. электроны связаны с атомами и не могут под действием электрического поля свободно перемещаться, из-за этого изображение получается «засвеченным», когда мы используем электронную микроскопию, где изображение строится за счёт испускающего пучка электронов. Но для исследования диэлектриков также можно использовать электронную микроскопию, если сделать проводящую плёнку на образце. Перед сканированием образца под растровым электронным микроскопом (РЭМ) была проведена следующая подготовка образца:

- погружение образца в жидкий азот;

- извлечение образца из жидкого азота с последующим его изломом;
- магнетронное напыление платины на образец проведено на оборудовании JFC-1600 с величиной ионного тока 30 мА [2, с. 867].

После вышеуказанных этапов образец помещался на медную подложку в растровый электронный микроскоп JEOL JSM-6610LV, под которым рассматривалась область излома образца (рис. 2).

Несмотря на то, что каучуки — диэлектрики, растровую электронную микроскопию можно использовать для исследования данных образцов, но для этого требуется напылить проводящую плёнку на образец и высокая точность настройки оборудования для получения качественного изображения.

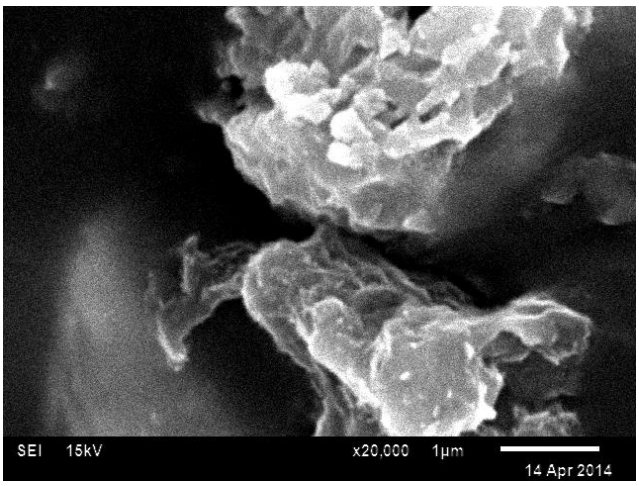



***Рисунок 2. РЭМ-изображение образца с МУНТ***

На полученных изображениях видны нитевидные структуры, которые могут быть нанотрубками, хотя явного проявления МУНТ не обнаружено. Авторы статьи [3, с. 1546] писали, что у них также не было найдено очевидных скоплений УНТ в резиновой матрице. Но косвенные показатели, такие как механические характеристики каучука [1, с. 58], однозначно свидетельствуют о присутствии в образце нанотрубок.

В статье [2] описываются получение, характеристики и физические свойства бутадиен-стирольного каучука и бутадиен-нитрильного каучука с углеродными нанотрубками, которые были синтезированы химическим осаждением из паровой фазы на железных и кобальтовых катализаторах,

поддерживаемых субстратов из карбоната кальция. Затем углеродные нанотрубки были дополнительно обработаны азотной кислотой с образованием гидроксильных и карбонильных функциональных групп на их поверхности. Также авторами статьи [2, с. 868] были получены изображения наполнителя на просвечивающем электронном микроскопе (ПЭМ). Суть метода просвечивающей электронной микроскопии заключается в том, что через образец пропускается пучок электронов, который регистрируется на флуоресцентном экране, фотоплёнке или сенсорном приборе с зарядовой связью (специализированной аналоговой интегральной микросхеме, состоящей из светочувствительных фотодиодов, выполненной на основе кремния). Затем строится изображение образца с помощью специального программного обеспечения. На ПЭМ-изображениях углеродные нанотрубки видны отчётливо, но подготовка образца к сканированию на просвечивающем электроном микроскопе гораздо сложнее, чем подготовка образца к сканированию с помощью растрового электронного микроскопа. Главной особенностью является то, что для получения качественного ПЭМ-изображения требуется ультратонкий образец (около 0,1 мкм).

При равномерном распределении нанотрубок, очевидно, что МУНТ можно обнаружить как на поверхности, так и в объёме образца, поэтому были применены методы исследования топографии образца — растровая и атомно-силовая микроскопии. С помощью зондовой микроскопии сложно исследовать такие образцы, как каучуки, потому что они являются аморфными. Практически невозможно получить изображение нанотрубок в образце, т. к. получение изображения поверхности подобных образцов является затруднительным. Сравнивая методы, можно сделать вывод, что лучшим методом исследования наполнителя в нанокомпозите является просвечивающая электронная микроскопия, т. к. она обладает высокой кратностью увеличения, высоким качеством изображения даже для диэлектриков, но для этого требуется сложная специализированная подготовка.

**Список литературы:**


1. Николаев И.В., Даньшина В.В. Исследование механических характеристик резинотехнических изделий, модифицированных углеродными нанотрубками // Вестник ПНИПУ. Машиностроение, материаловедение. — 2015. — Том 17, — № 1. — С. 54—60.
2. Perez L.D. et al. Preparation, characterization, and physical properties of multiwall carbon nanotube/elastomer composites // Polymer Engineering & Science. — 2009. — Т. 49. — № 5. — С. 866—874.
3. Sui G. et al. Preparation and properties of natural rubber composites reinforced with pretreated carbon nanotubes // Polymers for Advanced Technologies. — 2008. — Т. 19. — № 11. — С. 1543—1549.

# СЕКЦИЯ 5.

# РАДИОТЕХНИКА, ЭЛЕКТРОНИКА

## РАЗРАБОТКА КОМПЛЕКСА ДЛЯ АНТЕННЫХ ИЗМЕРЕНИЙ

***Иванов Александр Андреевич***
*студент 4 курса БПОУ Омской области «Омский государственный колледж управления и профессиональных технологий» специальность Техническое обслуживание и ремонт радиоэлектронной техники (по отраслям), РФ, г. Омск*

***Машинский Виталий Васильевич***
*студент 1 курса БПОУ Омской области «Омский государственный колледж управления и профессиональных технологий» специальность Техническое обслуживание и ремонт радиоэлектронной техники (по отраслям), РФ, г. Омск*
*E-mail: omsk.ogkuipt@yandex.ru*

***Бабиенко Лариса Дмитриевна***
*научный руководитель, канд. техн. наук, преподаватель БПОУ ОГКУиПТ, РФ, г. Омск*

В процессе настройки и испытания антенн приходится снимать диаграммы направленности антенн, измерять такие величины, как частоту, мощность колебаний в антенне, ее полное сопротивление, коэффициент стоячей волны в антенном фидере, напряженность поля, создаваемого антенной.

Для этих целей используются измерительные приборы. Приборов для измерения параметров антенн существует много [3], каждый из них измеряет определенные параметры антенн.

Наши студенты уже несколько лет разрабатывают различные антенны, которые служат наглядными пособиями при изучении дисциплины «Антенно-фидерные устройства». Кроме того мы рассматриваем и новые, нетрадиционные построения антенн, информация о которых появляется в литературе.

Проблема состоит в том, что мы без соответствующих приборов можем получить лишь качественные характеристики антенны, т. е. определить лишь

ее работоспособность. Кроме того, мы работаем в УКВ диапазоне, где размеры антенн малы, и мы можем изготавливать их в условиях колледжа.

Поэтому мы решили разработать устройства для измерения параметров антенн.

Актуальность проблемы состоит в том, что существующие промышленные приборы для испытаний антенн стоят непомерно дорого, сотни тысяч рублей. Поэтому создать самодельные устройства, недорогие, но мобильные, представляется актуальным. При этом мы стремимся решить и общегосударственную задачу импортозамещения, т. е. разработать устройства на отечественной элементной базе.

**Основные параметры антенн**

Основные параметры антенн известны [1].

1. Резонансная частота.

Антенна излучает электромагнитные волны, когда к ней приложено возбуждающее колебание. Эффективность ее излучения наибольшая, когда частота возбуждающего колебания совпадает с резонансной частотой. Как правило, длина антенны равна половине или четверти длины волны на центральной рабочей частоте.

2. Импеданс антенны.

Импеданс антенны меняется вдоль ее длины. Точка максимального тока и минимального напряжения соответствует наименьшему импедансу и называется точкой возбуждения. Импеданс в этой точке, называют входным импедансом и он состоит из активного сопротивления излучения антенны и реактивной составляющей. В резонансе реактивная составляющего входного импеданса должна быть равна нулю. На частотах выше резонансной импеданс имеет — индуктивный характер, а на частотах ниже резонансной — емкостной характер.

3. Диаграмма направленности антенны.

Диаграмму направленности можно снимать, поворачивая антенну и измеряя напряженность поля в фиксированной точке на частоте передачи. Эти измерения дают диаграмму направленности в полярных координатах.

Полярная диаграмма показывает направление, в котором концентрируется энергия антенны.

В радиолюбительской практике это наиболее сложный вид измерений. Проводя измерения в ближней зоне необходимо учитывать ряд факторов влияющих на достоверность измерений. Желательно размещать измерительные антенны на такой же высоте, как и исследуемая антенна и расстояние между ними выбирать от 1,5 до 2 длин волн.

4. КСВ (Коэффициент стоячей волны).

Как видим этот параметр стоит на последнем месте и не является первостепенным. Если антенна настроена в резонанс и в ходе настройки мы скомпенсировали ее реактивность, и согласовали с фидером питания по сопротивлению, К.С.В. будет — единица. Любая антенна, простая она или сложная, является резонансным устройством и требует настройки. Настройка включает в себя измерение основных параметров антенны и коррекция их путем подгонки линейных размеров элементов антенны. Так как антенну мы сами не рассчитываем, а изобретаем новые конструкции, возникает вопрос о необходимости измерения параметров антенн и сравнения их с некоторым эталоном, который представляет вертикальный штырь определенных размеров.

Самое главное, что КСВ дает представление о степени согласования антенны, так как, если антенна несогласована, то мощность, подаваемая в антенну не проходит в нагрузку, а возвращается обратно, к передатчику и вызывает помехи. Чем ближе КСВ к единице, тем лучше согласование. На практике КСВ стремятся получить не больше 2.

Исходя из того, что основная масса радиолюбителей и мы в том числе, не имеет хорошей базы специализированных приборов, определим минимум простых и самодельных приборов, необходимых для измерений основных параметров антенны.

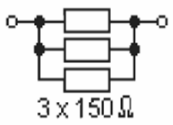
Комплекс для антенных измерений должен включать следующие устройства: радиопередатчик, эквивалент антенны, антенна, согласующее устройство, измеритель коэффициента стоячей волны (КСВ), измеритель напряженности поля. Кроме того, целесообразно иметь еще и антенный анализатор.

Передатчик мы используем уже готовый, разработанный нашими студентами ранее. Мы имеем два передатчика на частоты 88 МГц и 100 МГц. Это маломощные передатчики, мощность их составляет около 0,5 Вт, что достаточно для измерений в ближней зоне.

Эквивалент антенны — это устройство, имитирующее электрические параметры антенны (ее электрическое сопротивление), но не осуществляющее излучение и прием сигналов из эфира.

Эквивалент антенны должен обеспечивать возможность проведения этих работ во всей используемой полосе частот, иметь необходимое сопротивление, и допускать работу при требуемой (необходимой) мощности передатчика.

Эквивалент антенны мы собрали из параллельно включенных низкоомных резисторов, воспользовавшись формулами закона Ома




3 x 150 Ω/0,25 W = 50 Ω/0,75 W
3 x 150 Ω/0,5 W = 50 Ω/1,5 W
3 x 150 Ω/1 W = 50 Ω/3 W
3 x 150 Ω/2 W = 50 Ω/6 W

Расчетная мощность при работе около 1,5 Ватт долгосрочно, сопротивление 50 Ом. Такая конструкция, позволяет минимизировать влияние индуктивности выводов и создать близкие к оптимальным условия для охлаждения каждого резистора.

Классические схемы измерителей КСВ делятся на два класса: измерители с измерительной линией и измерители с трансформатором тока. Недостатком таких измерителей является его ограниченная полоса частот. Этих недостатков

лишен измеритель КСВ на основе небалансируемого моста [4]. Такой измеритель показан на рисунке 1.

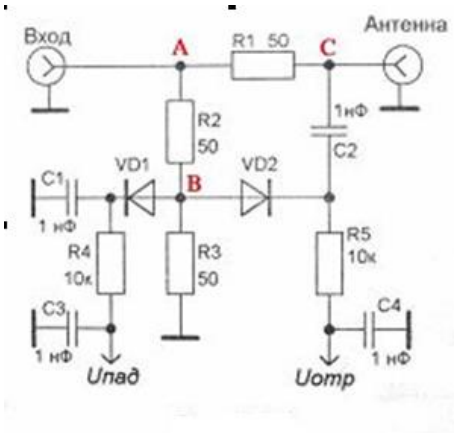



***Рисунок 1. Мостовой измеритель КСВ***

Основой прибора является мост R1-R2-R3-Za, где Za — волновое сопротивление антенны. Точки A, B, C, «земля» — углы моста. Импеданс самой антенны — одно из плеч.

Детектор на VD1 измеряет половину входного сигнала, детектор на VD2 (включенный в диагональ моста) — сигнал разбаланса моста, пропорциональный Uотр.

Если на выходе линии передачи подключен импеданс, отключающийся от ее волнового сопротивления, часть падающей на нагрузку сигнальной волны отразится обратно. Эта отраженная волна складывается с падающей, и результирующая амплитуда в любой точке является алгебраической суммой амплитуд двух волн. Узлы и пучности не движутся относительно линии передачи, т. е. стационарны. Такие волны называются стоячими.

Когда сопротивление нагрузки равно волновому сопротивлению линии передачи, падающая волна полностью поглощается в нагрузке, отраженная и стоячая волны отсутствуют. В этом случае система является идеальной, ее коэффициент стоячей волны равен 1.

Внешний вид собранного нами КСВ-метра представлен на рисунке 2.

***Рисунок 2. Внешний вид КСВ-метра***

КСВ определяется по формуле

$$КСВ = \frac{U_{прям.} + U_{отр.}}{U_{прям.} - U_{отр.}} \quad (1)$$

В тех случаях, когда требуется обнаружить поле излучения антенны или установить относительное изменение этого поля в пространстве, применяются простые индикаторы поля, содержащие рамочную антенну и измерительный прибор в виде лампового вольтметра.

Однако, часто необходимо знать точное значение напряженности поля. Для этих целей необходим измеритель напряженности. Он поможет при настройке антенн, при контроле работоспособности антенн. Особое значение измеритель напряженности будет иметь для передвижных радиостанций, когда стационарные приборы занимают много места. Измеритель напряженности может пригодиться и радиолюбителям, так как его конструкция проще традиционных приборов, используемых при настройке антенн.

Мы рассмотрели несколько схем индикаторов и измерителей напряженности поля и остановились на одной схеме, приведенной на рисунке 3.

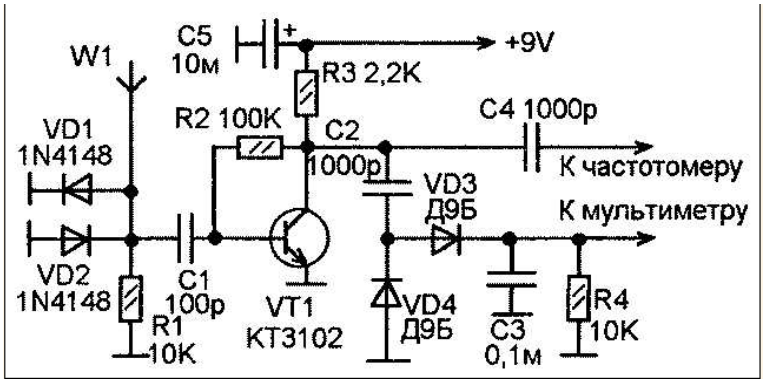



***Рисунок 3. Измеритель напряженности поля***

Мы столкнулись с проблемами нагрузки, подбора параметров усилителя, правильного выбора рабочей точки, «пролезаний» высокой частоты с выхода на вход устройства. В результате настройки устройство заработало. Внешний вид устройства показан на рисунке 4.

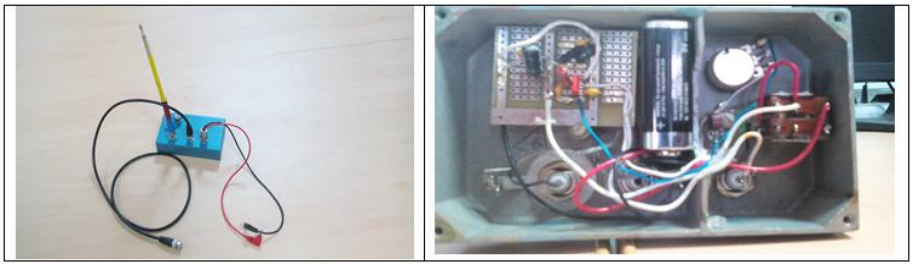


***Рисунок 4. Внешний вид индикатора поля***

Разработанные нами устройства позволяют измерить основные параметры антенн. Но для лучшей настройки новых типов антенн необходимо знать и импеданс антенны, т. е ее активное и реактивное сопротивления. Такие измерения производит антенный анализатор. Промышленные анализаторы стоят сотни долларов. В то же время можно изготовить простое устройство, дающее представление о импедансе антенны [6].

Схема такого устройства показана на рисунке 5.

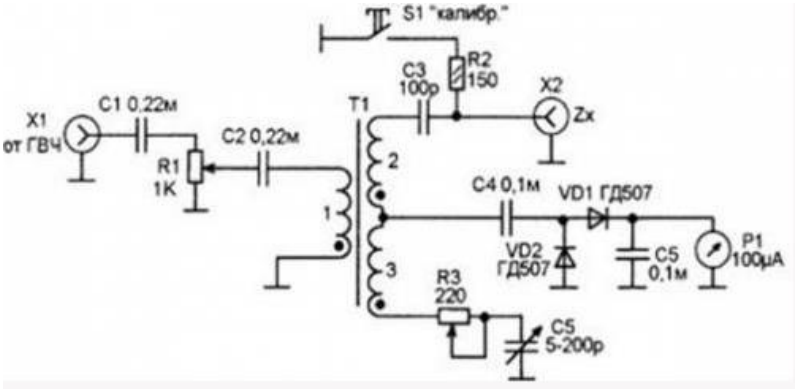



***Рисунок 5. Простой антенный анализатор***

Используя генератор высокой частоты, частотомер и дифференциальный мост можно получить систему, способную во многих случаях работать как антенный анализатор.

Сигнал от генератора подается на разъем X1. Резистором R1 регулируется уровень (можно R1 и не ставить, а пользоваться регулятором уровня, имеющимся у генератора).

К разъему X2 подключают анализируемую антенну. ВЧ напряжение поступает на первичную обмотку. ВЧ напряжение на вторичных обмотках трансформатора поступает на измеритель, состоящий из микроамперметра P1 и детектора на германиевых диодах VD1 и VD2 Диоды должны быть германиевыми, чтобы обеспечить наибольшую чувствительность измерителя при индикации минимальных показаний (баланс).

Баланса моста достигают регулировкой резистора R3 и переменного конденсатора C5. Эти детали необходимо снабдить шкалами с указанием сопротивлений и емкостей соответствующих углам поворота рукояток. Баланс достигается в случае равенства активных и реактивных сопротивлений в обоих плечах, Затем, добившись баланса, нужно прочитать значения сопротивления R3 и емкости C5. а затем рассчитать реактивное сопротивление C5 исходя из данной частоты. Таким образом можно будет определить активную (R3) и реактивную (C5) составляющую сопротивления анализируемой антенны.

Емкость C3, составляет 100 пФ, то есть, половину максимальной емкости C5. Если при измерениях окажется что емкость C5 в балансе установилась

больше 100 пФ, то это говорит о емкостном характере реактивного сопротивления антенны, а вот величина С5, установленная меньше 100 пФ, наоборот, говорит о индуктивном характере реактивного сопротивления в антенне.

Трансформатор Т1 намотан на ферритовом кольце 600 НН диаметром 10 мм. Обмотки одинаковые, они выполнены втрое сложенным обмоточным проводом типа ПЭВ диаметром 0,35. Восемь витков, равномерно распределенных по кольцу. Начала обмоток на схеме отмечены точками.

Схема требует налаживания и градуировки. Переменный резистор R3 и конденсатор С5 нужно, как уже сказано, обустроить шкалами со значениями сопротивления и емкости, соответственно (потребуется омметр и измеритель емкости).

Антенный анализатор мы изготовили на печатной плате, трассировка и вид которой показаны на рисунке 6.

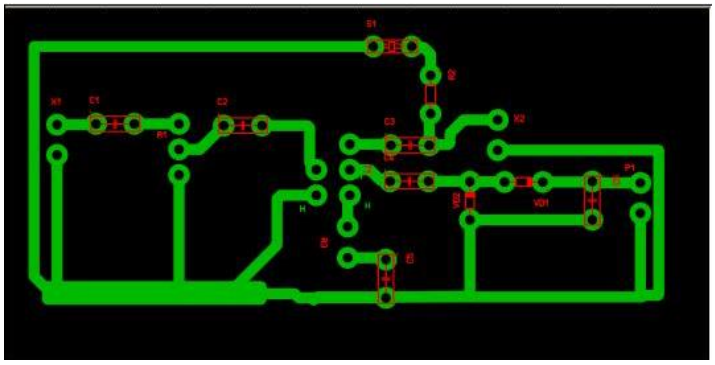


***Рисунок 6. Антенный анализатор***

Внешний вид платы и устройства антенного анализатора показан на рисунке 7.

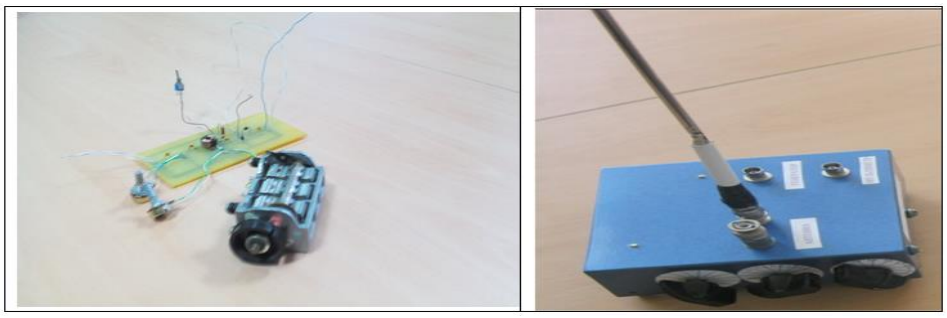


***Рисунок 7. Внешний вид платы и устройства антенного анализатора***

Таким образом, задачи, поставленные в работе, решены. Данный комплекс может найти применение в учебном процессе, а также он может быть полезен для радиолюбителей, в процессе настройки антенн. Возможно применение комплекса и для пользователей телевизионных антенн, поскольку позволяет количественно оценить используемую антенну. Кроме того комплекс позволяет производить настройку антенны и передатчика.

**Список литературы:**


1. Антенно-фидерные устройства и распространение радиоволн: Учебник для вузов/ Под ред. Г.А. Ерохина. М.: Радио и связь, 1996.
2. Бунтов В.Д., Макаров С.Б., Цифровые и микропроцессорные радиотехнические устройства: Учебн. пособие. СПб.: Изд-во Политехн. ун-та, 2005.
3. Григорьев И.Н. Антенны. Настройка и согласование: Справ. пособие, М.: ИП Радио.
4. Дубровский В.А., Гордеев В.А. Радиотехника и антенны. М.: Радио и связь, 1998.
5. Жан М. Рабаи, Ананта Чандракасан, Боривож Николич Цифровые интегральные схемы. Методология проектирования = Digital Integrated Circuits 2-е изд.. М.: «Вильямс», 2007.
6. Кашкаров А.П., Бутов А.Л. Радиолюбителям схемы для дома, МРБ-1275 2008.
7. Мышляева И.М. Цифровая схемотехника: Учебник для сред. проф. образования: Издательский центр «Академия», 2005.

# СЕКЦИЯ 6.

# ТЕЛЕКОММУНИКАЦИИ

## ОБЗОР ПРОБЛЕМНЫХ ОБЛАСТЕЙ В БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ, АТАК И МЕХАНИЗМОВ ИХ ЗАЩИТЫ

***Постольский Сергей Петрович***
*магистрант 2 курса, кафедра вычислительной техники и программного обеспечения, Международный Университет Информационных Технологий, Республика Казахстан, г. Алматы*
*E-mail: Postol91@gmail.com*

***Айтмагамбетов Алтай Зуфарович***
*научный руководитель, канд. тех. наук, профессор, Международный Университет Информационных Технологий, Республика Казахстан, г. Алматы*

### 1. Введение

Беспроводные сенсорные сети становятся как новым важным уровнем в ИТ экосистеме, так и объектом оживленных исследований, включающих аппаратную и программную архитектуру, сетевые технологии и соединения, распределенные алгоритмы, программные модели, управление данными, безопасность и так далее. Сенсорная сеть — это множество маленьких считывающих устройств (датчиков), способных регистрировать изменения различных параметров окружающей среды и транслировать эти параметры другим подобным устройствам, находящимся в зоне досягаемости с определенной целью, например: видеонаблюдение, мониторинг окружающей среды и т. д. Современные датчики способны отслеживать температуру, давление, влажность, состав почвы, автомобильное движение, уровни шума, условия освещения, наличие или отсутствие определенных видов объектов или веществ и другие свойства. Довольно часто сенсорные сети устанавливаются в агрессивных неблагоприятных средах, где могут быть предприняты намеренные попытки влияния на их работу. Ярким примером может служить их применение в зоне боевых действий, где секретность передаваемых данных

и местоположения, а также устойчивость к попыткам компрометации данных и уничтожения сети имеют ключевое значение. В данной статье приводится наиболее полная классификация атак на беспроводные сенсорные сети и механизмов их защиты.

**2. Цели обеспечения информационной безопасности в беспроводных сенсорных сетях**

Цели обеспечения информационной безопасности в беспроводных сенсорных сетях можно условно разделить на первоочередные и второстепенные [1, с. 3—5]. Первоочередные цели широко известны и включают в себя обеспечение конфиденциальности, целостности, аутентификации и доступности данных. Второстепенные цели обеспечения безопасности включают в себя такие понятия как свежесть данных, самоорганизация, временная синхронизация, защищенная локализация.

Конфиденциальность данных является фундаментальной задачей безопасности. Конфиденциальность в сенсорных сетях подразумевает необходимость защиты передаваемых по сети данных с целью закрыть к ним доступ для потенциальных злоумышленников посредством различных механизмов, таких как контроль доступа, шифрование и т. д.

Аутентификация данных необходима для подтверждения подлинности данных посредством идентификации их происхождения/первоисточника. Аутентификация данных позволяет проверить легитимность отправителя и получателя данных в сети. Аутентификация данных обеспечивается посредством применения симметричных и ассиметричных механизмов, где отправляющий и принимающий узлы сенсорной сети обмениваются секретными ключами. Благодаря беспроводной передаче данных и особенности работы сенсорных сетей без постоянного вовлечения человека обеспечение аутентификации данных становится довольно сложной задачей.

Целостность данных в сенсорных сетях определяется способностью обеспечения защиты данных таким способом, чтобы данные не могли быть изменены во время транспортировки между узлами сенсорной сети. Например,

целостность данных сети может находиться под угрозой в случае наличия в сети скомпрометированного узла, внедряющего в сеть ложные данные, в случае потери или повреждения данных вследствие нестабильных условий и беспроводной природы сенсорных сетей.

Доступность данных подразумевает возможность работы сенсорной сети посредством транспортировки данных между ее узлами. В случае нарушения этого свойства данных, сенсорная сеть не может продолжать функционировать и поддерживать предоставление возложенных на нее функций. Доступность данных сенсорной сети может быть легко скомпрометирована посредством атаки и вывода из строя базовой станции или главного узла кластера сенсорной сети.

Свежесть данных в беспроводных сенсорных сетях позволяет определить что данные были получены датчиком и отправлены по сети в первый раз, а не являются копией старых данных повторно отправленных в сеть. С целью обеспечения свежести данных в пакет данных может быть внедрен временной счетчик, который будет служить сигналом к удалению пакета в случае превышения определенного значения.

Самоорганизация требует от каждого сенсора сети быть достаточно независимым и гибким для возможности самовосстановления в топологии в зависимости от различных ситуаций. Данное свойство необходимо потому, что сенсорные сети обычно являются децентрализованными по своей природе, то есть не имеют фиксированной инфраструктуры. Данная особенность доставляет определенные трудности в обеспечении безопасности. В случае отсутствия самоорганизации ущерб, полученный в результате атаки, может быть разрушительным.

Временная синхронизация является необходимым свойством, на котором основывается успешная работа различных механизмов и протоколов в сенсорных сетях. Как и в любой распределенной системе, временная синхронизация необходима в сенсорных сетях для определения общей шкалы

времени для всех узлов сети и их локальных встроенных временных механизмов.

Защищенная локализация необходима для обеспечения способности сенсорной сети с точностью и автоматически обнаруживать каждый узел сети (например, неисправный узел). К сожалению, злоумышленник может с легкостью манипулировать незащищенной информацией о местоположении, например, посредством ложных сообщений об интенсивности сигнала или посредством воспроизведения сигналов.

**3. Атаки на беспроводные сенсорные сети**

Большинство угроз информационной безопасности в беспроводных сетях схожи с угрозами и атаками на проводные сети, за исключением того что беспроводные сети труднее защитить вследствие использования открытой среды в качестве канала передачи данных и широковещательной природы беспроводных соединений. Рисунки 1 и 2 иллюстрирует классификацию общих атак и атак на беспроводные сенсорные сети.

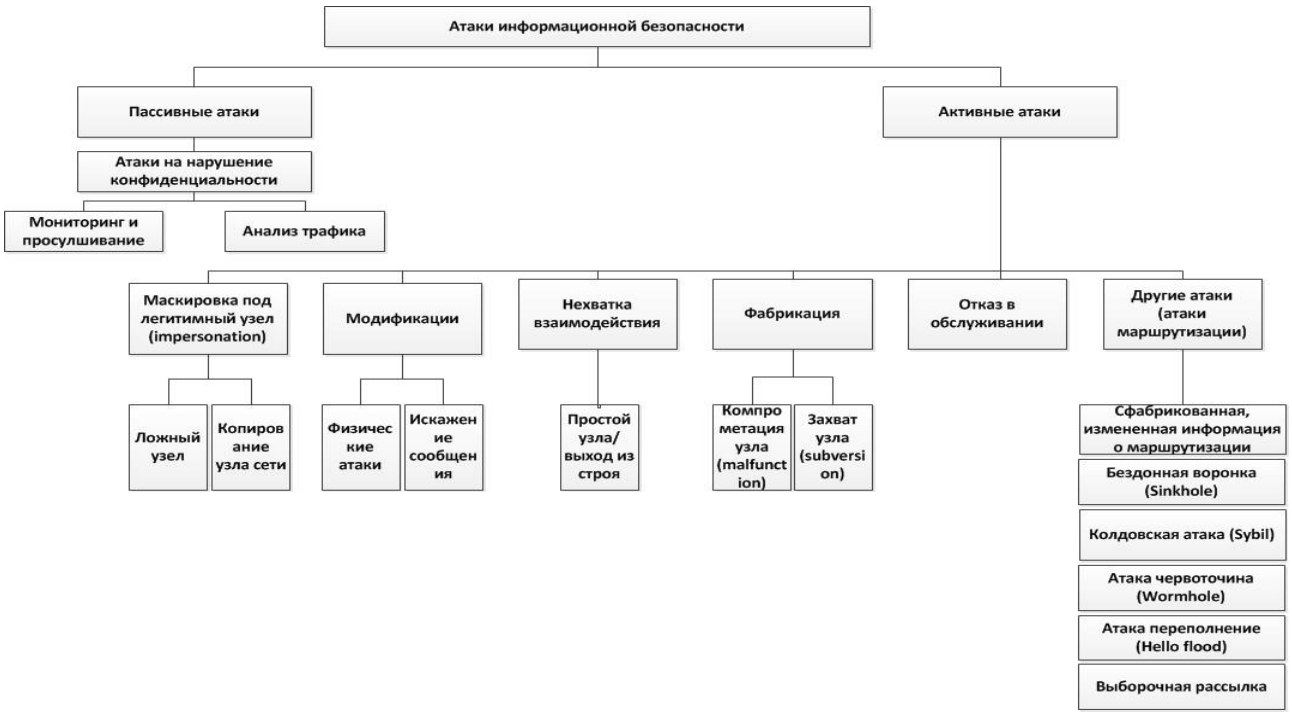



***Рисунок 1. Классификация общих атак***

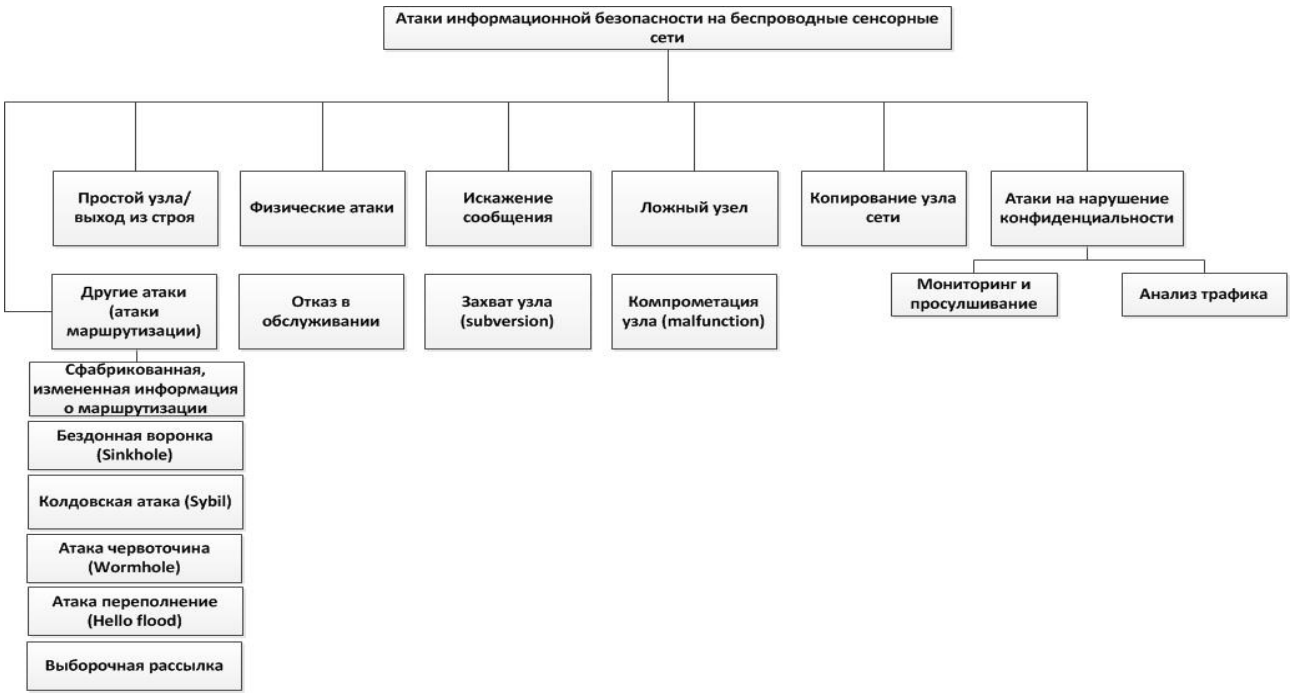



***Рисунок 2. Классификация атак на БСС***

### 3.1.Пассивные атаки

Анализ трафика и прослушивание коммуникационного канала неавторизованными лицами классифицируется как пассивная атака. Атаки, нацеленные исключительно на получение передающихся данных являются пассивными по своей натуре. Наиболее частыми являются следующие виды атак направленные на нарушение конфиденциальности данных:

*Мониторинг и прослушивание.* Данный вид атаки встречается наиболее часто. Посредством подслушивания злоумышленник может с легкостью получить доступ к передающимся данным. При передаче контрольной информации о конфигурации сети, данная техника может представлять наибольшую опасность для конфиденциальности данных.

*Анализ трафика.* Даже когда информация передается в зашифрованном виде, остается вероятность использования злоумышленником техники анализа коммуникационных паттернов. Активность сенсоров потенциально может раскрыть достаточно информации для нанесения злоумышленником вреда сенсорной сети.

### 3.2.Активные атаки

Различные модификации данных во время коммуникации, осуществляемые неавторизованными лицами, классифицируются как активные атаки. Ниже предоставляются описания активных атак.

#### 3.2.1. Атаки маршрутизации

Атаки, осуществляемые на сетевом уровне (network layer) модели OSI называются атаками маршрутизации. Следующие атаки маршрутизации встречаются наиболее часто:

*Измененная маршрутная информация.* Данной атаке наиболее подвержены децентрализованные сети, где каждый узел является маршрутизатором и соответственно может изменять маршрутную информацию. Вследствие данной атаки могут происходить закольцовывания маршрута, увеличиваться время пакета данных в пути до точки назначения и т. д.

*Выборочная рассылка.* Скомпрометированный узел сенсорной сети может выборочно удалять определенные пакеты. Особенно эффективной данная атака может быть в комбинации с атаками, которые собирают большое количество трафика на оном узле сети. В результате данной атаки серьезно страдает целостность и доступность данных, что может существенно снизить уровень сервиса, предоставляемый сенсорной сетью [2, с. 299—300].

*Атака «бездонная воронка» (Sinkhole Attack)*. Данная атака характерная тем, что скомпрометированный узел сети начинает действовать подробно воронке, привлекая весь трафик сенсорной сети [7, с. 681—683]. В особенности в сетях с протоколом маршрутизации, основанном на широковещательной рассылке, злоумышленник «слушает» запросы на маршруты и отвечает сенсорным узлам, что «знает» кротчайший маршрут до базовой станции. Как только скомпрометированному узлу удалось встать между транслирующим сенсорным узлом и базовой станцией, он может производить любые действия с приходящими пакетами данных.

*«Колдовская» атака (Sybil attack).* Во время данной атаки один скомпрометированный узел может использовать несколько псевдо идентификаторов,

выдавая себя сразу за несколько узлов. Подобные атаки используются для нарушения механизма распределенного хранения, механизмов маршрутизации, механизмов агрегации данных, механизмов голосования в сети и т. д. По существу любая сеть с равноправными узлами (в особенности беспроводные и децентрализованные сети) является подверженной данной атаке.

*Атака «червоточина» (Wormhole attack).* Данная атака предусматривает создание специального пути между двумя и более скомпрометированными узлами сенсорной сети для передачи по ним перехваченных пакетов, доступных только для атакующей системы [8, с. 1976—1978]. Подобные атаки представляют серьезную угрозу безопасности сенсорной сети потому, что не требуют компрометации узла сенсорной сети. Тогда когда узел B (базовая станция или обыкновенный узел) использует широковещательную рассылку для запроса маршрута, злоумышленник получает данный запрос и перенаправляет его ближайшему соседу. Любой узел, получивший подобный перенаправленный запрос рассматривает себя как узел, находящейся в зоне досягаемости узла B и запоминает узел B как своего «родителя». Даже если данный узел находится на большом расстоянии от узла B и его отделяют от узла B множество сенсорных узлов, он будет рассматривать узел B как следующий от себя.

*Атака «переполнение» (HELLO flood attack).* Данная атака является широковещательной атакой, призванной направить в сенсорную сеть массу необязательных сообщений, которые должны лишить сеть разнообразных ресурсов — канальной емкости, вычислительной мощности, энергетических ресурсов и т. д. Во время подобной атаки злоумышленник с помощью высокочастотного радиопередатчика с достаточной вычислительной мощностью рассылает Hello пакеты множеству узлов сенсорной сети. Узлы, получившие Hello пакеты, рассматривают скомпрометированный узел как своего соседа. Во время следующей передачи данных, они будут использовать полученный адрес из Hello пакетов для отправки. Таким образом, злоумышленник получит доступ к данным.

### 3.2.2. Отказ в обслуживании

Данный вид атаки может быть результатом неумышленного выхода из строя узлов сенсорной сети или же результатом действий злоумышленников. Простейшая атака такого рода направлена на трату всех ресурсов, доступных скомпрометированному узлу посредством отправки ненужных пакетов данных, таким образом препятствуя легитимным пользователям сети получать предназначенные им сервисы и ресурсы [6, p. 27]. Данная атака подразумевает не только попытки злоумышленника разрушить сеть или разорвать соединение, но и любое событие, снижающее способность сети предоставлять определенные сервисы и ресурсы. Множество типов подобных атак может быть осуществлено на разных уровнях модели OSI.

### 3.2.3. Захват узла (node subversion)

Захват узла злоумышленником может повлечь раскрытие важной информации, например, криптографических ключей, что в свою очередь может повлечь компрометацию всей сенсорной сети [3, с. 6].

### 3.2.4. Неисправность узла (malfunction)

Неисправный в результате атаки узел генерирует неверные данные, что может нарушить целостность сенсорной сети, в особенности, если неисправный узел является узлом агрегирующим данные, например, главным узлом кластера [3, с. 6].

### 3.2.5. Простой узла/выход из строя

Простой узла или его выход из строя случается тогда когда узел перестает функционировать. В случае выхода из строя главного узла кластера, протокол сенсорной сети должен быть способен предоставить альтернативный маршрут для пакетов данных.

### 3.2.6. Физические атаки

Узлы сенсорной сети часто устанавливаются в средах с внешними воздействиями. В таких средах маленький форм фактор узлов сенсорной сети в сочетании с отсутствием постоянного присмотра за ними делает их подвер-

женными различным физическим атакам. В отличии от других видов атак, физические атаки разрушают сенсоры необратимо.

### 3.2.7. Искажение сообщения

Любое изменение контента сообщения злоумышленником неизбежно компрометирует целостность передающихся данных [4, с. 40].

### 3.2.8. Ложный узел

Данный вид атак предполагает внедрение в сеть узла, который посылает узлам сенсорной сети некорректные данные. Данная атака является одной из наиболее опасных атак, поскольку внедренный узел, распространяющий злоумышленный код, может привести к гибели всю сенсорную сеть [4, с. 40].

### 3.2.9. Копирование узла сети

Концептуально данная атака состоит в следующем: злоумышленник пытается внедрить заранее подготовленные узлы в существующую сенсорную сеть, используя идентификаторы уже существующих узлов в данной сети. Для этого злоумышленник физически захватывает один узел сети с целью получения его уникальных данных. Полученные данные впоследствии используются для конфигурации заранее подготовленных узлов, которые впоследствии становятся клонами захваченного узла. Посредством внедрения реплицированных узлов в определенные точки сетевой топологии злоумышленник может с лёгкостью управлять сегментом сети.

## 4. Механизмы обеспечения безопасности

Механизмы обеспечения безопасности используются для идентификации, предотвращения и восстановления после атак. Механизмы обеспечения безопасности можно условно разделить на механизмы высокого и низкого уровня. Рисунок 3 иллюстрирует классификацию механизмов обеспечения безопасности.


***Рисунок 3. Механизмы безопасности***

### 4.1. Механизмы обеспечения безопасности низкого уровня

*Управление ключами и установление доверия.* Из-за лимитированных ресурсов, в особенности ресурсов энергетической батареи, ассиметричное шифрование ключами не должно использоваться для сенсорных сетей. Таким образом, необходимо использовать симметричное шифрование. Техники установления и управления ключами должны быть подходящими для использования в сетях с сотнями и тысячами узлов. Кроме того, коммуникационные паттерны сенсорных сетей отличаются от традиционных аналогов, узлы сенсорной сети должны устанавливать ключи с их соседями и с узлами, агрегирующими информацию. Недостаток этого метода состоит в том, что злоумышленники, скомпрометировав большое количество узлов сети, могут восстановить весь пул ключей и расшифровать данные [5, с. 53—57].

*Секретность и аутентификация.* Сенсорные сети требуют защиты от прослушивания, внедрения и модификации пакетов. Криптография является стандартной защитой. Сложности возникают в процессе применения криптографии для сенсорных сетей. В сетях с равноправными узлами, криптография с межконцевым шифрованием (end to end cryptography) позволяет достичь высокого уровня безопасности, однако требует установления ключей между всеми узлами сети и является несовместимой с широковещательной рассылкой и пассивным участием (технология, благодаря которой узел, прослушивающий соседний к нему узел сети может решить не передавать данные, в случае если точно такие данные передаются соседним узлом).

Криптография на канальном уровне упрощает установку ключей и поддерживает пассивное участие и широковещательную рассылку, однако позволяет промежуточным узлам перехватывать и изменять сообщения.

*Устойчивость к отказам в обслуживании (DOS).* Причинами отказа в обслуживании могут быть неполадки аппаратного обеспечения, ошибки в программном обеспечении, нехватка ресурсов, условия внешней среды или совокупность влияния перечисленных факторов. Например, злоумышленник может попытаться вывести сенсорную сеть из строя посредством передачи мощного сигнала, который способен полностью заглушить все коммуникации узлов сенсорной сети. Технология расширенного спектра используется для защиты сенсорных сетей от подобных атак. Она предполагает использование методов намеренного расширения диапазона частот сигнала. Диапазон частот становится большим, чем необходимо для передачи сообщения. Передача такого сигнала похожа на шум, что позволяет снизить риски намеренной интерференции сигнала со стороны злоумышленников.

*Защищенная маршрутизация.* Маршрутизация является ключевым процессом, без которого невозможно осуществление коммуникации между узлами сенсорной сети. Однако современные протоколы маршрутизации содержат множество уязвимостей информационной безопасности. Простейшие атаки могут подразумевать внедрение скомпрометированной маршрутной информации в сенсорную сеть, что впоследствии создает проблемы в передачи данных от отправителя в конечную точку назначения сети. Разработка новых схем аутентификации и защищённых протоколов маршрутизации может защитить сети от подобных атак.

*Защита от захвата узла.* Захват узла является серьезной проблемой защиты данных в сенсорных сетях. Часто сенсорные сети устанавливаются в легкодоступных для злоумышленников местах. Злоумышленник, захватив узел сети, может заполучить криптографическую информацию, перепрограммировать узел сети или заменить изъятый узел злоумышленными узлами. Наиболее распространенными методами защиты являются использование

защищенной от взлома упаковки, алгоритмических решений, техники хеширования.

### 4.2. Механизмы обеспечения безопасности высокого уровня.

*Защищенное управление группой.* Каждый узел беспроводной сенсорной сети ограничен в вычислительных ресурсах и коммуникационных возможностях. Однако такие функции как агрегацию сетевых данных и их анализ может осуществлять группа узлов сенсорной сети. Например, группа сенсоров сети может выполнять совместное слежение за передвижением определенного объекта. Узлы сенсорной сети в группе могут постоянно и быстро меняться. Вследствие этого, необходимы защищенные протоколы для управления группами узлов сенсорной сети, которые должны позволять защищенное принятие узлов в функциональные группы и поддерживать защищенные коммуникации узлов-членов функциональных группы.

*Идентификация вторжений.* Беспроводные сенсорные сети подвержены различным вторжениям. Основная задача механизмов идентификации вторжений состоит в мониторинге сенсорной сети, идентификации возможных попыток проникновения и рассылки соответствующих уведомлений пользователям. Для децентрализованных механизмов идентификации вторжений использование защищенных групп может быть перспективным подходом [5, с. 53—57].

*Защищенная агрегация данных.* Данные собираемые с узлов сенсорной сети затем часто агрегируются на уровне базовой станции. Благодаря агрегации данных с помощью сенсорной сети можно рассчитать среднюю температуру в географическом регионе, комбинировать данные сенсорных узлов для расчета местоположения и скорости транспортного средства и т. д. Точки агрегации данных подвержены различным видам атак и должны быть надежно защищены. Скомпрометированные узлы могут быть использованы для внедрения ложных данных, которые впоследствии приведут к неправильным агрегированным расчетам. Защищенные протоколы маршрутизации и схемы аутентификации полезны для предотвращения внедрения ложных данных в сенсорную сеть.

## 5. Заключение

Установка сетей в агрессивные среды с повышенным влиянием внешних факторов делает их подверженными атакам. Беспроводные сети применяются во многих сферах человеческой деятельности, например: в военных целях, для мониторинга окружающей среды, в медицине и т. д. Беспроводные сети имеют ряд отличительных свойств от проводных аналогов. Безопасность является важной составляющей установки и использования беспроводных сенсорных сетей. Данная статья содержит классификацию атак на беспроводные сенсорные сети и механизмов обеспечения безопасности беспроводных сенсорных сетей.

**Список литературы:**


1. John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, “Wireless Sensor Network Security: A Survey”, Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10—15, year 2006.
2. Chris Karlof, David Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, AdHoc Networks (elsevier), Page: 299—302, year 2003.
3. Pathan A.S.K.; Hyung-Woo Lee; Choong Seon Hong, “Security in wireless sensor networks: issues and challenges” Advanced Communication echnology (ICACT), Page(s):6, year 2006.
4. Zia T.; Zomaya A., “Security Issues in Wireless Sensor Networks”, Systems and Networks Communications (ICSNC) Page(s):40—40, year 2006.
5. Adrian Perrig, John Stankovic, David Wagner, “Security in Wireless Sensor Networks” Communications of the ACM, Page 53—57, year 2004.
6. Blackert W.J., Gregg D.M., Castner A.K., Kyle E.M., Hom R.L., and Jokerst R.M. Analyzing interaction between distributed denial of service attacks and mitigation technologies // Proc. DARPA Information Survivability Conference and Exposition, — Volume 1. — 24 April, — 2003. — Pp. 26—36.
7. Culpepper B.J., Tseng H.C. Sinkhole intrusion indicators in DSR MANETs // Proc. First International Conference on Broad band Networks. 2004. — Pp. 681—688.
8. Hu Y., C. Perrig, Johnson D.B. Packet leashes: a defense against wormhole attacks in wireless networks // Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, — Volume 3. — 3 April 2003. — Pp. 1976—1986.

# СЕКЦИЯ 7.

# ЭНЕРГЕТИКА

## УЛУЧШЕНИЕ КАЧЕСТВА РАБОТЫ СИСТЕМ ВЕНТИЛЯЦИИ

***Комбин Николай Николаевич***
*студент 3 курса, кафедра электроснабжения промышленных предприятий*
*ФГБОУ ВПО ОГУ,*
*РФ, г. Оренбург*
*E-mail: 2806293@gmail.com*

Рекомендация положительно внедряется на предприятиях промышленности, в образовательных и общественных учреждениях. Чаще всего применяется к вентиляционным системам притока и вытяжки

Для большинства предприятий с непрерывным производством характерна постоянная работа вентиляции независимо от времени года и условий окружающей среды.

При особых случаях оборудование вентиляции работает совместно с основным технологическим оборудованием, так как при работе выделяются вредные примеси, их необходимо удалять, обеспечивая воздухообмен. Таким образом, оборудование вентиляции притока и вытяжки должно обладать такими свойствами, как высокая надежность, безопасность, безаварийность.

Вентиляционная вытяжка внутри рабочего помещения улавливает и отводит опасные вещества, а также газ, дым, тепло от работы оборудования. Уже на этом уровне оборудование вентиляции работает эффективно, так как загрязнения воздуха удаляются сразу после их выделения оборудованием.

Стоит отметить, что система местной вентиляции не способна полностью удалить все химические вещества и локализовать их, тогда необходима система общего вентилирования [2].

ПРЕДЛАГАЕМОЕ ТЕХНИЧЕСКОЕ РЕШЕНИЕ

Предложено установить частотный регулятор вращения приточных вентиляторов. Таким образом, появляется возможность вывода вентиляционной

системы в рабочий режим, отвечающий требованиям проекта, снизив общее электропотребление.

Возможна установка преобразователей, обеспечивающих равномерный пуск приводов каждого вентилятора, отдельно от остальных.

Снаружи внутрь воздух проходит через входной канал и через центральный воздуховод подходит к вентиляционному мотору системы. Перед распределением в помещения, воздух очищается с помощью фильтров.

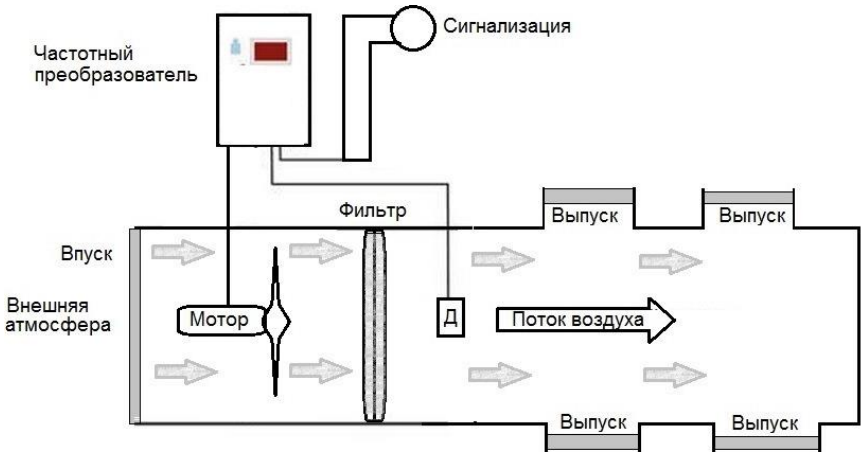



***Рисунок 1. Основной вариант схемы вентиляции***

Благодаря связи привода вентилятора и преобразователя частоты осуществляется регулирование скорости вращения привода для сохранения необходимого уровня давления и объема, подаваемого в систему воздуха. Датчик (Д) регистрирует изменения значений давления, то есть, налажен обратный контакт с частотным преобразователем. Засорение фильтра воздуха в основном канале определяется по изменению величины давления регистрируемого датчиком. Увеличивая скорость вращения вентилятора, частотный преобразователь поддерживает постоянное давление в системе. При полном засорении воздушного фильтра работа вентилятора прекращается и подается сигнал. До применения регуляторов частоты в основном использовали задвижки вентиляции [3]. Регулирование позволит получить следующий результат. (Рисунок 2).

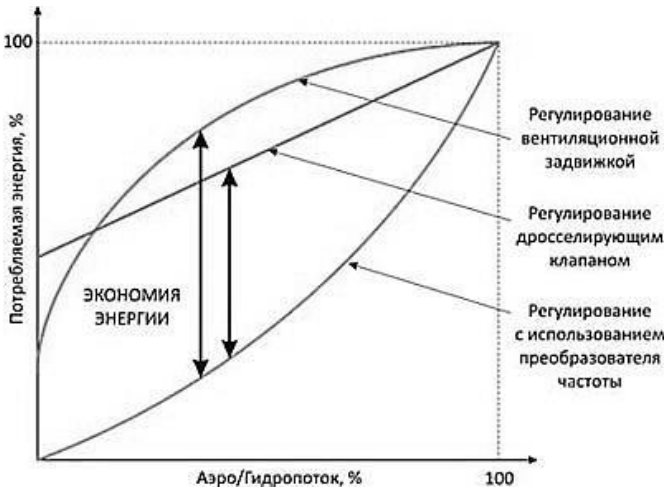



***Рисунок 2. Уменьшение затрат энергии преобразователем***

Техническое обоснование

Уменьшение количества оборотов вентилятора позволит снизить количество воздуха, попадающего в систему на 10 % [4].

$$n_2 = n_{\text{ном}} \cdot \frac{Q_{\text{факт}}}{Q_{\text{ном}}} \tag{1}$$

где: $n_{\text{ном}}$ — номинальное количество оборотов вала двигателя привода об/мин;

$Q_{\text{ном}}$ — общая номинальная эффективность вентиляторов притока;

$Q_{\text{факт}}$ — фактическая эффективность вентиляторов притока, зависит от характеристик установок вентиляции.

Сэкономленная энергия будет составлять:

$$\Delta W = P_{\text{потр}} - \frac{P_{\text{ном}}}{\eta_{\text{дв}} \cdot \eta_{\text{пч}}} \cdot \left(\frac{Q_{\text{факт}}}{Q_{\text{ном}}}\right)^3 \cdot T_{\text{см}} \cdot N_{\text{дн}} \tag{2}$$

где: $T_{\text{см}}$ — количество часов работы системы за смену,ч;

$N_{\text{дн}}$ — количество рабочих смен в году;

$\eta_{\text{пч}}$ — 0,95—0,99 КПД частотного преобразователя;

$\eta_{дв}$ — общий КПД приводных двигателей.

В денежном выражении экономия равна, руб:

$$\Delta Э = \Delta W \cdot Ц_{ЭЭ} \quad (3)$$

где $Ц_{ЭЭ}$ — цена на электричество, руб./кВт·ч.

Уменьшив пусковые токи установкой на привод двигателя регулятора частоты, получим меньший износ, то есть меньше затрат на ремонт, полученная таким образом экономия достаточно велика.

В результате, после внедрения данного мероприятия оптимизированы подача и отвод воздуха из помещения. Создана гибкая, легко регулируемая система, сохраняющая высокие значения КПД. Получен благоприятный режим работы с меньшей нагрузкой на оборудование и необходимостью ремонта. Улучшены условия труда, так как снижены шум и вибрация от работы оборудования вентиляции [1].

Внедрение на объект

Приведенные рекомендации использовали на предприятии (энергопотребление в 2010 году оценивалось в 64 тысячи т.у.т энергетических ресурсов, 57 тысяч МВт·ч электроэнергии) [4].

В данный момент эффективность вентиляционного оборудования вытяжки и притока воздуха (ВУ-2, ПУ-2) на участке не регулировалась. В процессе изучения работы техники, в частности электродвигателей, диагностика шла в течение полных суток, ночью при отключенном оборудовании.

Мощность привода электродвигателя вентилятора вытяжки: $P_{номВУ-2}$ = 35 кВт; КПД электродвигателя $\eta_{двВУ-2}$=0,92; также были проведены замеры коэффициента загрузки $K_{ЗВУ-2}$ = 0,57 и потребления мощности по факту.

Мощность привода электродвигателя вентилятора притока: $P_{номПУ-2}$ = 40кВт; КПД электродвигателя $\eta_{двПУ-2}$=0,88; после замеров определили коэффициент загрузки $K_{ЗПУ-2}$ = 0,35 и потребление мощности по факту.

Период работы вентилятора равен 17 часов ($T_{см}$) 248 дней ($N_{дн}$) в году. Проводим установку частоторегулятора на каждый вентилятор системы (ориентировочный КПД 97 %). Кроме этого перечисляется дополнительное оборудование для установки всей системы регулирования: частотный преобразователь 2 шт, 75 кВт; газоанализатор 2 шт; датчики температуры и давления.

При реализации мероприятия капитальные затраты будут равны К=950 тыс. руб. Значения эффективности колеблются в пределах 28—58 %, так как нагрузка вентиляторов динамична. Таким образом, когда эффективность снизилась на $Q_1 = (1 - 0.28) \cdot Q_{ном}$ рабочий режим ($2/3$ смены), вытяжные установки возьмут из сети $P^1_{ВУ-2} =$ 21,6 кВт., приточные $P^1_{ПУ-2} =$ 19.2 кВт. Без нагрузки – $Q_2 = (1 - 0.58) \cdot Q_{ном}$ (1/3 смены) то есть сети $P^2_{ВУ-2} =$ 12,6 кВт., приточные $P^2_{ПУ-2} =$ 11.3 кВт [5].

Учитывая вышесказанное, электропотребление двигателей вентиляторов можно снизить:

для вентиляции вытяжки:

$$\Delta P^1_{ВУ-2} = P^1_{ВУ-2} - \frac{P_{номВУ-2}}{\eta_{дв} \cdot \eta_{пч}} \cdot \left(\frac{Q_{факт}}{Q_{ном}}\right)^3 =$$

$$= 21{,}6 - \frac{35}{0{,}92 \cdot 0{,}97} \cdot \left(\frac{(1 - 0.28) \cdot Q_{ном}}{Q_{ном}}\right)^3 = 7 \text{ кВт.}$$

$$\Delta P^2_{ВУ-2} = P^2_{ВУ-2} - \frac{P_{номВУ-2}}{\eta_{дв} \cdot \eta_{пч}} \left(\frac{Q_{факт}}{Q_{ном}}\right)^3 =$$

$$= 12{,}6 - \frac{35}{0{,}92 \cdot 0{,}97} \cdot \left(\frac{(1 - 0.58) \cdot Q_{ном}}{Q_{ном}}\right)^3 = 9{,}7 \text{ кВт.}$$

$$\Delta W_{ВУ} = \left(\Delta P^1_{ВУ-2} \cdot \frac{2}{3} + P^2_{ВУ-2} \cdot \frac{1}{3}\right) \cdot T_{см} \cdot N_{дн} =$$

$$= \left(7{,}0 \cdot \frac{2}{3} + 9{,}7 \cdot \frac{1}{3}\right) \cdot 17 \cdot 248 = 33{,}3 \text{ МВт} \cdot \text{ч.}$$

для вентиляции притока:

$$\Delta P^1_{\text{ПУ}-2} = P^1_{\text{ПУ}-2} - \frac{P_{\text{номПУ}-2}}{\eta_{\text{дП}} \cdot \eta_{\text{пч}}} \cdot \left(\frac{Q_{\text{факт}}}{Q_{\text{ном}}}\right)^3 =$$

$$= 19{,}2 - \frac{40}{0{,}88 \cdot 0{,}97} \cdot \left(\frac{(1 - 0.28) \cdot Q_{\text{ном}}}{Q_{\text{ном}}}\right)^3 = 1{,}7 \text{ кВт.}$$

$$\Delta P^2_{\text{ПУ}-2} = P^2_{\text{ПУ}-2} - \frac{P_{\text{номПУ}-2}}{\eta_{\text{дП}} \cdot \eta_{\text{пч}}} \cdot \left(\frac{Q_{\text{факт}}}{Q_{\text{ном}}}\right)^3 =$$

$$= 11{,}3 - \frac{40}{0{,}88 \cdot 0{,}97} \cdot \left(\frac{(1 - 0.58) \cdot Q_{\text{ном}}}{Q_{\text{ном}}}\right)^3 = 7{,}8 \text{ кВт.}$$

$$\Delta W_{\text{ПУ}} = \left(\Delta P^1_{\text{ПУ}-2} \cdot \frac{2}{3} + P^2_{\text{ПУ}-2} \cdot \frac{1}{3}\right) \cdot T_{\text{см}} \cdot N_{\text{дн}} =$$

$$= \left(1{,}7 \cdot \frac{2}{3} + 7{,}8 \cdot \frac{1}{3}\right) \cdot 17 \cdot 248 = 15{,}7 \text{ МВт} \cdot \text{ч.}$$

Общая сэкономленная электроэнергия:

$$\Delta W_{\Sigma} = (\Delta P_{\text{ВУ}-2} + P_{\text{ПУ}-2}) = 33{,}3 + 15{,}7 = 49 \text{ МВт} \cdot \text{ч}$$

В денежном эквиваленте экономия электроэнергии при тарифе $\text{Ц}_{\text{ЭЭ}} = 2{,}85 \text{ руб./кВт} \cdot \text{ч}$ будет равна:

$$\Delta Э = \Delta W \cdot \text{Ц}_{\text{ЭЭ}} = 49 \cdot 2{,}85 = 139{,}6 \text{ тыс. руб.}$$

При данных условиях мероприятия окупится:

$$\text{С} = \frac{K}{\Delta Э} = \frac{950}{139{,}6} = 6.8 \text{ года.}$$

**Список литературы:**


1. Методы составления энергобалансов промышленных предприятий. Под редакцией А.А. Ефимова. М.: Изд-во МЭИ, М.: 2000. — 48 с.
2. Преобразователи частоты. — 2015. [Электронный ресурс] — Режим доступа. — URL: http://renakom-center.ru/auxpage_nashi-uslugi/ (дата обращения 10.05.2015).
3. Системы вентиляции. — 2015. [Электронный ресурс] — Режим доступа. — URL: http://www.technowell.ru/pi-control-typical-fun-application/ (дата обращения 10.05.2015).
4. Сборник энергосберегающих мероприятий. Под редакцией М.О. Решетникова: практическое руководство. М.: Москва, 2014. — 453 с.
5. Чоджой М.Х., Энергосбережение в промышленности. М.: Металлургия, 1987. — 270 с.

# ИНТЕРГАРМОНИКИ

***Райхерт Артур Сергеевич***

***Телек Дмитрий Николаевич***

***Шпота Артём Андреевич***
*магистранты 1 курса, кафедры ЭсППОмГТУ,*
*РФ, г. Омск*
*E-mail: artyr.raickert@mail.ru*

***Планков Александр Анатольевич***
*научный руководитель, канд. техн. наук, ст. преподаватель кафедры ЭсППОмГТУ,*
*РФ, г. Омск*
*E-mail: a.a.plankov@mail.ru*

Интергармоники означают гармонические колебания с частотами, не кратными частоте питающей сети. В амплитудно-частотном спектре они расположены между каноническими гармониками, включая основную, а так же между постоянной составляющей и основной гармоникой [1].

Интергармоники возникают в процессе модуляции основной частоты и высших гармоник, и проявляются при работе таких нагрузок, как электродуговые сталеплавильные печи, статические преобразователи частоты, сварочные оборудования. Из этого следует, что интергармоники оказывают те же воздействия, что и высшие гармоники. Однако интергармоники оказывают больше влияния на электрическую сеть, чем влияние высших гармоник. При появление интергармоник происходит возникновение ненужных потерь мощности и электроэнергии [1].

Рассмотрим два механизма из-за которых также могут возникнуть интергармоники. Смысл первого заключается в возникновении составляющих в частоте питающего напряжения и его гармониках в результате изменения их амплитуд и/или углов фаз. Это вызывается быстрым изменением значений тока в электроустановках и оборудовании, которые могут быть причиной перепада напряжения. Возмущения вызываются нагрузками в переходных режимах постоянно или временно или во многих случаях при возникновении

модуляции токов и напряжений. Эти возмущения носят случайный характер и зависят от оборудования и действующих процессов [5].

Вторым механизмом является асинхронное переключение (т. е. несинхронизированное с частотой питания) полупроводниковых устройств статических преобразователей. Типичным примером являются преобразователи частоты и устройства с широтно-импульсной модуляцией. Производимые ими интергармоники можно обнаружить практически в любой части спектра питания [5].

Интергармоники видна при разных значениях напряжения и перехода из одних систем в другие. Таким образом, интергармоники, создавшиеся в сетях высокого и среднего напряжения, перетекают в сети низкого напряжения и наоборот. Амплитуда интергармоник почти не превышает 0,5 % значения амплитуды основной частоты, но в условиях резонанса могут возникнуть и большие значения [5].

Отрицательное воздействие интергармоник отражается в виде мерцания света — фликера. Основной причиной является наложение интергармоник на основную гармонику и высшие гармоники питающего напряжения. Фликер отлично просматривается в лампах накаливания и в люминесцентных лампах. Интергармоники создают колебания напряжения, тем самым вносят помехи в низкочастотные линии питания управляющих сигналов. Интергармоники вместе с колебаниями, создают искажения формы кривой напряжения питающей сети. Причина перегрузки резонансных и полосовых фильтров высших гармоник, вероятнее всего вызвана токами интергармоник [1].

На рис. 1 показан пример мерцание в типичном процессе работы дуговой печи, измеренное на вторичном контуре трансформатора [5].

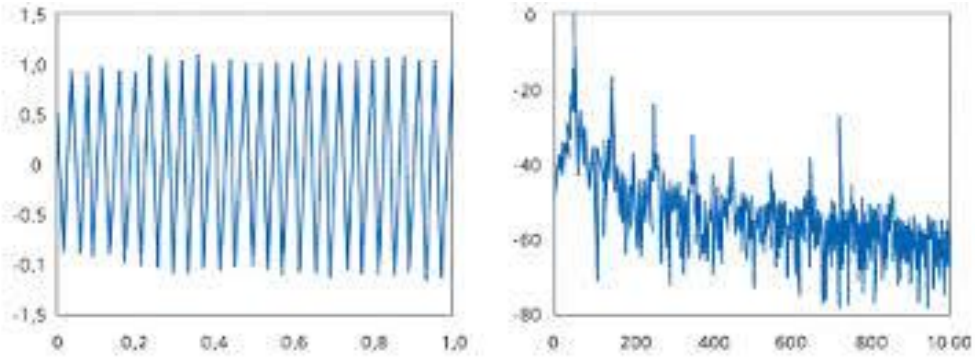



***Рисунок 1. мерцание в типичном процессе работы дуговой печи***

Значения интергармоник регулируется в [3; 4; 6].

1. ГОСТ Р 51317.4.7-2008

Указанный стандарт, используется для измерений параметров гармонических токов и напряжений в функционирующих системах электроснабжения [4].

В [3] утверждено различие между гармониками и интергармониками с одной стороны, и другими спектральными составляющими, распределёнными выше области частот гармоник до частоты 9 кГц, с другой стороны [4].

Стандарт распространяется на средства измерений (СИ), применяется для измерений спектральных составляющих напряжения и тока в полосе частот до 9 кГц, которые берутся за основу в системах электроснабжения с частотой 50 и 60 Гц [4].

На сегодняшний день стандарт отменён.

2. ГОСТ 30804.4.11-2013

В [4] представлены способы проверки электротехнических, электронных и радиоэлектронных изделий и устройств, подсоединённых к низковольтным (не должны превышать 1000 В) электрическим сетям переменного тока, на надежность к воздействию провалов, кратковременных прерываний и перепадов напряжения электропитания, а также предложные уровни испытательных напряжений при проведении испытаний на помехоустойчивость [2].

Главная задача данного стандарта заключается в установлении общих правил оценки помехоустойчивости ТС при воздействии провалов, кратковременных прерываний и перепадов напряжения электропитания [2].

3. ГОСТ Р 51317.4.30-2008

В стандарте [5]используются способы измерений показателей качества электрической энергии (КЭ) в системах электроснабжения переменного однофазного и трехфазного тока частотой 50/60 Гц и порядок оценки результатов измерений [3].

В стандарте перечислены показатели КЭ, которые относятся к:

- частоте в системе электроснабжения;
- значению напряжения системы электроснабжения;
- фликеру;
- обрывам напряжения и перенапряжениям;
- перепадом напряжения;
- переходным процессам напряжения;
- несимметрии напряжений;
- гармоникам и интергармоникам напряжения;
- сигналам, передаваемым по электрическим сетям;
- быстрым изменениям напряжения;
- установившемуся отклонению напряжения в системах электроснабжения частотой 50 Гц.

В зависимости от целей измерений могут быть проведены измерения всех показателей из указанного выше перечня либо их части [3].

Прибор для измерения интергармоники Fluke 6105A

Эталон-калибратор электрической мощности Fluke 6105A (рис. 2) был разработан как высокоточный, универсальный источник сигналов электрической мощности. Он может широко применятся для подтверждения результатов измерений в простых калибровочных лабораториях, а также для инженерного проектирования и производственных испытаний. Помимо того, что эталон-калибратор 6105A обладает мощной высокоточной «чистотой»,

он также имеет способность воспроизводить различные формы искажений с большой степенью точности. Это позволяет использовать 6105A для проверки на работоспособность стандартных устройств традиционными методами, а также при наличии искажений, различаемых в электрических системах. Указанный эталон-калибратор может помочь в решение проблем калибровки современных устройств, которые измеряют искажение напрямую [6].

**Рисунок 2. Эталон-калибратор электрической мощности Fluke 6105A**

Эталон-калибратор является точным контролируемым источником:

- чистой синусоидальной фиктивной электрической мощности,
- гармонически деформированной электрической мощности с отдельно смоделированными гармониками,
- флуктуирующих гармоник,
- интергармоник,
- провалов и выбросов,
- мерцания (фликкера),
- дисбаланса (расхождения) фаз.

Прибор 6105A является эталоном-калибратором электрической мощности; он доступен любому пользователю и применяется для проведения калибровки и измерений, а также используется для разработки огромного ряда продукции для измерения параметров электроэнергии, включая эталоны электроэнергии, трансформаторы тока и напряжения и наиболее точные анализаторы качества электроэнергии [6].

**Вывод:**

Наука, все время продвигается вперед, вместе с ней и развивается электроснабжение сетей, в которых всегда присутствуют интергармоники и создают отрицательное влияние на элементы систем электроснабжения. Из этого следует, что исследования интергармоник очень слабо изучено, на мой взгляд интергармоникам, стоит больше уделять внимание, так как это тема не раскрыта полностью.

**Список литературы:**


1. Аничков С.П. Интергармоники в электрической сети предприятий; III-я Международная научная заочная конференция «АКТУАЛЬНЫЕ ВОПРОСЫ СОВРЕМЕННОЙ ТЕХНИКИ И ТЕХНОЛОГИИ» СБОРНИК ДОКЛАДОВ,2011. — 169 с.
2. ГОСТ 30804.4.11-2013 Совместимость технических средств электромагнитная. Устойчивость к провалам, кратковременным прерываниям и изменениям напряжения электропитания. Требования и методы испытаний.
3. ГОСТ Р 51317.4.30-2008 Совместимость технических средств электромагнитная. Методы измерений показателей качества электрической энергии.
4. ГОСТ Р 51317.4.7-2008 Совместимость технический средств электромагнитная. Общее руководство по средствам измерений и измерениям гармоник и интергармоник для систем электроснабжения и подключаемых к ним технических средств.
5. Збигнев Ханзелка (ZbigniewHanzelka), АнжейБьень (AndrzejBien) AGH-UST, Краков, Республика Польша журнал«Энергосбережение», 2005.
6. Эталон-калибратор электрической мощности Fluke 6105A[Электронный ресурс] — Режим доступа. — URL: http://www.flukerussia.ru/show_full.asp?uic=28112011175124&login=fluke(дата обращения: 3.05.2015).

# АНАЛИЗ ПРЕИМУЩЕСТВ ВНЕДРЕНИЯ «УМНЫХ» ТЕХНОЛОГИЙ (SMART GRID) В РАСПРЕДЕЛИТЕЛЬНЫЕ СЕТИ 10(6)/0,4 КВ

***Токарчук Анастасия Игоревна***
*студент 4 курса, фак. Авионики, энергетики и инфокоммуникаций, УГАТУ, РФ, г. Уфа*
*E-mail: 89173623401@yandex.ru*

В настоящее время до 80 % аварийных отключений потребителей происходит из-за отказов в сетях 10(6) кВ.

Около 45 % основных фондов сетей находятся в эксплуатации более установленных нормативных сроков, а степень их износа — зачастую в критической зоне.

Очевидно, что совершенствование функционирования электроэнергетики, повышение качества и надежности электроснабжения потребителей в современных условиях возможно лишь при условии инновационного развития отрасли на основе достижений фундаментальной науки, создания и внедрения новых эффективных, более надежных и долговечных материалов, оборудования и технологий, глубокого и всестороннего диагностирования, аудита и мониторинга состояния оборудования, энергообъектов, систем управления [3].

Необходимо не просто модернизировать сеть, а автоматизировать и интеллектуализировать ее.

В настоящее время в мире, и в России в частности, исследуются и формируются новые концептуальные положения развития электроэнергетики, соответствующие новым целям и тенденциям функционирования с использованием современных методов и средств управления, оборудования и технологий производства, преобразования, транспортировки, распределения и применения электрической энергии.

Новая концепция управления, получившая за рубежом название «умной» (Smart Grids), а в России, как более соответствующая сути, — «интеллектуальной» системы, является логическим следствием эволюционного технологического развития в формирующемся информационном и предполагаемом в будущем универсальном типе общественного производства.[3]

Концепция «Smart Grid» предусматривает следующие основные задачи:

- обеспечение и повышение надежности распределительной сети;
- автоматическое управление элементами сети по адаптивным алгоритмам;
- управление режимами сети и локализация повреждений [1].

Интеллектуальная сеть или Smart Grid — это новая философия, воплощенная в комплексе организационно-технических мероприятий, основанных на информационных технологиях и современных аппаратных средствах, позволяющих достигать целевых показателей деятельности энергокомпании, не проводя глобальной реновации основных фондов:

- надежность электроснабжения потребителей;
- качество электрической энергии;
- потери электрической энергии;
- эксплуатационные затраты.

Сегодня принято выделять три ключевых подсистемы Smart Grid:

1. автоматизированные системы управления активами и режимами сетевой компании (DMS)→ выбор оптимальных стратегий развития на основании объективных данных;

2. автоматизированные системы управления аварийными режимами работы сетей (DA) → минимизация последствий повреждений в сети;

3. автоматизированные системы управления энергопотреблением (AMS) → оптимизация режимов энергопотребления и минимизация потерь электрической энергии.[2]

В России идея Smart Grid в настоящее время выступает в качестве концепции интеллектуальной активно-адаптивной сети, которую можно описать следующими признаками:

- насыщенность сети активными элементами, позволяющими изменять топологические параметры сети;

- большое количество датчиков, измеряющих текущие режимные параметры для оценки состояния сети в различных режимах работы энергосистемы;
- система сбора и обработки данных (программно-аппаратные комплексы), а также средства управления активными элементами сети и электроустановками потребителей;
- наличие необходимых исполнительных органов и механизмов, позволяющих в режиме реального времени изменять топологические параметры сети, а также взаимодействовать со смежными энергетическими объектами;
- средства автоматической оценки текущей ситуации и построения прогнозов работы сети;
- высокое быстродействие управляющей системы и информационного обмена [4].

Многократно реконструируемые существующие городские радиальные распределительные сети имеют большое количество резервных связей между распределительными пунктами 6—10 кВ (резервных перемычек), которые в нормальном режиме отключены. При авариях перемычки часто не справляются с обеспечением послеаварийного режима. В итоге низкая надежность сети.

Поиск разнообразных схемных решений направлен на создание схем позволяющих автоматизировать процесс управления ими.

При построении схем используется большое многообразие конфигураций электрических сетей. Условно их можно разделить на радиальные и замкнутые.

Схемы реальных распределительных сетей достаточно сложны и представляют собой комбинации типовых схем с большим числом ответвлений. Сложность структур распределительных сетей объясняется их историческим развитием, а также сооружением в последние годы значительного числа новых промышленных и социальных объектов, что не всегда согласовывалось с требованиями технико-экономической целесообразности.

Для примера выбрана упрощенная городская сеть, с двумя центрами питания РП-1 и РП-2. В нормальном режиме центры питания не связаны друг с другом. В таком виде сеть представляет с собой две двойные радиальные сети.

Рассмотрим как внедрение автоматизированных систем управления и систем сбора и обработки данных способствуют быстрому поиску поврежденного участка и минимизируют длительность отключения у потребителей электроэнергии.

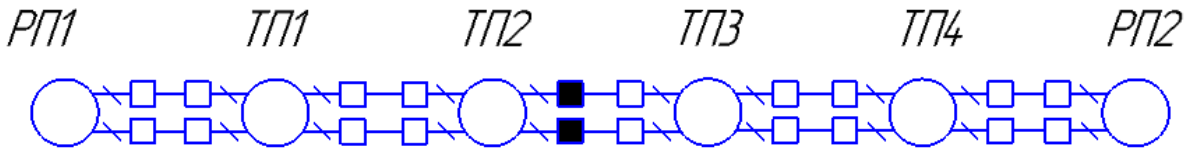



***Рисунок 1. Упрощенная схема распределительной сети 10 (6) кв.***

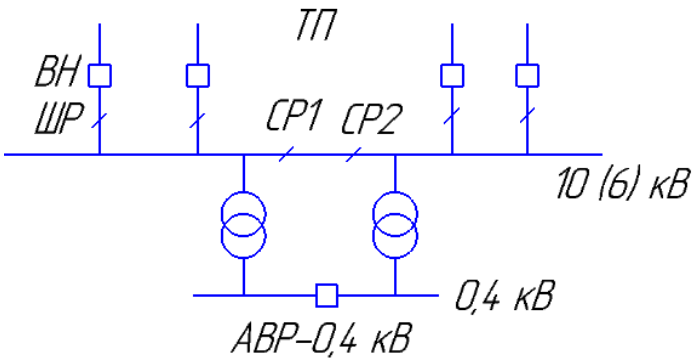



***Рисунок 2. Схема трансформаторной подстанции 10 (6) кв.***

Особенностью распределительных сетей являются недостаточная автоматизация послеаварийных переключений. Они выполняются, в основном, вручную действиями оперативно-выездной бригады (ОВБ). Поэтому, длительность отключения линии и перерыва в электроснабжении потребителей определяется длиной и конфигурацией линии, местами установки коммутационных аппаратов, местными условиями оперативного обслуживания (состоянием дорог, наличием естественных преград, пробок и т. п.), последовательностью выполняемых ОВБ операций.

Так для реализации интелектуальной сети в трансформаторых подстанций (ТП) вместо маслянных выключателей и выключателей нагрузок (ВН) с механическими приводами возможно установка вакуумных или выключателей нагрузок с подержкой управления по телемеханики. Питание каждой ТП должно осуществляется от двух разных источников питания, от разных секций шин РП. Для распределительного устройства 0,4 кВ целесообразно лишь реализация АВР-0,4 кВ.

При повреждении какой-либо линии, например участка между РП-1/1 сек. и ТП-1/1 сек. релейная защита и противоаварийная автоматика отключает поврежденный участок. В ТП-1 и в ТП-2 отработает АВР-0,4 кВ. При этом на диспетчерском пункте появляется сообщение об отключенном коммутационном оборудовании 10 кВ в РП-1 и в ТП-1. Большое количество датчиков, измеряющих и передающих текущие режимные параметры в диспетчерский пункт позволяют определить характер аварийного отключения и определить коннкретный участок повреждения. Если необходимо, то можно подать напряжение на шины 10 кВ включением коммутационного оборудования между ТП-2/1 сек. и ТП-3/1 сек. ОВБ остается выехать в ТП и проверить работу АВР-0,4 кВ и испытать кабельную линию на повреждение и вывести поврежденный участок в ремонт.

Smart Grid — это новый импульс к развитию современной энергетики, который, с одной стороны, открывает перед энергетиками новые возможности автоматизации и оптимизации процесса принятия решений в условиях постоянной неопределенности [2].

Преимущества использования сетей Smart Grid:

- увеличение надежности энергосистемы;
- сокращение времени устранения аварийных ситуаций;
- увеличение стабильности и качества подачи электричества, за счет наличия систем сбора и обработки данных;
- увеличение гибкости подачи питания, за счет создания новой архитектуры распределительной сети;

- постоянный мониторинг и контроль за электрическими режимами;
- уменьшение потерь путем выбора оптимальной конфигурации сети.

Внедрение «умных сетей» в распределительные сети требует больших капиталовложений по модернизация и расширение существующих комплексов телемеханики, замене коммутационного оборудования, а также установка измерительных трансформаторов тока и напряжения для передачи измерений режимных параметров сети. С другой стороны высокий износ основного оборудования распределительных электрических сетей напряжением 6—10 кВ на сегодняшний день, является одним из главных вопросов, который приходится решать организациям, эксплуатирующим эти сети. Существующие объемы и темпы проведения капитальных ремонтов, технического перевооружения и реконструкции распределительных сетей, позволяют только остановить наращивание темпов износа объектов электросетевого комплекса. Техническое состояние сетей и желание сократить затраты на их техническое обслуживание приводят к снижению надежности электроснабжения.

**Список литературы:**


1. Воротницкий В.В. Smart Grid: умнеть или не умнеть — вот в чем вопрос!.// В МИРЕ TEL № 1(10) 2010.
2. Ковалев Г.Ф. Электроэнергетики России.//Свободная мысль № 1(4) 2015.
3. Ледин С.С. Интеллектуальные сети Smart Grid — будущее российской энергетики.//Автоматизация и IT в энергетике — № 11 (16) — 2010. — С. 4—8.
4. Лоскутов А.Б. Городские распределительные сети 10—20 кВ с гексогональной конфигурацией.// Электротехника и электроэнергетика — № 5(102) — 2013. — С. 309—315.

# СЕКЦИЯ 8.

# МАТЕМАТИКА

## О ВЕРОЯТНОСТИ ПРОГНОЗИРОВАНИЯ АВАРИЙНОСТИ

***Аблязимов Эмиль***
*студент 2 курса, кафедра судовождения ФГБОУ ВО «КГМТУ», РФ, г. Керчь*
*E-mail: emil.a.r@mail.ru*

***Логвиненко Александр***
*студент 2 курса, кафедра судовождения ФГБОУ ВО «КГМТУ», РФ, г. Керчь*
*E-mail: sanshun@mail.ru*

***Егорова Светлана Николаевна***
*научный руководитель, старший преподаватель кафедры высшей математики и физики ФГБОУ ВО «КГМТУ», РФ, г. Керчь*

Несмотря на постоянное развитие методов, способов и технических средств обеспечения безопасности мореплавания, в море ежегодно терпит кораблекрушение более 200 крупных судов. Ежегодно в мире погибает свыше 2 000 человек, теряется более миллиона тонн грузов [1, с. 276]. Авария современного судна, построенного по последнему слову техники, наносит значительный ущерб мировому флоту. Например, за период с 1970 по 1975 г. в результате тяжелых аварий во всем мире было потеряно в общей сложности 1081 крупное морское судно. Суммарный тоннаж их превышает 5,9 млн. рег. т. В среднем, морское судоходство потеряло 15 судов каждый месяц. За последнее двадцатилетие число погибших судов увеличилось более чем в 2, а их тоннаж — в 3,6 раза [2, с. 70]. Все эти данные определяют ***актуальность проблемы*** и необходимость мероприятий, предупреждающих аварии. В современных условиях, для разработки обоснованных мер по борьбе с аварийностью необходим глубокий анализ, который выявил бы ее главные

причины, определил объективный характер ошибок и нарушений, допускаемых судоводительским составом.

Анализ статистики морских происшествий показывает, что основными причинам аварийных случаев на морском транспорте можно считать:

- ошибки судоводительского состава в управлении судном;
- низкую квалификацию членов экипажей судов;
- износ механизмов и оборудования судов;
- невнимание судовладельцев к вопросам безопасности на море [1, с. 278].

В своей работе мы анализируем статистику по всем причинам аварий за 2012—2013 год судов, плавающих под российским флагом, типом которых является рыбопромысловые и торговые суда [4, с. 3], и ставим перед собой ***задачу*** о подсчете вероятности прогнозирования аварийности с целью расстановки флота на последующие временные периоды.

В качестве математической модели процесса аварийности выберем простейший поток числа аварий $n_a$, которые происходят в группе из $N$ судов в интервале времени от $t$ до $t + \Delta t$. Понятие такого потока включает в себя три требования [3, с. 69—71]. В нашем случае: 1) стационарность потока аварий означает, что за непересекающиеся промежутки времени $\Delta t_i$ вероятности $K_i$ аварий зависят только от $\Delta t_i$ и $K_i$, а не от расположения промежутков $\Delta t_i$ на оси времени; 2) отсутствие последствия означает, что вероятность аварий в интервале времени от $t$ до $t + \Delta t$ не зависит от аварийности за время от 0 до $t$; 3) ординарность потока аварий означает практическую невозможность двух или большего числа аварий в один момент времени.

В исследовании [2, с. 91] подчеркнуто, что этим требованиям реальный процесс удовлетворяет с некоторыми оговорками. Так, отклонение процесса от стационарного связано с известной сезонностью лова, что меняет характеристики процесса, делая их зависящими от времени. В реальных условиях эксплуатации, безусловно, возможно последствие, связанное,

например, с радиооповещением об участившихся авариях из-за метеоусловий и т. п. Однако эти оговорки не исключают использования аппарата теории массового обслуживания для описания аварийности в рамках простейшего потока: с этой теории мы и начнем, а оговорки обусловливают лишь некоторое усложнение в дальнейшем.

Согласно выбранному математическому аппарату, вероятность $P_{(K)}$ числа аварий $K$ за период времени от 0 до *t* можно задать формулой вида:

$$\mathrm{P}_{(\mathrm{K})} = \frac{(\lambda nt)^K}{K!} e^{-\lambda nt}, \tag{1}$$

в которую будет входить интенсивность потока аварий $\lambda$ — число аварий на одно судно в единицу времени; $\lambda$ предполагается постоянной — согласно требованию 1. Практически эта величина может быть найдена простой обработкой статистический данных аварийности.

$$\lambda = \frac{n_a}{NT}, \tag{2}$$

где: $n_a$ — число аварий;

$N$ — общее число судов группы;

$T$ — время их эксплуатации.

Если в исследуемой группе судов отдельные подгруппы $n_i(N_i)$ эксплуатируются разное время $t_i(T_i)$, вместо *nt* или *NT* в выражениях (1) и (2) следует использовать значения $\sum_i n_i t_i$ или $\sum_i N_i T_i$ соответственно.

С помощью простых соотношений (1) и (2) можно исследовать и сравнивать аварийность в группах судов разного типа, различные виды аварийности, аварийность на различных флотах, при разнообразных условиях эксплуатации, в различных промысловых районах и т. д. При этом изменяются лишь исходные данные, используемые для определения интенсивности аварий изучаемого вида $n_a$ и $N$.

Считая $\lambda$ постоянным, запишем (1) в виде:

$$P_{(K)} = \frac{x^K}{K!} e^{-x}, \tag{3}$$

где величина $x = \lambda n t$ легко находится при известном значении $\lambda$ и заданных $n$ и $t$. Самое важное состоит в том, что зависимость вероятности $P_{(K)}$ от аргумента $x$ оказывается универсальной; в ней число аварий $K$ можно считать параметром.

При одном и том же $x$ вероятность каждого числа аварий $P_{(K)}$ оказывается различной; одна среди них является наибольшей, то есть определенное число аварий будет наивероятнейшим. Детальные исследования, не приводимые здесь, показывают, что при $K \le x \le K+1$ наивероятнейшим оказывается именно $K$ аварий.

Следовательно, для прогнозирования нужно воспользоваться не единым выражением (3) для всех $x$, а кусочно-аналитической функцией для наивероятнейшего числа аварий:

$$P_{\text{н (К)}} = \frac{x^K}{K!} e^{-x}; \; x \in (K; K+1); \; K = 0,1,2\ldots, \tag{4}$$

дающей в каждом интервале изменения аргумента $x$ вероятность того числа аварий, которое является наивероятнейшим.

Построим кривую, соответствующую этой функции, где на каждом «куске» кривой в качестве параметра проставлено наивероятнейшее число аварий $K$. Естественно, что при увеличении аргумента $x$, то есть при увеличении либо времени эксплуатации $t$, либо числа эксплуатируемых в тех же условиях судов $n$, наивероятнейшим оказывается большее число аварий, хотя сама эта вероятность падает, так как растет число различных возможных вариантов.

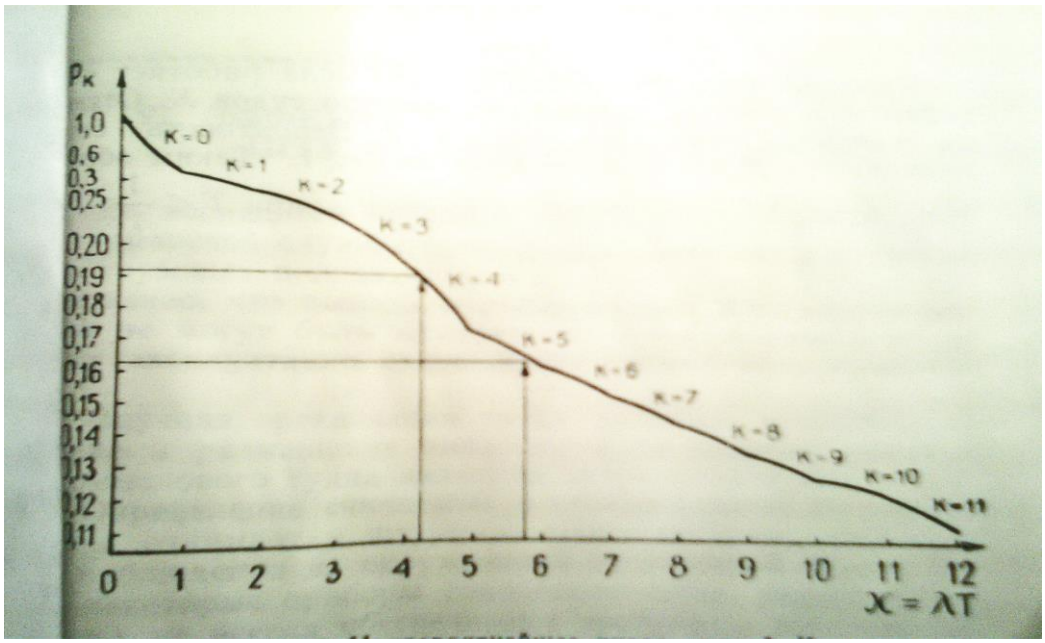



***Рисунок 1. Наивероятнейшее число аварий K***

Хорошо видно, что если $x<1$, то есть $nt<\frac{1}{\lambda}$, то наиболее вероятна безаварийная работа данной группы судов. При увеличении эксплуатационного времени или числа судов так, что $nt$ становится больше единицы, вероятнее оказывается какое-то число аварий в зависимости от величины $x$. Пользоваться графиком на рис. 1 исключительно просто. После обработки статистических данных ряда предыдущих лет эксплуатации по количеству

аварий $n_a$, по общему числу $N$ эксплуатировавшихся судов изучаемой группы и времени их эксплуатации $T$ с помощью формулы (2) находят интенсивность потока аварий. По планам расстановки флота на будущий период (график наивероятнейшего числа ) эксплуатации определяют значения $n$ и $t$ и находят величину аргумента $x = \lambda nt$. С найденным значением $x$ осуществляется вход в график рис. 1 ( показан стрелкой), по которому находят наивероятнейшее число аварий в данных условиях эксплуатации и саму вероятность. В принципе же, с помощью соотношения (3) можно найти не только наибольшую вероятность, соответствующую наивероятнейшему числу аварий, но и вероятность любого числа аварий $K$.

3

**СОСТОЯНИЕ АВАРИЙНОСТИ**
**НА ВОДНОМ ТРАНСПОРТЕ В 2013 ГОДУ**

**Состояние аварийности на море и внутренних водных путях в 2013 году по сравнению с 2012 годом**

| Классификация аварийных случаев | Год | |
|---|---|---|
| | 2012 | 2013 |
| **Аварийные случаи на море, всего** | **42** | **59** |
| **Из них:** | | |
| **Очень серьезные аварии** | **6** | **1** |
| Из них: | | |
| с судами торгового мореплавания | 2 | - |
| с рыбопромысловыми судами | 4 | 1 |
| **Аварии на море** | **36** | **58** |
| Из них: | | |
| с судами торгового мореплавания | 23 | 43 |
| с рыбопромысловыми судами | 13 | 15 |
| **Аварии на внутренних водных путях** | **4** | **5** |
| **Аварийные случаи на водном транспорте, всего** | **48** | **64** |
| **Количество погибших, человек** | **12** | **30** |
| Из них: | | |
| на море | 11 | **19** |
| на ВВП | 1 | **11** |
| Количество травмированных, человек | 3 | 49 |

**Соотношение состояния аварийности на море по месяцам**

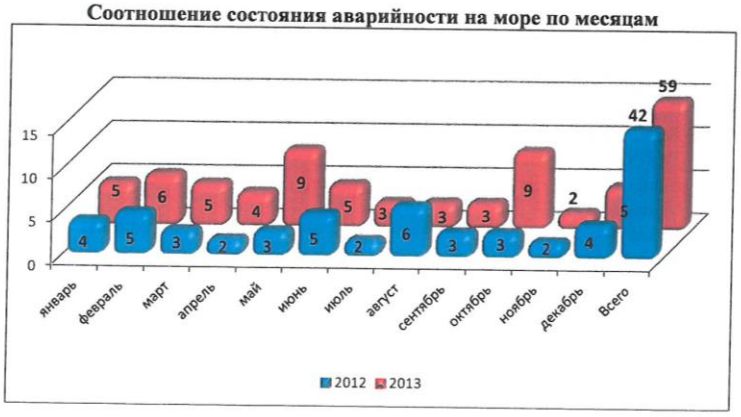


***Рисунок 2. Состояние аварийности на водном транспорте 2012—2013 гг.***

В экспериментальной части нашей работы, опираясь на данные по состоянию аварийности на водном транспорте 2012—2013 гг. [] и используя вышеприведенные формулы (1—4), мы попытались составить прогноз аварийности на 2012 год и сравнить его с реальными данными. В нашем случая $T$ = 1 год = 365 дней; $N$ = 70; $n_a$ = 42 (число аварий за год); $t$ = (28;31) в зависимости от месяца; а $\lambda$ рассчитываем по формуле (2), то есть $\lambda$ = 0,0016. Рассчитав вероятность аварий на каждый месяц данного года, строим график. За ось Ох принимаем количество месяцев, а за ось Оу- вероятность аварий на каждый месяц, в качестве параметра проставлено найвероятнейшее число аварий $K$.

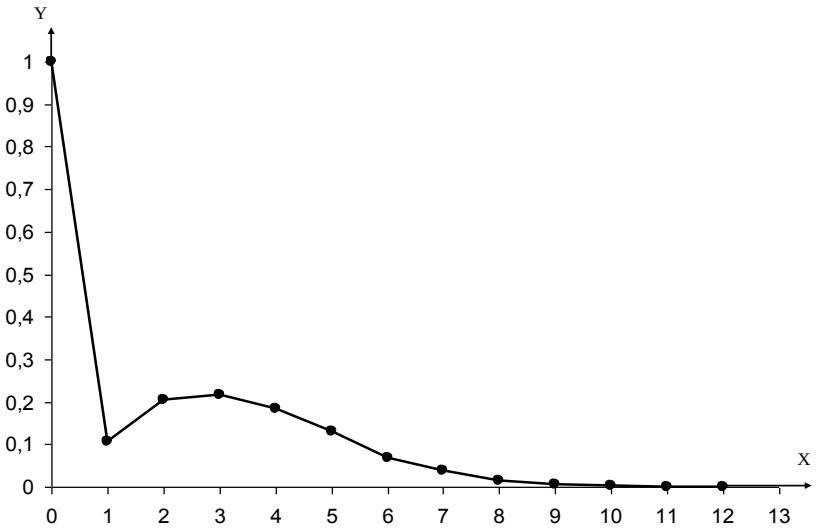



***Рисунок 3. Наивероятнейшее число аварий К за 2012 г.***

Аналогичным способом составляем прогноз на 2013 год. Здесь $T$ = 365 дней; $N$ = 70; $n_a$ =59; $t$ = (28;31) в зависимости от месяца; а $\lambda$ рассчитываем по формуле (2), то есть $\lambda$ =0,0023.

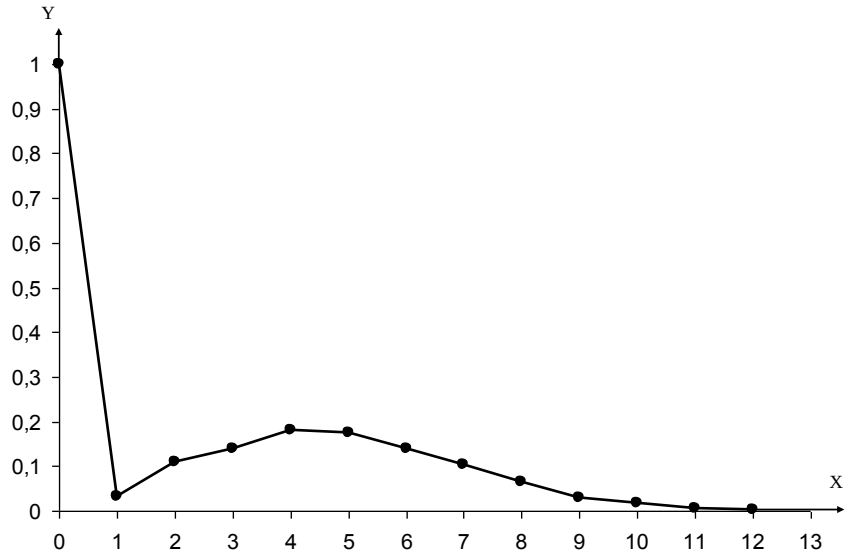



***Рисунок 4. Наивероятнейшее число аварий К за 2013 г.***

Сравнивая графики, делаем ***вывод***, что прогноз и реальные показания аварийности за 2012—2013 гг. практически совпадают. Это наблюдение доказывает эффективность использованной методики подсчета вероятности аварийности и делает ее эффективной для использования непосредственно на промысле, для оперативной расстановки флота, для информации о возможной аварийности.

**Список литературы:**

1. Авраменко Д.В., И.П. Касаткин. Причины аварийности морских судов и повышение безопасности мореплавания. [Электронный ресурс] — Режим доступа. — URL: http://shipdesign.ru/Sea/2011-02-15/3_276-279.pdf (дата обращения 18.01.2015).
2. Брандт Р.Б. Эффективность и качество работы судоводителя. Мурманск: Мурманское книжное издательство, 1978. — 112 с.
3. Гмурман В.Е. Теория вероятностей и математическая статистика. [Электронный ресурс] — Режим доступа. — URL: http://bau-enginer.ru/u/66852438/Matematika/Gmurman.pdf (дата обращения 18.01.2015).
4. Сборник аварийных случаев, произошедших в 2013 году с судами, плавающими под флагом Российской Федерации. М.: Ространснадзор, 2014. — 22 с.

# ПРОГРАММНОЕ РЕШЕНИЕ ЗАДАЧИ О ВЕРШИННОМ ПОКРЫТИИ С ПОМОЩЬЮ ПРИБЛИЖЕННЫХ АЛГОРИТМОВ

***Абрамов Андрей Викторович***
*студент 3 курса, кафедра геоинформатики и информационной безопасности,*
*СГАУ им. Королёва,*
*РФ, г. Самара*
*E-mail: Advent51@inbox.ru*

***Максимов Алексей Игоревич***
*студент 3 курса, кафедра геоинформатики и информационной безопасности,*
*СГАУ им. Королёва,*
*РФ, г. Самара*
*E-mail: fh451@yandex.ru*

***Тишин Владимир Викторович***
*научный руководитель, доцент, кафедра прикладной математики,*
*СГАУ им. Королёва,*
*РФ, г. Самара*

**Введение**

Задача о нахождении наименьшего вершинного покрытия графа на сегодняшний день является крайне актуальной, можно даже заявить, что она находится на переднем крае науки, так как точного алгоритма нахождения вершинный покрытий до сих пор не разработано. Вершинные покрытия находят широкое практическое применение — от размещения военных гарнизонов по населенным пунктам до выбора книг для прочтения из серии.

С точки зрения информатики, эта задача является NP-полной, это значит, что решить эту задачу можно за время, зависящее полиномиально от числа входных данных. Полнота же задачи означает, что к ней можно сводить другие полиномиальные задачи за конечное число операций. Таким образом, задача нахождения наименьшего вершинного покрытия является «типовой» задачей, разрешив которую, мы автоматически решаем широкий класс задач, которые можно к ней свести.

Цель нашей исследовательской работы — реализовать программу, способную строить минимальные вершинные покрытия графов.

Для ее достижения были поставлены следующие задачи:

1. Изучить алгоритмы решения задачи о наименьшем вершинном покрытии,

2. Использовать выбранные алгоритмы при создании программы.

**Основные понятия**

На всякий случай напомним основные понятия, которые фигурируют в нашей исследовательской работе. Граф — пара множеств (V,E), где V — множество вершин, E — множество ребер, представляющее собой пару элементов множества V. Если пары множества E упорядочены, то граф называется ориентированным (направленным), если нет, то неориентированным (ненаправленным). В нашей работе мы рассмотрим неориентированные графы, хотя программа, ставшая результатом нашей работы, может работать как с направленными, так и с ненаправленными графами.

Граф называется взвешенным, если его ребрам приписаны некоторые числа — веса. Веса можно интерпретировать по-разному, например, как расстояние между населенными пунктами, время проезда от одного пункта к другому, стоимость проезда между остановками и т. д. Граф часто изображается в виде диаграмм, где вершины изображаются точками, а ребра — линиями, соединяющими вершины.

Граф можно задать в виде матрицы весов – квадратной матрицы, каждый столбец и строка которой соответствуют вершине графа, а элементами являются веса ребер между данными вершинами. Именно в таком виде граф задается для нашей программы.

Вершина покрывает ребро (или ребро покрывает вершину), если они инцидентны.

Покрывающее множество вершин — множество вершин, покрывающее, все ребра графа (аналогично определяется покрывающее множество ребер).

Минимальное покрывающее множество вершин — такое покрывающее множество вершин, что удаление одной вершины из него приводит к тому, что оно перестает быть покрывающим.

Наименьшее покрывающее множество вершин — минимальное покрывающее множество с минимальным числом элементов из возможных. Число элементов в этом множестве — число вершинного покрытия.

**Формулировка задачи о вершинном покрытии**

Теперь строго сформулируем задачу, решению которой мы посвятили свою работу.

Задача нахождения вершинного покрытия графа — нахождение наименьшего покрывающего множества вершин графа.

**Приближенные алгоритмы нахождения решения**

Точного алгоритмического решения выбранной нами задачи на сегодняшний день не существует, есть только алгоритмы, дающие приближенный ответ с определенной погрешностью. Такая ситуация является вполне типичной для NP-полных задач. Однако стоит отметить, что сегодня активно разрабатываются новые и все более точные приближенные алгоритмы для вершинных покрытий. Поскольку они приближенные, то ни один из них не может гарантировать, что найденное покрытие будет наименьшим или хотя бы минимальным.

Рассмотрим два наипростейших приближенных алгоритма с «говорящими» именами, которые мы будем использовать при реализации программы.

**«Ленивый» алгоритм**

Этот алгоритм предельно прост, как в реализации, так и в понимании — мы просто берем любое ребро наугад и добавляем в покрытие одну из инцидентных ему вершин, совершенно не задумываясь о ее степени.

«Ленивый» алгоритм для вершинного покрытия заключается в следующем:

На каждом шаге, пока не кончатся все ребра в графе:

1. Выбираем случайное ребро графа $e = (u, v)$.

2. Добавляем в решение $S$ одну из выбранных вершин $u$ или $v$.

3. Удаляем из графа все ребра, инцидентные вершинам $u$ или $v$.

Алгоритм ошибается не более чем в 2 раза, за «лень» приходится дорого заплатить, однако для небольших графов этот алгоритм вполне актуален.

**«Жадный» алгоритм**

Название этого алгоритма говорит само за себя, его идея состоит в добавлении в покрытие в первую очередь вершин с наибольшей степенью, ведь они покрывают большее число ребер.

Алгоритмически это выглядит так:

На каждом шаге, пока не кончатся все ребра в графе:

1. Выбираем вершину, покрывающую наибольшее число ребер
2. Добавляем ее в решение $S$
3. Удаляем ее из графа и все ребра, ей инцидентные

Алгоритм ошибается не более чем в $1 + \ln m$ раз (m — число вершин наименьшего покрытия). Кажется, что ошибка этого алгоритма еще больше, чем у предыдущего, да еще и растет с ростом числа вершин, однако этот рост логарифмический, значит не очень резкий. На небольших графах алгоритм с большой вероятностью дает верное значение покрытия.

**Решение задачи вершинного покрытия**

Результатом нашей работы стала программа, способная находить наименьшие вершинные покрытия обоими из рассмотренных алгоритмов — и «жадным», и «ленивым». Она способна работать как с ориентированными, так и с неориентированными, как с взвешенными, так и невзвешенными графами. Так же программный продукт способен визуализировать граф в виде диаграммы.

Скажем несколько слов о том, что из себя представляет наш программнй продукт. Программа написана на Qt 5 — самой последней реализации кроссплатформенного фреймворка, возможна компиляция под все сущест-вующие платформы. Фреймворк дополняет язык C++ для более удобного программирования. Программа создана с учётом последующей возможности перевода интерфейса. Используется динамически выделяемое пространство памяти под реализацию сцены (отрисовки графических объектов) так что перегрузить программу трудно, а при минимальном количестве узлов —

расходуется минимальное количество необходимой памяти. Интерфейс понятен и с пояснениями. Так же программа собрана со статической линковкой DLL файлов, что позволяет использовать её без предварительной установки (не оставляет никаких следов в системе).

В качестве наглядного и актуального примера мы решили решить следующую практическую задачу — разместить военные гарнизоны по Центральному военному округу РФ так, чтобы они контролировали все дороги между населенными пунктами, причем в наименьшем числе городов, чтобы не распылять военные ресурсы. Вершинами графа в контексте нашей задачи будут населенные пункты, а ребрами — соединяющие их дороги. Получился ненаправленный граф на 38 вершинах.

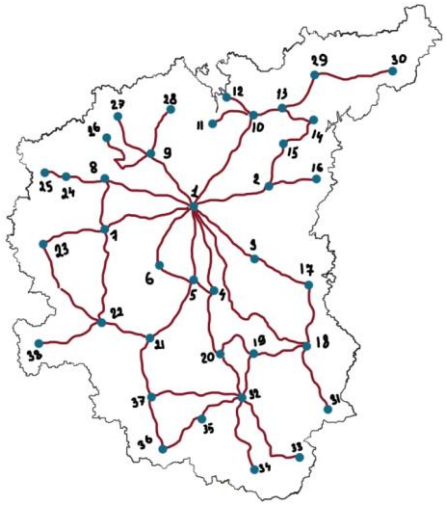


***Рисунок 1. Граф на основе карты***

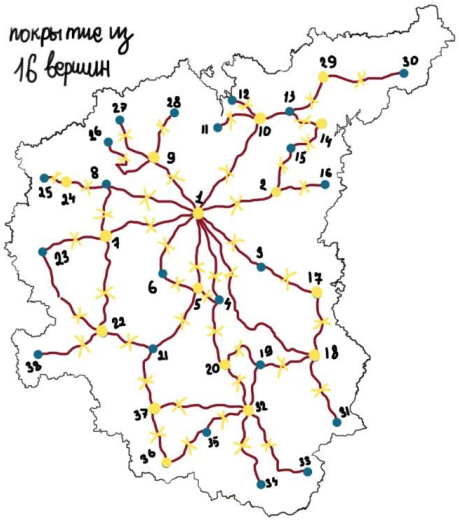



***Рисунок 2. Решение задачи без программы***

При решении задачи собственными силами в покрывающем множестве оказалось 16 вершин. Теперь посмотрим, как с этой задачей справится наша программа. Заполним матрицу смежности графа и визуализируем его.

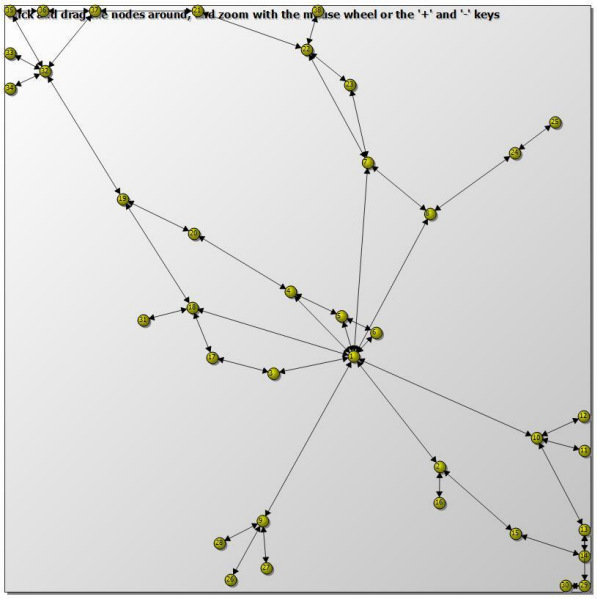


***Рисунок 3. Программная визуализация графа***

Запустим алгоритмы и проанализируем результаты их работы.

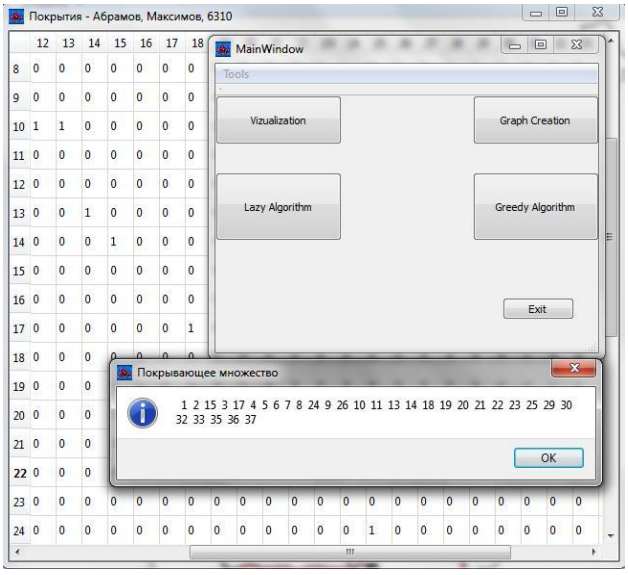



***Рисунок 4. Результат «ленивого» алгоритма***

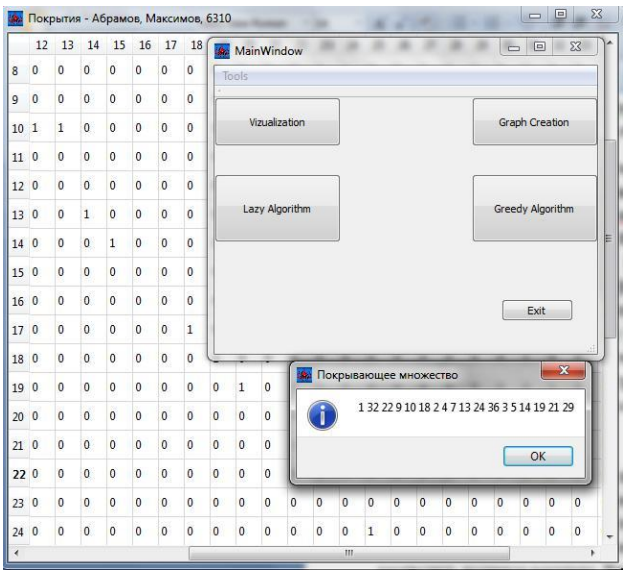



***Рисунок 5. Результат «жадного» алгоритма***

«Ленивый» алгоритм выдал нам список из 31 вершины, с одной сторон, результат не очень впечатляет, однако, как мы выяснили, алгоритм может выдать покрывающее множество в два раза боль400--ше наименьшего, так что результат его работы вполне согласуется с теорией. «Жадный» алгоритм показал себя гораздо лучше, выдав 18 вершин. Ошибка составила всего 2 вершины.

**Заключение**

Теория графов как научная дисциплина крайне интересна широтой практических задач, которые возможно решить с ее применением. Эту работу мы посвятили одной задаче этой теории — нахождению наименьшего вершинного покрытия. В рамках этой задачи был решен сугубо практический вопрос — как разместить вооруженные силы в военном округе.

Задачи, которые мы поставили на пути к достижению поставленной цели, были выполнены — изучены два алгоритма нахождения покрытий, оба они реализованы в программном виде. Так же достигнута наша основная цель — программа для нахождения вершинных покрытий успешно реализована.

Однако мы не намерены останавливаться на достигнутом, ведь задача о точном алгоритмическом нахождении наименьшего вершинного покрытия графа остается открытой.

**Список литературы:**


1. Додонова Н.Л. Конспект лекций по дисциплине теория конечных графов и ее применения Самара: 2010 — с. 52.
2. Свами М., Тхуласираман К. Графы, сети и алгоритмы. М.: Мир, 1984, — 454 с.
3. Жадные алгоритмы в задачах о покрытии Н.Н. Кузюрин С.А. Фомин [Электронный ресурс] — режим доступа. — URL: http://discopal.custis.ru/images/archive/8/82/20101202232637!Greedy-covering.beam.pdf (дата обращения 10.04.2015).

# МАТЕМАТИЧЕСКАЯ ОЦЕНКА ЭФФЕКТИВНОСТИ РАБОЧЕГО МЕСТА СУДОВОДИТЕЛЯ

***Иванцов Владимир Александрович***
*студент 1 курса, кафедра судовождения ФГБОУ ВО «КГМТУ», РФ, г. Керчь*
*E-mail: vivantsow@mail.ru*

***Куликовский Валерий Вадимович***
*студент 1 курса, кафедра судовождения ФГБОУ ВО «КГМТУ», РФ, г. Керчь*
*E-mail: kulikovskii1997@mail.ru*

***Хапугин Вадим Андреевич***
*студент 1 курса, кафедра судовождения ФГБОУ ВО «КГМТУ», РФ, г. Керчь*
*E-mail: pympa-vadim@mail.ru*

***Василенко Марк Игоревич***
*студент 1 курса, кафедра судовождения ФГБОУ ВО «КГМТУ», РФ, г. Керчь*
*E-mail: vasilenkomark@gmail.com*

***Егорова Светлана Николаевна***
*научный руководитель, старший преподаватель кафедры высшей математики и физики ФГБОУ ВО «КГМТУ», РФ, г. Керчь*

***Актуальность.*** Вопрос совершенствования штурманской службы привлекает широкое внимание отечественных и зарубежных специалистов, поскольку этот вопрос тесно связан с производительностью труда, надежностью системы «человек-машина», безаварийностью, зависит от уровня профессионального мастерства штурманского состава, новизны навигационного и промыслового оборудования [2].

Внедрение информационных технологий позволило освободить судоводителя от выполнения однообразных рутинных действий, снабдило его необходимой информацией в удобной и наглядной форме. В системах управления морскими судами (на ходовых мостиках судов) появились электронные карты, системы автоматической радиолокационной прокладки, автоматические

идентификационные системы, компьютерные системы для выполнения грузовых операций и многое другое.

Несмотря на хорошую техническую оснащенность современных судов, вопрос об эффективности рабочего места судоводителя продолжает играть одну из основных ролей в процессе правильной эксплуатации судового оборудования, обеспечивающего безопасность плавания.

***Анализ публикаций.*** Вопросам обеспечения и повышения безопасности мореплавания, судовым системам управления, автоматизации рабочего места судоводителя посвящено немало работ [1—6; 8].

Заслуживает внимание работа [2], посвященная исследованию деятельности судоводителя промыслового судна и возможных путей ее оптимизации. Автор рассматривает возможности оптимизации и повышения эффективности работы судоводителя на рыболовецком судне типа «Горизонт», где ходовой мостик совмещен с кормовой и штурманской рубками. Проблема заключалась в том, что при таком расположении помещений, судоводителю приходилось слишком долго перемещаться между приборами, а из разных частей мостика обзор был неполным или его практически не было. Р.Б. Брандт старался решить эту проблему лишь заменой приборов местами, уменьшением расстояния между ними, ликвидацией переборок и стен между помещениями и приборами, а также внося некоторые коррективы в структуру судна (например, предлагал целесообразно располагать дымоходные трубы и мачты, чтобы избежать появления так называемых «мертвых» зон в обзоре окружающего пространства из рубки).

В период его исследований это было единственным способом оптимизации рабочего места судоводителя и его функциональности. Именно поэтому мы решили сравнить его работу и современные исследования по данному вопросу, где с внедрением информационных технологий работа судоводителя сводится вплоть до удаленного управления судном.

***Целями*** нашего исследования стали:

1. изучение математических основ и особенностей работы судоводителя;

2. исследование зависимости эффективности работы судоводителя от архитектуры его рабочего места;

3. получение ряда количественных характеристик деятельности судоводителя и исследование влияния на них размещения аппаратуры в рубке.

Цели работы определили главную ***задачу***: на основании ряда количественных характеристик деятельности судоводителя сопоставить возможные пути оптимизации рабочего места, выявить наиболее актуальные и целесообразные способы решения этого вопроса.

***Основное изложение вопроса.*** Рассмотрим деятельность штурмана на ходовом мостике с количественной стороны.

Размещение приборов на ходовом мостике судна в процессе проектирования осуществляется на основе накопленного опыта: либо это экспертные оценки специалистов, либо традиции. Научное обоснованное решение этого вопроса возможно только при количественном анализе деятельности вахтенного штурмана. Цель такого анализа — получить ряд количественных характеристик деятельности и исследовать влияние на них размещения аппаратуры в рубке. Информацию о количественных характеристиках работы судоводителя в рубке можно получить, хронометрируя судовые вахты в форме кинограмм.

В работе [2] было выбрано несколько наборов характеристик: частота обращения, время перехода от одного прибора к другому, продолжительность работы с прибором в течение вахты, по различным типам промысловых судов в различных производственных ситуациях, в естественной рабочей обстановке. Это привело к необходимости применить для обработки результатов хронометража приёмы математической статистики, такие как получение средних значений и средних квадратичных отклонений.

Обозначим номера приборов нижними индексами $i$, $j$=1, 2… $N$, где $N$ — общее число приборов в рубке. Тогда введём $\omega_{ij}$ — среднюю частоту общений

от прибора с номером $j$ к прибору с номером $i$. Сумма частот по всем номерам $j$ даёт общую среднюю частоту обращения к прибору с номером $i$ за вахту:

$$\omega_i = \sum_{j=1}^{N} \omega_{ij} \tag{1}$$

Среднее время работы за вахту:

$$t_i = t_{0i}\omega_i, \tag{2}$$

где $t_{0i}$ — среднее время работы с прибором $i$ за один подход.

Аналогично можно ввести общее среднее время, затраченное на однократные переходы к прибору $i$:

$$\tau_i = \frac{\sum_{j=1}^{N} \tau_{ij}\omega_{ij}}{\omega_i}, \tag{3}$$

где $\tau_{ij}$ — среднее время перехода от прибора $j$ к прибору $i$.

Это время перехода к $i$-му прибору, пользуясь эргономической терминологией, можно назвать временем подготовки $i$-й операции — однократной работы с $i$-м прибором.

Считая скорость перемещения судоводителя в рубке примерно постоянной, независимо от ситуации и номера операции, можно вместо времени $\tau_{ij}$ ввести его координаты. Для этого в план рубки вводится произвольная система декартовых координат, где ось OX — по линии лобовой переборки, ось OY — по линии диаметральной плоскости и в этой системе каждый прибор получает свои координаты $(x_i; y_i)$:

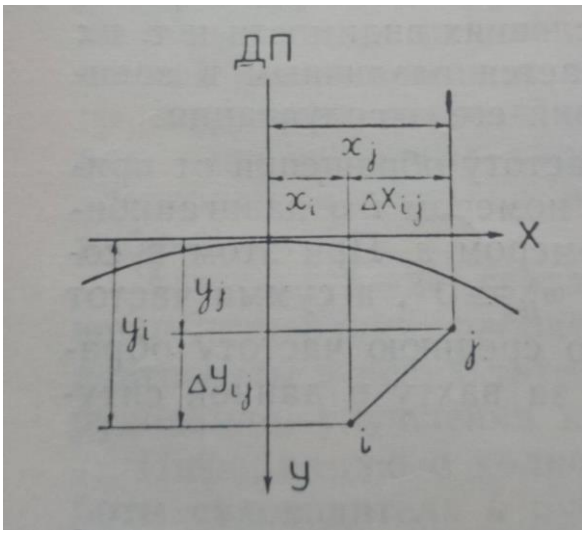



***Рисунок 1. Система декартовых координат в рубке***

Тогда расстояние между приборами $i$ и $j$:

$$d_{ij} = \sqrt{\Delta x_{ij}^{\ 2} + \Delta y_{ij}^{\ 2}} \tag{4}$$

где $\Delta x_{ij}$, $\Delta y_{ij}$ — проекции этого расстояния на выбранные оси координат.

Обозначив скорость перемещения судоводителя в рубке $V_0$, можно записать:

$$\tau_{ij} = \frac{d_{ij}}{V_0} \ , \tag{5}$$

$$\tau_i = \frac{1}{V_0 \omega_i} \sum_{j=1}^{N} d_{ij} \omega_{ij} \ . \tag{6}$$

Введенный набор средних величин можно представить комплексом в виде ориентированного графа, вершины которого соответствуют определенному прибору, а дуги — отношениям между приборами. Количественно можно сопоставить вершины и время работы с прибором, соответствующим данной вершине, дуги и частоту взаимных обращений между вершинами и расстояние между ними. На рис. 2 приведены экспериментально полученные значения вероятности использования судоводителем наиболее важных навигационно-промысловых приборов.

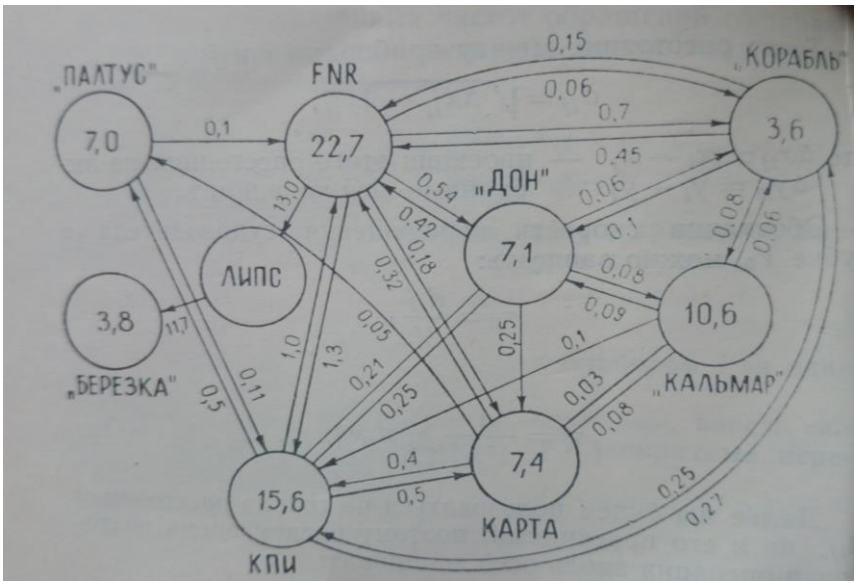



***Рисунок 2. Вероятность обращения к навигационно-промысловым приборам***

Эти данные можно ориентировочно использовать при размещении приборов на ходовом мостике. Например, вероятность обращений от FNR к ЛИПСу, от FNR к КПИ, от ЛИПСа к «Березке» достаточно высока. Отсюда следует, что эти приборы должны располагаться рядом.

В нашей работе мы также исследовали эффективность расположения средств управления навигационной и гидроакустической аппаратурой на судне *Alexander B* типа контейнеровоз. Вместимость: 14072 т., тоннаж: 18530 т.


***Рисунок 3. Контейнеровоз Alexander B***

Данные наблюдений приведены в табл. 1, где в 1-й строке указаны названия приборов, во 2-й строке показано время одного обращения к прибору (в секундах), в 3-й строке показано количество обращений к прибору за вахту,

в 4-й строке показана общая длительность использования прибора за вахту (в секундах).

***Таблица 1.***

**Количественные характеристики использования навигационной аппаратуры контейнеровоза Alexander B**

| Радар | GPS | Электр. карты | AIS | Гиро-компас | Секс-тант | Курсо-граф | Эхо-лот | Баро-граф |
|---|---|---|---|---|---|---|---|---|
| ≈3—4 | ≈5—6 | ≈5—6 | ≈5—6 | ≈10—15 | ≈10 | ≈7—8 | ≈5 | ≈3—4 |
| 5—8 | 4—5 | 10 | 10 | 10 | 5—6 | 1—2 | 3—4 | 1—2 |
| 15—32 | 20—30 | 50—60 | 50—60 | 100—150 | 50—60 | 10—20 | 20—30 | 5—10 |

Анализ наблюдений показывает, что контейнеровозы указанной модификации современной постройки (2006 г.) имеют наиболее удачное эргономическое расположение приборов на ходовом мостике. Среднее время обращения к прибору минимизировано, все приборы компактно размещены:

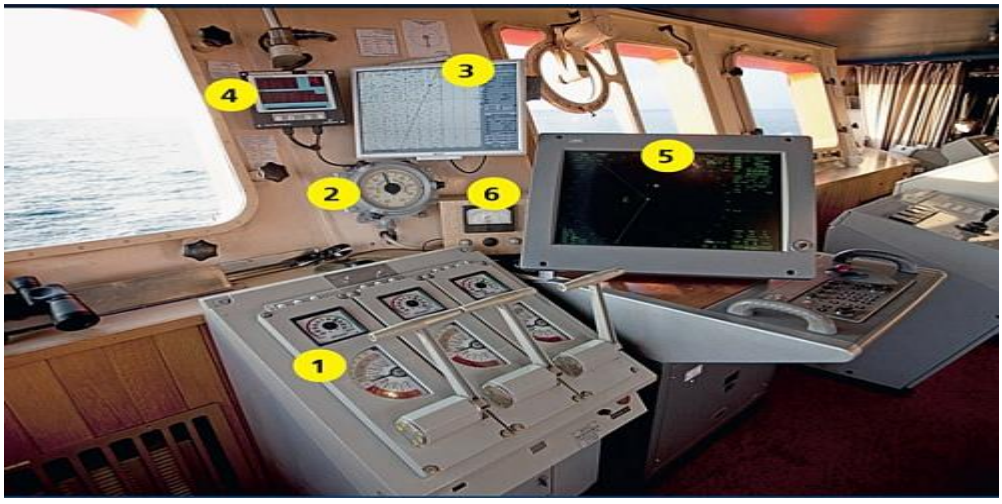



***Рисунок 4. Размещение навигационного оборудования: 1) пульт управления электродвигателями; 2) аксиометр — указатель положения руля; 3) электронная картография; 4) репитер (повторитель) эхолота и лага; 5) радиолокационная станция; 6) датчик тягового усилия лебедки***

Штурман сидит на мостике вместе с остальными членами команды. Кроме классических линеек и циркулей ему помогает современное оборудование: два GPS-навигатора и автоматическая система идентификации судов в радиусе 30 миль (нижний ряд), репитеры лага и гирокомпаса, метеостанция (средний ряд), два эхолота с самописцем (верхний ряд) на рис. 5.

***Рисунок 5. Классическое оборудование***

Перспективные исследования в области эргономики судовождения [3; 6] показывают, что в 2025 году капитанские мостики на грузовых кораблях будут выглядеть совершенно не так, как они выглядят сейчас. Основываясь на исследовании работы и нужд капитана, а также его помощников и команды, **Университет Аалто**, **VTT** и **Rolls-Royce Marine** разработали уникальную концепцию универсального капитанского мостика с дополненной реальностью:

***Рисунок 6. Капитанский мостик будущего***

Это будет система, способная распознавать каждого члена команды и подстраиваться под его индивидуальные нужды: показывать на экране, который занимает всё стекло рубки, различную запрашиваемую информацию, регулировать спинку кресла, и многое другое. На экране могут отображаться невидимые из-за тумана препятствия, курс самого корабля и проходящих рядом

морских судов, он позволит членам экипажа обмениваться между собой информацией и видеть в тёмное время суток. Кроме всего прочего, бортовой компьютер будет сообщать эти данные другим кораблям.

Параллельно с этим проектом разработчики планируют реализовать ещё одну идею: ввести дистанционное управление кораблями. Предполагается, что это позволит повысить безопасность и эффективность морских грузоперевозок и путешествий. Автономные системы начнут проникать в крупные морские суда уже в самом ближайшем будущем, и VTT и Rolls-Royce уже работают над их первым поколением. Первоначально они будут включать в себя блоки контроля, которыми можно будет дистанционно управлять с мостика или с суши. «С позиции требуемых технологий, дистанционное управление контейнерным судном возможно уже сейчас», говорит VTT в официальном релизе [6]. «Однако, до того как полностью автономные грузовые суда выйдут в море, эта концепция должна получить повсеместное общественное одобрение» [там же]. И это произойдёт до того, как VTT и Rolls-Royce создадут новый капитанский мостик будущего, и первые дистанционно управляемые корабли заступят на свою службу уже в ближайшие годы.

***Выводы.*** Исходя из результатов проделанных исследований, можно утверждать, что управление судном представляет собой большой комплекс взаимодействия технических средств и человека-оператора. Проведенная математическая оценка эффективности рабочего места судоводителя доказала необходимость эргономичного размещения навигационного оборудования. Использование автоматизированного рабочего места поможет повысить эффективность и безопасность мореплавания. На данный момент уже имеется система, находящаяся на стадии разработки, которая может выполнить данные требования по обеспечению требуемого уровня безопасности. Если будет принято решение о вводе данной системы в эксплуатацию, значительно уменьшится количество аварийных случаев и упростится порядок управления судном.

**Список литературы:**


1. Адерихин И.В., Воротынцева М.Г. Метод оценивания показателей готовности системы управления судном. Научный журнал «Вестник Астраханского государственного технического университета». Астрахань: Изд. АГТУ, — № 2, — 2005. — С. 199—204.
2. Брандт Р.Б. Эффективность и качество работы судоводителя. Мурманск: Мурманское книжное издательство, 1978. — 112 с.
3. Вагущенко Л.Л. Интегрированные системы ходового мостика. Одесса: Лат-стар, 2003. — 170 с.
4. Воротынцева М.Г. Методика оценивания показателей функционирования эргатической системы управления морским судном: дис…канд. т. н. [Электронный ресурс]. — Режим доступа: — URL: http://www.dissercat.com/content/metodika-otsenivaniya-pokazatelei-funktsionirovaniya-ergaticheskoi-sistemy-upravleniya-morsk (дата обращения: 20.01.2015).
5. Зеленин М.П. Эргономика на морском транспорте. М.: Транспорт. 1980. — 276 с.
6. Концепт виртуального капитанского мостика от Rolls-Royce: корабль без экипажа [Электронный ресурс]. — Режим доступа: — URL: http:// www.novate.ru/blogs/151214/29126 (дата обращения: 20.01.2015).
7. Пустальнин Е.И. Статистическая обработка результатов наблюдений. М.: Физматгиз, 1968. — 216 с.
8. Чертов В.В. Методика оценивания готовности эргатической системы управления судном к решению задач расхождения. Диссертация на соиск. уч. степени к.т.н. МГАВТ. М., 2001. — 172 с.

# КОЛИЧЕСТВО ОБРАЗУЮЩИХ МАТРИЦ СИСТЕМАТИЧЕСКОГО ЦИКЛИЧЕСКОГО КОДА (15,11)

***Хантова Анна Дмитриевна***
*студент 3 курса, факультет информатики*
*СГАУ им. академика С.П. Королева,*
*РФ, г. Самара*
*E-mail: ad.khantova@yandex.ru*

***Додонова Наталья Леонидовна***
*научный руководитель, доцент, кафедра прикладной математики*
*СГАУ им. академика С.П. Королева,*
*РФ, г. Самара*

**Введение**

Передачей информации можно назвать своего рода физический процесс, посредством которого осуществляется перемещение информации в пространстве и времени.

Для того чтобы перенести информацию в пространстве и времени, её представляют форме сообщения. Сообщение же всегда представляется в виде сигнала. Построение сигнала по определенным правилам, обеспечивающим соответствие между сообщением и сигналом, называют кодированием.

Если понимать кодирование в широком смысле, то это преобразование сообщения в сигнал. Кодирование в узком смысле — это представление дискретных сообщений определенными сочетаниями символов.

Одним из наиболее важных кодов является циклический код. Циклические коды применяются при записи на CD и DVD, при передаче аудио и видео информации ,при использовании USB-портов для обмена информацией.

Циклический код — это линейный код, обладающий свойством цикличности. Иначе говоря, каждая циклическая перестановка кодового слова также является кодовым словом. Циклические коды легко реализуются технически. Благодаря этому они нашли широкое применение. Также циклические коды незаменимы при необходимости передачи информации по каналам связи, в которых отсутствует возможность повторной передачи.

**Построение циклического кода.**

В процессе кодирования сообщений длинная последовательность обычно формируется из кодовых комбинаций, каждая из которых соответствует одному знаку. Число символов, из которых составлена такая кодовая комбинация, называется длиной кода.

Пусть сообщение состоит из k = 11 символов. Построим код, обнаруживающий и исправляющий одиночные ошибки.

Чтобы исправить одиночную ошибку в принятой комбинации из n разрядов, сначала нужно определить, какой именно из разрядов был искажен. Чтобы это сделать, каждой одиночной ошибке в определенном разряде должен соответствовать свой опознаватель. В циклическом коде опознавателями ошибок служат остатки от деления многочленов ошибок на образующий многочлен кода. Поэтому образующий многочлен должен обеспечить требуемое число различных остатков при делении векторов ошибок с единицей в искаженном разряде. Наибольшее число остатков дает неприводимый многочлен. При степени многочлена m=n -k он может дать 2n-k-1 ненулевых остатков. Таким образом, выполнение неравенства (1) является необходимым условием исправления любой одиночной ошибки.

$$2^{n-k}-1 \geqslant C_n^1 = n\,, \tag{1}$$

Cn — это общее число разновидностей одиночных ошибок в кодовой комбинации из n символов. Тогда степень образующего многочлена кода.

$$m = n-k \geqslant \log_2(n+1) \tag{2}$$

Посчитаем длину кода при k=11 согласно формуле (1).

Возьмем n=14

$2^{14-11}>=15$

8>=15

Это выражение не верно.

Возьмем n=15

$2^{15-11}>=16$

16>=16

Выражение верно, значит n=15,m=15-11=4.

Таким образом, мы получили код (15,11).Выберем образующий многочлен. Образующий многочлен должен быть делителем многочлена $x^n+1$, то есть в нашем случае $x^{15}+1$.

Многочлен $x^n+1$ можно представить в виде произведения всех неприводимых многочленов, степени которых являются делителями числа m.

Делители m=4: 4,2,1.

Для нахождения неприводимых многочленов нужных степеней можно воспользоваться таблицей неприводимых многочленов:

неприводимые многочлены первой степени: x+1

неприводимые многочлены второй степени: $x^2+x+1$

неприводимые многочлены четвертой степени: $x^4+x+1$; $x^4+x^3+1$; $x^4+x^3+x^2+x+1$

$x^{15}+1=(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$

Верность этого утверждения можно проверить, перемножив все неприводимые многочлены. Однако это вычисление весьма громоздкое, и я не буду приводить его здесь.

Один из сомножителей степени m=4 может быть принят за образующий многочлен код.

Составим таблицу остатков для трех неприводимых многочленов четвертой степени

***Таблица 1.***

**Таблица остатков от деления на многочлен**

| | | $g_1= x^4+x+1$ | $g_2= x^4+x^3+1$ | $g_3= x^4+x^3+x^2+x+1$ |
|---|---|---|---|---|
| E0 | 000 000 000 000 001 | 0001 | 0001 | 0001 |
| E1 | 000 000 000 000 010 | 0010 | 0010 | 0010 |
| E2 | 000 000 000 000 100 | 0100 | 0100 | 0100 |
| E3 | 000 000 000 001 000 | 1000 | 1000 | 1000 |
| E4 | 000 000 000 010 000 | 0011 | 1001 | 1111 |
| E5 | 000 000 000 100 000 | 0110 | 1011 | 0001 |

| | | | | |
|---|---|---|---|---|
| E6 | 000 000 001 000 000 | 1100 | 1111 | 0010 |
| E7 | 000 000 010 000 000 | 1011 | 0111 | 0100 |
| E8 | 000 000 100 000 000 | 0101 | 1110 | 1000 |
| E9 | 000 001 000 000 000 | 1010 | 0101 | 1111 |
| E10 | 000 010 000 000 000 | 0111 | 1010 | 0001 |
| E11 | 000 100 000 000 000 | 1110 | 1101 | 0010 |
| E12 | 001 000 000 000 000 | 1111 | 0011 | 0100 |
| E13 | 010 000 000 000 000 | 1101 | 0110 | 1000 |
| E14 | 100 000 000 000 000 | 1001 | 1100 | 1111 |

Остатки получим, деля на g(x) комбинацию в виде единицы с рядом нулей и выписывая все промежуточные остатки.

1) $g_1 = x^4+x+1$

Этому многочлену соответствует кодовая комбинация 10011

```
 100000000000000000
+10011
 00011000                R4=0011
+00010011
    010110               R7=1011
   +010011
     0010100             R8=0101
    +0010011
      0011100            R10=0111
     +0010011
       0001111 0         R12=1111
      +00010011
          011010         R13=1101
         +010011
           01001         R14=1001
```

Таким образом, многочлен $g_1 = x^4+x+1$образует 15 остатков, а значит может быть выбран в качестве образующего.

2) $g_2 = x^4+x^3+1$

```
  100000000000
 +11001
  010010                 R4=1001
 +011001
    01011                R5=1011
   +01101
     11110               R6=1111
    +11001
      0011100            R7=0111
     +0011001
       000010100         R9=0101
      +000011001
           011010        R11=1101
          +011001
            00011        R12=0011
```

Таким образом, многочлен $g_2= x^4+x^3+1$ образует 15 остатков, а значит может быть выбран в качестве образующего.

3) $g_3= x^4+x^3+x^2+x+1$

```
 1000000000000000
+11111
  011110                R4=1111
 +011111
    000010000           R5=0001
       +11111
         011110         R9=1111
        +011111
          0000010000    R10=0001
             +11111
               01111    R14=1111
```

Таким образом, многочлен $g_3= x^4+x^3+x^2+x+1$

образует всего 5 остатков, а значит не может быть выбран в качестве образующего.

Составим образующие матрицы для каждого из образующих многочленов.

Образующей называется матрица, которая состоит k линейно независимых строк. Каждая из этих строк является разрешенной кодовой комбинацией. Все остальные разрешенные комбинации могут быть представлены в виде линейной комбинации строк образующей матрицы.

Если код должен быть систематическим, то образующая матрица представляется в виде двух блоков: единичной матрицы и матрицы-дополнения. Строки матрицы-дополнения определяются путем вычисления многочленов $r(x)$ для каждой строки, то есть делением на $g(x)$.

$$\mathbf{M}_{n,k} = \left[\mathbf{E}_k \vdots \mathbf{P}_{k,n-k}\right] = \left[\begin{array}{ccc|ccc} 1 & \dots & 0 & p_{1,k+1} & \cdots & p_{1,n} \\ \vdots & \ddots & \vdots & \vdots & p_{i,j} & \vdots \\ 0 & \dots & 1 & p_{k,k+1} & \cdots & p_{k,n} \end{array}\right], \quad (3)$$

Для составления образующих матриц воспользуемся результатами таблицы 1.

*Таблица 2.*

**Образующая матрица для многочлена $g_1 = x^4+x+1$**

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |

*Таблица 3.*

**Образующая матрица для многочлена $g_2 = x^4+x^3+1$**

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |

**Подсчет количества матриц.**

Перестановка строк (столбцов) образующей матрицы приводит к эквивалентному коду с той же корректирующей способностью.

Однако, поскольку код должен оставаться систематическим, мы можем переставлять только последние m столбцов.

То есть, надо посчитать, сколько всего существует перестановок из m элементов. Это можно сделать по формуле

$$P_n = m \cdot (m-1) \cdot (m-2) \ldots 3 \cdot 2 \cdot 1 = m! \qquad (4)$$

4!=4*3*2*1=24

Значит, для каждого образующего многочлена мы можем получить 24 образующих матриц систематического кода.

**Список литературы:**


1. Дмитриев В.И. Прикладная теория информации. Учебник для студентов ВУЗов по специальности «Автоматизированные системы обработки информации и управления». М.: Высшая школа, 1989 — 320 с.
2. Евсеев А.И Передача информации [Электронный ресурс] — Режим доступа. — URL: http://peredacha-informacii.ru/ (дата обращения 30.04.2015).
3. Прохоров В.С. ТЕОРИЯ ИНФОРМАЦИИ Лекции [Электронный ресурс] — Режим доступа. — URL: http://profbeckman.narod.ru/Informat.files/Teorinf.pdf (дата обращения 28.04.2015).
4. Фурсов В.А. Лекции по теории информации: Учеб. пособие под редакцией Н.А. Кузнецова Самара: Изд-во СГАУ,2006. — 148 с.

*ДЛЯ ЗАМЕТОК*

# «НАУЧНОЕ СООБЩЕСТВО СТУДЕНТОВ XXI СТОЛЕТИЯ. ТЕХНИЧЕСКИЕ НАУКИ»

*Электронный сборник статей по материалам XXXII студенческой международной заочной научно-практической конференции*

№ 5 (31)
Май 2015 г.

В авторской редакции

Издательство «СибАК»
630099, г. Новосибирск, Вокзальная магистраль, 16, офис 807.
E-mail: mail@sibac.info

СибАК

www.sibac.info