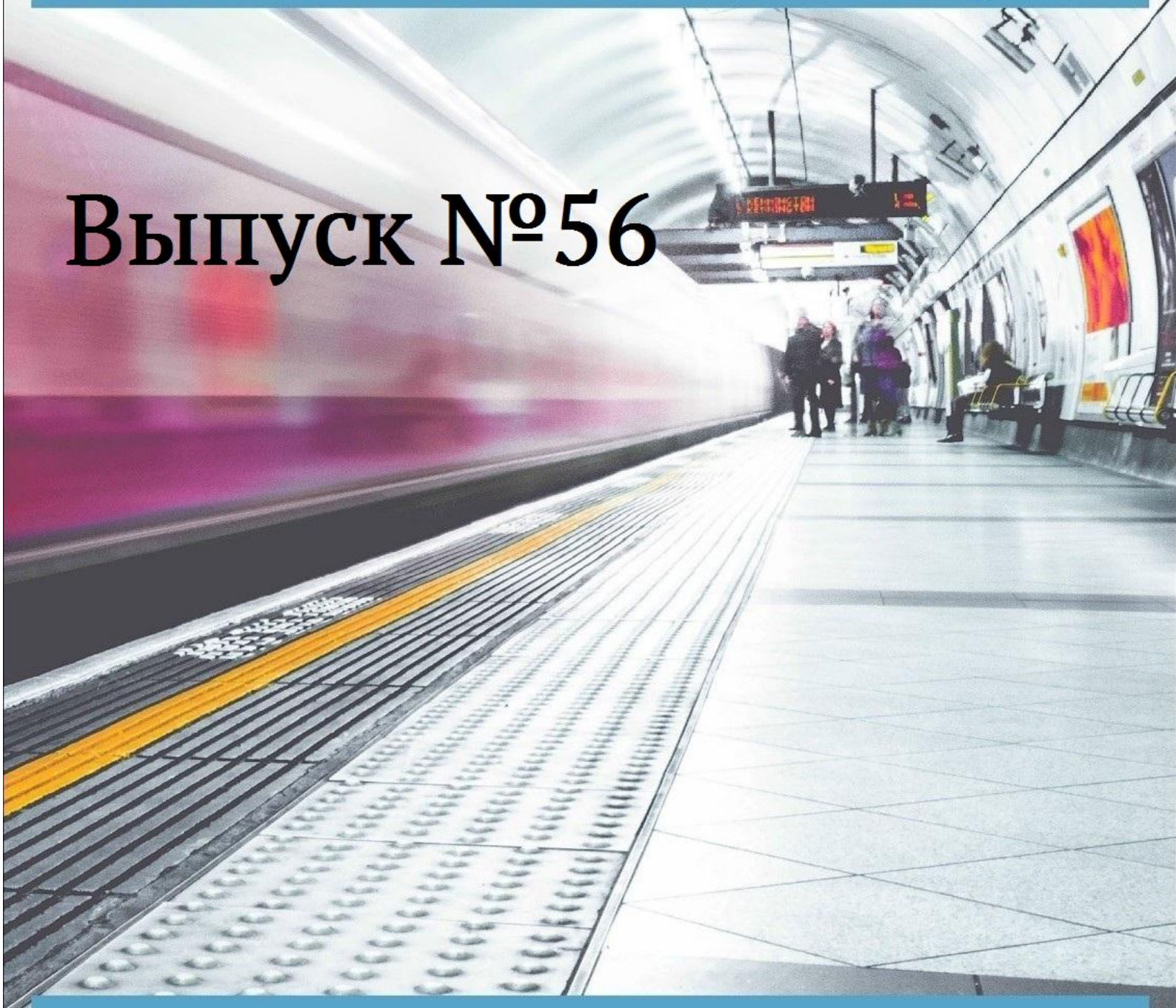
ТОЧНАЯ НАУКА

естественнонаучный журнал

Публикации для студентов, молодых ученых и научно-преподавательского состава на www.t-nauka.ru

ISSN 2500-1132 Издательский дом "Плутон" www.idpluton.ru



Выпуск №56

КЕМЕРОВО 2019

05 августа 2019 г.
ББК Ч 214(2Рос-4Ке)73я431
ISSN 2500-1132
УДК 378.001
Кемерово
Журнал выпускается ежемесячно, публикует статьи по естественным наукам. Подробнее на www.t-nauka.ru
За точность приведенных сведений и содержание данных, не подлежащих открытой публикации, несут ответственность авторы.
Редкол.:
Никитин Павел Игоревич - главный редактор, ответственный за выпуск журнала
Баянов Игорь Вадимович - математик, специалист по построению информационно-аналитических систем, ответственный за первичную модерацию, редактирование и рецензирование статей
Артемасов Валерий Валерьевич - кандидат технических наук, ответственный за финальную модерацию и рецензирование статей
Зимина Мария Игоревна - кандидат технических наук, ответственный за финальную модерацию и рецензирование статей
Нормирзаев Абдукаюм Рахимбердиеви - кандидат технических наук, Наманганский инжинерно-строительный институт (НамМПИ)
Безуглов Александр Михайлович - доктор технических наук, профессор кафедры математики и математического моделирования, Южно-российский государственный политехнический университет (Новочеркасский политехнический институт) им. М.И .Платова,
Наджарян Микаел Товмасович - кандидат технических наук, доцент, Национальный политехнический университет Армении
Шушлебин Игорь Михайлович - кандидат физико-математических наук, кафедра физики твёрдого тела Воронежского государственного технического университета
Равшанов Дилшод Чоршанбиевич - кандидат технических наук, заведующий кафедрой «Технология, машины и оборудования полиграфического производства», Таджикский технический университет имени академика М.С.Осими
Крутякова Маргарита Викторовна – доцент, кандидат технических наук, Московский политехнический университет
Гладков Роман Викторович - кандидат технических наук, доцент кафедры эксплуатации вооружения и военной техники Рязанского гвардейского высшего воздушно-десантного командного училища
Моногаров Сергей Иванович - кандидат технических наук доцент Армавирского механико-технологического института (филиал) ФГОУ ВО КубГТУ
Шевченко Сергей Николаевич - кандидат технических наук, доцент кафедры СЭУ, Балтийская государственная академия рыбопромыслового флота РФ
Отакулов Салим - Доктор физико-математических наук, профессор кафедры высшей математики Джизакского политехнического института
А.О. Сергеева (ответственный администратор)[и др.];

Естественнонаучный журнал «Точная наука», входящий в состав «Издательского дома «Плутон», был создан с целью популяризации естественных наук. Мы рады приветствовать студентов, аспирантов, преподавателей и научных сотрудников. Надеемся подарить Вам множество полезной информации, вдохновить на новые научные исследования.
Издательский дом «Плутон» www.idpluton.ru e-mail: admin@idpluton.ru
Подписано в печать 05.08.2019 г. Формат 14,8×21 1/4. | Усл. печ. л. 2.2. | Тираж 500.
Все статьи проходят рецензирование (экспертную оценку).
Точка зрения редакции не всегда совпадает с точкой зрения авторов публикуемых статей.
Авторы статей несут полную ответственность за содержание статей и за сам факт их публикации.
Редакция не несет ответственности перед авторами и/или третьими лицами и организациями за возможный ущерб, вызванный публикацией статьи.
При использовании и заимствовании материалов ссылка обязательна.

Содержание

1. ПОТЕРИ ЭЛЕКТРОЭНЕРГИИ И СПОСОБЫ БОРЬБЫ С НИМИ…..……...…….2
Маргаринт А.О.

2. ПРОИЗВОДСТВО ИЗОБУТИЛЕНА……....…….…….……..4
Ерычев М.А.

3. ОБЗОР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СЕТИ ИНТЕРНЕТ….……..7
Ерычев М.А.

4. МЕТОД НАИМЕНЬШИХ ЗНАЧАЩИХ БИТОВ ДЛЯ НАДЕЖНОГО СОКРЫТИЯ ИНФОРМАЦИИ В ГРАФИЧЕСКИХ ФАЙЛАХ……..……10
Тимофеев М.В., Дудоладова П.Г.

5. ПОВЫШЕНИЕ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ С ПОМОЩЬЮ СТЕГАНОГРАФИИ……14
Тимофеев М.В., Дудоладова П.Г.

6. ИССЛЕДОВАНИЕ ПРОБЛЕМ БЕЗОПАСНОСТИ GOOGLE КАРТ……..……17
Тимофеев М.В., Дудоладова П.Г.

7. ВЛИЯНИЕ АЭС НА ОКРУЖАЮЩУЮ СРЕДУ……..……..……..……20
Маргаринт А.О.

Маргаринт Артем Олегович
Margarine Artem Olegovich
Студент Донского Государственного Технического Университета , факультет «Энергетика и нефтегазопромышленность» ,направление « Электроэнергетика и электротехника»

УДК 517.312

ПОТЕРИ ЭЛЕКТРОЭНЕРГИИ И СПОСОБЫ БОРЬБЫ С НИМИ

LOSS OF ELECTRICITY AND WAYS TO DEAL WITH IT

Аннотация: статье представлены основные проблемы электроэнергетики, такие как потери электрической энергии. Проведён анализ источников потерь в электрических сетях.

Abstract: the article presents the main problems of the electric power industry, such as the loss of electrical energy. The analysis of sources of losses in electric networks is carried out.

Ключевые слова: электроэнергия, электрическая сеть, источники энергии, нагрузки сети, мощность энергии

Key words : electric power, electric network, energy sources, network loads, power of energy

Электрическая энергия является единственным видом продукции, для перемещения которого от мест производства до мест потребления не используются другие ресурсы. Для этого расходуется часть самой передаваемой электроэнергии, поэтому ее потери неизбежны, задача состоит в определении их экономически обоснованного уровня. Снижение потерь электроэнергии в электрических сетях до этого уровня одно из важных направлений энергосбережения [1]. Рост потерь энергии в электрических сетях определен действием вполне объективных закономерностей в развитии всей энергетики в целом. Основными из них являются: тенденция к концентрации производства электроэнергии на крупных электростанциях; непрерывный рост нагрузок электрических сетей, связанный с естественным ростом нагрузок потребителей и отставанием темпов прироста пропускной способности сети от темпов прироста потребления электроэнергии и генерирующих мощностей. Потери электроэнергии в электрических сетях являются экономическим показателем состояния сетей. По мнению международных экспертов, в области энергетики относительные потери электроэнергии при ее передаче в электрических сетях не должны превышать 4 %. Потери электроэнергии на уровне 10 % можно считать максимально допустимыми [2]. На основании уровня потерь электроэнергии можно сделать выводы о необходимости и объеме внедрения энергосберегающих мероприятий. Фактические потери определяют как разность электроэнергии, поступившей в сеть отпущенной из сети потребителям, их можно разделить на три составляющие: 1) технические потери электроэнергии, обусловленные физическими процессами в проводах и электрооборудовании, происходящими при передаче электроэнергии по электрическим сетям, включают в себя расход электроэнергии на собственные нужды подстанций; 2) потери электроэнергии, обусловленные погрешностью системы учета, как правило, представляют недоучет электроэнергии, обусловленный техническими характеристиками и режимами работы приборов учета электроэнергии на объекте; 3) коммерческие потери, обусловленные несанкционированным отбором мощности электроэнергии, несоответствием оплаты за электроэнергию бытовыми потребителями показаниям счетчиков и другими причинами в сфере организации контроля за потреблением энергии. Коммерческие потери не имеют самостоятельного математического описания и, как следствие, не могут быть рассчитаны автономно. Их значение определяют как разницу между фактическими потерями и суммой первых двух составляющих, представляющих собой технологические потери. Потери электроэнергии в сетях определяются тремя основными факторами [1]: 1. За счёт погрешности измерений фактически отпущенной в сеть энергии и полезно отпущенной электроэнергии для потребителей. 2. За счёт занижения полезного отпуска в результате технических потерь. 3. За счёт неучтённых подключений потребителей (в частности, хищений электроэнергии). Высокие потери электроэнергии в сетях, как правило, говорят либо о каких-либо накапливающихся проблемах сетей электропередачи, либо о неэффективной работе оборудования. По сути, любые потери электроэнергии в сетях, выходящие за рамки некой минимальной планки — это сигнал для специалиста, означающий, что требуется реконструировать или же технически переоснащать имеющийся комплекс. Если уровень потерь электроэнергии слишком высок, это говорит об

очевидных проблемах, связанных со следующими вопросами: 1. Медленное развитие электросети; 2. Устаревшее техническое оборудование; 3. Несовершенство методов управления сетью; 4. Несовершенство методов учета электроэнергии; 5. Неэффективность процесса сбора платы за поставляемую электроэнергию. Разумеется, в идеальном состоянии потери электроэнергии в сетях должны полностью отсутствовать, однако всегда существуют невосполнимые технические потери (из-за физических процессов передачи электроэнергии, её трансформации и распределения), определяемые расчётом с некоторой погрешностью [2]. В случае, если погрешность высока, как правило, такая сеть малоэффективна, так как вызывает высокие коммерческие потери. Способы борьбы с потерями: Первый способ основан на снижении сопротивления нулевого провода. Как известно ток течет по двум проводам: нулевому и фазному. Если увеличение сечения фазного провода достаточно затратное(стоимость меди или алюминия плюс работы по демонтажу и монтажу), то сопротивление нулевого провода можно уменьшить достаточно просто и очень дешево. Этот способ использовался с момента прокладки первых линий электропередач, но в настоящее время часто не используется. Заключается он в повторном заземлении нулевого провода на каждом столбе электролинии или (и) на каждой нагрузке. В этом случае параллельно сопротивлению нулевого провода подключается сопротивление земли между нулем трансформатора подстанции и нулем потребителя. Второй простейший способ тоже основан на снижении сопротивления. Только в этом случае необходимо проверять оба провода ноль и фазу. В процессе эксплуатации воздушных линий из-за обрыва проводов образуется места локального повышения сопротивления — скрутки, сростки и т. д. В процессе работы в этих местах происходит локальный разогрев и дальнейшая деградация провода, грозящая разрывом. Такие места видны ночью из-за искрения и свечения. Необходимо периодически визуально проверять электролинию и заменять особо плохие ее отрезки или линию целиком. Для ремонта лучше всего применить самонесущие алюминиевые изолированные кабели СИП. Они называются самонесущими, т. к. не требуют стального троса для подвески и не рвутся под тяжестью снега и льда. Такие кабели долговечны, есть специальные аксессуары для легкого и удобного крепления их к столбам и зданиям. Третьим способом является замена отслужившей воздушной линии на новую. 4. Способ основан на применении специальных стабилизаторов напряжения на входе в дом или другой объект. Такие стабилизаторы бывают как однофазного, так и трехфазного типа. Они увеличивают cos φ и обеспечивают стабилизацию напряжения на выходе в пределах ±5 %, при изменении напряжения на входе ±30 %. Их мощностной ряд может быть от сотен Вт до сотен кВт [1]. 5. Способ компенсации потерь электроэнергии. Это способ использования устройств компенсации реактивной мощности. Если нагрузка индуктивная, например, различные электромоторы, то это конденсаторы, если емкостная, то это специальные индуктивности.

Таким образом , самым эффективным решением является вынос электросчетчика из здания и установка его на опоре линии электропередачи в специальном герметичном боксе. В этом же боксе устанавливаются вводный автомат с пожарным УЗО и разрядники защиты от перенапряжений. Этот способ снижения потерь за счет использования трехфазного подключения. При таком подключении снижаются токи по каждой фазе, а, следовательно, потери в линии и можно равномерно распределить нагрузку.

Библиографический список:

1.Артемьев А.В, Савченко О.В. Расчет , анализ и нормирование потерь электроэнергии в электрических сетях : Руководство для практических расчетов – М.: Изд-во НЦ ЭНАС , 2004 – С.280.

2.Железко Ю.С. Потери электроэнергии. Реактивная мощность. Качество электроэнергии: Руководство для практических расчетов -М.: НЦ ЭНАС, 2009 – С.456.

Ерычев Михаил Андреевич
Erychev Mikhail Andreevich
студент 4 курса технологического факультета
Нижнекамский Химико-технологический институт. ФГБОУ ВО «КНИТУ».
E-mail: erychev97@mail.ru

УДК 66.093.47

ПРОИЗВОДСТВО ИЗОБУТИЛЕНА

PRODUCTION OF ISOBUTYLENE

Аннотация: в данной работе представлен небольшой обзор по производству изобутилена, в особенности производство на ионообменном катализаторе.

Abstract: this paper presents a small overview of the production of isobutylene, in particular the production on the ion-exchange catalyst.

Ключевые слова: изобутилен, катализатор.

Keywords: isobutylene, catalyst.

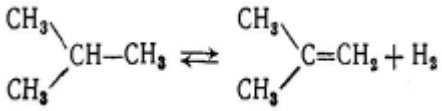
В промышленности синтетического каучука изобутилен используется как мономер для производства бутилкаучука и полиизобутилена, а также для производства изопрена методом конденсации изобутилена с формальдегидом.

Изобутилен $(CH_3)_2C{=}CH_2$ при нормальных условиях представляет собой бесцветный газ с неприятным запахом, Изобутилен нерастворим в воде; растворяется в этиловом спирте и диэтиловом эфире. Вступает во все реакции, характерные для олефинов; легко полимеризуется в присутствии кислых агентов. Взрывоопасен. Пределы взрывоопасных концентраций с воздухом 1,7-9,0% (об.). При вдыхании оказывает наркотическое действие.

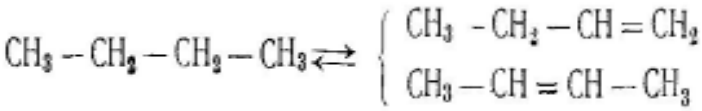
Основным источником получения изобутилена являются газы нефтедобычи и нефтепереработки, содержащие изобутан и изобутилен. Изобутилен может быть получен дегидрированием изобутана.

В настоящее время все большее значение приобретают процессы извлечения изобутилена из пиролизных фракций C_4. Промышленное выделение изобутилена из фракции C_4 осуществляется либо с помощью серной кислоты, либо жидкофазной гидратацией на ионообменных смолах.[1]

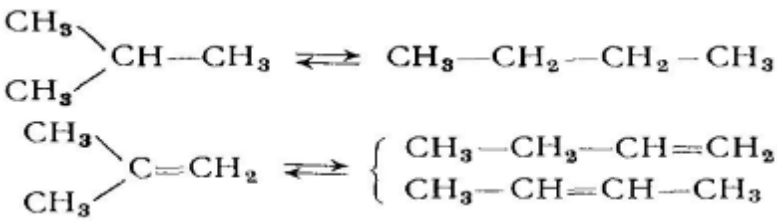
Дегидрирование изобутана в изобутилен протекает по реакции:



Параллельно протекают следующие побочные реакций. Дегидрирование бутана в бутены:



Изомеризация:



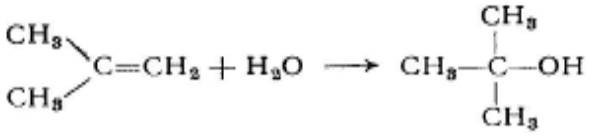
Крекинг с образованием легкокипящих углеводородов (CH_4, C_2H_4, C_2H_6, C_3H_6, C_3H_8), тяжелокипящих углеводородов (C_5 и выше) и кокса.

Выделение изобутилена из фракции C_4 на ионообменных смолах

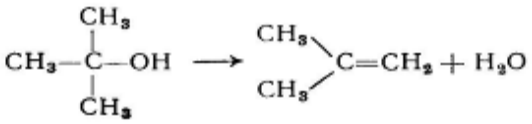
Процесс извлечения изобутилена на ионообменных смолах основан на способности изобутилена в присутствии сульфокатионита вступать в реакцию с водой с образованием бутилового спирта-триметилкарбинола (ТМК).[2]

Процесс состоит из двух основных стадий.

1. Гидратация изобутилена в ТМК:



2. Дегидратация ТМК в изобутилен:



Для извлечения изобутилена используются ионообменные смолы на основе сополимеров стирола с дивинилбензолом (КУ-1, КУ-2). На нижнекамском химкомбинате используется ионообменный катализатор – сульфокатионит, формованный на полипропилене (КУ – 2ФПП). Сырьем для данного процесса могут служить различные изобутилен - содержащие фракции C_4 (полученные при дегидрировании бутана, пиролизные, крекинговые и др.). Конверсия процесса составляет 50%. Из процесса выделяется изобутилен полимеризационной чистоты – 99,99%, что очень важно для получения синтетических каучуков, так как содержание примесей в сырье затрудняет процесс полимеризации.[3]

Достоинством метода является отсутствие коррозионно-активных сред, возможность многократного использования катализатора и высокая чистота получаемого изобутилена.[4]

Изобутилен является важнейшим мономером олефинового ряда. На его основе получают синтетический каучук, пластмассы, топливо, смазки, присадки к маслам, поверхностно-активные вещества, разнообразные добавки и другие продукты, которые широко используются практически во всех отраслях народного хозяйства.[5]

На первый взгляд химия изобутилена проста и не может представлять особого интереса для химиков с точки зрения получения новых продуктов, улучшения свойств известных соединений, расширения областей применения. Действительно, способ получения полиизобутилена-катионная полимеризация--довольно ординарен. Более того, в полиизобутилене отсутствуют дефекты структуры цепи, способные служить центрами модификации полимера и содействовать изменению его свойств.[6]

Между тем многие аспекты химии и технологии изобутилена и его полимеров не ясны и в лучшем случае дискуссионны. Поэтому глубокий интерес к фундаментальным и перспективным исследованиям в области изобутилена и его полимеров поддерживается уже многие десятилетия и постоянно стимулируется новыми экспериментальными данными. Очевидно, что ряд традиционных представлений, в частности о механизме и кинетике полимеризации мономера, оформлении технологического процесса производства полимеров изобутилена, нуждаются в основательном пересмотре или более того в развитии существенно новых и принципиально отличающихся теоретических и практических подходов.[7]

Многие вопросы химии и технологии изобутилена и полиизобутилена далеко не так просты, как кажется на первый взгляд. Вряд ли найдутся в отечественной и зарубежной химической технологии другие подобные процессы, которые бы с таким трудом поддавались расчету, регулированию и управлению, как процесс катионной поли - и сополимеризации изобутилена.

Библиографический список:

1. Минскер К.С., Сангалов Ю.А., Изобутилен и его полимеры, -М.:Химия, 1986. - 224с.

2. Литвинов О.Б. Основы технологии синтеза каучуков. -М.:Химия, 1972. - 528с.

3. Миракла И. Метод дегидрирования изобутана. Патент. Россия №5010201/04

4. Гютербок Г. Полиизобутилен и сополимеры изобутилена, Л.:Гостоптехиздат, 1962, 363с.

5. Такияма Йосихиро. Исследование прямого синтеза изобутилена и бутана // Kyushu daigaku Kogaku Shuho=Technol Repots Kyushu Univ.- 1998-71 №4 с.340-342 Япон.

6. Bekheet M.E. Селективная изомеризация н-бутиленов. // Petrol Sci and Texnol. 1999-17 №1-2 с.189-206.

7. Chen Hong-vo, yu La-jia. Влияние ферритных цеолитов допированных ZSM-23 на селективность изомеризации бутена в изобутилен. // Ximen daxual Xuebao. Zitan Kexuc ban=J.Xiamen Univ. Natur Sci. 2000.39 №4 с. 570-576. Кит.

Ерычев Михаил Андреевич
Erychev Mikhail Andreevich
студент технологического факультета
Нижнекамский химико-технологический институт. ФГБОУ ВО «КНИТУ», РФ, г. Нижнекамск
E-mail: erychev97@mail.ru

УДК 004

ОБЗОР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СЕТИ ИНТЕРНЕТ

REVIEW OF INFORMATION TECHNOLOGIES ON THE INTERNET NETWORK

Аннотация: в данной статье проводится обзор различных информационных подразделов сети Интернет, проводится обсуждение различных видов связи.

Abstract: this article reviews the various information subdivisions of the Internet, discusses various types of communication.

Ключевые слова: сеть Интернет, связь. Информационные технологии.

Keywords: Internet, communication. Information Technology.

1. Работа с информацией в глобальных компьютерных сетях.

World-Wide-Web (Всемирная информационная сеть)

WWW является одной из самых популярных информационных служб Internet Две основные особенности отличают WWW: использование гипертекста и возможность клиентов взаимодействовать с другими приложениями Internet.

Все серверы WWW используют специальный язык HTML (Hypertext Markup Language – язык разметки гипертекста). HTML-документы представляют собой текстовые файлы, в которые встроены специальные команды.

Телеконференции Usenet

Система Usenet была разработана для перемещения новостей между компьютерами по всему миру. В дальнейшем она практически полностью интегрировалась в Internet, и теперь Internetобеспечивает распространение всех ее сообщений. Серверы Usenet имеют средства для разделения телеконференций по темам.

Телеконференции организованы по иерархическому принципу, и для верхнего уровня выбраны семь основных рубрик. В свою очередь, каждая из них охватывает сотни подгрупп. Образуется древовидная структура, напоминающая организацию файловой системы. Из числа основных рубрик следует выделить:

⇒ comp - темы, связанные с компьютерами;
⇒ sci – темы из области научных исследований;
⇒ news – информация и новости Usenet;
⇒ soc – социальная тематика;
⇒ talk – дискуссии.

Существуют, кроме того, специальные рубрики и региональное разделение телеконференций.

Управляют доступом к службе Usenet специальные программы, позволяющие выбирать телеконференции, работать с цепочками сообщений и читать сообщения и ответы на них.

При участии в какой – либо телеконференции любой абонент может направить свое сообщение по интересующей его теме.

Существует два способа выполнения этой процедуры:

⇒ посылка посредственного ответа автору статьи по адресу его электронной почты;
⇒ предоставление своего сообщения в распоряжение всех участников телеконференции.

Второй способ обозначается термином "Follow-up".

После электронной почты Usenet является самой популярной службой глобальной сети Internet.

Взаимодействие с другим компьютером (Telnet)

Telnet обеспечивает взаимодействие с удаленным компьютером. Установив такую связь через Telnet пользователь получает возможность работать с удаленным компьютером, как со "своим", т. е. теоретически получить в свое распоряжение все ресурсы, если к ним разрешен доступ. Реально

Telnet предоставляет открытый доступ, но организация взаимодействия полностью определяется удаленным компьютером. Два вида услуг Internet требует подключения к серверам через Telnet: библиотечные каталоги и электронные доски объявлений (BBS).

2. Локальные и глобальные компьютерные информационные сети.

Локальные сети. Если все компьютеры сети действуют в общем адресном пространстве согласно общему протоколу, то такая сеть называется ***локальной***. Локальные сети обычно невелики по размерам – расстояния между компьютерами не превышают около нескольких сот метров. С помощью локальных сетей объединяют компьютеры одной рабочей группы, одного подразделения, одного предприятия.

Глобальные сети. Локальные сети можно соединять друг с другом. При этом образуются ***глобальные компьютерные сети.*** Если объединяются две локальные сети, действующие по общим протоколам, то узел, в котором они стыкуются, называется **шлюзом.** Если каждая из сетей продолжает работать по своим протоколам, то узел между ними называется **мостом.** Если мост настолько совершенен, что способен представлять адресное пространство одной сети устройствам другой сети, то его называют **маршрутизатором.**

3. Типы сетей электронной коммуникации.

Электронная почта - Она является наиболее распространенной из всех служб Сети интернет. Электронная почта – первая информационная услуга компьютерных сетей. Она не требует обязательного наличия высокоскоростного интернета. Ее основное назначение – поддержка обмена письмами между пользователями.

Видеосвязь – это способ передачи аудио и видео данных между удаленными пользователями. Видеосвязь возможно осуществить в виде персонального звонка 1-на-1 или групповой видеоконференции. Реализуется **видеосвязь** не только на компьютере, ноутбуке или специализированном устройстве видеосвязи, но также на смартфонах, коммуникаторах, планшетных компьютерах и других мобильных устройствах.

Видеосвязь типа «точка-точка» популярна среди пользователей интернет сервисов.

Программное обеспечение видеосвязи подразделяется на пиринговое, поставляемое в качестве сервиса или через сервер.

1. **Видеосвязь через сервер:** в этом случае выделяются специализированный сервер, обрабатывающий поступающую информацию, и клиентское ПО, которое устанавливается на компьютеры пользователей и напрямую связывается с сервером. Такой тип видеоконференцсвязи может работать как через интернет, так и в локальных сетях предприятий.
2. **Видеосвязь как сервис:** пользователь скачивает клиентское приложение, работающее через интернет. Поток аудио и видео данных передается через удаленный сервер провайдера.
3. **Пиринговая видеосвязь** подразумевает маршрутизацию звонков через компьютеры пользователей программы. Это позволяет компании-провайдеру избежать внедрения дорогостоящей инфраструктуры централизованных серверов, но в то же время увеличивает нагрузку на персональные компьютеры пользователей. В пиринговых системах видеосвязи центральным элементом является сервер идентификации, который хранит минимальную необходимую информацию: учетные записи пользователей, копии их списков контактов и тому подобное.

Чат — средство обмена сообщениями по компьютерной сети в режиме реального времени, а также программное обеспечение, позволяющее организовывать такое общение. Характерной особенностью является коммуникация именно в реальном времени или близкая к этому, что отличает чат от форумов и других «медленных» средств.

Библиографический список:

1. Информатика: Учебник/под ред. Н.В. Макаровой. - М.: Финансы и статистика, 2000. - 768 с.

2. Информатика. Базовый курс. Учебник для Вузов/под ред. С.В. Симо-новича, - СПб.: Питер, 2000.

3. Симонович С. В., Евсеев Г.А., Практическая информатика, Учебное пособие. М.: АСТпресс, 1999.

4. Фигурнов В. Э. IBM PC для пользователя. М.: Инфра-М, 2001 г.

5. Симонович С.В., Евсеев Г.А., Алексеев А.Г. Специальная информатика, Учебное пособие. М.: АСТпресс, 1999.

6. Информатика: Практикум по технологии работы на компьютере./ Под ред. Н.В. Макаровой. - М.: Финансы и статистика, 2000 .

7. А.В.Могилев, Н.И.Пак, Е.К.Хеннер, Информатика, Учебник для ВУЗов – М.: Издательство Academa, 1999.

8. Денисов А., Вихарев И., Белов А.. Самоучитель Интернет. – Спб: Питер, 2001. - 461 с.

9. Евдокимов В.В. и др. Экономическая информатика. Учебник для вузов. Под ред. д. э. н., проф. В.В. Евдокимова. СПб.: Питер паблишинг, 1997.

10. Основы современных компьютерных технологий. Ред. Хомченко А.Д.

Тимофеев Михаил Вячеславович
Timofeev Mikhail Vyacheslavovich
студент, Морской Государственный Университет имени адмирала. Г.И. Невельского, кафедра Безопасности информации и телекоммуникационных систем
г. Владивосток. E-mail: tmv5.96@mail.ru

Дудоладова Полина Геннадьевна
Dudoladova Polina Gennadievna
студент, Морской Государственный Университет имени адмирала. Г.И. Невельского, кафедра Безопасности информации и телекоммуникационных систем
г. Владивосток

УДК 004.056.5

МЕТОД НАИМЕНЬШИХ ЗНАЧАЩИХ БИТОВ ДЛЯ НАДЕЖНОГО СОКРЫТИЯ ИНФОРМАЦИИ В ГРАФИЧЕСКИХ ФАЙЛАХ

THE LEAST SIGNIFICANT BITS METHOD FOR MORE RELIABLE HIDING OF INFORMATION IN GRAPHIC FILES

Аннотация: Одним из основных направлений защиты информации от несанкционированного получения и раскрытия информации является криптография, которая занимается вопросами сокрытия смысла и содержания информации. В статье предложена модифицированная версия метода наименьших значащих битов (LSB) с двумя графическими файлами для повышения надежности.

Abstract: Cryptography is one of the main directions of protecting information from unauthorized receipt and disclosure of information. It deals with the concealment of the meaning and content of information. The article proposes a modified version of the least significant bits (LSB) method with two graphic files to increase reliability.

Ключевые слова: стеганография, LSB –метод, модифицированная версия метода наименьших значащих битов.

Keywords: steganography, LSB method, a modified version of the least significant bits method.

Для повышения надежности предлагается модифицированная версия метода младших разрядов (LSB) с двумя графическими файлами.

Наиболее распространенными методами цифровой стеганографии являются методы сокрытия информации в графических файлах (BMP, JPG и др.). Одним из этих методов является метод наименьших значащих битов (LSB), который основан на ограниченных возможностях органов чувств человека, в результате чего очень трудно различить незначительные изменения цвета.

В этой статье предлагается модифицированная версия этого метода - метод младших разрядов с двумя графическими файлами. Этот метод использует два графических файла, один из которых является контейнером, а другой - стеганографическим ключом. То есть принимая во внимание последние два бита RGB-каналов пикселей второго графического файла (т.е. ключа) и биты скрытой информации, последние два бита RGB-каналов пикселей контейнера изменяются особым образом.

То есть информация о соответствии или различии битов передаваемой информации и последних двух бит пикселей стеганографического ключа встраивается в контейнер. Поскольку файл-ключ не передается по каналу связи, он не может быть известен противнику. И невозможно раскрыть информацию только на основе модифицированного контейнера, который не содержит скрытой информации.

Метод LSB - младшие биты.

Одним из наиболее известных методов цифровой стеганографии является метод наименее значимых битов, суть которого состоит в следующем:

Пусть в качестве контейнера используется 24-битное растровое RGB-изображение. В таком изображении каждый пиксель кодируется тремя байтами, которые определяют интенсивность красного, зеленого и синего цветов соответственно. Значения этих три байта вместе определяют оттенок этого пикселя. В этих байтах младшие биты (биты справа) вносят незначительный вклад в

изображение по сравнению с старшими битами. Замена одного или двух младших битов этих байтов приведет к изменению модификации изображения, которая невидима для человеческого глаза.

Предположим, нужно скрыть сообщение «LSB» - название стеганографического метода в 24-битном растровом RGB-изображении. Двоичный код сообщения «LSB» будет «01001100 01010011 01000010». Следовательно, должна быть встроена в изображение эта последовательность, для которой требуется четыре пикселя (то есть двенадцать байтов) изображения. В таблице 1 приведены значения битов до и после реализации этой последовательности в четыре пикселя изображения.

Таблица 1. Пример изменения битов пикселей графического файла

Канал цвета	Код цвета пикселя перед изменением		Код цвета пикселя после изменения	
	Десятичный код	Двоичный код	Десятичный код	Двоичный код
К	36	00100100	37	00100101
З	201	11001001	200	11001000
С	121	01111001	123	01111011
К	105	01101001	104	01101000
З	108	01101100	109	01101101
С	24	00011000	25	00011001
К	141	10001101	140	10001100
З	23	00010111	23	00010111
С	206	11001110	205	11001101
К	125	01111101	124	01111100
З	42	00101010	40	00101000
С	68	01000100	70	01000110

Как видно из их таблиц, когда последние два бита меняются, цвет пикселей изменяется настолько незначительно, что практически невозможно различить цвета до и после реализации информации.

Модифицированный метод LSB с двумя графическими файлами.

Известно, что метод наименее значимых битов имеет следующий недостаток: заполненный контейнер отправляется по открытому каналу связи, он может быть захвачен злоумышленником, что дает ему возможность раскрыть конфиденциальную информацию. Для устранения указанного недостатка предлагается метод младших разрядов с двумя графическими файлами, который рассмотрен ниже.

В этом методе используются два графических файла PIC1 и PIC2 (например, 24-битный растровый RGB изображения в формате BMP), размеры и графические параметры которого идентичны. Графический файл PIC1 является стеганографическим ключом, который доступен для обеих сторон и используется для сокрытия и раскрытия информации. Стороны обмениваются этим файлом заранее по скрытому каналу или по предварительной договоренности берут из какого-то открытого источника, например, с какого-то сайта.

Графический файл PIC2 используется отправителем в качестве контейнера для сокрытия информации, после чего он отправляется получателю. Следует отметить, что в контейнер вставляется не сама передаваемая информация, а сведения об этой информации. Последние биты каналов RGB пикселей контейнера изменяются особым образом на основе графического файла PIC1 и переданной информации. Получив измененный файл PIC2, получатель восстанавливает скрытую информацию из этого файла, используя ранее существующий ему ключевой графический файл PIC1.

Поскольку файл ключа PIC1 не передается по каналу связи и не известен противнику, раскрытие информации невозможно только на основе модифицированного контейнера, то есть графического файла PIC2.

Переданная (скрытая) информация заранее преобразуется в двоичную форму. В то же время для усиления защиты эта информация может быть заранее зашифрована. В соответствии с предлагаемым способом шесть битов встроены в каждый пиксель изображения, то есть два бита в каждом канале цветов. Следовательно, зависимость объема скрытой информации от размера контейнера составит:

$L \leq 6 * I$, (4)

где L - это размер (в битах) скрытой информации, то есть количество скрытых битов, I - количество пикселей контейнера, то есть изображения PIC2 (включая PIC1).

Алгоритм сокрытия информации можно в устной форме описать следующим образом.

Первый бит передаваемой информации берется и сравнивается с последним (первым справа) битом первого байта первого пикселя PIC1. Если они равны, последний (первый справа) бит первого байта первого пикселя PIC2 изменяется на «1», в противном случае на «0» (эквивалентный оператор).

Затем второй бит передаваемой информации сравнивается с предпоследним (вторым справа) битом первого байта первого пикселя PIC1. Если они равны, предпоследний (второй справа) бит первого байта первого пикселя PIC2 изменяется на «1», в противном случае на «0».

Третий бит передаваемой информации сравнивается с последним битом второго байта первого пикселя PIC1. Если они равны, последний бит второго байта первого пикселя PIC2 изменяется на «1», в противном случае на «0».

Четвертый бит передаваемой информации сравнивается с предпоследним битом второго байта первого пикселя PIC1. Если они равны, предпоследний бит второго байта первого пикселя PIC2 изменяется на «1», в противном случае на «0».

Пятый бит передаваемой информации сравнивается с последним битом третьего байта первого пикселя PIC1. Если они равны, последний бит третьего байта первого пикселя PIC2 изменяется на «1», в противном случае на «0».

Шестой бит передаваемой информации сравнивается с предпоследним битом третьего байта первого пикселя PIC1. Если они равны, предпоследний бит третьего байта первого пикселя PIC2 изменяется на «1», в противном случае на «0» (рис. 2).

Посредством циклического повторения процедуры все биты передаваемой информации сравниваются с последними двумя битами соответствующих (по порядковому номеру) пикселей PIC1 и, в зависимости от результатов сравнения, последние два бита соответствующих пикселей PIC2 изменены.

Результатом является модифицированный графический файл PIC2, который не содержит передаваемой информации, поскольку он содержит только информацию о разнице или совпадении битов передаваемой информации и битов ключевого графического файла PIC1 (Таблица 2).

Измененный файл PIC2 отправляется отправителем по адресу назначения без какой-либо опасности. Таким образом, если злоумышленник даже подозревает, что переданный файл PIC2 изменен, и пытается извлечь скрытую информацию, он не может этого сделать, поскольку файл PIC1 ему неизвестен.

Таблица 2. Пример изменения битов пикселей графического файла PIC2

Номер пикселя	Байт ключевого файла (PIC1)	Переданные биты	Байт файла-контейнера перед вставкой	Байт файла-контейнера после вставки	Запись
1	10001111	01	00011100	00011110	последний бит изменен предпоследний бит изменен
	00111100	10	11000111	11000110	последний бит изменен предпоследний бит не изменен
	11111001	01	10001101	10001100	последний бит изменен предпоследний бит не изменен

Описанный выше алгоритм приведен ниже.

Пусть $T = \{t_l\}$ - битовая последовательность передаваемой информации, $F = \{f_{ij}{}^k\}$ и $G = \{g_{ij}{}^k\}$ - матрицы битовых последовательностей графических файлов PIC1 и PIC2. Здесь $i = 1, I$ - номер пикселя изображения, $j = 1,8$ - номер бита в байте, $k = 1,3$ - номер байта (канала) цвета пикселя. Тогда алгоритм модифицированного метода LSB с двумя графическими файлами (24-битные растровые изображения в формате BMP) будет следующим:

1. Начало

2. bit = $\{t_l\}$ / * битовой последовательности передаваемой информации
3. bit = $\{f_{ij}^k\}$ / * битовой последовательности файла PIC1
4. G=$\{g_{ij}^k\}$ /* битовая последовательность файла PIC2
5. l=1 / * количество бит передаваемой информации
6. i=0 / * количество пикселей изображения
7. k=1 / * номер канала (байт) пикселя
8. Если t_l=f_{i8}^k, то g_{i8}^k=1, то g_{i8}^k=0
9. Если t_{l+1}=f_{i7}^k, тогда g_{i7}^k =1, иначе $g_{i7}k$ = 0
10. l=l+2
11. Если l >L, то перейти к пункту 15
12. k=k+1
13. Если $k \leq 3$, то перейти к пункту 814. $i = i + 1$
13. Перейти к пункту 7
15. Сохранить битовую последовательность $G = \{g_{ij}^k\}$ в графическом файле PIC2.
16. Отправить PIC2 получателю.
17. Конец.

Разработанный метод LSB с двумя графическими файлами позволяет устранить недостатки обычного метода LSB. В этом методе информация о скрытом сообщении вставляется в один графический файл, который является контейнером. Информация о скрытом сообщении составляется на основе этого сообщения и некоторого другого графического файла, называемого стеганографическим ключом. Благодаря этому методу защита скрытой информации обеспечивается эффективно.

Библиографический список:

1. Aura T. Invisible communication. In Proc. of the HUT Seminar on Network Security '95, Espoo, Finland, November 1995. Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology
2. Pahati O.J. Confounding Carnivore: Как защитить свою конфиденциальность в Интернете (англ.). AlterNet (29 ноября 2001 года).
3. Алгоритмы выявления стеганографического скрытия информации в jpeg-файлах. М.А. Дрюченко Воронежский государственный университет.
4. Применение rs-стегоанализа для обнаружения lsb-стеганографии. Бобченков А.В., Бородин Г.А.

Тимофеев Михаил Вячеславович
Timofeev Mikhail Vyacheslavovich
студент, Морской Государственный Университет имени адмирала. Г.И. Невельского, кафедра Безопасности информации и телекоммуникационных систем
г. Владивосток. E-mail: tmv5.96@mail.ru

Дудоладова Полина Геннадьевна
Dudoladova Polina Gennadievna
студент, Морской Государственный Университет имени адмирала. Г.И. Невельского, кафедра Безопасности информации и телекоммуникационных систем
г. Владивосток

УДК 004.056.5

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ С ПОМОЩЬЮ СТЕГАНОГРАФИИ

IMPROVING SECURITY OF MOBILE CLOUD COMPUTING USING STEGANOGRAPHY

Аннотация: Одной из критических угроз, с которыми сталкиваются пользователи облачных вычислений, является несанкционированный доступ со стороны инсайдеров, в котором работают поставщики облачных услуг. Несмотря на то, что существует множество механизмов безопасности для предотвращения несанкционированного доступа неавторизованного пользователя администрацией облака, но нет никаких средств обеспечения безопасности, чтобы предотвратить несанкционированный доступ администраторов облака к данным клиента в облачных вычислениях. В этой статье рассказывается как стеганография может повысить безопасность конфиденциальности данных, хранящихся в облаке мобильными приложениями. Эта модель работает с ключом, который встроен в изображение вместе с данными, чтобы обеспечить дополнительный уровень безопасности.

Abstract: One of the critical threats that cloud computing users face is unauthorized access by insiders, in which cloud service providers operate. Despite the fact that there are many security mechanisms to prevent unauthorized access by the cloud administration, there are no security measures to prevent unauthorized access by cloud administrators to client data in cloud computing. This article discusses how steganography can increase the confidentiality of data stored in the cloud by mobile applications. This model works with a key that is embedded in the image along with the data to provide an additional level of security.

Ключевые слова: стеганография, LSB –метод, облачные вычисления

Keywords: steganography, LSB method, cloud computing

В предлагаемом алгоритме используется защита ASCII и BCD со стеганографией, в которой зашифрованные данные хранятся в файле изображения, который будет отправлен. Алгоритм безопасности использует CDM (Common Deployment Model), который также обеспечивает совместимые сервисы безопасности через облако. Основной целью предлагаемого алгоритма является контроль и отправка данных в зашифрованном виде клиенту.

На рисунке 1 показана программная архитектура предлагаемой системы со стеганографическим приложением. Ключевые элементы модели включают в себя следующие компоненты:

пользователь, который выбирает изображение и вводит ключ и данные;

мобильное устройство (смартфон), которое работает как промежуточное устройство, преодолевая разрыв между информация об отправителе и получателе, над которой работает приложение стеганографии;

приложение стеганографии, которое представляет собой мобильное приложение, работающее на мобильном устройстве для встраивания данных и ввода ключа в изображение, предоставленное пользователем; затем генерирует стего-изображение и извлекает данные из изображения, если введенный пользователем ключ совпадает, поставщик облачных вычислений, предоставляющий различные услуги (например, SaaS).

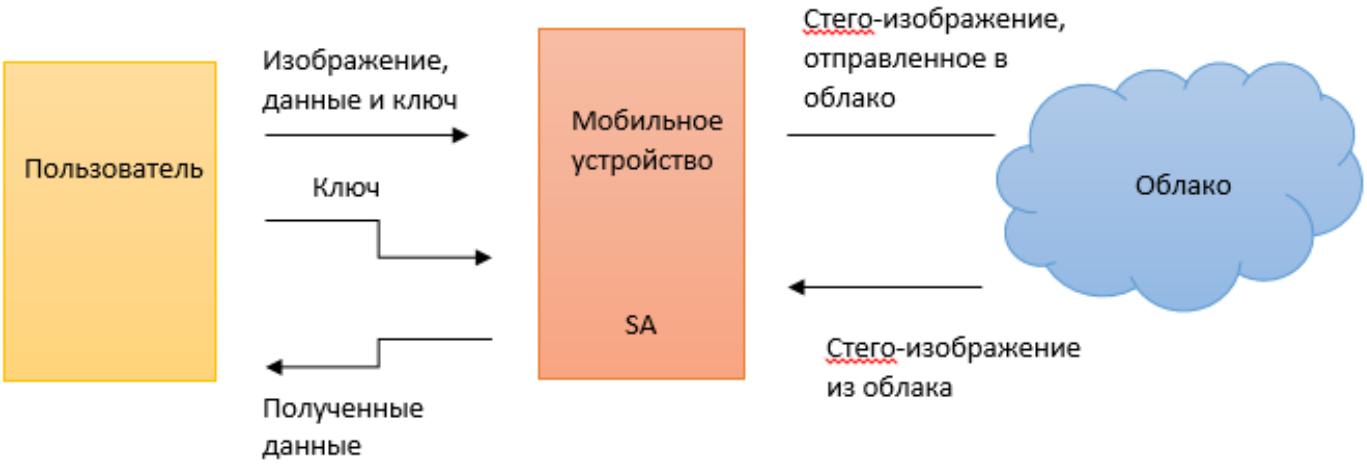


Рисунок 1

Предлагаемая архитектурная модель основана на архитектуре клиент-сервер. Система сочетает в себе основные функции облачных вычислений и стеганографии. В этой модели именно пользователь отвечает за выбор изображения, ввод данных в качестве ввода; входные данные используются специальным стеганографическим приложением (SA), которое настраивается на мобильном устройстве пользователя. Стеганографическое приложение обрабатывает все эти входные данные и создает в качестве выходных данных стего-изображение для хранения в облаке. Во время извлечения данных изображение извлекается из облака и снова обрабатывается стеганографическим приложением для отображения данных пользователю, если введенный пользователем ключ соответствует встроенному ключу.

Представленный метод использует стеганографию 24-битного изображения для встраивания данных и ключа в изображение. Различные методы сокрытия сообщений работают с разными типами изображений

Процесс внедрения данных с использованием LSB (Least Significant Bit) можно описать следующим образом. Предполагая, что пользователь хочет встроить букву «А» в 24-битное изображение, а двоичное значение «А» равно 10000011. В 24-битном изображении каждый пиксель имеет восемь битов для каждого цвета в модели RGB: красный, зеленый и синий. Пользователь должен изменить младшие значащие биты, которые требуют только 3 пикселя для сокрытия 8-битной буквы «А». Исходные три пикселя представлены в таблице 1 . Каждая строка таблицы представляет каждый пиксель, а каждый столбец представляет значение RGB каждого пикселя.

Таблица 1. Представление 24-битного слова.

	Красный	Зелёный	Синий
Пиксель 0	00100111	11101001	11001000
Пиксель 1	00100111	11001000	11101001
Пиксель 2	11001000	00100111	11101001

После встраивания двоичного значения «А», которое равно 10000011, в три пикселя, начиная с верхнего левого байта в таблице и заканчивая правым концом. Следование той же последовательности для каждой строки будет генерировать представленный результат в таблице 2. Для красного байта пикселя 0 последний бит заменяется первым битом буквы А, и процесс продолжается до последнего бита буквы «А». В этом примере мы использовали 8-битную букву «А» для замены 9 байтов; синий байт пикселя 2 остается неизменным. Подчеркнутые значения - это те, которые модифицируются методом преобразования LSB.

Таблица 2. Представление 24-битного слова после вставки буквы А.

	Красный	Зелёный	Синий
Пиксель 0	00100111	11101000	11001000
Пиксель 1	00100110	11001000	11101000
Пиксель 2	11001001	00100111	11101001

Наиболее важными функциями этого приложения являются то, что пользователь может использовать разные ключи для разной информации, поэтому даже если злоумышленник угадывает ключ для одного стего-изображения, он не сможет использовать тот же ключ для других изображений, что снижает шансы похищения данных, и если пользователь теряет мобильное устройство, то пользователь может получить доступ к облачным данным с любого другого мобильного устройства, просто загрузив специальное приложение на это мобильное устройство.

Библиографический список:

1.Miller R. Who Has the Most Web Servers? URL: http://www.datacenterknowledge.com/archives/2009/05/14/whos-got-the-most-web-servers/

2. Медведев А. Облачные технологии: тенденции развития, примеры исполнения // Современные технологии автоматизации. 2013. № 2. С. 6-9.

3. Amrhein D., Quint S. Cloud computing for the enterprise: Part 1: Capturing the cloud. URL: http://www.ibm.com/developer-works/websphere/techjournal/0904_amrhein/0904_amrhein.html

4.Облачные вычисления (Cloud computing). URL: http://www.tadviser.ru/index.php/Статья:Облачные_вычисления_ (Cloud_computing)

5. Орландо Д. Модели сервисов облачных вычислений: инфраструктура как сервис. URL: http://www.ibm.com/deve-loperworks/ru/library/cloudservices1iaas/

Тимофеев Михаил Вячеславович
Timofeev Mikhail Vyacheslavovich
студент, Морской Государственный Университет имени адмирала. Г.И. Невельского, кафедра Безопасности информации и телекоммуникационных систем
г. Владивосток. E-mail: tmv5.96@mail.ru

Дудоладова Полина Геннадьевна
Dudoladova Polina Gennadievna
студент, Морской Государственный Университет имени адмирала. Г.И. Невельского, кафедра Безопасности информации и телекоммуникационных систем
г. Владивосток

УДК 004.056.5

ИССЛЕДОВАНИЕ ПРОБЛЕМ БЕЗОПАСНОСТИ GOOGLE КАРТ

RESEARCH GOOGLE CARD SECURITY PROBLEMS

Аннотация: Карты Google оказывают большое влияние на жизнь общества. Однако у Google Карт есть множество проблем с безопасностью. Это связано с тем, что всякий раз, когда пользователь ищет географическое местоположение на Картах Google, невозможно понять намерения человека. В результате, что бы ни запросил пользователь, Google карта представится без проверок безопасности. Злоумышленники могут использовать эту технологию для осуществления преступных действий, таких как террористические атаки, убийство, преследование потенциальной жертвы, похищение людей и т. д. Данная статья повествует о проблемах безопасности Google Карт, а также предлагаются способы минимизации преступлений, которые осуществляются при помощи Google Карт.

Abstract: Google Maps has a big impact on society. However, Google Maps has many security issues. This is because whenever a user searches for a geographical location on Google Maps, it is impossible to understand the intentions of a person. As a result, no matter what the user asks for, the Google map will provide without security checks. Attackers can use this technology to carry out criminal actions, such as terrorist attacks, murder, prosecution of a potential victim, kidnapping, etc. This article describes the security problems of Google Maps, and suggests ways to minimize crimes that are carried out using Google Maps.

Ключевые слова: Карты Google, проблемы безопасности, киберпреступность.

Keywords: Google maps, security issues, cybercrime

После запуска технологии Google Maps миллионы пользователей ежедневно используют эту технологию для поиска различных географических местоположений и сокращения трудоемких задач, таких как поиск пути, время, необходимое для достижения пункта назначения и т. д. Кроме того, пользователи являются анонимными для Карт Google, поскольку не требуется аутентификация или авторизация, вход в систему, журналы сеансов или проверка безопасности. Следовательно, миллионы пользователей по-прежнему анонимны для Google, и их намерения неизвестны.

На рисунке 1 показано, что пользователи Карт Google могут быть разделены на две основные категории:

•Анонимный пользователь с хорошими намерениями;

• Анонимный пользователь с плохими намерениями.

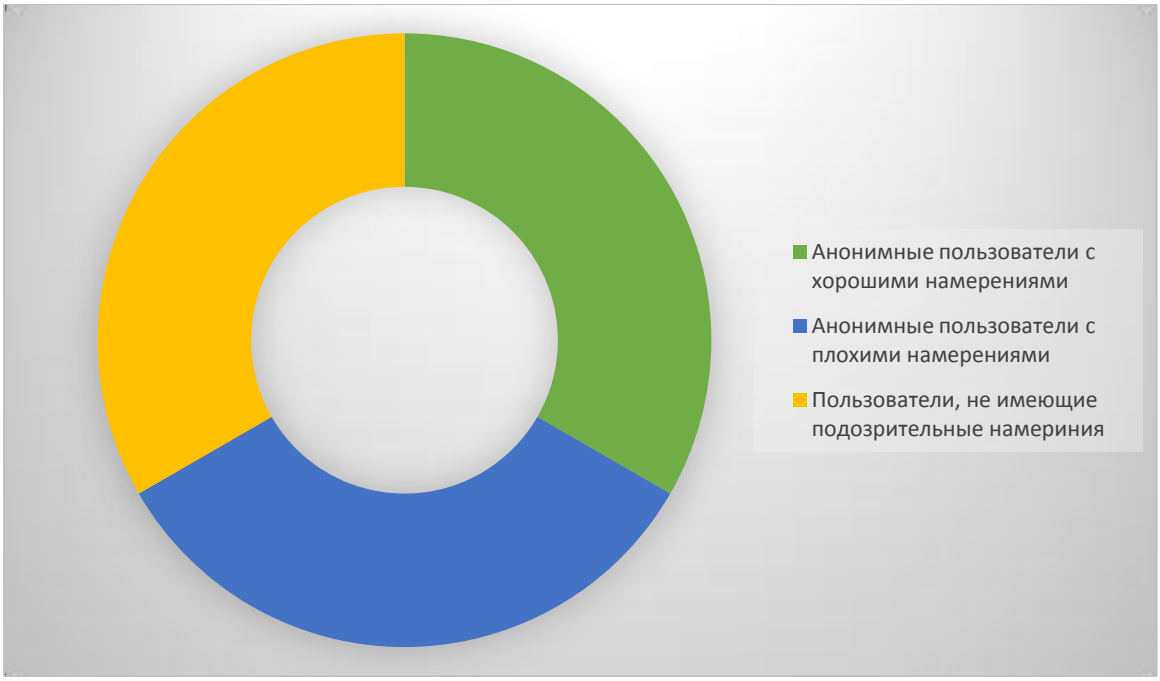


Рисунок 1 Категории пользователей Карт Google

Карты Google должны представить пользователям процесс регистрации, как показано на рисунке 2. Должна быть обязательная регистрация пользователя после предоставления необходимых учетных данных в Картах Google.

Рисунок 2. Процесс регистрации для минимизации злоумышленников

Чтобы справиться с проблемами безопасности Карт Google, основные направления будущего развития должны быть сосредоточены на следующем:

1) Создание аккаунта должно быть обязательным для пользователей Google Maps.

2) Необходимые учетные данные пользователей должны быть заполнены во время процесса регистрации.

3) Журналы сеансов, история просмотров и журналы активности должны вестись для каждого пользователя.

4) Пользователи должны подписать принятие условий и положений о том, что в случае любого подозрительного действия со стороны аккаунта Google Карты, могут быть приняты юридические меры против конкретного пользователя.

5) В результате процесса регистрации миллионы анонимных пользователей в дальнейшем не будут оставаться анонимными.

6) Карты Google должны показывать всплывающие предупреждения своим пользователям, если он пытается получить доступ к любому безопасному или конфиденциальному месту для просмотра.

7) Статистический анализ данных могут использоваться для прогнозирования и оценки поведения подозреваемого пользователя путем применения этих методов в истории просмотра.

8) Акты о киберпреступности могут использоваться пользователями Google Карт, если они признаны виновными.

9) Если какой-либо инцидент или теракт произошел в определенном месте, необходимо просмотреть историю посещений пользователя об этом месте и сопоставить полученные данные с другой доступной информацией для поиска преступника.

Карты Google и другие подобные карты имеют большое значение в жизни каждого человека в современном мире благодаря потребностям в нахождении определенной локации или маршрута. К сожалению, в настоящее время невозможно отследить передвижения преступников и предотвратить их дальнейшие запретные действия. Несмотря на это, если сосредоточиться на основных предлагаемых направления развития Google Карт, можно избежать множество преступлений.

Библиографический список:

1. Учебник-справочник Google, Петелин А.
2. Учебник Google Maps API

Маргаринт Артем Олегович
Margarint Artem Olegovich
Студент Донского Государственного Технического Университета , факультет «Энергетика и нефтегазопромышленность» ,направление « Электроэнергетика и электротехника»

УДК.504.05

ВЛИЯНИЕ АЭС НА ОКРУЖАЮЩУЮ СРЕДУ

THE NPP IMPACT ON THE ENVIRONMENT

Аннотация: В статье рассматриваются особенности влияния атомных электростанций на окружающую среду.

Abstract: The article discusses the features of the impact of nuclear power plants on the environment.

Ключевые слова: Атомные электростанции, реакторы, экологическая катастрофа, радиоактивные вещества, ядерное топливо.

Keywords: Nuclear power plants, reactors, ecological catastrophe, radioactive substances, nuclear fuel.

О вреде атомных электростанций можно говорить вечно. Последствия, произошедшие под влиянием АЭС, оказались, губительны для людей и окружающей среды. Что же будет в ближайшем будущем? Этот ответ не знает никто. Однако, приходится разбирать те проблемы, которые уже случилось. И одна из них – это экологическая проблема.

Атомные электростанции (АЭС) – это ядерная установка для производства энергии в заданных режимах и условиях применения, располагающаяся в пределах определенной проектом территорий, на которой для осуществления этой цели используется ядерный реактор и комплекс необходимых систем, устройств, оборудований, сооружений с необходимым персоналом. Опасность атомной энергетики лежит не только в сфере аварий и катастроф. Даже когда атомная электростанция (АЭС) работает нормально, она выбрасывает изрядное количество радиоактивных изотопов (углерод-14, криптон-85, стронций-90, йод-129 и 131 и др.). Наиболее опасным в выбросах современных АЭС считается тритий. Он может замещать водород во всех соединениях с кислородом, серой, азотом. А эти соединения составляют значительную часть массы животных организмов. Доказано, что он легко связывается протоплазмой живых клеток и накапливается в пищевых цепях. Распадаясь, тритий превращается в гелий и испускает в-частицы. Такая трансмутация должна быть очень опасна для живых организмов. Экологическое состояние различных районов вызывает тревогу. Серьезные проблемы возникли с мелиорацией земель. Сильное загрязнение происходит стоковыми водами коммунальных и промышленных предприятий. Происходят выбросы углекислого газа, сернистых соединений в атмосферу, в результате промышленных работ, это все приводит к возникновению парникового эффекта, который в дальнейшем приведет к потеплению климата. Глобальное потепление, по оценкам ученых, может произойти , если не будут предприняты меры по сокращению выбросов. Также потепление климата, будет способствовать увеличению уровня океана на 60 – 80 см, который приведет к экологической катастрофе невиданного масштаба, и будет пагубно влиять на человеческое общество. Еще одна проблема связана с дефицитом воды. 3000 куб. воды в год потребляет промышленность, 40% приблизительно возвращается в цикл, но с отходами. В ней содержаться различные примеси: частицы золы, продукты коррозии, смол, все те компоненты радиоактивных веществ. Все это попадает в воду, откладывается в пищевых путях рыб, и попадает на стол человека. Атмосфера загрязняется продуктами ядерных взрывов. Выбросы пыли загрязняют воздух, территории загрязняются шлаками, содержащимися в радиоактивных веществах при сжигании топлива в казнах электростанций. Важной особенностью возможного воздействия АЭС на окружающую среду является необходимость захоронения отработанного ядерного топлива и элементов оборудования, обладающих радиоактивностью, по окончанию срока службы. При нормальной работе в окружающую среду попадают лишь немногие ядра газообразных и летучих элементов типа криптона, ксенона, йода. Расчёты показывают, что даже при увеличении мощностей атомной энергетики в 40 раз её вклад в глобальное радиоактивное загрязнение составит не более 1% от

уровня естественной радиации на планете. На электростанциях с кипящими реакторами (одноконтурными) большая часть радиоактивных летучих веществ выделяется из теплоносителя в конденсаторах турбин, откуда вместе с газами радиолиза воды выбрасываются эжекторами в виде парогазовой смеси в специальные камеры для первичной обработки или сжигания. Остальная часть газообразных изотопов выделяется при дезактивации растворов в баках выдержки . На электростанциях с реакторами, охлаждаемыми водой под давлением, газообразные радиоактивные отходы выделяются в баках выдержки . Газообразные и аэрозольные отходы из монтажных пространств, боксов парогенераторов и насосов, защитных кожухов оборудования, ёмкостей с жидкими отходами выводятся с помощью вентиляционных систем с соблюдением нормативов по выбросу радиоактивных веществ . Воздушные потоки из вентиляторов очищаются от большей части аэрозолей на тканевых, волокнистых, зерновых и керамических фильтрах. Перед выбросом в вентиляционную трубу воздух проходит через газовые отстойники, в которых происходит распад короткоживущих изотопов (азота, аргона, хлора и др.) Помимо выбросов, связанных радиационным загрязнением, для АЭС, как и для ТЭС, характерны выбросы теплоты, влияющие на окружающую среду. Расход охлаждающей воды для типового блока АЭС мощностью 1100 МВт с испарительными градирнями составляет 120 тыс. т/ч (при температуре окружающей воды 14°С). При нормальном солесодержании подпиточной воды за год выделяется около 13,5 тыс. тонн солей, выпадающих на поверхность окружающей территории .Однако сейчас на АЭС предусматриваются меры для полного исключения сброса сточных вод, загрязнённых радиоактивными веществами. В водоёмы разрешается отводить строго определённое количество очищенной воды с концентрацией радионуклидов, не превышающей уровень для питьевой воды.

Таким образом ,можно сделать вывод о том ,что работа АЭС оказывает сильное негативное влияния на окружающую среду. Особое значение имеет распространение радиоактивных веществ в окружающем пространстве. В комплексе сложных вопросов по защите окружающей среды большую общественную значимость имеют проблемы безопасности атомных станций, пришедших на смену тепловым станциям на органическом ископаемом топливе. Однако, при авариях, атомные станции могут оказывать существенное радиационное воздействие на людей, экосистемы. Поэтому обеспечение безопасности окружающей среды от вредных воздействий АЭС- крупная научная и технологическая задача ядерной энергетики.

Библиографический список:

1. Мисбахов Р.Ш., Гуреев В.М., Гортышов Ю.Ф. Влияние добавок водорода на характеристики газопоршневого двигателя при изменении угла опережения зажигания: Известия высших учебных заведений– М.: Авиационная техника, 2009– С.73-74.

2. Мисбахов Р.Ш., Мизонов В.Е. Моделирование теплопроводности в составной области с фазовыми переходами: Вестник Ивановского государственного энергетического университета – М.: 2015– С. 39-43.

3. Шуина Е.А., Мизонов В.Е., Мисбахов Р.Ш. Влияние поперечной неоднородности потока газа на кривую разделения гравитационного классификатора: Вестник Ивановского государственного энергетического университета – М.: 2015– С. 60-63.

Научное издание

Коллектив авторов

ISSN 2500-1140

Техниконаучный журнал «Техноконгресс»

Кемерово 2019