**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ХАБАРОВСКИЙ ИНСТИТУТ ИНФОКОММУНИКАЦИЙ (ФИЛИАЛ)
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО
ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»
ХИИК СибГУТИ**

НАУКА – ЭТО ИНТЕРЕСНО!

Сборник материалов межкафедральных студенческих научных семинаров и конференций (ноябрь-декабрь 2023г.)

**ХАБАРОВСК
2023**

УДК 004.2; 37.1; 52.7
ББК 60.05

НАУКА – это интересно!: Сборник материалов межкафедральных студенческих научных семинаров и конференций (октябрь - декабрь 2023г.) / Сост.: Щербаков А.Г.; Отв. ред. Шульженко Н.В. – Хабаровск: Изд-во ХИИК СибГУТИ, 2023. – 35с.

В очередной сборник «НАУКА – это интересно!» помещены лучшие доклады, отражающие результаты труда студентов и их преподавателей в сложном, но интересном разделе научной работы – научно-поисковой.

Именно это вид учебной деятельности связан с научным поиском, проведением исследований, экспериментами в целях расширения имеющихся и получения новых знаний, проверки научных гипотез, установления закономерностей, проявляющихся в природе и в обществе, научных обобщений, научного обоснования проектов.

Цель данного сборника – побудить интерес студентов к научной деятельности, а это в свою очередь поможет им более качественно освоить свою будущую профессию.

Издаётся согласно Плана работы
ХИИК (филиал) ФГБОУ ВО СибГУТИ на 2023 год

СОДЕРЖАНИЕ

УДК 658.75

ПРОБЛЕМЫ В СОЗДАНИИ ЭЛЕКТРОННЫХ КАРТ

Грищенко И.М.
студент 1 курса, Специальность «Информационные системы и программирование»
Епанешникова Д.Ю.
преподаватель кафедры «Информационные технологии»

Аннотация: В статье рассказывается об основных проблемах для создания электронных географических карт, а также предлагаются решения этих проблем.
Ключевые слова: спутник, программист, бюджет, оборудование, конкурентоспособность.

Что нужно для создания электронной карты? Оборудование для съёмки, серверы для хранения информации, команда программистов для создания сайта или приложения, которая займётся его конструированием, и обязательно разрешение, которое получается в центральном картографо-геодезический фонде.

Все начинается со сьемки местности, и здесь важно использовать следующие основные инструменты:

1. Спутники – они позволяют выполнить аэрофотосъёмку больших площадей территории, такой способ потребует серьезных финансовых затрат, но остается как удобным, так и популярным.

2. Адресные базы – сайт в которых есть адреса зданий и их географические координаты (долгота и широта). Базы адресов приобретаются у поставщиков, приводятся к единому виду и добавляются в геоинформационную систему.

Говоря об крупных картах или о картах целой планеты, необходимо отметить, что для такой задачи нужны значительные затраты, следовательно, финансирование для создания карт может позволить выделить либо правительство страны для улучшения жизни своего населения, либо крупная компания для повышения конкурентоспособности своей продукции.

Подводя итог, отметим, с какими проблемами можно столкнуться при необходимости создания электронной карты:

- значительные затраты. Вариантом решения видится размещение рекламы предприятий, купивших приложение с электронными картами, в самом этом приложении;
- оборудование для съёмки. При изготовлении карты с высокими требованиями по качеству целесообразно использовать адресные базы;
- созданное приложение необходимо оценивать с точки зрения эргономики;
- отсутствие клиентов, возможное решение – покупка рекламы и рекомендации у компаний, нуждающихся в приложении.

С какими проблемами возможно встретиться после создания приложения? Прежде всего, необходимо обеспечить конкурентоспособность на необходимом нам уровне. Как же обеспечить конкурентоспособность? Рассмотрим несколько способов:

- улучшение качества съёмки облегчит ориентирование на местности;
- улучшение сайта, прежде всего построение грамотной схемы обратной связи от клиентов;
- увеличение числа потенциальных клиентов, путем привлечения дополнительной рекламы;
- инновации, выраженные в актуальных обновлениях приложения, устаревшая карта - опасна.

Электронные карты делают нашу жизнь более легкой и безопасной. Указывают самый рациональный путь до пункта назначения, и кроме того, мобильный телефон позволяет держать все необходимые карты под рукой, а также с помощью мобильного интернета можно загружать карты новых городов и обновлять существующие карты.

Мы рассмотрели процесс создания электронных карт, узнали, какие сложности и решения встречаются на пути их создания.

Перечень использованной литературы и источников:
1. URL: https://habr.com/ru/companies/vk/articles/406521/
2. URL: https://www.turboreferat.ru/programming-computer/geoinformacionnye-tehnologii-sozdanie-jelektronnyh-kart/32185-154315-page2.html
3. URL: https://cyberleninka.ru/article/n/problemy-ispolzovaniya-sovremennogo-instrumentariya-dlya-sozdaniya-interaktivnyh-turistskih-veb-kart-i-geoportalov/viewer
4. URL: https://moluch.ru/archive/137/38285/
5. URL: https://studfile.net/preview/8981166/page:36/

УДК 004.056

ТЕХНОЛОГИЯ БЛОКЧЕЙН: ПРЕИМУЩЕСТВА И ПРОБЛЕМЫ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Иванов Н.В; Усик П.
студенты 4 курса, специальность «Сети связи и системы коммутации»
Щербаков А.Г.
преподаватель кафедры «Информационные технологии»

Аннотация: В статье рассматриваются основные преимущества и проблемы технологии блокчейн для информационной безопасности, а также перспективы ее развития и применения в различных сферах.

***Ключевые слова*:** блокчейн, криптография, информационная безопасность, децентрализация, анонимность, биткоин, алгоритм хеширования, NFT-метка.

Блокчейн – инновационная технология, которая имеет большой потенциал для улучшения информационной безопасности в разных сферах и отраслях, позволяет создавать распределенные, неподделываемые и согласованные базы данных, содержащие информацию о транзакциях, событиях или любых других данных. Блокчейн состоит из цепочки блоков, каждый из которых содержит хеш-сумму предыдущего блока, временную метку и данные. Блоки формируются и проверяются участниками сети по определенным правилам, которые обеспечивают консенсус и безопасность. Блокчейн может быть публичным, частным или консорциумным, в зависимости от того, кто имеет доступ к данным, и кто может добавлять новые блоки.

Преимущества технологии.

1. Децентрализация. Блокчейн работает на основе сети, где нет единого центра управления. Это обеспечивает большую безопасность и устойчивость к атакам.

2. Прозрачность и отслеживаемость. Блокчейн позволяет видеть всю историю транзакций или событий, которые записаны в базе данных, и проверять их подлинность. Это увеличивает доверие и сотрудничество между участниками сети, а также упрощает аудит и контроль.

2. Неизменность и устойчивость. Блокчейн защищает данные от подделки, удаления или изменения, так как любая попытка сделать это потребует изменения всей цепочки блоков, что практически невозможно без согласия большинства участников сети. Блокчейн также устойчив к атакам, так как не имеет единой точки отказа, а распределен между множеством *нод*.

3. Эффективность и экономичность. Блокчейн упрощает и ускоряет процессы, связанные с обменом, проверкой и хранением данных, так как не требует посредников, центральных органов или дополнительных слоев абстракции. Блокчейн также снижает затраты на инфраструктуру, обслуживание и транзакционные комиссии.

Недостатки технологии.

1. Масштабируемость и производительность. Блокчейн сталкивается с ограничениями по скорости и объему обработки транзакций, так как каждый блок

имеет фиксированный размер и интервал времени, а также требует достаточного количества участников для подтверждения. Это может приводить к задержкам, перегрузкам и высокому потреблению ресурсов, особенно в публичных блокчейнах с большим числом узлов и транзакций.

2. Конфиденциальность и регулирование. Данные в блокчейне обычно открыты для всех или для определенной группы участников, что может создавать риски для личных данных, интеллектуальной собственности, коммерческой тайны и других чувствительных данных. Блокчейн также может столкнуться с проблемами регулирования и соблюдения законов, так как разные страны и организации могут иметь разные требования и стандарты к защите данных, идентификации пользователей, ответственности за нарушения и т.д.

3. Неподвижность данных. Как только данные записаны в сеть, их сложно изменить и практически невозможно удалить. Например, если в блокчейне хранится неправильная информация о правах собственности на недвижимость, её будет сложно исправить без вмешательства большинства участников сети.

4. Отсутствие стандартов. Блокчейн-проекты разрабатывают на разных языках и консенсусах. При этом все они обособлены друг от друга. Перенести активы из одного блокчейна в другой в разы сложнее, чем перевести деньги между вкладами в разных банках.

5. Риск «атаки большинства» (атака 51%). Если группа мошенников всё же сможет завладеть 51% какого-либо блокчейна, они будут контролировать его. Махинации с активами в такой сети будут проходить под видом обычных транзакций. Вероятность, что такое произойдёт, невелика – злоумышленникам понадобится много ресурсов и слаженная работа. Но этот недостаток системы невозможно исправить.

6. Использование для взлома квантовых компьютеров. Квантовые компьютеры представляют угрозу для блокчейна, так как они могут взломать криптографические алгоритмы, которые обеспечивают безопасность и консенсус в сети.

Одна из основных уязвимостей блокчейна – алгоритм хеширования, который используется для создания идентификаторов блоков и транзакций, а также для проверки подписей и доказательства работы. Алгоритм хеширования – функция, которая преобразует любые данные в уникальный и непредсказуемый код фиксированной длины. Алгоритм хеширования должен быть односторонним, то есть легко вычислять хеш из данных, но сложно восстановить данные из хеша. Большинство блокчейнов используют алгоритмы хеширования, такие как SHA-256 или SHA-3, которые считаются надежными для классических компьютеров.

Однако квантовые компьютеры могут взломать эти алгоритмы с помощью алгоритма Гровера, который позволяет находить обратные функции с квадратичным ускорением. Это означает, что квантовый компьютер может найти данные, соответствующие заданному хешу, за время, пропорциональное квадратному корню из размера пространства поиска.

Это может привести к серьезным последствиям для блокчейна, таким как:

– взлом приватных ключей. Квантовый компьютер может вычислить приватный ключ из публичного ключа, который используется для подписи транзакций и идентификации участников. Это может позволить квантовому хакеру украсть криптовалюту, подделать транзакции или выдать себя за другого пользователя;

– проблема двойной траты. Квантовый компьютер может создать две конфликтующие транзакции, которые будут иметь одинаковый хеш, но разные данные. Это может позволить квантовому хакеру потратить одни и те же деньги дважды, нарушив правило единственности транзакций.

– атака 51%. Квантовый компьютер может контролировать больше половины вычислительной мощности сети, что позволит ему создавать самую длинную цепочку блоков и игнорировать другие цепочки. Это может позволить квантовому хакеру

переписать историю транзакций, отменить или изменить уже подтвержденные транзакции, или предотвратить добавление новых транзакций.

7. Социальные атаки – атаки, которые используют психологические и социальные факторы для манипуляции людьми и заставления их раскрыть конфиденциальную информацию, выполнить нежелательные действия или нарушить правила безопасности. Социальные атаки могут быть направлены как на отдельных пользователей, так и на целые сообщества, которые участвуют в блокчейне и могут использовать различные методы, такие как фишинг, спуфинг, вредоносное ПО, социальная инженерия, дезинформация, пропаганда и т.д.

Основной опасностью социальных атак является то, что они могут нарушить доверие, консенсус и сотрудничество между участниками сети. Одна из основных целей социальных атак – получение доступа к приватным ключам пользователей, которые являются единственным способом управления их цифровыми активами.

Другая цель социальных атак – влияние на поведение и мнение пользователей, чтобы изменить ход развития блокчейна. Социальные атаки могут использовать различные средства, чтобы распространять дезинформацию, пропаганду, слухи, скандалы и т.д., чтобы дискредитировать оппонентов, создать разделение в сообществе, спровоцировать конфликты и сомнения, подорвать доверие и лояльность, повлиять на голосование и принятие решений.

Сферы применения блокчейна.

1. Финансы. Блокчейн широко используется для создания альтернативных валют, которые называются криптовалютами. Криптовалюты – цифровые деньги, которые не зависят от центральных банков или правительств. Они работают на основе криптографии, которая обеспечивает безопасность и анонимность транзакций. Блокчейн также позволяет совершать быстрые и дешевые международные переводы, выполнять смарт-контракты и проводить аудит финансовых операций.

Самая известная криптовалюта – биткоин, который был создан в 2009 году анонимным разработчиком под псевдонимом Сатоши Накамото. Биткоин – финансовая платформа, которая использует блокчейн для выпуска и обмена одноименной валюты.

2. Идентификация. Блокчейн может использоваться для создания цифровых удостоверений личности, которые подтверждают подлинность и принадлежность данных. Блокчейн может помочь в борьбе с мошенничеством, кибератаками и утечками личной информации, а также может облегчить доступ к различным сервисам, таким как банки, страховые компании, государственные учреждения и т.д.

Блокчейн используется для создания цифровых активов, таких как невзаимозаменяемые токены (NFT). NFT – уникальные и неделимые цифровые объекты, которые могут представлять любые вещи, например, искусство, музыку, видео, игры, спорт и т.д. NFT подтверждают подлинность и принадлежность цифровых объектов и позволяют торговать ими на специализированных площадках.

3. Медицина. Блокчейн может использоваться для хранения и обмена медицинскими данными, такими как истории болезней, рецепты, анализы и т.д. Технология может обеспечить конфиденциальность и безопасность пациентов, а также улучшить качество и эффективность медицинского обслуживания, способствовать развитию телемедицины, искусственного интеллекта и персонализированной медицины.

4. Логистика. Блокчейн может использоваться для отслеживания и управления поставками товаров и услуг, может повысить прозрачность и надежность логистических процессов, а также снизить издержки и риски, а также может помочь в борьбе с контрафактом, кражами и потерями грузов.

Перечень использованной литературы и источников:

1. Что такое блокчейн: принцип работы, сферы применения. [Электронный ресурс]. – URL: https://emcd.io/ru/articles/news/chto-takoe-blockchain/ (дата обращения: 10.11.2023).

2. Что такое блокчейн и как он работает. [Электронный ресурс]. – URL: https://academy.binance.com/ru/articles/what-is-blockchain-and-how-does-it-work (дата обращения: 10.11.2023).

УДК 530.145

КВАНТОВАЯ РЕВОЛЮЦИЯ: КАК КВАНТОВЫЙ КОМПЬЮТЕР ИЗМЕНИТ МИР И НАУКУ

Колесников Р.А.
студенты 1 курса, специальность: «Информационные системы и программирование»
Щербаков А.Г.
преподаватель кафедры «Информационная безопасность»

Аннотация: Квантовые компьютеры представляют собой новый уровень вычислительной мощности, который может решать задачи, недоступные для классических компьютеров, что позволяет параллельно обрабатывать большое количество информации и быстро находить оптимальные решения для сложных задач, таких как: оптимизация, криптография, машинное обучение, искусственный интеллект, химия, физика и многие другие.
***Ключевые слова*:** квантовый компьютер, кубит, суперпозиция, запутанность, декогеренция, алгоритм Шора, алгоритм Гровера, алгоритм Дойча-Йожи, постквантовая криптография.

Идея создания квантового компьютера возникла в начале 1980-х годов, когда физики столкнулись с проблемой моделирования сложных квантовых систем, таких как атомы, молекулы и свет. Они поняли, что классические компьютеры не способны эффективно обрабатывать такие задачи, так как пространство квантовых состояний растет экспоненциально с увеличением числа частиц. Поэтому они предложили использовать квантовые явления, такие как суперпозиция и запутанность, для передачи и обработки данных на квантовом уровне. Среди первопроходцев в этой области были Пол Бениофф, Юрий Манин, Ричард Фейнман, Стивен Визнер, Дэвид Дойч и другие. Они разработали теоретические основы, алгоритмы и модели квантового компьютера.

Само создание квантового компьютера началось в 1998-м году. В первую очередь им оснастили университеты, лаборатории и центры исследований. Спустя двадцать лет IBM смогли использовать квантовый компьютер через облачную базу. Эта опция поддерживается до сих пор. Облачные вычисления имеют непосредственный доступ к процессорам. Это также ускоряет передачу данных. Разработка может получить широкое распространение в повседневной жизни. Это решит ряд проблем в сферах машиностроения, экономики и дешифровки. Квантовые компьютеры способны выстраивать наиболее удобные маршруты. Из всех вероятных путей устройства выбирают кратчайший. Это можно использовать для навигации.

Квантовый компьютер – вычислительное устройство, которое использует явления квантовой механики для передачи и обработки данных. Такой компьютер оперирует кубитами, имеющими значения одновременно и 0, и 1, в отличие от бита, который может принимать значения либо 0, либо 1. Кубиты имеют два состояния: суперпозиция и запутанность. В первом случае возможна любая линейная комбинация элементов, запутанные кубиты в свою очередь образуют систему. Все ее составляющие взаимно влияют друг на друга. Это в разы повышает скорость вычисления и так же это позволяет обрабатывать все возможные состояния одновременно, достигая существенного преимущества перед обычными ПК в ряде алгоритмов (квантовым преимуществом). Работу над такими компьютерами уже ведут: «IBM», «Microsoft», «Intel», «Toyota» (в объединении с «QunaSys»). В суперпозиции квантовые частицы представляют собой комбинацию всех возможных состояний, пока не произойдет их наблюдение и измерение. Запутанные кубиты образуют единую систему и влияют друг на друга. Компьютер может использовать эту связь между кубитами, чтобы передавать и обрабатывать информацию без потерь. С увеличением числа запутанных кубитов

экспоненциально растет способность квантовых компьютеров обрабатывать информацию. Таким образом, квантовый компьютер может решать сложные задачи, которые невозможно или очень долго решать на обычном компьютере, например, взламывать шифры, моделировать молекулы, обучать искусственный интеллект и т.д. Квантовые компьютеры имеют большой потенциал для развития науки, технологии, бизнеса и общества в целом, но также представляют собой сложный и дорогостоящий проект, который требует преодоления многих технических и теоретических проблем.

В работе квантовых компьютеров используются определенные алгоритмы, такие как: алгоритм Шора (разложения числа на простые множители), алгоритм Гровера (быстрый поиск в неупорядоченной базе данных), алгоритм Дойча-Йожи (ответ на вопрос, постоянная или сбалансированная функция). Квантовый компьютер работает на вероятностном принципе. Его результатом работы является распределение вероятностей возможных ответов, наиболее вероятный ответ обычно является лучшим решением. Настоящий уровень развития технологий позволяет создать большое количество кубитов, сложность возникает с устойчивостью такой системы. Как и все квантовые системы, кубиты легко теряют заданное квантовое состояние при взаимодействии с окружением (происходит их декогеренция). При этом в работе квантового компьютера растет количество ошибок вычислений. Чтобы обеспечить ее устойчивость при проведении вычислений, требуется оградить систему от любого фонового шума, например, в случае сверхпроводниковых систем, охлаждая их до температур, близких к нулю по Кельвину (-273,1°C). Разработчики используют сверхтекучие жидкости, чтобы добиться такого охлаждения.

Практическое использование и разработки в наши дни

Ученые из Университета Дьюка представили свое открытие в области квантовых технологий. Они научили компьютер исправлять логические ошибки. Точность вычислений составила больше девяноста девяти процентов. Для этого они сложили несколько кубитов в общий логический кубит. Он не просто обнаруживает и исправляет недочеты. Он пресекает их дальнейшее повторение и распространение. Благодаря этому можно перестать опасаться сбоев системы.

На данный момент компания Toyota в объединении с QunaSys готова к использованию квантовых компьютеров для генерации идеальных материалов для создания аккумулятора. Устройство должно сгенерировать модель сочетаний материалов с идеальными свойствами для достижения своей цели. И квантовый компьютер в отличие от суперкомпьютера справится с этой задачей в разы быстрее и точнее. В случае успеха будет решена проблема разработки аккумуляторов для автомобилей. Даже лучшие аккумуляторы показывают относительно низкие статистики: огнеопасны, дорого обходятся для владельцев, быстро выходят из строя.

Юлихский исследовательский центр объявил о подготовке нового адиабатического компьютера на основе 150 кубитов. В разработке принимает участием команда французов Pasqal. Адиабатический компьютер может использовать несколько сотен кубитов. Разработчики уверены, что устройство в 150 кубитов позволит достигнуть квантового превосходства. И в это же время ученые из Китайского университета разработали два вычислительных устройства на фотонах. Они справляются с задачами в 24 раза быстрее, чем суперкомпьютер. А компания IBM анонсировала чип Eagle на 127 кубитов и в 2023 году компания намерена запустить квантовую систему на его основе.

Квантовые компьютеры, благодаря огромной скорости разложения на простые множители, позволит расшифровывать сообщения, зашифрованные широко применяемым криптографическим алгоритмом RSA. До сих пор этот алгоритм считается сравнительно надёжным, так как эффективный способ разложения чисел на простые множители для классического компьютера в настоящее время неизвестен. Для того, например, чтобы получить доступ к кредитной карте, нужно разложить на два

простых множителя число длиной в сотни цифр (даже для суперкомпьютеров выполнение этой задачи заняло бы в сотни раз больше времени, чем возраст Вселенной). Благодаря квантовому алгоритму Шора эта задача становится вполне осуществимой. В связи с этим особую актуальность приобретают исследования по постквантовой криптографии — криптографическим алгоритмам, обеспечивающим конфиденциальность в условиях квантовых атак. В конце декабря 2022 года была опубликована работа группы китайских учёных, которая продемонстрировала возможность взлома достаточно длинных RSA-ключей с помощью современных квантовых компьютеров. В работе рассказано о первом в истории взломе 48-битного ключа. Применение идей квантовой механики уже открыло новую эпоху в области криптографии, так как методы квантовой криптографии открывают новые возможности в области передачи сообщений. Прототипы систем подобного рода находятся на стадии разработки.

Перечень использованных литературы и источников:

1. В.И. Ключко, Н.В. Кушнир, Д.С. Шелехань. Квантовые технологии как основа квантового компьютера // Научные труды КубГТУ. – 2017. - № 3. – С. 136-144. [Электронный ресурс]. – URL: https://ntk.kubstu.ru/data/mc/0040/1548.pdf (дата обращения: 25.11.2023).
2. Игрушки с перспективой: на что способны новейшие квантовые компьютеры: [Электронный ресурс]. – URL: https://www.forbes.ru/tekhnologii/446705-igruski-s-perspektivoj-na-cto-sposobny-novejsie-kvantovye-komp-utery (дата обращения: 25.11.2023).
3. Квантовый компьютер. [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki/Квантовый_компьютер#Квантовая_телепортация (дата обращения: 25.11.2023).
4. Квантовый компьютер: победитель получит всё. [Электронный ресурс]. – URL: https://www.isp.nsc.ru/sobytiya/novosti?task=view&id=2351 (дата обращения: 25.11.2023).
5. Немного о квантовых компьютерах и о том, изменят ли они нашу жизнь. [Электронный ресурс]. –- URL: https://geektimes.ru/company/ua-hosting/blog/247424 (дата обращения: 25.11.2023).
6. Google заявила о достижении квантового превосходства – квантовый компьютер решил задачу в 220 млн. раз быстрее обычного: [Электронный ресурс]. – URL: https://3dnews.ru/1089450/google-zayavila-o-dostigenii-kvantovogo-prevoshodstva-v-vichisleniyah-sekunda-na-kvantovom-kompyutere-ravna-desyatiletiyam-raboti-superkompyuterov (дата обращения: 25.11.2023).

УДК 535.022

СКОРОСТЬ СВЕТА: ОТ ЭЙНШТЕЙНА ДО АЛЬКУБЬЕРРЕ

Маркова Е.М., Киселёва Ю.А.
студенты 1 курса, специальность: «Информационные системы и программирование»
Щербаков А.Г.
преподаватель кафедры «Информационная безопасность»

Аннотация: В статье поднимается тема возможности достижения и преодоления скорости света, её теоретические модели и экспериментальные проверки, определение и принцип действия варп-двигателя, пузырь Алькубьерре.

***Ключевые слова*:** скорость света, сверхсветовое движение, специальная теория относительности, тахионы, кротовые норы, варп-двигатель, Пузырь Алькубьерре.

Возможно, ли достичь и преодолеть скорость света?

Для начала вспомним, что скорость света - величина, с которой свет движется в вакууме и равна приблизительно 300 000 км/с. И чем быстрее что-то движется, тем более массивным оно становится, и тем больше замедляется время. На малых скоростях это практически неощутимо, но при приближении к скорости света это становится резко заметным. Из-за этого следует, что, если вы хотите ускорить хотя бы один электрон до световой скорости, вам понадобится бесконечное количество энергии поскольку этот электрон становится бесконечно тяжёлым. Так как у света нет массы, у него не возникает такой проблемы. В этом и заключается сложность преодоления скорости света. Впервые теорию выдвинул Альберт Эйнштейн в 1905 году, которая

гласит об объектах, которые движутся с постоянной скоростью по отношению друг к другу. Эта теория имеет название специальная теория относительности. Согласно этой теории, ничто во Вселенной не может двигаться быстрее скорости света, так как это нарушало бы принцип причинности и потребовало бы бесконечного запаса энергии.

Сверхсветовое движение - движение со скоростью, превышающей скорость света в вакууме. Несмотря на то, что скорость согласно специальной теории относительности скорость света в вакууме является максимально достижимой скоростью распространения сигналов, энергия частицы положительной массы стремится к бесконечности при приближении её к скорости света, объекты, движения которых не связано с переносом информации, могут иметь сколь угодно большую скорость.

Однако, существуют некоторые гипотетические ситуации, в которых возможно сверхсветовое движение, то есть движение быстрее скорости света в вакууме. О них мы сегодня поговорим

Тахионы – гипотетические частицы, которые могут двигаться быстрее света в вакууме и имеют мнимую массу. Они были предложены в 1960-х годах как возможное решение некоторых проблем в квантовой теории поля. Однако, существование тахионов не подтверждено экспериментально и противоречит специальной теории относительности, которая утверждает, что ничто не может превысить скорость света. Тахионы также вызывают трудности с принципом причинности, так как они могут позволить передавать информацию в прошлое.

Кротовые норы – гипотетические объекты, которые могут соединять разные области пространства-времени или даже разные вселенные. Они представляют собой тоннели, которые имеют два устья, открывающиеся в удаленных друг от друга местах. Кротовые норы были предложены в 1935 году Альбертом Эйнштейном и Натаном Розеном как решение уравнений общей теории относительности. Они также называются мостами Эйнштейна-Розена или червоточинами.

Кротовые норы могут иметь разные типы и свойства, в зависимости от их метрики, то есть способа измерения расстояний и времени внутри них. Некоторые кротовые норы могут быть проходимыми, то есть позволять перемещаться из одного устья в другое, а некоторые - непроходимыми, то есть выглядеть как черные дыры. Некоторые кротовые норы могут быть статичными, то есть не меняться со временем, а некоторые - динамичными, то есть изменять свою форму и размер. Некоторые кротовые норы могут быть симметричными, то есть иметь одинаковые устья, а некоторые - асимметричными, то есть иметь разные устья

Кротовые норы привлекают внимание ученых и фантастов, так как они могут теоретически позволить путешествовать во времени и между вселенными. Однако, для этого необходимо решить ряд проблем, таких как стабилизация кротовой норы, защита от высоких температур и радиации, согласование с принципом причинности и т.д. Поэтому, пока что кротовые норы остаются только теоретической возможностью, которая требует дальнейших исследований и экспериментов

Пузырь Алькубьерре – решение уравнений Эйнштейна, которое описывает искривление пространства-времени вокруг объекта, которое позволяет ему двигаться быстрее света без нарушения принципа причинности. Эти ситуации не противоречат теории относительности, но требуют дополнительных предположений и не подтверждены экспериментально.

Варп-двигатель – технология, которая позволяет путешествовать в космосе со скоростью, превышающей скорость света. Он работает, генерируя деформационные поля для формирования подпространственного пузыря, который окутывает космический корабль, искажая пространственно-временной континуум и перемещая корабль со скоростями, которые могут значительно превышать скорость света. Само судно находится в своеобразном пузыре, которая защищает корабль от деформаций.

Корабль внутри поля искажения фактически остаётся неподвижным, - перемещается само искажённое пространство, в котором он находится.

Чисто теоретически такое сверхсветовое перемещение возможно, если создать перераспределение темной энергии в охватывающем корабль космическом пространстве, чтобы позади корабля был ее избыток, а спереди — область отрицательной энергии. Но, во-первых, о темной энергии на сегодняшний день практически ничего не известно, а во-вторых, исходя из общей теории относительности Эйнштейна, перераспределение огромного количества гипотетических частиц материи, обладающей экзотическими свойствами, потребует гигантского количества энергии.

Новое исследование, проведенное в Геттингенском университете, позволяет обойти эти проблемы с помощью нового класса сверхбыстрых устойчивых одиночных волн – солитонов, созданных только за счет источников с положительной энергией. Никаких «экзотических» отрицательных плотностей энергии для этого не требуется.

Автор исследования доктор Эрик Ленц описывает теоретически возможные конфигурации кривизны пространства-времени, организованные в солитоны, или «пузыри искривления» – компактные волны, которые, сохраняя свою форму, могут двигаться с любой скоростью. Помещенный внутрь такого пузыря космический корабль будет перемещаться вместе с самим солитоном.

По расчетам ученого, если бы можно было выработать достаточно энергии, путь до ближайшей звезды Проксима Центавра внутри пузыря искривления занял бы всего четыре года. Для сравнения, при нынешних ракетных технологиях время такого путешествия составит более 50 тысяч лет. При этом все уравнения, использованные автором исследования, основаны на традиционной физике.

Ленц вывел уравнения Эйнштейна – Максвелла для неизученных солитонных конфигураций и обнаружил, что измененная геометрия пространства-времени может быть сформирована таким образом, чтобы работать даже с обычными источниками энергии. По сути, новый метод использует саму структуру пространства и времени, организованную в солитон, чтобы обеспечить решение проблемы сверхсветового путешествия.

Кроме того, солитоны Ленца сконфигурированы так, чтобы минимизировать действие приливных сил, так что течение времени внутри и снаружи пузыря совпадает. Это позволяет избежать так называемого «парадокса близнецов», согласно которому один близнец, путешествующий со скоростью, близкой к скорости света, будет стареть намного медленнее другого, оставшегося на Земле.

В настоящее время количество энергии, требуемой для этого нового типа космической силовой установки, по-прежнему огромно.

Перечень использованной литературы и источников:

1. Альберт Эйнштейн и его уникальное наследие. [Электронный ресурс]. – URL: https://naked-science.ru/article/nakedscience/albert-eynshteyn-i-ego (дата обращения: 25.11.2023).

2. Новая волна в исследованиях варп-двигателя. Решение Ленца и что из него следует. [Электронный ресурс]. – URL: https://habr.com/ru/articles/548612 (дата обращения: 25.11.2023).

3. Давайте разберемся: почему ничто не может быть быстрее света?. [Электронный ресурс]. – URL: https://hi-news.ru/science/davajte-razberemsya-pochemu-nichto-ne-mozhet-byt-bystree-sveta.html (дата обращения: 25.11.2023)

3. Варп-двигатель – космический Тянитолкай. [Электронный ресурс]. – URL: https://elementy.ru/nauchno-populyarnaya_biblioteka/436233/Varp_dvigatel_kosmicheskiy_Tyanitolkay (дата обращения: 25.11.2023).

ТЕОРИЯ УЗЛОВ И КОС

Нигей А.С.

студент 1 курса, специальность «Информационные системы и программирование»

Калиниченко Ю.А.

преподаватель высшей категории, преподаватель кафедры «Информационные технологии»

Аннотация: Проведя исследование по данной теме, мы изучили математические понятия «коса», «узел», историю возникновения и развития теорий кос и узлов, а также классификацию кос, узлов и их свойства. Было рассмотрено приложение кос и узлов в различных сферах жизни и деятельности человека.
Ключевые слова: теория кос, теория узлов, алгоритм распутывания улов, умножение кос, танглоид.

Любой разумный человек умеет завязывать узлы и практически каждый заплетать косу из трех прядей волос. Однако не каждый знает, что это ещё и математические объекты.

В этой статье будет показана взаимосвязь между косами, узлами и математикой. Теория кос, как и теория узлов – это молодая, развивающаяся наука, возникшая в 20-х годах XIX века, ещё не завершена и не исчерпала своих приложений. Математики впервые заинтересовались косами и узлами лишь в XIX веке и с того времени теория кос и узлов обрела статус самостоятельного раздела математики.

Теория кос, основания которой были построены немецким алгебраистом Эмилем Артином (1898-1962), является синтезом геометрии, алгебры и алгоритмических методов.

Первоначально косы были предложены Артином в качестве математической модели для текстильной промышленности. Теперь они занимают важное место в комплексном анализе, комбинаторике, квантовой механике и квантовой теории поля, химии, генетике.

Иоганн Гаусс был первым, кто рассматривал узел как математический объект. Сам Гаусс мало написал об узлах и зацеплениях, однако его ученик И.Б. Листинг посвятил узлам значительную часть своей монографии.

В последние 30 лет математики и физики с огромным интересом стали заниматься соответствующими теориями (особенно, теорией узлов).

Достаточно сказать, что за это время 4 из 66 медалей Филдса (от автора: *Филдсовская международная премия и медаль, которые вручаются один раз в 4 года на каждом международном математическом конгрессе двум, трём или четырём молодым математикам не старше 40 лет (или достигшим 40-летия в год вручения премии*), были получены именно за работы, связанные с этой теорией.

Теория кос: Коса – это формальная модель того, что понимается под словом «сплетение» в обычной жизни (девичья коса, плетёный ремень, обычный трос из переплетённых жил и т.д.), т. е. множество нитей, запутанных определённым образом; нити попарно не пересекаются и всё время должны опускаться вниз (нить не имеет права повернувшись, начать подниматься вверх). Касательный вектор в любой точке кривой должен всё время «смотреть вниз», ему запрещается быть горизонтальным и тем более «смотреть вверх».

Классификация кос (См. Рис. 1):

- Девичья коса – *символ девичества, молодости, красоты, чистоты. В Древней Руси девушки берегли косу до замужества. С древнейших времен длинные волосы считаются символом красоты и женственности.*

- Тривиальная коса – *коса, все нити которой вертикальные прямые (не запутанные), называется тривиальной. Тривиальная коса – частный случай крашеной косы.*

- Крашеная коса – *так называется любая коса, которая сохраняющая порядок номеров нитей.*

- Циклическая коса – *это косы, переставляющие все номера нитей по единому циклу.*

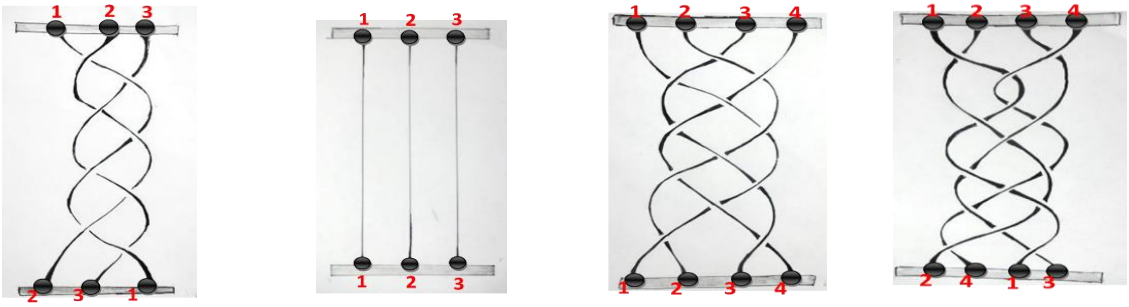

Рисунок 1 – Классификация кос

Фигуры, которые не являются косами, если их нити имеют восходящий характер, что запрещено теорией кос представлены на рисунке 2.

Рисунок 2

Алгебраизация кос. Так как косы – один из простейших геометрических объектов, легко поддающийся «алгебраизации»: косы с одинаковым числом нитей можно умножать.

Нужно приложить одну косу к другой, склеив соответствующие нити, и удалить ставшие ненужными гвоздики.

Возьмём две косы *a* и *b* с одинаковым числом нитей и соединим нижние концы нитей первой косы с верхними концами нитей второй косы; полученную косу, сжатую в два раза в вертикальном направлении, **называют произведением** этих двух кос и обозначают ***ab*** (См. Рис. 3). Следует заметить, что известное всем нам правило «о перемене мест множителей» не распространяется на косы.

Умножение кос обладает следующими свойствами:

1. Ассоциативный закон (сочетательный). Общий у кос и у чисел.

$$(a*b)*c=a*(b*c)$$

2. Наличие единицы, т.е. существует такая коса 1, что для любой косы, а выполняется

$$a*1=a=1*a$$

3. У каждой косы b имеется обратная коса b^{-1}. Выполняется следующее равенство:

$$b^{-1}=b*b^{-1}=1$$

Всякий раз, когда некоторое множество снабжено операцией, обладающей тремя свойствами, о которых мы только что упоминали, математики говорят, что они имеют дело *с группой*.

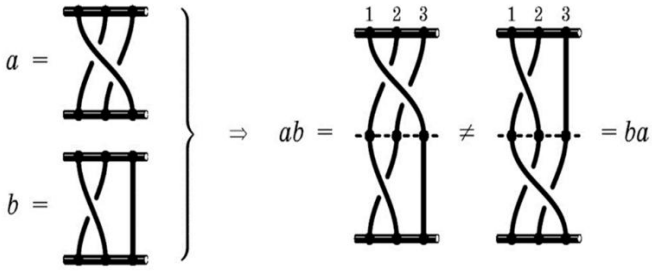

Рисунок 3

Теория узлов.

Узел – это некая абстракция, рассматривается не веревка и не шнур, а бесконечно тонкая, гибкая и растяжимая нить с зафиксированными (соединенными) концами (или уходящими в бесконечность в противоположные стороны) представлена на рисунке 4.

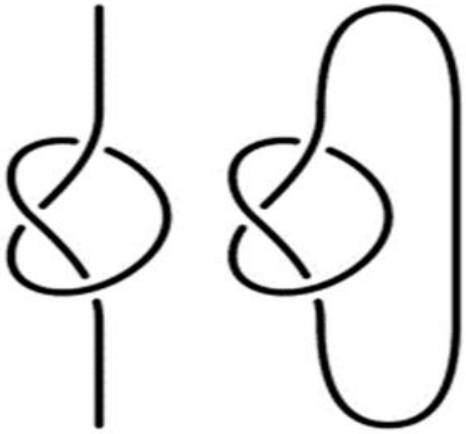

Рисунок 4

Таблица основных узлов (См. Рис. 5). Для облегчения поиска и унификации узлы имеют стандартное обозначение: первая цифра указывает число двойных точек, а вторая (расположенная в индексе) – порядковый номер узла**.**

Самый простой узел – тривиальный (на плоскости в виде окружности). Узел называется нетривиальным, если он не эквивалентен тривиальному, т.е. его нельзя «пошевелить» (возможно, растягивая, но не разрывая веревку) так, чтобы он превратился в тривиальный.

Узел 3_1 –трилистник;

Узел 4_1 – «восьмёрка», или узел Листинга;

Узел 5_1 – узел «Печать Соломона».

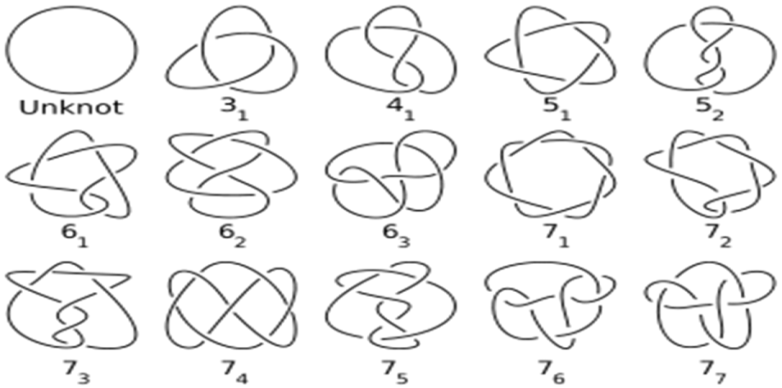

Рисунок 5

Существует способ превратить косу в узел. Для этого необходимо замкнуть ее, т.е. соединить верхние концы нитей с нижними.

Теорема Александра состоит в том, что любой узел – это замкнутая коса. Соответственно, если считать узлы кривыми, концы которых уходят в бесконечность, то умножение узлов определяется так: произведение узлов a и b – это просто нить, на которой завязан сначала узел a, затем узел b.

Алгоритм развязывания узла: В теории узлов есть две связанные задачи: распознать тривиальный узел и понять, представляют ли две запутанные диаграммы одно и то же или нет.

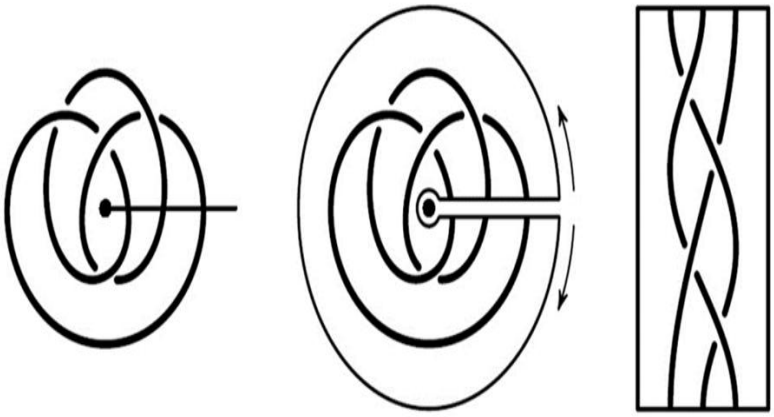

Рисунок 6

С 1860 года топологи много раз возвращались к решению этой задачи. Но реальный прорыв произошел в 20-е годы XX века в Германии благодаря работе Курта Рейдемейстера. Он задался вопросом, что значит, когда два узла эквивалентны, изотопны. Он рассмотрел локально диаграмму узлов возле отдельных перекрестков и показал, что два узла изотопны, если их диаграммы переводятся друг в друга с помощью наборов простых движений (См. Рис. 7).

Приложения теории кос и узлов. У теории кос и узлов существуют вполне серьезные приложения, например, к комплексному анализу, механике и физике элементарных частиц, а так же идея кодирования химической информации в маленьких узелках (и косах!) при изучении ДНК. Теория узлов и кос имеет много приложений, как в математике, так и за её пределами.

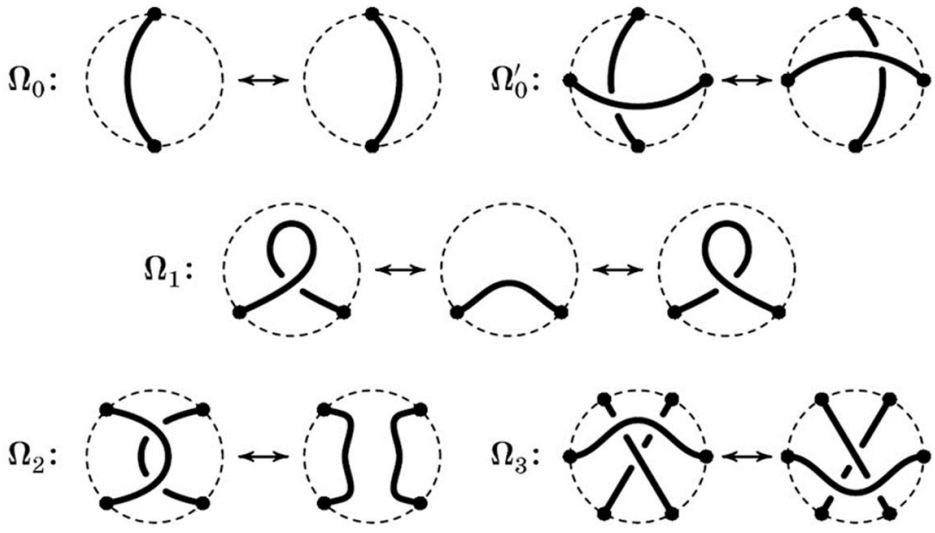

Рисунок 7 – Схема движений Рейдемейстера

На Солнце перенос энергии от поверхности к короне происходит часто в форме торнадо, сплетающихся в косы.

Физикам из Университета Чикаго впервые удалось создать в лаборатории узел из вихря воды и наблюдать за его эволюцией и распадом.

Реконструкция потоков воды вблизи узла трилистника. Белым цветом показано движение пузырьков, а красным и синим – восстановленная физиками картина.

Молекула ДНК. Её молекулы имеют огромную по молекулярным масштабам длину и состоят из двух нитей, сплетённых между собой в двойную спираль.

Заключение: В статье рассмотрены основные моменты касающиеся теории кос и узлов: математическое понятие «коса», «узел», историю возникновения и развития теорий кос и узлов, а также классификацию кос, узлов и их свойства. Было представлено приложение кос и узлов в различных сферах жизни и деятельности человека. Установлена связь между плетением кос, завязыванием узлов и математикой.

Перечень использованной литературы и источников:

1. Ковыев Н.П. Узлы и косы. [Электронный ресурс]. Интернет-сайт Интернет портал «Одаренные дети» математика и физика. – URL: http://genius.pstu.ru/file.php/1/pupils_works_2012/Kovyev_Nikita.pdf (дата обращения: 14.11.2023)
2. Кроуэлл Р., Фокс Р. Введение в теорию узлов [учебник] / Кроуэлл Р., Фокс Р.; пер. с англ. Виноградов А. М. – Череповец: Меркурий-Пресс, 2000. – 306 с.
3. Мантуров В.О. Лекции по теории узлов и их инвариантов / О.В. Мантуров. – Москва: Эдиториал УРСС, 2001. – 304 с.
4. Мантуров В.О. Экскурс в теорию кос / В.О. Мантуров // Математическое просвещение. – Москва: МЦНМО, 2010. – Т. 3, вып. 14. – С. 107–142. [Электронный ресурс]. – URL: http://www.varf.ru/rudn/manturov/braids.pdf (дата обращения: 14.11.2023)
5. Скрипченко А. FAQ: Теория узлов. [Электронный ресурс]. Интернет-сайт «Издательский дом «ПостНаука». – URL: https://postnauka.ru/tv/157252. (дата обращения: 14.11.2023).
6. Сосинский А.Б. Узлы и косы / А.Б. Сосинский. – Москва: МЦНМО, 2001. – 24 с.
7. Сосинский А.Б. Косы и узлы. [Электронный ресурс]. Интернет-сайт Журнал «Квант». – URL: http://kvant.mccme.ru/1989/02/kosy_i_uzly.htm (дата обращения: 14.11.2023).

УДК 004

ИСПОЛЬЗОВАНИЯ МЕТОДОВ СТЕГАНОГРАФИИ ДЛЯ ИНФОРМАЦИИ В ИЗОБРАЖЕНИИ И ЗВУКЕ

Петров Д.И.
студент 4 курса специальность «Информационные системы и программирование»
Кузнецова М.В.
преподаватель кафедры «Информационная безопасность»

Аннотация: В статье авторами рассмотрены особенности реализации методов стеганографии для изображений с целью скрытой передачи и охраны информации.
Ключевые слова: информация, стенография, техники стеганографии, цифровая стеганография.

Стеганография – это способ спрятать информацию внутри другой информации или физического объекта так, чтобы ее нельзя было обнаружить.

Стеганографию иногда сравнивают с криптографией, поскольку и то и другое – это способы секретной коммуникации. Однако между ними есть разница, поскольку при стеганографии данные при отправке не шифруются, а при получении не нужен ключ для расшифровки.

Стеганография позволяет скрывать информацию так, чтобы не вызвать подозрений. Одна из самых распространенных техник стеганографии – LSB (least significant bit – «наименее значащий бит»): секретные данные встраиваются в наименее значащие биты медиафайла.

Рассмотрим этапы LSB:

- Каждый пиксель в изображении состоит из трех байтов данных, соответствующих красному, зеленому и синему цветам. Некоторые форматы изображения содержат дополнительный, четвертый байт для прозрачности, так называемый «альфа-канал».

- LSB-стеганография позволяет изменять последний бит каждого из этих байтов так, чтобы спрятать один бит информации. Таким образом, чтобы спрятать 1Мб данных с помощью этой техники, понадобится графический файл объемом 8 Мбайт.

- Изменение последних битов пикселя не влияет на зрительное восприятие картинки, так что при сравнении оригинального и измененного файлов разница незаметна.

Та же техника может применяться к другим медиафайлам, таким как звук или видео, когда информация встраивается в файл практически без изменения аудио- или видеоряда.

Еще одна техника стеганографии предполагает замену букв или слов. При этом текст секретного сообщения внедряется в другой текст, гораздо большего размера, а слова размещаются через определенные интервалы. Хотя метод замены прост в использовании, но при этом конечный текст может выглядеть странно и неестественно, поскольку секретные слова могут по смыслу выпадать из предложений.

Другие техники стеганографии позволяют скрывать целые разделы жестких дисков или встраивать данные в заголовки файлов и сетевых пакетов. Эффективность этих техник определяется тем, какой объем данных они позволяют скрыть и насколько легко эти данные обнаружить.

3) Виды стеганографии. Существует пять основных видов цифровой стеганографии:

- текстовая стеганография;
- стеганография в изображениях;
- стеганография в видео;
- стеганография в звуке;
- сетевая стеганография;
- текстовая стеганография

Текстовая стеганография означает сокрытие данных внутри текстовых файлов. Это может быть форматирование текста, изменение слов внутри текста, использование контекстно-свободных грамматик для генерации читабельных текстов или генерация случайных последовательностей символов.

Стеганография в изображениях: *Это означает сокрытие данных внутри графических файлов. Этот вид стеганографии часто используют, чтобы скрыть информацию, поскольку цифровое изображение состоит из большого числа элементов и есть много способов спрятать данные внутри него.*

Стеганография в звуке: Секретные сообщения встраиваются в аудиосигнал, что изменяет бинарную последовательность соответствующего аудиофайла. Встраивание секретных сообщений в цифровой звук – это более сложный процесс по сравнению с другими.

Стеганография в видео: *Данные прячутся внутрь цифровых видеоформатов. Стеганография в видео позволяет скрывать большие объемы данных в движущемся потоке изображения и звука. Есть две разновидности стеганографии в видео:*

- встраивание данных в некомпрессированное видео с последующей компрессией;
- встраивание данных прямо в сжатый поток видео.

Сетевая стеганография или протокольная – *это техника встраивания информации в сетевые протоколы, используемые при передаче данных, такие как TCP, UDP, ICMP и др.*

Перечень использованной литературы и источников:

1. Один из крупнейших в рунете сайтов, в котором люди делятся своим опытом в прикладном использовании тех или иных алгоритмов стеганографии. [Электронный ресурс]. – URL: https://tproger.ru/digest/learning-crypto/ (дата обращения: 10.10.2023).
2. Официальный сайт компании, специализирующийся на разработке систем защиты от киберугроз «Kaspersky». [Электронный ресурс]. – URL: https://www.kaspersky.ru/blog/digital-steganography/23025/ (дата обращения: 10.10.2023).
3. Официальный сайт электронного журнала «SecurityLab». [Электронный ресурс]. – URL: https://www.securitylab.ru/ (дата обращения: 10.10.2023).
4. Сайт-справочник: Ру-стеганография. [Электронный ресурс]. – URL: http://ru-steganography.narod.ru/ (дата обращения: 10.10.2023).
5. Федосеев В.А. Цифровые водяные знаки и стеганография: Учебное пособие / В.А. Федосеев. – Самара: Издательство Самарского университета, 2019. – 144с.

УДК 004.056

DOS-АТАКИ: МЕХАНИЗМ, РИСК И МЕРЫ ПРЕДОСТОРОЖНОСТИ

Савин А.Е., Трещалов П.С.
студенты 4 курса, специальность «Сети связи и системы коммутации»
Щербаков А.Г.
преподаватель кафедры «Информационные технологии»

Аннотация: Статья посвящена анализу проблемы атак типа «отказ в обслуживании» (DoS), которые могут нарушить работу сетевых сервисов и ресурсов. Авторы рассматривают основные виды, цели, методы и последствия DoS-атак, а также современные способы их обнаружения и предотвращения.
***Ключевые слова*:** DoS-атака, DDoS-атака, отказ в обслуживании, сетевая безопасность, модель OSI.

Виды DoS-атаки: DoS-атака (отказ в обслуживании) – атака на сетевой сервис или ресурс, которая направлена на то, чтобы сделать его недоступным для легитимных пользователей. Для этого атакующий посылает на сервис или ресурс большое количество запросов или пакетов, которые перегружают его возможности или исчерпывают его ресурсы. В результате сервис или ресурс не может обрабатывать нормальный трафик и отказывает в обслуживании.

Существует несколько видов DoS-атак, которые можно классифицировать по разным критериям. Например, **по числу источников атаки** можно выделить:

– одноисточниковые DoS-атаки, когда атака идет с одного компьютера или устройства;

– многоисточниковые DoS-атаки, когда атака идет с нескольких компьютеров или устройств, которые могут быть распределены по разным сетям или географическим регионам;

– распределенные DoS-атаки (DDoS), когда атака идет с большого числа компьютеров или устройств, которые заражены вредоносным программным обеспечением и объединены в ботнет. Ботнет – сеть зараженных компьютеров, которые подчиняются командам атакующего. DDoS-атака более мощная, сложная и труднообнаружимая, чем одиночная DoS-атака. DDoS-атаки могут нанести больший ущерб и длиться дольше, чем DoS-атаки.

По типу атакуемого ресурса можно выделить:

– атаки на пропускную способность, когда атакующий посылает на сервис или ресурс большой объем данных, который превышает его пропускную способность и забивает канал связи;

– атаки на ресурсы, когда атакующий посылает на сервис или ресурс специально подобранные запросы или пакеты, которые требуют большого количества процессорного времени, памяти, дискового пространства или других ресурсов, и тем самым исчерпывает их;

– атаки на приложения, когда атакующий эксплуатирует уязвимости или ошибки в программном обеспечении сервиса или ресурса, которые приводят к его сбою, зависанию или некорректной работе.

По типу атакуемого сервиса или ресурса можно выделить:

– атаки на веб-серверы, когда атакующий посылает на веб-сервер большое количество HTTP-запросов, которые могут быть легитимными или нелегитимными, с целью снизить его производительность или вывести из строя;

– атаки на DNS-серверы, когда атакующий посылает на DNS-сервер большое количество DNS-запросов, которые могут быть легитимными или нелегитимными, с целью снизить его производительность или вывести из строя. DNS-сервер – сервер, который отвечает за преобразование доменных имен в IP-адреса и наоборот;

– атаки на почтовые серверы, когда атакующий посылает на почтовый сервер большое количество электронных писем, которые могут быть легитимными или нелегитимными, с целью снизить его производительность или вывести из строя. Почтовый сервер – сервер, который отвечает за прием и отправку электронной почты.

– атаки на базы данных, когда атакующий посылает на базу данных большое количество SQL-запросов, которые могут быть легитимными или нелегитимными, с целью снизить ее производительность или вывести из строя. База данных – система, которая хранит и обрабатывает структурированную информацию.

– атаки на сетевые протоколы, когда атакующий посылает на сетевой протокол большое количество пакетов, которые могут быть легитимными или нелегитимными, с целью нарушить его работу или вывести из строя. Сетевой протокол – набор правил, которые определяют, как обмениваться данными между компьютерами или устройствами в сети.

Цели и последствия DoS-атак.

Цели DoS-атак могут быть разными, в зависимости от мотивов атакующего. Например, DoS-атаки могут быть направлены на:

– экономический ущерб, когда атакующий хочет лишить жертву дохода, вызвав простой или снижение качества сервиса или ресурса;

– репутационный ущерб, когда атакующий хочет подорвать доверие к жертве, вызвав недовольство или разочарование у пользователей или клиентов сервиса или ресурса;

– политический или идеологический протест, когда атакующий хочет выразить свое несогласие или недовольство с политикой или идеологией жертвы, вызвав нарушение ее деятельности или коммуникации;

– шантаж или вымогательство, когда атакующий хочет заставить жертву выполнить его требования или угрожает продолжить атаку, если она не заплатит выкуп или не сделает что-то еще;

– разведка или подготовка к другой атаке, когда атакующий хочет получить информацию о сервисе или ресурсе, выявить его уязвимости или отвлечь его внимание от другой атаки.

Последствия DoS-атак могут быть серьезными, в зависимости от масштаба, продолжительности и цели атаки

Классификации DDoS-атак по уровням модели OSI.

Модель OSI (Open System Interconnection), или эталонная модель взаимодействия открытых систем описывает, как устройства в локальных и глобальных сетях обмениваются данными и что происходит с этими данными. Её предложили в 1984 году инженеры из Международной организации по стандартизации (ISO), которая работала над единым стандартом передачи данных по интернету.

При этом сама по себе эталонная модель – не стандарт интернета, как, например, TCP/IP; её можно сравнить с фреймворками в мире языков программирования: в OSI

«из коробки» доступны разные веб-стандарты – UDP, HTTP, FTP, Telnet и другие. Всего таких протоколов – более 100 штук.

Модель OSI включает семь слоёв, или уровней, – причём каждый из них выполняет определённую функцию: например, передать данные или представить их в понятном для человека виде на компьютере.

DDoS-атаки могут быть проведены на разных уровнях модели OSI, которая описывает семь уровней взаимодействия между сетевыми устройствами: физический, канальный, сетевой, транспортный, сеансовый, представительский и прикладной. Каждый уровень имеет свои протоколы, ресурсы и уязвимости, которые могут быть эксплуатированы атакующими.

Низкоуровневые.

Они происходят на L3-L4 модели OSI, то есть в районе сетевого и транспортного протокола:

– сетевой уровень (L3): DDoS-атаки по протоколам IPv4, IPv6, ICMP, IGMP, IPsec, RIP, OSPF. Цели таких атак, в первую очередь, сетевые устройства;

– транспортный уровень (L4): воздействие по протоколам TCP и UDP. Цели таких атак – конечные серверы и некоторые интернет-сервисы.

Такие атаки весьма распространены. Дело в том, что стандарты интернета делались с расчётом на то, что все участники будут добросовестно их использовать. Например, в протоколе UDP, который работает поверх IP, информация передаётся датаграммами, и в заголовках пакета не содержится IP ни источника, ни получателя. UDP доверяет адресацию протоколу IP, поверх которого работает, а в протоколе IP эти заголовки есть, но они никак не проверяются. Соответственно, очень многие атаки основаны на том, что меняется один из IP-адресов, как правило, это IP-адрес источника. Это называется спуфингом, т.е. атакой с подменой данных одного из узлов.

Такие атаки характерны тем, что нагружают какие-то части вашей инфраструктуры, забивают канал или заполняют служебные таблицы.

Высокоуровневые: Они затрагивают уровень приложения, L7, и воздействуют по прикладным протоколам, например, HTTP. Цели таких атак – конечные серверы и сервисы.

Самые распространённые виды атак: Существует несколько разновидностей DDoS-атак в зависимости от того, на что и как конкретно они воздействуют.

1. UDP Flood: UDP работает поверх протокола IP, и там нет установки соединения как такового – данные просто отсылаются без всякого контроля целостности. Поэтому злоумышленник может, например, подменить IP-адрес источника – рассылать пакеты со своего устройства, но делать, вид, что они приходят из других мест. Проверить это нельзя, и именно в таком виде они придут на сервер.

При такой атаке злоумышленник генерирует множество пакетов максимального размера и отправляет на сервер-жертву. Опасность в том, что, даже если сервер закрыт на firewall, невозможно повлиять на фильтрацию таких данных до их получения сетевым интерфейсом. «Последняя миля» от граничного маршрутизатора до сетевого интерфейса зачастую является наиболее уязвимым местом по пропускной способности. Пакеты всё равно пойдут через ваш канал и заполнят полосу пропускания.

2. Фрагментированный UDP Flood: Данная атака похожа на предыдущую, но у нее есть дополнительное действие: атакующий присылает на сервер жертвы пакет, но говорит, что это только часть. Сервер-жертва резервирует у себя ресурс, чтобы собрать пакет, но новые фрагменты не приходят.

3. TCP SYN Flood: У TCP есть механизм установки соединения. Сначала источник посылает SYN-запрос о том, что хочет установить соединение. Сервер-получатель отвечает пакетом SYN+ACK о том, что готов к соединению. Источник отвечает ACK-пакетом, подтверждая получение SYN+ACK. Соединение

устанавливается, потому что обе стороны подтвердили готовность, и начинают передаваться данные.

Здесь уже есть проверка соответствия IP-адреса, поэтому подменить его не получится. Но атакующий может генерировать SYN-пакет, инициируя новую сессию с сервером-жертвой, а соединение не установить, не отправляя ACK. Такая атака переполняет таблицу соединений, вызывая падение производительности. На настоящие запросы просто не остаётся места.

4. HTTP Flood: Направлена уже не на соединение, а непосредственно на ваш сервис, и обычно воздействует на прикладной уровень модели OSI.

HTTP Flood – просто генерация запросов. Здесь не происходит какой-то подмены, нарушений стандартов или тому подобного. Это распределённые запросы с целью вызвать недоступность вашего веб-сервера. Банально – злоумышленник отправляет миллионы запросов по генерации главной страницы вашего сайта, и сервер просто не справляется. Это как реальное обрушение в Черную пятницу, только вызванное искусственно.

Методы предотвращения и защиты от DDoS-атак: Для защиты от таких атак существуют различные методы, которые можно разделить на две группы: сетевые и прикладные.

Сетевые методы защиты от DDoS-атак включают в себя использование специализированного оборудования, программного обеспечения или облачных сервисов, которые способны распознавать аномальный трафик и фильтровать его, пропуская только легитимные запросы. Они могут использовать различные технологии, такие как:

– балансировка нагрузки, когда трафик распределяется между несколькими серверами, увеличивая их производительность и устойчивость к атакам;

– георасределение, когда трафик направляется на ближайший к пользователю сервер, снижая задержку и риск перегрузки;

– анти-DDoS, когда трафик проходит через специальные устройства или сервисы, которые анализируют его и блокируют подозрительные пакеты или IP-адреса;

– VPN, когда трафик шифруется и передается через защищенное соединение, скрывая реальный IP-адрес сервера и уменьшая вероятность его блокировки.

Прикладные методы защиты от DDoS-атак включают в себя использование различных техник и инструментов, которые направлены на улучшение работы приложений и сервисов, уменьшение их уязвимости и повышение их безопасности. Они могут использовать различные подходы, такие как:

– кэширование, когда часто запрашиваемые данные хранятся в памяти или на диске, уменьшая нагрузку на сервер и ускоряя отдачу контента;

– сжатие, когда данные сжимаются перед передачей, уменьшая объем трафика и ускоряя загрузку страниц;

– минификация, когда удаляются лишние символы из кода, уменьшая его размер и ускоряя его обработку;

– обфускация, когда код делается трудночитаемым для человека, затрудняя его анализ и модификацию;

капча, когда запрашивается ввод специального кода или символа, подтверждающего, что запрос идет от человека, а не от бота.

Перечень использованной литературы и источников:

1. DDoS-атаки в 2022 и методы защиты от них [Электронный ресурс]. – URL: https://habr.com/ru/companies/slurm/articles/674218/ (дата обращения: 10.11.2023)

2. Как защититься от DDoS-атак: ТОП-10 способов [Электронный ресурс]. – URL: https://ddos-guard.net/ru/blog/sposoby-zashity-ot-ddos-atak (дата обращения: 10.11.2023)

3. Защита сервера от DDoS-атак [Электронный ресурс]. – URL: https://itelon.ru/blog/zashchita-servera-ot-ddos-atak/ (дата обращения: 10.11.2023).

УДК 004.032.26

НЕЙРОСЕТИ. ПРИНЦИПЫ ДЕЙСТВИЯ И ИХ НАЗНАЧЕНИЕ

Соломин Д.Д. Коробов Д.М.
студенты 1 курса, специальность «Информационные системы и программирование»
Райлян М.Н.
преподаватель высшей категории, преподаватель кафедры «Информационные технологии»

Аннотация: В данной статье дается определение нейросетей, рассматриваются принципы работы и области применения нейросетей.
Ключевые слова: Нейросети, принцип действия, искусственный интеллект, нейроны, обработка данных, алгоритмы, самообучение, прогнозирование.

Нейросеть – это тип компьютерной программы, которая имитирует работу человеческого мозга. Она состоит из множества узлов, называемых нейронами, которые соединены между собой. Нейросети способны обрабатывать большие объемы данных и находить в них закономерности, которые затем могут быть использованы для принятия решений.

Нейросети – это класс алгоритмов машинного обучения, вдохновленных структурой и принципами работы человеческого мозга и нервной системы. Они состоят из большого количества связанных между собой простых процессоров, называемых нейронами, и вместе способны выполнять сложные задачи по обработке данных.

Написание нейросетей может быть выполнено на разных языках программирования, включая «Python», «Java», «C++» и другие. «Python» является наиболее популярным языком для разработки нейросетей из-за наличия большого количества библиотек, таких как: «TensorFlow», «Keras» и «PyTorch».

Основным принципом действия нейросетей является обучение, которое происходит на большом объеме данных. В процессе обучения нейросеть выявляет закономерности в данных и учится предсказывать результаты на основе этих закономерностей. Обучение происходит путем изменения весов связей между нейронами таким образом, чтобы минимизировать ошибку в предсказаниях. Пример работы с нейросетью:

Запрос: “Создай мне изображение кота”.

В этом случае нейросеть «DeepArt» создаст новое изображение кота на основе существующих изображений.

Запрос: “Обнаружить мошенничество в этой транзакции”.

Здесь нейросеть SAS Anti-Fraud анализирует транзакцию и выдает вероятность того, что это мошенничество.

Трудности при работе с нейросетями могут быть связаны с необходимостью большого количества данных для обучения, а также с необходимостью настройки множества параметров.

Использование нейросетей может быть сложным и требует определенных знаний и навыков. Однако, благодаря их способности к обучению и обобщению данных, нейросети могут быть очень полезными инструментами для решения различных задач.

Сфера применения нейросетей очень широка. Они используются в распознавании образов, классификации, прогнозировании, обработке естественного языка и других задачах. Создание изображений с помощью нейросети:

1. **DeepArt** – программа, которая может создавать новые изображения на основе существующих. Она использует нейронную сеть для обработки изображений. «Artbreeder» – платформа, которая позволяет пользователям смешивать стили между двумя изображениями. Это достигается путем обработки изображений с использованием нейросети.

2. **Распознавание речи:** «Google Assistant» – использует нейросеть для распознавания речи и ответов на запросы.

3. **Обработка естественного языка (NLP):** BERT – это метод обучения для представления слов в контексте. Он используется для улучшения качества обработки текста. Генерация текста: GPT-2 – генеративная предварительно обученная трансформерная сеть, которая используется для генерации текста.

4. **Написание кода:** «GitHub Copilot» – инструмент, который помогает программистам писать код. Он использует нейросети для предложения вариантов кода.

5. **Самоуправляемые автомобили:** «Tesla Autopilot» – система, которая использует нейросети и машинное обучение для автономного вождения.

Преимущества нейросетей заключаются в их способности к обучению и обобщению данных, что делает их эффективными при работе с большими объемами информации. Кроме того, они способны обнаруживать сложные взаимосвязи в данных, которые могут быть незаметны для человека. Однако, у нейросетей есть и недостатки:

- во-первых – *они требуют больших вычислительных ресурсов для обучения и работы*;

- во-вторых – *интерпретация результатов работы нейросетей может быть затруднительной, поскольку они работают на основе сложных математических операций, которые трудно объяснить с точки зрения человеческого понимания*;

- в-третьих – *для того чтобы нейросеть работала хорошо, необходимо иметь большой объем качественных данных для обучения. Данные должны быть разнообразными и представлять все возможные ситуации, с которыми может столкнуться нейросеть.*

Несмотря на эти ограничения, нейросети продолжают развиваться и совершенствоваться, что делает их перспективным направлением в области искусственного интеллекта.

В целом, нейросети являются мощным инструментом для обработки и анализа данных, который находит широкое применение в различных сферах деятельности. Они постоянно развиваются и улучшаются, и можно ожидать, что в будущем их использование станет еще более распространенным и эффективным.

Перечень использованной литературы и источников:

1 Гафаров Ф.М Искусственные нейронные сети и приложения: учеб. пособие / Ф.М. Гафаров, А.Ф. Галимянов. – Казань: Изд-во Казан. ун-та, 2018. – 121 с.

2. Галушкин, А.И. Нейронные сети: история развития теории: Учебное пособие для вузов. / А.И. Галушкин, Я.З. Цыпкин. - Москва: Альянс, 2015. - 840 с

3. Ясницкий Л.Н. Поучительное прошлое, блестящее настоящее и сомнительное будущее искусственного интеллекта / Л.Н. Ясницкий. [Электронный ресурс] // Искусственный интеллект в решении актуальных социальных и экономических проблем XXI века: сб. ст. по материалам Третьей всерос. науч.-практ. конф. (г. Пермь, 14–18 мая 2018 г.) / Перм. гос. нац. исслед. ун-т. – Пермь, 2018. – С. 9-19. – URL: http://math.psu.ru/wp-content/uploads/Sbornik-statej-po-materialam-konferentsii-Iskusstvennyj-intellekt-v-reshenii-aktualnyh-sotsialnyh-i-ekonomicheskih-problem-XXI-veka-2018.pdf (дата обращения: 20.11.2023).

УДК 004.056

СЕТЕВАЯ БЕЗОПАСНОСТЬ. БЕСПЛАТНЫЕ СЕТИ WI-FI

Тимошкин С.А.
студент 4 курса, специальность «Программирование в компьютерных системах»
Райлян М.Н.
преподаватель кафедры «Информационные технологии»

Аннотация: В представленной статье автором поднимается тема безопасности использования Wi-Fi сетей, какими видами угроз может столкнуться пользователь, и как их избежать. Авторизации в бесплатных Wi-Fi сетях.

Ключевые слова: авторизация, информационная безопасность, бесплатный доступ, сетевая безопасность (СБ), хакинг, Wi-Fi.

В современном обществе информационная безопасность (ИБ) и как часть ее, безопасность сети имеет главное значение. В мире цифровизации общества в глобальном понимании вопрос безопасности информации и компьютерных сетей становиться наиболее остро и актуально. Сегодня для каждой узкогрупповой сети необходимо иметь точную политику в области безопасности. Предприятиям необходимо создавать безопасный доступ к своим информационным системам, для чего современная стратегия обеспечения сетевой безопасности должна учитывать ряд таких факторов, как увеличение надежности сети, эффективное управление безопасностью и защиту от постоянно эволюционирующих угроз и новых методов несанкционированного доступа и атак.

Сетевая безопасность – это набор действий, направленных на защиту работоспособности и целостности сети и данных. Она обеспечивает защиту от множества угроз и предотвращает их проникновение и распространение в сети.

С точки зрения ИБ, в беспроводных сетях получить доступ к информации проще, нежели в проводных сетях. Практически все точки доступа Wi-Fi на данный момент поддерживают последний стандарт безопасности WPA2. WPA2 -это мощные алгоритмы шифрования, надёжные механизмы целостности информации, но зачастую, общественные сети не имеют пароля для доступа к ней. Такие сети особо опасны, так как подключиться к ней и просматривать трафик может любой. Самой опасной угрозой является сниффинг трафика. Злоумышленник становится связующим звеном между пользователем и точкой доступа, то есть «встаёт посередине».

Рассмотрим жизненный пример. У меня есть друг, который увлекается компьютерными сетями, его балкон выходит на Площадь 60-летия Октября, и он сделал так, что бы Wi-Fi, который был у него в квартире, смог покрывать всю эту площадь. Целый год он раздавал бесплатный открытый Wi-Fi, через который можно было заходить на все сайты, потому что он, с помощью знакомого из Америки смог настроить собственный VPN. Спустя год ему написали сотрудники Роскомнадзора обращение о том, что он обязан установить пароль на сеть, ведь согласно Постановлений Правительства Российской Федерации № 758 от 31.07.2014 и № 2607 от 31.12.2021, запрещено размещать публичные открытые сети.

Вы наверняка так же взаимодействовали с этим законом, пытаясь подключиться к открытым Wi-Fi сетям. Когда человек подключается к публичному Wi-Fi без авторизации, его невозможно идентифицировать, поэтому злоумышленники могут воспользоваться анонимным доступом, чтобы рассылать спам, склонять к экстремизму и насилию, вести террористическую деятельность. Все эти действия противозаконны, поэтому важно их пресекать. Таким образом, необходимо либо ставить пароль на сеть, либо делать так, что бы пользователь был идентифицирован и подтверждал свою личность.

Авторизацию можно осуществлять тремя способами:

1. *По номеру телефона.* Гость попадает на страницу авторизации, указывает свой номер телефона и получает SMS с кодом. Этот код он указывает на странице, после чего может получить доступ в интернет. Другой метод – когда на оставленный гостем мобильный номер звонит робот. Отвечать на звонок не нужно, достаточно ввести четыре последние цифры входящего номера на странице авторизации.

2. *Логин и пароль от Госуслуг* (ЕСИА). Чтобы получить доступ в интернет, гостю нужно ввести логин и пароль от портала Госуслуг, после чего система пропустит его в сеть. Это надежный способ, который могут использовать в отделениях органов госвласти или МФЦ Бизнес часто рассматривает этот способ как альтернативу SMS. Но у некоторых пользователей нет аккаунта на Госуслугах, кто-то не хочет вводить важные данные в открытой сети. Поэтому часть клиентов не сможет воспользоваться Wi-Fi.

3. *Серия и номер паспорта*. Такой способ авторизации часто используют в гостиницах, где SMS или звонки не проходят из-за роуминга или запрета со стороны оператора. Для этого используют ваучеры. Гость передает администратору паспорт для заселения. Он вносит его данные в специальную систему, защищенную от утечки данных. Она генерирует логин и пароль. Пользователь вводит их на странице авторизации и получает доступ в интернет. Похожий алгоритм авторизации используют, например, в поездах «Ласточка».

Авторизация, при бесплатной сети может является двигателем бизнеса, например, страницу авторизации можно превратить в инструмент для продаж или рекламы своего бизнеса. Для этого необходимо настроить стартовую страницу портала авторизации: добавить дизайн бренда, рекламные баннеры и ролики, опросы, ссылку на сайт – любые данные, которые важно показать пользователю. Таким образом, для подключения к бесплатному интернету, клиенту придётся посмотреть рекламу. Статистика по подключениям сохраняется в личном кабинете на сайте оператора. Можно посчитать количество авторизаций в сети, время и продолжительность подключений.

Как много людей не знают про опасность бесплатных серей Wi-Fi? Прошлой зимой специалисты из Avast провели эксперимент над участниками Mobile World Congress. Они создали три открытые Wi-Fi точки возле стенда для регистрации посетителей выставки в аэропорту и назвали их стандартными именами «Starbucks», «MWC Free WiFi» и «Airport_Free_Wifi_AENA». За 4 часа к ним подключились 2000 человек. По итогам эксперимента был сделан доклад. Специалисты смогли проанализировать трафик всех этих людей и узнать, какие сайты они посещали. Также исследование позволило узнать личную информацию 63% участников: логины, пароли, адреса электронной почты и т.п. И жертвы никогда бы не узнали о том, что их данные попали в руки к кому-то еще, если бы эксперты из Avast не раскрыли свой секрет.

В чем конкретно проблема бесплатных сетей Wi-Fi?

1) Владелец Wi-Fi точки или человек, который получил к ней доступ может просматривать весь трафик, который проходит через неё. И с помощью анализатора пакетов данных (например, Wireshark или CommView) узнавать на какие страницы люди заходили с подключенных устройств и что вводили в формы на сайтах, которые используют протокол http. Это могут быть данные для входа, тексты писем, сообщения на форумах.

2) При подключении к Wi-Fi в общественном месте, то пользователя могут направлять на страницу для подтверждения своей личности по номеру телефона или авторизацию через социальные сети. Все введенные на этих страницах данные владелец точки может собирать для личного пользования. Также человек, у которого есть доступ к управлению роутером может настроить, например, перенаправление с facebook.com на сайт facebb00k.com, на котором будет размещена копия главной страницы популярной соцсети, созданная для воровства паролей.

3) Пользователя бесплатно сети, как и в случае рассмотренном выше, можно перекидывать не только на фишинговые сайты, но и на страницы для скачивания троянов и вирусов, которые могут похитить с компьютера множество ценной для мошенника информации (пароли, документы). Результат зависит от того, насколько жертва заботится о безопасности своего компьютера или мобильного телефона.

Как защитить себя при подключении к неизвестным Wi-Fi сетям?

- Использовать VPN для шифрования трафика.

- Использовать менеджеры паролей для защиты от ввода своих учетных данных на фишинговых сайтах.

- Везде, где это возможно, подключить подтверждение пароля по SMS или другие методы двухэтапной авторизации.

- Избегать скачивания подозрительных файлов, а так же использовать антивирус.

- Отключить на всех своих устройствах автоматическое подключение к Wi-Fi сетям.

Наиболее осторожным следует быть в аэропортах, на вокзалах и прочих местах скопления туристов. Но следует помнить о том, что «в руки хакеров» может попасть и роутер вашего соседа.

Перечень использованной литературы и источников:

1. Российская Федерация. Правительство Российской Федерации. Об утверждении Правил оказания телематических услуг связи: Постановление Правительства РФ от 31.12.2021 № 2607 // СПС «КонсультантПлюс».

2. Российская Федерация. Правительство Российской Федерации. О внесении изменений в некоторые акты правительства российской федерации в связи с принятием Федерального закона «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей: Постановление Правительства РФ от 31.07.2014 № 758 // СПС «КонсультантПлюс».

Благовещенский А., Кривошапко Ю. Почему бесплатный Wi-Fi может быть опасен / А. Благовещенский, Ю. Кривошапко // РГ: федеральный выпуск. – 2018. - № 182. [Электронный ресурс]. – URL: https://moluch.ru/archive/110/26798/ (Дата обращения: 20.11.2023).

Варлатая С.К. Анализ методов защиты беспроводной сети Wi-Fi от известных способов взлома злоумышленником / С.К. Варлатая, О.С. Рогова, Д. Р. Юрьев // Молодой ученый. – 2015. - № 1 (81). – С. 36-37. – URL: https://moluch.ru/archive/81/14770/ (Дата обращения: 21.11.2023).

Викулов А.В., Парамонов А.И. Введение в сети Wi-Fi с высокой плотностью пользователей / А.В. Викулов, А.И. Парамонов // Информационные технологии и телекоммуникации. – 2018. – Т. 6 - №1. – С. 12-20. [Электронный ресурс]. – URL: https://www.sut.ru/doci/nauka/review/20185/12-20.pdf (Дата обращения: 17.11.2023).

Рудниченко А.К. Аспекты безопасности использования общественной Wi-Fi сети / А.К. Рудниченко // Молодой ученый. – 2016. - № 6 (110). – С. 44-45. [Электронный ресурс]. – URL: https://moluch.ru/archive/110/26798/ (дата обращения: 20.11.2023).

5. [Электронный ресурс]. – URL: https://www.iphones.ru/iNotes/689126 (Дата обращения: 18.11.2023).

6. [Электронный ресурс]. – URL: https://moscow.b2b.dom.ru/blog/vidy-i-sposoby-avtorizacii-wi-fi (Дата обращения: 18.11.2023).

УДК 577.21

ИСПОЛЬЗОВАНИЕ ГЕННОЙ ИНЖЕНЕРИИ ДЛЯ ПРОИЗВОДСТВА ИНСУЛИНА

Шевченко А.С.
студент 1 курса, специальность «Информационные системы и программирование»
Юрова А.А.
преподаватель кафедры «Информационные технологии»

Аннотация: В статье рассматривается тема производства инсулина с помощью технологии рекомбинантных ДНК с использованием генно-инженерных штаммов E. Coli.

Ключевые слова: диабет, рекомбинантный инсулин, аминокислотную последовательность, E. Coli., биотехнология.

Инсулин – гормон, образующийся в клетках островков Лангерганса поджелудочной железы. Основная функция – стимулирование перехода глюкозы из крови в клетки, что вызывает снижение концентрации глюкозы, помимо этого данный гормон стимулирует синтез гликогена из глюкозы в мышцах и печени. При недостатке инсулина развивается заболевание сахарный диабет.

Сахарный диабет бывает двух типов. Сахарным диабетом 1 типа – (его еще называют инсулинзависимым) – официально больны свыше 3 млн. людей в нашей стране, «неофициально» – до 10 млн. Инсулинозависимый диабет наряду с сердечно-сосудистыми и онкологическими заболеваниями занимает одно из ведущих мест по медико-социальной значимости и приводит к ранней инвалидности и высокой

смертности. Диабет 2 типа – инсулиннезависимый включает легкие формы диабета. Диабетом этого типа чаще болеют тучные люди.

История открытия инсулина связана с именем русского врача И.М. Соболева (диссертация о патоморфологии поджелудочной железы), доказавшего, что уровень сахара в крови человека регулируется островками Лангерганса. В последствии гормон назвали «инсулин», от латинского – «insula», что в переводе тоже означает «островок».

Первым пациентом с диабетом, получившим препарат инсулина 11 января 1922г., стал 14-летний мальчик Леонард Томпсон. Гормон для первой инъекции был выделен из клеток поджелудочной железы собак.

В 1923 году за открытие инсулина была присуждена Нобелевская премия по физиологии или медицине, Д. Маклеоду и Ф. Бантингу

Инсулин вначале выделяли из поджелудочной железы свиней и крупного рогатого скота. Однако инсулин животных вызывает побочные негативные эффекты, которых не удается избежать даже при глубокой очистки биоматериала. В связи с этим возникла насущная необходимость синтезировать человеческий инсулин сначала в лабораторных условиях, а затем расширить до промышленных масштабов.

По своей природе инсулин – белок, состоящий из двух аминокислотных цепей (А- и В-цепи), соединенных дисульфидными мостиками.

В островковых клетках поджелудочной железы инсулин синтезируется в несколько этапов. На первом этапе происходит синтез молекулы предшественника инсулина – препроинсулина. На втором этапе от молекулы препроинсулина отделяется сигнальный пептид, после чего образуется проинсулин. После созревания происходит образование окончательной молекулы инсулина. На этапе созревания от молекулы проинсулина отделяется С-пептид, который не оказывает биологического действия. После отделения С-пептида формируется активная форма инсулина.

В 1979 году учёные из Национального медицинского центра Калифорнии синтезировали гены, кодирующие обе цепи инсулина. В дальнейшем синтетический ген внедряли в плазмиду в конце гена β-галактозидазы кишечной палочки (E. coli K 12). Полученный полипептиды отщепляли от фермента, очищали, образовавшиеся цепи соединяли в условиях invitro, что позволяло получить полноценную молекулу инсулина.

В клетках кишечной палочки проводился также биосинтез проинсулина, а не только её отдельных А- и В-цепей. С этой целью на матричной РНК проинсулина при использовании метода обратной транскриптазы преобразовывали её ДНК копию.

Образование молекул инсулина путём сворачивания проинсулина с целью создания дисульфидных связей имеет много преимуществ по сравнению с другими методами, поскольку различные этапы экстракции и выделения гормона сведены к минимуму.

В 1980 г. датская фармацевтическая компания «Novo» разработала метод превращения инсулина свиньи в инсулин человека ферментативным замещением аланина, последний является 30-й аминокислотой в цепи В, на остаток треонина с последующей хроматографической очисткой продукта, в результате был получен однокомпонентный инсулин человека 99% чистоты.

Достижения молекулярной биологии позволили установить, что биосинтез инсулина в b-клетках островковой ткани происходит по следующим основным этапам:

- закодированная информация о структуре гормона содержится в инсулиновом гене (участок ДНК) 11-й хромосомы;

- в результате стимулирующего действия, прежде всего глюкозы и некоторых других веществ, эта информация списывается РНК-полимеразой с инсулинового гена в виде мРНК на рибосомах, в которых осуществляется соединение аминокислот с образованием белков. На рибосомах происходит сборка полипептидной цепи из 109

аминокислот с образованием препроинсулина под влиянием рестриктаз, в результате образуются фрагменты от нескольких сотен до нескольких тысяч нуклеотидов;

- при синтезе препроинсулина в b-клетках поджелудочной железы первые 23 аминокислоты «проводят» молекулу через мембрану клетки. Эти аминокислоты отщепляются рестриктазами и образуется пептид проинсулин, состоящий из 86 аминокислот. Молекула проинсулина сворачивается таким образом, что начальный и конечный ее сегменты сближаются, а центральная часть молекулы удаляется под влиянием ферментов рестрикции; роль центральной части сводится к правильному взаимному расположению двух цепей инсулина.

Использование аффинной хроматографии значительно снизило содержание в препарате загрязняющих белков с более высокой м.м., чем у инсулина. К таким белкам относятся проинсулин и частично расщепленные проинсулины, которые способны индуцировать выработку антиинсулиновых антител. Стандартизация инсулина по загрязнению классифицирует препараты на обычные, содержащие проинсулина более 1%, монопиковые – менее 0,3%, улучшенные монопиковые – менее 0,005% и многокомпонентные, содержащие менее 0,001% проинсулина.

Компания «Eli Lilly» в массовом производстве человеческого инсулина использует технологию рекомбинантных ДНК, помещая кДНК гена человеческого проинсулина в E. coli или S. serevisae и гидролизуя наработанный проинсулин до молекулы инсулина. Человеческие инсулины этой фирмы носят название «Хумулин». В медицинской практике используют рекомбинантные человеческие инсулины из серии Хумулин – регулярный, ленте, ультраленте и их комбинированные составы. Человеческий инсулин быстрее абсорбируется и независимо от формы препарата имеет более короткую длительность действия, чем животные инсулины. Человеческие инсулины менее иммуногены, чем свиные, особенно смешанные бычьи и свиные инсулины.

В молекуле инсулина обнаружены области, играющие повышенную роль в его физико-химических и биологических свойствах. При внесении мутационных изменений в аминокислотную последовательность этих областей, существенным образом изменяются свойства молекулы в целом. Удалось получить аналоги с модификацией В-цепи, что привело к значительному увеличению гормональной активности по сравнению с природным инсулином.

Контроль качества генноинженерного инсулина предполагает контроль дополнительных показателей, характеризующих стабильность рекомбинантного штамма и плазмиды, отсутствие постороннего генетического материала в препарате, идентичность экспрессируемого гена и др. (всего 22 показателя).

В Великобритании с помощью E. coli синтезированы обе цепи человеческого инсулина, которые затем были соединены в молекулу биологически активного гормона. Чтобы одноклеточный организм мог синтезировать на своих рибосомах молекулы инсулина, необходимо снабдить его нужной программой, т. е. ввести ему ген гормона. Химическим способом (операцию проводят специалисты биохимики) получают ген, программирующий биосинтез предшественника инсулина или два гена, программирующие в отдельности биосинтез цепей А и В инсулина. Следующий этап – включение гена предшественника инсулина (или гены цепей инсулина порознь) в геном E. coli – особого штамма кишечной палочки, выращенного в лабораторных условиях; эту задачу выполняет генная инженерия. Из E. coli вычленяют плазмиду соответствующей рестриктазой. Синтетический ген встраивается в плазмиду (клонированием с функциональной активной С-концевой частью b-галактозидазы E. coli). В результате E. coli приобретает способность синтезировать белковую цепь, состоящую из галактозидазы и инсулина. Синтезированные полипептиды отщепляют от фермента химическим путем, затем проводят их очистку. В бактериях синтезируется около 100000 молекул инсулина на бактериальную клетку

Природа гормонального вещества, продуцируемого E. coli, обусловлена тем, какой ген встраивается в геном одноклеточного организма. Если клонирован ген предшественника инсулина, бактерия синтезирует предшественник инсулина, который подвергается затем обработке рестриктазами для отщепления препептида с вычленением С-пептида, вследствие чего получается биологически активный инсулин. Для получения очищенного инсулина человека выделенный из биомассы гибридный белок подвергают химико-ферментативной трансформации и соответствующей хроматографической очистке (фронтальной, гель-проникающей, анионообменной).

В Институте биоорганической химии РАН получен рекомбинантный инсулин с использованием генно-инженерных штаммов E. coli. Из выращенной биомассы выделяется предшественник, гибридный белок, экспрессируемый в количестве 40 % от всего клеточного белка, содержащий препроинсулин. Превращение его в инсулин in vitro осуществляется в той же последовательности, что и in vivo – отщепляется лидирующий полипептид, препроинсулин превращается в инсулин через стадии окислительного сульфитолиза с последующим восстановительным замыканием трех дисульфидных связей и ферментативным вычленением связывающего С-пептида. После ряда хроматографических очисток, включающих ионообменные, гелевые и ВЭЖХ, получают человеческий инсулин высокой частоты и природной активности.

Производство инсулина совершило переворот, как в эндокринологии, так и медицине в целом. Это знаменательное событие подарило миллионам больных сахарным диабетом не только саму возможность жить, но и надежду на то, чтобы жизнь с этим заболеванием была полноценной.

Перечень использованной литературы и источников:

1. Биотехнология: Учебное пособие для ВУЗов в 8-ми книгах / Под ред. Н.С. Егорова, В.Д. Самуилова. – Москва: Высшая школа, 1987. – С. 15-25.

2. Генно-инженерный инсулин человека. Повышение эффективности хроматографического разделения при использовании принципа бифункциональности / Романчиков А.Б., Якимов С.А., Клюшниченко В.Е., Арутунян А.М., Вульфсон А.Н. // Биоорганическая химия. – 1997. Том 23. - № 2. – С. 98-103. [Электронный ресурс]. – URL: https://naukarus.com/genno-inzhenernyy-insulin-cheloveka-vii-povyshenie-effektivnosti-hromatograficheskogo-razdeleniya-pri-ispolzovanii-prints (дата обращения: 18.10.2023).

3. Глик Б., Пастернак Дж. Молекулярная биотехнология. Принципы и применение / Глик Б.; Пастернак Дж; Перевод с английского канд. мед. наук Н.В. Баскаковой, О.А. Колесниковой, д-ра биол. наук Ю.М. Романовой, М. А. Серовой, канд. мед. наук А.Л. Чухровой под редакцией д-ра биол. наук Н.К. Янковского. – Москва: Мир, 2002. – 589с.

4. Егоров Н.С., Самуилов В.Д. Современные методы создания промышленных штаммов микроорганизмов: Биотехнология. Кн. 2 / В.Г. Дебабов, В.А. Лившиц; ред.: Н.С. Егоров, В.Д. Самуилов. – Москва: Высшая школа, 1988. – 208 с.

УДК 004.43

БЕЛЫЕ ХАКЕРЫ

Штельма М.Н.
студент 1 курса, специальности «Информационные системы и программирование»
Иванова А.В.
преподаватель кафедры «Информационные технологии»

Аннотация: В данной статье поднимается тема: Кто такие белые хакеры? Чем они занимаются?

Ключевые слова: хакер, белые хакеры, пентестер, Bug Bounty.

Проблемы информационной безопасности (ИБ) были и остаются источником головной боли для специалистов по данному направлению. Интересная статистика: каждые 39 секунд происходит хакерская атака. Ежедневно злоумышленники создают более 300 000 вредоносных программ. Самые быстрые в мире – русские хакеры. Им нужно всего 18 минут, чтобы проникнуть в компьютерную сеть. Для сравнения: хакерам из Северной Кореи нужно для этого 2,5 часа, а китайцам – 4 часа. [1]

Кто же такие хакеры? Изначально хакерами (от англ. to hack – колоть, отёсывать) называли специалистов, способных быстро и необычным способом исправить ошибку в компьютерной программе. С конца 20 века термин стал обозначать взломщика компьютерных систем. В наше время различают: «белых», «серых» и «чёрных» хакеров, в зависимости от законности их действий [2].

Методы у хакеров похожи – но цели могут быть диаметрально противоположные. Исходя из целей и степени скрытности/открытости деятельности выделяют 3 основные группы хакеров: «белые», «черные» и «серы».

«Белые хакеры» (White Hat), или пентестеры работают в области информационной безопасности. Они действуют легально и с согласия владельцев систем, которые проверяют. «Белые хакеры» (БХ) ищут уязвимости в системах и помогают закрыть их, предупреждая владельцев о возможных проблемах. Их цель – обеспечить безопасность и защитить данные. [1]

«Чёрные хакеры» (Black Hat) – это злоумышленники, которые занимаются незаконными действиями и проникновением в компьютерные системы с целью получения незаконной выгоды. Они могут воровать личные данные, финансовую информацию, вредить системам или использовать их в криминальных целях. Деятельность чёрных хакеров незаконна. [1]

«Серые хакеры» (Grey Hat) – находятся между белыми и чёрными хакерами. Они, как правило, имеют хорошие навыки в области информационной безопасности, но могут выполнять незаконные действия без согласия владельца системы с целью исследования и предупреждения об уязвимостях. В отличие от чёрных хакеров, серые хакеры обычно не манипулируют или воруют данные для личной выгоды, но их деятельность все равно нарушает закон и может нанести вред владельцам системы. [1]

Ответим на вопрос. Кто такие «белые хакеры»?

БХ (также известны как Пентестеры (penetration test) – это метод тестирования безопасности и анализа информационной системы на наличие уязвимостей. Пентестер моделирует атаки злоумышленников и пытается проникнуть в систему с позиции потенциального атакующего. Этот подход позволяет оценить уровень безопасности системы и выявить уязвимости, которые могут использовать злоумышленники для несанкционированного доступа к данным или ресурсам.) являются неотъемлемой частью современного кибербезопасного сообщества. Они играют важную роль в обеспечении безопасности компьютерных систем и защите от кибератак. Пентестеры используют свои знания и опыт, чтобы проникнуть в системы и сети, но их цель отличается от целей хакеров. Белые хакеры стремятся обнаружить и устранить уязвимости, чтобы предотвратить потенциальные атаки, в то время как хакеры используют эти уязвимости для незаконного доступа и посягательства на чужие данные.

Хорошая возможность заработка для хакеров – это баг-баунти. Bug Bounty (вознаграждение за нахождение ошибок) – это программа, предлагаемая организациями-разработчиками программного обеспечения, которая позволяет хакерам и исследователям безопасности находить уязвимости в их ПО, веб- и мобильных приложениях и других системах [3].

В рамках Bug Bounty программы организация устанавливает правила и политику, согласно которым хакеры могут тестировать безопасность системы. Если пентестер находит уязвимость и сообщает об этом организации, последняя вознаграждает его за найденный баг. Суммы вознаграждений при этом могут быть впечатляющими.

Захват флага (Capture The Flag) – это форма соревнования или тренировки в области компьютерной безопасности, которая позволяет участникам решать различные задачи с целью найти и захватить «флаг». В соревновательной форме CTF участники могут состязаться в команде или индивидуально. Участники должны использовать свои

знания и навыки в области компьютерной безопасности, чтобы найти и использовать уязвимости в программе для получения флагов и получения очков.

В зависимости от формата CTF, участники могут использовать разные подходы для захвата флагов [1, 3]:

- в соревнованиях в стиле Анализ рисков «Jeopardy» или Решение задач «Task-Based» участники решают различные задачи, такие как криптография, эксплойты, веб-уязвимости и другие, чтобы найти флаги и получить очки;

- в соревнованиях в стиле атаки/защиты «Attack-Defense», команды должны оборонять свои системы от атак других участников и одновременно атаковать системы других команд;

- в соревнованиях в смешанном стиле «Mixed» совмещаются задачи из двух предыдущих стилей;

- в соревнованиях в стиле Царь Горы «King of the Hill» основная цель заключается во взломе системы, закреплении в ней и удержании последней от захвата соперниками.

В заключении хочется отметить, что бы быть белым хакером требует постоянного самообразования и стремления к совершенству. Но работа белого хакера не только технически сложна, но и предоставляет массу возможностей для развития и роста в IT-индустрии.

Перечень использованной литературы и источников:

1. Электронный ресурс. – URL: https://digital-academy.ru/blog/white-hat-hacker

2. Нечкин В.Н., Михайлов Р.Д. Хакеры в современном мире [Электронный ресурс] / В.Н. Нечкин, Р.Д. Михайлов // Инновационные технологии в образовании, науке и бизнесе: материалы Всероссийской научно-практической конференции с международным участие (5 июля 2019г., г. Улан-Удэ). – Улан-Удэ: изд-во БГУ, 2019. – С. 92-96. – URL: https://www.bsu.ru/university/publisher/publication/publications/?id=50.

3. Лапонина О.Р., Матошенко В.А. Сравнительный анализ CTF-платформ для обучения кибербезопасности // International Journal of Open Information Technologies. – 2022. Том 10, № 4. - С.31-44.

УДК 53

ВЫДАЮЩИЕСЯ ФИЗИКИ РОССИИ И ИХ ДОСТИЖЕНИЯ

Шутко В.И.
студентка 1 курса, специальность «Информационные системы и программирование»
Стерлигова И.И.
преподаватель высшей категории
преподаватель кафедры «Информационные технологии»

Аннотация: Все мы много слышали о них еще в школе. Благодаря блестящим умам величайших физиков мира, человечество имеет телефон, электрический свет, понимание законов Вселенной. Мы изучали их теории и принципы, изобретения и открытия, их успехи и достижения по текстам параграфов в учебниках. Но гениальные физики – тоже люди, со своими особенностями и причудами.

Ключевые слова: наука, российские физики, достижения.

Российская наука не только одна из самых великих в мире, она еще является кузницей кадров для других стран. Русские учёные отодвинули завесу непознанного, внеся свою лепту в эволюцию научной мысли во всем мире. Наши земляки сотрудничали со многими выдающимися научными умами. Открытия русских учёных стали катализатором развития технологии и знания во всем мире, а многие революционные идеи и открытия в мире создавались на фундаменте научных достижений известных русских учёных.

С каждым новым днём, происходят новые открытия в разных областях. Для России развитие науки очень важно, поэтому 8 февраля отмечают день российской науки. Этот праздник приурочен к дате основания Российской академии наук,

учреждённой по повелению императора Петра I указом правительствующего Сената от 28 января (8 февраля по новому стилю) 1724 года.

Если бы не величайшие умы человечества, мы все еще жили бы в Средневековье. Всё, чем мы пользуемся, включая автомобили, электричество, здравоохранение и науку – результат изобретений и открытий разных учёных.

Выдающимися отечественными учеными, внесшими большой вклад в развитие физики являются Ломоносов Михаил Васильевич, Кулибин Иван Петрович, Королев Сергей Павлович, Ленц Эмилий Христианович, Попов Александр Степанович.

Ломоносов Михаил Васильевич (1711–1765) – великий русский ученый, химик, физик, художник, историк, поэт и писатель, труды которого стали известны во всем мире. Прославился в таких областях знаний, как: астрономия, геология, приборостроение, география и многие другие. Биография Ломоносова знаменательна открытием закона сохранения материи, написанием работ по теории цвета, построением множества оптических приборов. Одним из выдающихся естественнонаучных достижений М.В. Ломоносова является его молекулярно-кинетическая теория тепла.

Родился Михаил Васильевич в небольшой деревне в Архангельской губернии, где в его родителей не было возможности дать ему хорошее образование. Но страсть к знаниям и жажда учиться побуждали Ломоносова искать возможности для получения образования. И вот, стараясь найти путь к знаниям, Ломоносов отправился в путь, чтобы достичь центра образования — Москвы. Путь в Москву был долгим и не очень простым для молодого Ломоносова. Дорога занимала несколько недель, и пешком, пересекая реки, леса и болота, Михаил добирался до Москвы. Однако эти трудности не поколебали его решительности и желания получить образование. Через множество испытаний и преград, Ломоносов достиг Москвы и зарекомендовал себя как один из величайших умов своего времени.

Кулибин Иван Петрович (1735–1818) – выдающийся русский механико-изобретатель и инженер. Создатель новых мостовых конструкций, разработал несколько проектов 298-метрового одноарочного моста через Неву и тем самым доказал возможность моделирования мостовых конструкций. За годы жизни он изобрел множество оригинальных механизмов: фонарь-прожектор, систему зеркал для освещения темных переходов Царскосельского дворца, прототипы современных автомобиля и велосипеда, ножной протез, лифт и многое другое. Он основоположник отечественной технологии производства оптического стекла. За свои уникальные изобретения был прозван «нижегородским Архимедом». Он руководил изготовлением навигационных, астрономических и физических инструментов и приборов.

Великий изобретатель был самоучкой: он никогда не учился в школе и осваивал механику самостоятельно. В его комнате были собраны все имеющиеся на тот момент приспособления для токарных, слесарных и прочих работ.

Королёв Сергей Павлович (30 декабря 1906 – 14 января 1966) – советский учёный, инженер-конструктор, академик АН СССР. Генеральный конструктор ракетно-космической промышленности СССР. Сергей Королёв является создателем советской ракетно-космической техники, ключевой фигурой в освоении человеком космоса, создателем практической космонавтики. По его инициативе и под его руководством был осуществлён запуск первого искусственного спутника Земли и первого космонавта планеты Юрия Гагарина.

Он мечтал об освоении космоса с юношеских лет, постоянно совершенствовался и предъявлял высокие требования не только к тем людям, с которыми ему доводилось работать, но и к самому себе, трудился, не щадя собственного здоровья. Он мог погибнуть в лагерях, но остался жив, перенёс жесточайшие допросы и стал лучшим в своём деле.

Ленц Эмилий Христианович (12 февраля 1804 – 29 января 1865) – русский физик немецкого происхождения. Ленц является одним из основоположников электротехники. Открыл закон, определяющего тепловое действие тока, закон, определяющий направление индукционного тока, профессор и ректор Императорского Санкт-Петербургского университета (1863–1865), академик. Многие его научные исследования относятся к физической географии, например, об измерении магнитного наклонения и напряженности земного магнетизма.

Попов Александр Степанович (4 марта 1859 – 31 декабря 1905) – русский физик и электротехник, профессор, изобретатель, статский советник, Почётный инженер-электрик (1899). Изобретатель радио. В 1889-98 годах всё своё свободное время Попов посвящает физическим опытам, главным образом, изучению электромагнитных колебаний. 7 мая 1895 года А. С. Попов продемонстрировал возможность передачи и приема коротких и продолжительных сигналов на расстояние до 64 м посредством электромагнитных волн. 25 марта 1896 г. провёл опыты с радиотелеграфией, соединив свой аппарат с телеграфом и послав на расстояние 250 м радиограмму из двух слов: «Генрих Герц».

Перечень используемой литературы и источников:

1. Мухин К.Н. Российская физика Нобелевского уровня / К.Н. Мухин, А.Ф. Суставов, В.Н. Тихонов. – 2-е изд., перераб. и доп. – Москва: Физматлит, 2011. – 238 с.
2. Россияне - лауреаты Нобелевской премии = Russians - Nobel prize winners: биогр. справ. (1901-2001) / Ассоц. юрид. центр, Рос. акад. естеств. наук; авт.-сост. И.М. Авраменко. – СПб.: Юрид. центр Пресс, 2003. – 137 с.

Научно-информационное издание

НАУКА – ЭТО ИНТЕРЕСНО!

сборник материалов межкафедральных студенческих научных семинаров и конференций (ноябрь-декабрь 2023г.)

Подписано в печать 19.12.2023г.
Сдано в печать 20.12.2023г.
Бумага для множительных аппаратов.
Формат 60х84/16. Тираж 8 экз. Усл. печ. л. 2,0

Группа НИРиДО УМО
Редакционно-издательская группа
Хабаровский институт инфокоммуникай (филиал) ФГОБУ ВО
«Сибирский государственный университет
коммуникаций и информатики»
ХИИК СибГУТИ
680000, г. Хабаровск, ул. Ленина 73.