ТОЧНАЯ НАУКА

естественнонаучный журнал

LVIII Международная научная конференция
"Техноконгресс"

Сборник статей международной естественнонаучной конференции с публикацией в НЭБ elibrary.ru

t-nauka.ru

Кемерово 2020

СБОРНИК СТАТЕЙ ПЯТЬДЕСЯТ ВОСЬМОЙ МЕЖДУНАРОДНОЙ НАУЧНОЙ КОНФЕРЕНЦИИ «ТЕХНОКОНГРЕСС»

10 августа 2020 г.

ББК Ч 214(2Рос-4Ке)73я431

ISBN 978-5-6040934-2-9

Кемерово УДК 378.001. Сборник статей студентов, аспирантов и профессорско-преподавательского состава. По результатам LVIII Международной научной конференции «Техноконгресс», 10 августа 2020 г. www.idpluton.ru / Редкол.:

Кемерово 2020

В сборнике представлены материалы докладов по результатам научной конференции.

Цель – привлечение студентов к научной деятельности, формирование навыков выполнения научно-исследовательских работ, развитие инициативы в учебе и будущей деятельности в условиях рыночной экономики.

Для студентов, молодых ученых и преподавателей вузов.

Издательский дом «Плутон» www.idpluton.ru e-mail: admin@idpluton.ru

Подписано в печать 10.08.2020 г. Формат 14,8×21 1/4. | Усл. печ. л. 3.2. | Тираж 300.

Оглавление

1. ЭЛЕКТРОННАЯ ВАЛЮТА ЗАМЕНИТ БУМАЖНЫЕ ДЕНЬГИ 3
Рамзин В.А.
2. РАЗРАБОТКА СИНТЕЗАТОРА РЕЧИ ДЛЯ ЛЮДЕЙ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ……..…….....6
Рамзин В.А., Лобзова А.И.
3. ЗАЩИТА БОЛЬШИХ ДАННЫХ НА МОРСКОМ ТРАНСПОРТЕ 10
Донкан К.М., Дудоладова П.Г.
4. РАЗРАБОТКА ПОЛИТИК БЕЗОПАСНОСТИ ДЛЯ ЗАЩИТЫ КОРПОРАТИВНЫХ АКТИВОВ 12
Донкан К.М., Дудоладова П.Г.
5. АКТУАЛЬНЫЕ КОНЦЕПЦИИ НАУЧНОГО ЗНАНИЯ В АРХИТЕКТУРЕ 17
Антонова В.В.

Рамзин Вячеслав Алексеевич
Ramzin Vyacheslav Alekseyevich
Студент Пензенского государственного университета

УДК 004

ЭЛЕКТРОННАЯ ВАЛЮТА ЗАМЕНИТ БУМАЖНЫЕ ДЕНЬГИ

ELECTRONIC CURRENCY TO REPLACE PAPER MONEY

Аннотация: в статье описана история появления электронных денег и обзор систем для транзакции через интернет.

Abstract: The article describes the history of the emergence of electronic money and an overview of systems for transactions via the Internet.

Ключевые слова: электронные деньги, электронный кошелек, онлайн платеж, транзакция, валюта.

Keyword: electronic money, e-wallet, online payment, transaction, currency.

В наш век стремительно развивающихся информационных технологий, многие вещи изменились, улучшились и приобрели новые качества. Это коснулось и денег. Теперь люди могут оплачивать покупки, счета за интернет, телефон и даже пиццу, просто пару раз щелкнув своей мышкой.

Итак, для начала немного истории. Когда-то людям был доступен только наличный расчет и тяжелые монеты. Со временем появились бумажные листки с водяными знаками, которые поначалу являлись всего лишь обязательством, по которому следовало расплачиваться монетами или драгоценностями. Позднее банкноты сами по себе стали средством платежа, у них было явное преимущество в весе и удобстве использования.

Еще позже, деньги стали храниться в банках, был придуман безналичный расчет, банковские счета и пластиковые карточки. Теперь можно было носить с собой лишь небольшой пластиковый прямоугольник и при этом распоряжаться большой суммой денег. В наши же дни, было разработано специальное программное обеспечение, работающее через интернет, для использования денег в электронном виде, позволяющее их хранить в электронных кошельках, быстро переводить (в отличие от банковского перевода, электронный перевод, осуществляется за одну секунду), а также производить различные финансовые операции.

Электронные деньги появились сравнительно недавно, лишь в 1993 году.

Пока они являются лишь обязательством плательщика и требуют перевода в одну из привычных денежных форм. Но оглядываясь на историю о банкнотах, можно смело предположить, что электронные деньги в недалеком будущем станут одной из форм традиционного расчета, таких как монеты, банкноты и различные виды безналичных денег.

Использовать электронную валюту можно в любой точке мира, где есть интернет. Расчеты через электронные платежные системы используют интернет-магазины, операторы сотовой связи, интернет-провайдеры, продавцы PIN-кодов, телефонные компании и т. д. Электронная платежная система действует при помощи различных платежных устройств, таких как платежные карты, электронные кошельки, банкоматы и терминалы. В последнее время появились устройства со встроенными микросхемами, например, мобильные телефоны, брелки, браслеты и другие подобные вещи, с помощью которых также можно обращаться с электронными деньгами.

Для того, чтобы перевести реальные деньги в электронные, используется прямое зачисление или же зачисление с помощью карты. Во втором случае у дилеров приобретается специальная карта с определенным номиналом и после ее активации, данная сумма появляется в вашем электронном кошельке.

Сегодня, практически, в каждом государстве есть ряд учреждений, в которых можно обналичивать электронные деньги. В этом случае средства с вашего кошелька перечисляются на

электронный кошелек дилера, а затем их можно вывести. А в некоторых платежных системах можно переводить электронные деньги, даже на банковские счета.

Все электронные платежные системы делятся на два вида.

Для использования одних, требуется установка на компьютер пользователя специальной программы, другие используются при помощи веб-интерфейса.

Сейчас в мире, где электронные деньги завоевывают все большую популярность, фактически любой пользователь может открыть электронный счет. Однако, выбрать он может всего один из типов: анонимный и персонифицированный. Анонимная система, при которой не требуется идентификации, похожа на оплату наличными деньгами, когда у покупателя не спрашивают его имя и адрес. Персонифицированную, или не анонимную систему, при которой идентификация необходима, можно сравнить с безналичными расчетами, где нужно указывать свои данные. В основном, регуляторы платежных систем стараются стимулировать пользователей больше использовать персонифицированную систему. Например, ограничивают лимит анонимов, при этом поощряя персонифицированных пользователей.

Если электронные деньги выражены в одной из государственных валют, с ними производятся расчеты согласно законодательству данного государства, такие деньги называются фиатными электронными деньгами. Существуют также, нефиатные электронные деньги, это денежные единицы, которые существуют вне государственных платежных систем. Обмен нефиатных денег на фиатные, их обналичивание и обращение, соответственно регулируются негосударственными платежными системами и различаются в разных странах.

Преимущества электронных денег:

- Расчеты производятся очень быстро, поэтому на лицо экономия времени;

- Не нужно стоять в очередях, соответственно экономия не только времени, но и нервов; - Не нужно выдавать сдачу, что избавляет от необходимости искать разменную купюру или терять время на ее, пересчитывание;

- Величина суммы не влияет на вес, как в случае с наличными деньгами, значит не нужно тратить сил для перетаскивания тяжелых мешков (в случае, если денег много);

- Экономия средств на производстве денег. Не нужно чеканить монеты, печатать банкноты, затрачивать материалы и использовать труд людей на их изготовление;

- Не нужно физически отсчитывать и пересчитывать деньги;

- Не нужно их упаковывать, перевозить в специальные помещения для их хранения и производить с ними другие физические операции;

- Момент платежа фиксируется электронными системами, что позволяет вам точно знать когда и сколько вы потратили;

- Сохраняемость. Электронные деньги не портятся с годами, не износятся и не меняют свой внешний вид; Однородность.

- Зависимость от наличия доступа в интернет и устройства, на котором можно будет запустить программу или браузер, для доступа в кошелек;

- Можно отслеживать персональные данные плательщиков, что может сыграть на руку посторонним заинтересованным лицам;

- Не смотря на высокую степень защиты электронных денег, хакеры и подобные мошенники постоянно разрабатывают новые способы взлома, поэтому теоретически возможны незаконные операции и хищения денежных средств; Поскольку электронные деньги появились сравнительно недавно, еще не устоялись надежные способы их защиты и управления ими. Вот такие, плюсы и минусы. Они дают некоторое представление о надежности интернет денег.

WebMoney Transfer. Крупнейшая и основная платежная система в рунете, существующая с 1998 года. Для того, чтобы зарегистрироваться в системе, необходимо установить на свой компьютер (или другое электронное устройство) программу WM Keeper, получив при этом свой идентификационный номер. С помощью этой платежной системы вы сможете: оплачивать товары, сотовую связь, интернет, конвертировать WebMoney на другие электронные валюты. Также система позволяет использовать мобильный телефон в качестве кошелька. Система работает с различными валютами - долларами, евро, а также с некоторыми валютами стран СНГ.

Яндекс Деньги. Чтобы открыть счет, достаточно пройти простую регистрацию в системе.

Благодаря ей, вы сможете покупать, продавать и обменивать электронные валюты, производить переводы между счетами пользователей, оплачивать различные виды услуг, принимать

платежи. Пополнить свой счет в системе можно с помощью карты Яндекс. Деньги, наличным переводом в банках, в почтовых отделениях России, с помощью платежных терминалов, через банкоматы Росбанка. К сожалению Яндекс. Деньги оперирует только рублями.

PayPal. Крупнейшая в мире платежная система, действующая во многих странах мира. Всемирно известный аукцион ebay, работает исключительно с этой системой электронных платежей.

Библиографический список:

1. С. А. Белозеров «Электронные формы денег и новые виды платёжных систем» — Известия СПбГУЭФ

2. Пункт 18 статьи 3 Федерального закона Российской Федерации № 161-ФЗ г. «О национальной платёжной системе» от 27 июня 2011 года

3. «Государственные криптовалюты на подходе» - https://bits.media/gosudarstvennye-kriptovalyuty-na-podkhode/. Дата обращения: 15 июня 2020 г.

Рамзин Вячеслав Алексеевич
Ramzin Vyacheslav Alekseyevich
Студент Пензенского государственного университета

Лобзова Анастасия Игоревна
Lobzova Anastasiya Igorevna
Студент Пензенского государственного университета

УДК 681.51

РАЗРАБОТКА СИНТЕЗАТОРА РЕЧИ ДЛЯ ЛЮДЕЙ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ

DEVELOPMENT OF SPEECH SYNTHESIZER FOR PEOPLE WITH DISABILITIES

Аннотация: Статья посвящена разработке синтезаторов речи для людей с ограниченными возможностями. Проводится анализ синтезаторов речи, приводятся их преимущества, недостатки и основные особенности. На основе проведенного исследования выявлены условия эффективного использования синтезаторов речи для лиц с ограниченными возможностями.

Abstract: The article is devoted to the development of speech synthesizers for people with disabilities. The analysis of speech synthesizers is carried out, their advantages, disadvantages and main features are given. On the basis of the study, the conditions for the effective use of speech synthesizers for persons with disabilities have been identified.

Ключевые слова: синтезатор речи, озвучивание текста, люди с ограниченными возможностями здоровья

Keywords: speech synthesizer, text scoring, people with disabilities

В настоящее время в мире существует огромное количество людей с ограниченными возможностями, и у большинства из них часто возникают проблемы с адаптацией в социуме.

Помочь им призваны определенные информационные технологии, в частности, синтезаторы речи, которые позволяют людям, имеющим проблемы со зрением обращаться с электронными устройствами, понимать и находить необходимую текстовую информацию, а лицам с нарушением речевого аппарата помогают общаться и сообщать окружающим о своих мыслях и потребностях.

Среди наиболее популярных программных разработок, помогающих людям с проблемами зрения, можно указать такие аллофонные синтезаторы речи, как Ivona2, Volcalizer. ESpeak, и Acapela Group. Данные синтезаторы зависимы от позиции и фонетического окружения с современным интерфейсом SAPI5.

Ivona2 – синтезатор речи, который позволяет сохранять текст в аудиофайл. Программа является платной [5]. Озвучивание происходит только на русском языке с помощью KMPlayer. Может читать многие форматы текстовых файлов. Подходит для устройств с Windows [8]. В программе иногда возникают проблемы с ударением.

Volcalizer – представляет собой голосовой движок от компании Nuance. Для его работы необходима установка дополнительных драйверов типа синтезаторов Nuance Vocalizer Expressive [12]. Позволяет выбрать различные параметры озвучивания текста, имеет в своем арсенале 42 языка и использует минималистичный стиль. Синтезатор является условно бесплатным, поскольку голоса для него покупаются отдельно. Подходит для устройств с Windows [13].

ESpeak – довольно компактный синтезатор речи, имеющий простую установку. Выпущен в 2006 году и обновлялся вплоть до 2013 года [3]. Подходит для устройств с Windows, Linux, MacOSx, и RISCOS. Программа есть и для мобильных устройств, однако она имеет значительные проблемы с русскими словарями. Доступно 4 голоса для чтения. Позволяет с сохранять текст в аудиофайл формата WAV [7]. Относительно недорогое приложение.

Acapela Group – синтезатор экранного доступа Nvda, который был разработан в 2008 году для устройств с системой Windows [6]. Имеет две версии в виде сайта с онлайн доступом и приложения. Имеет доступ к 30 языкам и большое количество голосов для озвучивания [4]. Имеется возможность изменять громкость и скорость воспроизведения, что, однако может привести к искажению слов.

Наиболее распространенными синтезаторами речи для людей с нарушением речи в России

считаются: Sakrament, Speaking Mouse и Digalo. Кроме того, существует обновленная версия русской программы Горыныч, фундаментом которой выступают российские разработки в сфере распознавания устной речи. Данный синтезатор довольно удобен и прост в использовании, и служит для вывода надиктовываемого текста и управления отдельными функциями ОС Windows [2]. Кроме русской распознает английскую речь.

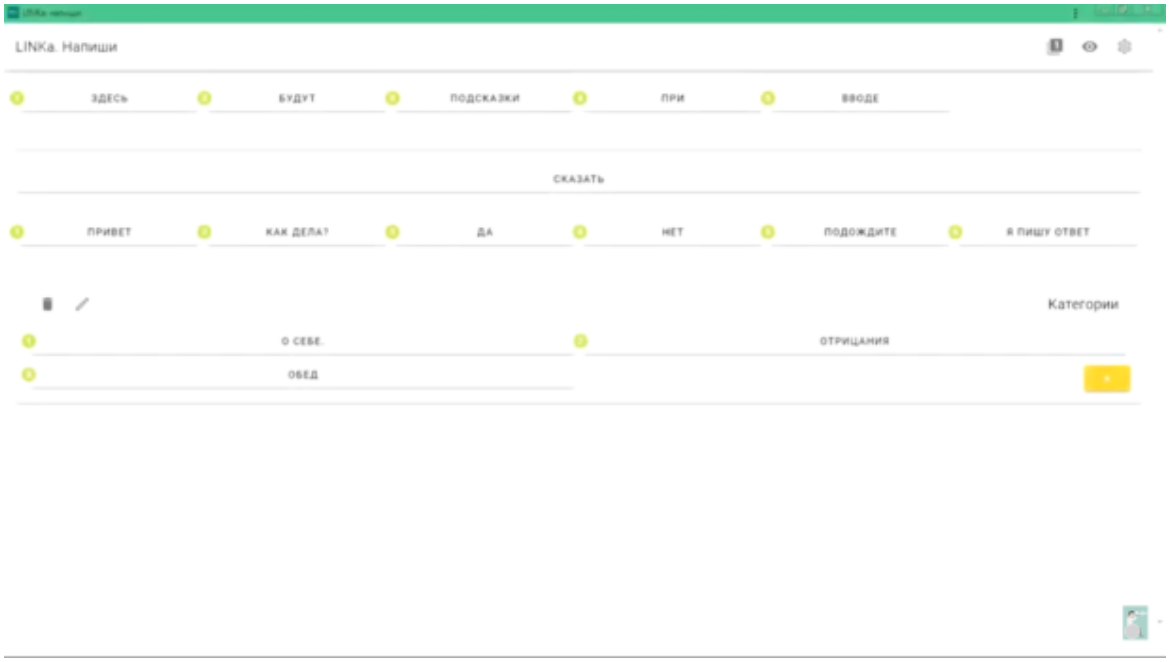
Интерфейс Горыныча имеет следующий вид:

Одной из известнейших разработок синтезатора речи последнего времени в России является проект LINKa, получивший свое название в честь девочки страдающей тяжелой формой детского церебрального паралича - Ангелины Титовой, и разработанный Иваном Бакаидовым, который также страдает ДЦП. Данная программа для синтеза речи предназначена для людей ДЦП, аутизмом, осложнениями после инсульта и другими заболеваниями, которые сопровождаются нарушением речи, развернуто общаться с окружающими [1].

Синтезаторы речи названного проекта представлены в трех видах.

Первый представляет собой программу «LINKa: напиши» (DisType). Она призвана помочь тем, кто имеет проблемы речевого аппарата, но способны легко набирать текст на компьютерной клавиатуре или экране мобильного устройства. «LINKa: напиши» доступна бесплатному скачиванию на сайте https://linka.su/ и подходит для устройств с Android и iOS, Windows и macOS X. Также ею можно пользоваться непосредственно в браузере [10].

Интерфейс программы делится на три основных блока: блок ввода текста, блок быстрых фраз и блок их хранилища:



Блок ввода текста является основным. Для того чтобы курсор попал в поле ввода требуется нажать клавишу «i». При вводе текста появляются подсказки, которые можно выбрать, зажав сочетание клавиш «Ctrl» и цифры с нужным вариантом. При невозможности зажать сразу две кнопки, необходимо включить залипание клавиш в настройках на вкладке «Адаптация интерфейса», а дальше последовательно нажать клавиши. После ввода текста необходимо нажать клавишу «Enter»,

и программа произнесет напечатанное.

Для более живой речи можно выбрать в настройках вы можете выбрать функцию чтения каждого слова при наборе.

Также поле ввода имеет режим «Показать», который позволяет крупно показать написанное на экране, что помогает в общении, например в шумных помещениях. Режим активируется при помощи клавиш «Ctrl» и «B» или же значка глаза на панели. Для произношения, напечатанного в этом режиме, служит совместное нажатие клавиш «Ctrl» и «Enter».

Второй блок – это блок быстрых фраз. Он нужен для быстрых реакций на окружающий мир. Для того чтобы, перейти в данный блок с клавиатуры, зажимается сочетание клавиш «Ctrl» и «0», а дальше можно выбирать необходимые фразы цифрами от 1 до 6.

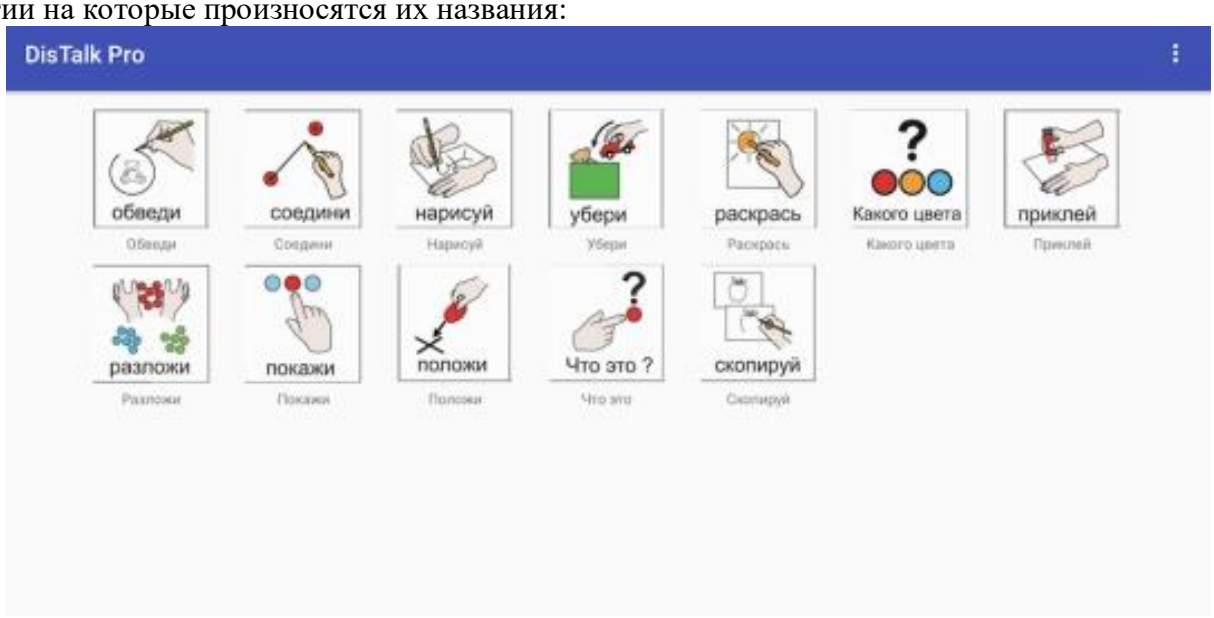
Третий блок – место, где хранятся готовые высказывания, которые можно добавлять самим или же загружать готовые категории на соответствующей вкладке в настройках.

Для управления названным блоком с клавиатуры зажимается сочетание клавиш «Ctrl» с буквой «Ж», или же кликнуть по слову «Категория». Дальше можно выбирать категории цифрами и буквами, указанными в кружках. Фразы и категории добавляются кнопкой «+» внизу экрана.

Кроме того, в программе имеются дополнительные кнопки на панели инструментов. Первая - переключатель режима вставки, после его включения фраза будет не произноситься вслух, а вставляться в поле ввода текста (с клавиатуры включается кнопкой «V»). Вторая (молния) выбирает случайную фразу в категории («R»).

Следующая кнопка позволяет редактировать целиком категорию в одном поле ввода [10].

Следующая программа – это «LINKa: покажи» (DisTalk). Данный синтезатор речи представляет собой доработанный аналог GoTalk, ее интерфейс состоит из таблицы с картинками, при нажатии на которые произносятся их названия:



На экран можно добавлять любые картинки или пиктограммы. «LINKa: покажи» служит как для повседневного общения людей, которые не могут общаться ни в письменной, ни в устной форме, так и для процесса обучения. Ее преимуществом перед другими подобными программами является то, что она русифицирована и оснащена озвучиванием подписей [11].

И, наконец, третья программа – это программа «LINKa: нажми» (DisQwerty). Она создана для тех, кто может нажимать только одну кнопку. Различные варианты слов и фраз здесь выбираются посредством их перебора в таблице. Таблица состоит из раскладки клавиатуры слов и картинок:

Строчки таблицы последовательно изменяют свой цвет, и пользователь выбирает необходимый ему вариант [9].

Таким образом, синтезаторы речи имеют незаменимое значение для людей с ограниченными возможностями. Однако несмотря на их многообразие, представленное в современных реалиях, они все имеют значительные недостатки и ограниченность использования. Их основная проблема состоит в неправильном произношении и понимании слов.

Необходима дальнейшая разработка и усовершенствование синтезаторов речи, направленное на устранение имеющихся недостатков, и добавление необходимых дополнительных настроек.

Библиографический список:

1. В России запущена платформа LINKa – синтезаторы речи для инвалидов с речевыми расстройствами [Электронный ресурс] - Режим доступа: URL: http://www.bolshoyvopros.ru/questions/2893377-kak-oformit-inostrannyj-istochnik-v-spiske-literatury.html
2. Горыныч ПРОФ 5.0 [Электронный ресурс] - Режим доступа: URL: https://soft.sibnet.ru/soft/16838-gorinic-prof-5-0/
3. Речевой Синтезатор «eSpeak». Дистрибутив. [Электронный ресурс] - Режим доступа: URL: http://jaws.tiflocomp.ru/synths/espeak/index.php
4. Синтезаторы речи Acapelagroup. [Электронный ресурс] - Режим доступа: URL: https://nvda.ru/sintezatory-rechi-acapela-group
5. Синтезаторы речи Ivona2. [Электронный ресурс]- Режим доступа: URL: https://nvda.ru/sintezatory-rechi-ivona2
6. Acapela Group: Text To Speech solutions [Электронный ресурс] - Режим доступа: URL: To Speech https://www.acapela-group.com/
7. ESpeak text to speech [Электронный ресурс] - Режим доступа: URL: http://espeak.sourceforge.net/
8. IVONA Voices 2 [Электронный ресурс]- Режим доступа: URL: https://ivona.ru.softonic.com/
9. LINKa. Нажми [Электронный ресурс] - Режим доступа: URL: https://linka.su/linka-push/
10. LINKa. Напиши [Электронный ресурс] - Режим доступа: URL: https://linka.su/linka-type/
11. LINKa. Покажи [Электронный ресурс] - Режим доступа: URL: https://linka.su/linka-show/
12. Vocalizer, Acapela, SVOX и другие - Читаем книги голосом. [Электронный ресурс] - Режим доступа: URL: https://helpix.ru/appinion/201309/385-vocalizer_acapela_svox_i_drugie-chitaem_knigi_golosom.html
13. Vocalizer for NVDA [Электронный ресурс] - Режим доступа: URL: https://vocalizer-nvda.com/downloads

Донкан Кристина Максимовна
Donkan Kristina Maksimovna
Студент МГУ им. адм. Г.И. Невельского, физико-технический факультет.

Дудоладова Полина Геннадьевна
Dudoladova Polina Gennadievna
Студент МГУ им. адм. Г.И. Невельского, физико-технический факультет.

УДК 004.7

ЗАЩИТА БОЛЬШИХ ДАННЫХ НА МОРСКОМ ТРАНСПОРТЕ

PROTECTING BIG DATA IN MARITIME TRANSPORT

Аннотация: Термин «большие данные» - уже не будущее, а настоящее. Сегодняшний век ознаменуется с цифровизацией всех окружающих нас процессов. В работе представлен комплекс мер информационной безопасности для защиты больших данных на морском транспорте.

Abstract: The term "big data" is no longer the future, but the present. Today's century will be marked by the digitalization of all the processes around us. The paper presents a set of information security measures to protect big data in Maritime transport.

Ключевые слова: Большие данные, морской транспорт, атака, защита.

Keywords: Big data, sea transport, attack, protection.

Термин «большие данные» - уже не будущее, а настоящее. Это различные инструменты, подходы и методы обработки как структурированных, так и неструктурированных данных для того, чтобы их использовать для конкретных задач и целей.

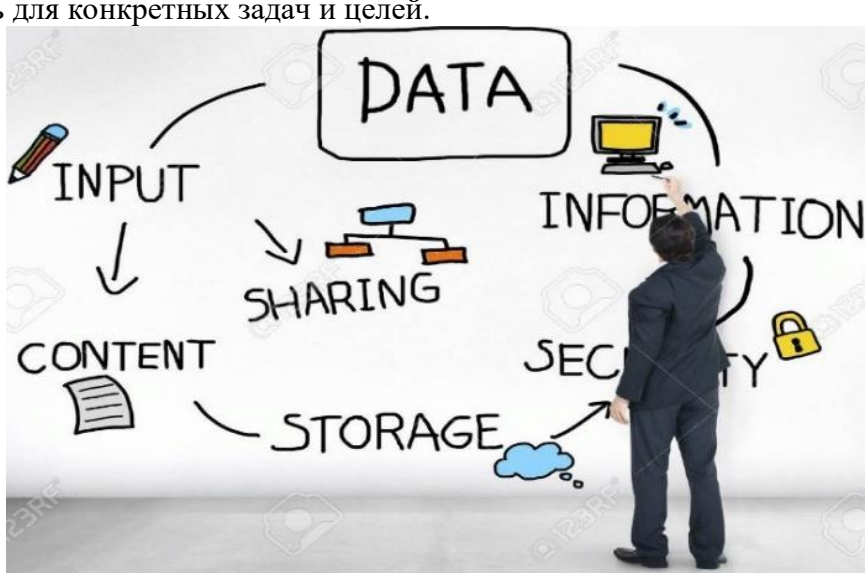


Рис.1. Устройство системы «больших данных».

Сегодняшний век ознаменуется с цифровизацией всех окружающих нас процессов. Не исключение - логистические процессы на морском транспорте. В портах и на морских судах внедряются системы хранения информации: поток данных возрастает, их нужно структурировать. Обработка больших данных выполняется посредством специального программного обеспечения. В частности, в процессе логистики контейнерных перевозок могут быть задействованы следующие разновидности данных: время погрузки, тип груза, вес груза, тип контейнера, номер ячейки в которой находится контейнер на судне и другое. Весь этот кластер данных представляет большую ценность не только для лиц, участвующих в логистических процессах, но и для третьих лиц, желающих завладеть коммерческой информацией. Вместе с тем до сих пор нет общепринятой политики защиты больших данных на морском транспорте.

Требования к политике информационной безопасности вырабатываются на основе специфики исследуемой области. На морском транспорте следует учитывать особенности сетевых технологий для передачи данных (как правило, спутниковые системы связи), технические характеристики оборудования для хранения данных (как правило, высокие мощности находятся на берегу), факторы

внешней среды (как правило, качество связи зависит от координат нахождения судна и от погодных условий).

Также на разработку политики защиты информации влияет специфичность больших данных. Штатные антивирусные системы, межсетевые экраны, системы предотвращения вторжений либо вообще не предназначены для защиты большого объема данных, либо тормозят вычислительные процессы. К тому же на практике требуется защита не только данных, но и программного обеспечения, которое занимается обработкой.

На основе вышеизложенных требований к защите больших данных на морском транспорте выработан комплекс мер информационной безопасности.

Парольная аутентификация сегодня не способна обеспечить необходимый уровень ИТ-безопасности, о чем свидетельствуют регулярные сообщения об утечках корпоративной информации. Слабые пароли и связанные с ними проблемы продолжают оставаться главными уязвимостями.

Для решения этих проблем используются технологии строгой аутентификации и единого входа, реализуемые системами соответствующего класса. Настройка прав и групп пользователей.

Защита таблиц паролями. Ограничить доступ к документу Numbers можно с помощью пароля. Пароли могут содержать практически любые комбинации цифр и заглавных или строчных букв и некоторые специальные символы. Пароли, содержащие комбинации букв, цифр и других символов обычно считаются более надежными. При сохранении электронной таблицы iWork ‘08 или Excel защиту паролем использовать нельзя, но при экспорте таблицы в файл PDF ее можно защитить паролем.

Защита сегментов данных, реализованных в сторонних облачных хранилищах, через защиту каналов связи посредством криптографических методов (например, AES, RSA, SHA-256).

Защита логов транзакций с помощью криптографических методов.

Хэширование табличных данных.

Применение надежного антивирусного ПО для судового и берегового оборудования.

Использование межсетевых экранов. Размещение межсетевого экрана в качестве пограничного устройства между внутренней сетью и Интернетом позволяет контролировать весь исходящий и входящий интернет-трафик и управлять его прохождением.

Проведение периодического аудита безопасности посредством проверки оборудования на уязвимости.

Анонимизация данных. Представляет собой метод удаления персональных данных из набора данных с целью защиты частной жизни физического лица или компании, от которых эти данные были получены.

Библиографический список:

1. Rick Smolan, Jennifer Erwitt. The Human Face of Big Data. - Against All Odds Productions, 2012. - 213 pp.

2. Виктор Майер-Шенбергер, Кеннет Кукьер. Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим. - Москва: Манн, Иванов и Фербер, 2014. - 310 с.

3. Timandra Harkness. Big data does size matter. - Bloomsbury Publishing, 2016. - 304 pp.

Донкан Кристина Максимовна
Donkan Kristina Maksimovna
Студент МГУ им. адм. Г.И. Невельского, физико-технический факультет.

Дудоладова Полина Геннадьевна
Dudoladova Polina Gennadievna
Студент МГУ им. адм. Г.И. Невельского, физико-технический факультет.

УДК 004.7

РАЗРАБОТКА ПОЛИТИК БЕЗОПАСНОСТИ ДЛЯ ЗАЩИТЫ КОРПОРАТИВНЫХ АКТИВОВ

DEVELOPING SECURITY POLICIES FOR PROTECTING CORPORATE ASSETS

Аннотация: В связи с постоянно растущим числом подключений и ростом Интернета, безопасность стала проблемой не только для корпоративной среды, но и для домашнего пользователя. Политики безопасности регулируют шаги и процедуры, предпринимаемые для защиты активов бизнеса и конфиденциальной информации от вторжения посредством использования технологий или физического вмешательства.

Abstract: Due to the ever-increasing number of connections and the growth of the Internet, security has become a problem not only for the corporate environment, but also for the home user. Security policies regulate steps and procedures taken to protect business assets and confidential information from intrusion through the use of technology or physical interference.

Ключевые слова: Политики, аудит, оценка рисков, безопасность.

Keywords: Policies, audit, risk assessment, security.

1. Введение

В связи с постоянно растущим числом подключений и ростом Интернета, безопасность стала проблемой не только для корпоративной среды, но и для домашнего пользователя.

Безопасность - обширная область; поэтому невозможно охватить все аспекты в рамках этой статьи. Документ будет посвящен некоторым аспектам политики безопасности с целью защиты активов от рисков.

2. Сфера возможных политик

Политики безопасности регулируют шаги и процедуры, предпринимаемые для защиты активов бизнеса и конфиденциальной информации от вторжения посредством использования технологий или физического вмешательства. При рассмотрении возможности ведения бизнеса через общедоступные сети, цель должна заключаться в том, как наилучшим образом защитить корпоративные активы, целостность данных и конфиденциальность.

Бизнес-активы могут рассматриваться как включающие такие элементы, как ценные и конфиденциальные данные, которые необходимо хранить в безопасности и конфиденциальности. Основным аспектом политики безопасности является использование паролей для защиты бизнес-с истем и пользователей. Как правило, это будет основным шагом к защите информации.

Распространено использование письменных материалов в бизнес-среде. это

Важно, чтобы все сотрудники несли ответственность за недопущение распространения конфиденциальной информации посторонним лицам. Руководящие принципы, изложенные в политике безопасности, должны обеспечить и решить эту проблему.

3. Оценка рисков

Сначала бизнес должен определить, какие активы он должен защищать и почему. Предприятия сталкиваются с рисками из-за неправильного использования программного и аппаратного обеспечения со стороны своих сотрудников. Соединения с выходом в Интернет создают угрозы для хакеров и взломщиков, которые могут запускать спуфинг и атаки типа «отказ в обслуживании», используя список из естных уязвимостей и методов, что делает бизнес-сайт недоступным для его сотрудников и клиентов. Угрозы от вирусов, червей и троянов также являются серьезной проблемой. Нельзя исключать злонамеренные атаки, такие как бомбы и кража оборудования, или стихийные бедствия, такие как пожар, наводнения и землетрясения.

Опасности также существуют от внутренних пользователей, которые не относятся к

безопасности всерьез, поскольку она не до конца понята и оценена.

4. Области исследования

Процедуры «наилучшей практики» следует использовать для защиты активов предприятия от рисков. Практическое правило для любой политики должно быть «все, к чему не следует обращаться, запрещено». Контролируемая копия политики безопасности должна быть легко доступна для всех сотрудников. Администраторы и руководители отделов должны обеспечить внедрение и соблюдение правильных процедур, демонстрируя свою поддержку и важность политик безопасности.

Политики должны соответствовать всем существующим правилам, положениям и законам, соответствующим данной организации.

Четкие, точные и легкодоступные политики вместе с приемлемыми инструментами дадут сотрудникам возможность принимать обоснованные решения.Области, подлежащие исследованию:

- Аудит и его использование для выявления уязвимостей;
- Политика администраторов;
- Политика паролей;
- Сетевая политика;
- Политика удаленного доступа;
- Политика резервного копирования и восстановления;
- Политика физической безопасности;
- Политика пользователя компьютера и обучение пользователей.

4.1 Аудит и его использование для выявления уязвимостей

Регулярный аудит систем является важным помощником в понимании слабых мест системы. Проверьте инфраструктуру, проводя регулярные тесты на проникновение. Проверьте журналы аудита и отчеты и убедитесь, что необходимые действия предприняты для любых обнаруженных уязвимостей.

Когда журналы аудита проанализированы, проверьте их на соответствие политике безопасности и при необходимости обновите их. Например, если в журнале событий безопасности обнаружено слишком много попыток сбоя журнала, проследите за пользователем, которому не удалось войти в систему, и убедитесь, что он является подлинным пользователем системы. Проверьте, установлена ли политика безопасности для блокировки учетных записей после указанного числа попыток входа в систему. Если нет, то проведите оценку рисков для бизнеса и, если необходимо, пересмотрите и измените политику. Защищать журналы аудита; например, используя устройства-черви или одноразовые CDS с возможностью записи, чтобы они не были подделаны, так как это единственные системные записи, которые показывают любые события, которые произошли и могут потребоваться для юридического расследования.

4.2 Политика администраторов

Системные администраторы играют важную роль в реализации политик безопасности. Если они не знают о политиках безопасности, системы могут быть скомпрометированы. Следует придерживаться принципа наименьших привилегий, но в то же время сотрудники не должны останавливаться в достижении своих целей. Всегда поддерживайте и следуйте процедурам настройки и будьте в курсе последних уязвимостей. Применяйте процедуры усиления защиты операционных систем для защиты от известных лазеек в безопасности. Администраторы также несут ответственность за реализацию контроля доступа к каталогам, базам данных и политикам паролей. Администраторы должны обеспечить изменение паролей для вновь выданных идентификаторов, любых скомпрометированных паролей и своевременное отключение прекращенных идентификаторов пользователей. Повторное использование паролей не должно быть разрешено. Системные администраторы должны регулярно менять и поддерживать пароли системных и программных приложений и хранить эти пароли в безопасности, используя такие инструменты защиты паролем, как «Info Keep».

Важно, чтобы политика осуществлялась с использованием утвержденного компанией программного обеспечения для проверки на вирусы, установленного на всех серверах, настольных компьютерах и ноутбуках.

Регулярное успешное резервное копирование и хранение резервных носителей на месте и вне его в безопасных местах дает администраторам возможность при необходимости выполнять процесс восстановления. Администраторы должны осознавать, что сохранение конфиденциальности является

частью работы и должно строго соблюдаться.

4.3 Политика паролей

Пароли не подразумевают конфиденциальность, но позволяют авторизованным пользователям получать доступ к необходимым приложениям, файлам и электронным сообщениям. Слабые пароли не имеют значения и не будут выполнять свою задачу. Пароли должны быть более надежными в случае критических систем или при использовании доступа на административном уровне.

Когда удаленным пользователям разрешен доступ через брандмауэр, внедрите одноразовые инструменты генерации паролей для аутентификации брандмауэра. Защитите такие инструменты и программное обеспечение, используемые администраторами, с помощью шифрования или другого аналогичного метода. Ограничение и мониторинг последовательных неудачных попыток входа в систему пароля полезны. Шифрование паролей следует использовать при передаче данных между внешними сетями. Пароли, предоставляемые поставщиком, всегда должны быть изменены перед установлением связи в сети. Все пользователи должны нести ответственность за любые действия, выполняемые под их индивидуальными идентификаторами и паролями. Используйте надежные пароли, заменяя буквенные символы цифрами и знаками, используя первую букву фразы или предложения для формирования слова, таким образом получая не словарные слова.

4.4 Политика резервного копирования и восстановления

Предприятия полагаются на хорошие процедуры резервного копирования для восстановления критически важных систем и данных.

Важно, чтобы эта функция рассматривалась и выполнялась без слабость в политике. Резервные копии должны давать руководству гарантию того, что в случае сбоя какой-либо части инфраструктуры ее можно восстановить с помощью резервных копий.

Все резервные данные должны быть четко обозначены и храниться в надежном месте. Всегда используйте доступные инструменты для выполнения резервного копирования и проверки его целостности. В зависимости от критического характера бизнеса может возникнуть необходимость в составлении планов действий на случай сбоя оборудования. Используйте брандмауэры высокой доступности с возможностью полного переключения при сбое или используйте RAID-массивы для сбоя жесткого диска.

Защитите оборудование от перебоев в питании, используя источники бесперебойного питания или генераторы, и защитите все устройства от злонамеренного вмешательства.

4.5 Политика пользователей компьютеров и обучение пользователей

Хотя сотрудникам предоставляются ПК, чтобы они могли выполнять порученную им задачу, следует понимать, что эти ПК являются собственностью компании и не должны использоваться в личных целях. Компьютерные ресурсы дороги, поэтому оскорбительные материалы нельзя загружать и хранить на рабочих ПК.

Системы электронной почты, предоставляемые Компанией, должны использоваться только в деловых целях, и необходимо соблюдать осторожность в отношении любых материалов, отправляемых по электронной п чте. Компания несет ответственность за действия сотрудника.

Спам, списки рассылки, игра в игры или участие в онлайн-группах должны быть запрещены.

Пользователи настольных компьютеров и ноутбуков должны использовать загруженное в бизнесе антивирусное программное обеспечение для проверки всех данных на своих ПК, загруженных данных или данных, передаваемых через диски. Данные, загруженные на сетевые серверы или отправленные за пределы компании, должны быть проверены на вирусы. Пользователям не должно быть разрешено отключать такое программное обеспечение. Администраторы могут лучше контролировать ПК, применяя групповые политики в соответствии с функциями департамента, чтобы пользователи не могли вмешиваться в конфигурации.

Всегда следите за тем, чтобы были установлены последние обновления / исправления для всех операционных систем и приложений, что обеспечит устранение всех известных уязвимостей. Программное обеспечение и инструменты, предоставляемые Systems Management Server, могут использоваться для аудита всех ПК.

Важно, чтобы пользователи знали о политике безопасности и рисках, с которыми может столкнуться бизнес, если они не соблюдаются правильно. Обучайте пользователей, регулярно рассылая электронные письма, проводя информационные сессии и размещая плакаты на досках объявлений. Обучение пользователей нельзя воспринимать легкомысленно после вируса

ILOVEYOU, для которого требовалось, чтобы только один пользователь открыл это сообщение электронной почты и вложение на серверах и шлюзах электронной почты.

4.6 Сетевая политика

Используя разнородные сетевые компоненты и многоуровневый подход, можно получить удовлетворительно хороший дизайн инфраструктуры. Различные технологии и платформы усложняют хакерам взлом системы, используя одну уязвимость.

Обмен информацией с внешними источниками или из них должен осуществляться через единый шлюз. Это минимизирует риск раскрытия информации, связанной с внутренними сетями. Реализация политики с использованием правил фильтрации позволит или запрещает доступ по адресам источника и назначения, помогая ограничить доступ к сетям неавторизованным персоналом. Маршрутизаторы, транслирующие внутренние IP-адреса RFC1980, можно использовать для добавления еще одного уровня безопасности, который злоумышленники могут преодолеть с помощью сетевых / общедоступных проблем маршрутизации.

Прокси-серверы приложений в зоне демилитаризации (DMZ) разрешают все защищенные соединения от внутреннего к прокси-серверу, что снижает риск внутреннего и внешнего маршрутизируемого трафика. Важно поддерживать все операционные системы и программные приложения с последним обновлением / патчем. Все изменения должны быть документированы. План возврата должен быть рассмотрен в случае возникновения проблем. Следуйте процедурам «наилучшей практики», тестируя обновления перед внедрением в тестовой среде.

Используйте предоставляемые поставщиком инструменты для аудита и мониторинга действий пользователей. Администраторы должны использовать принцип наименьших привилегий при назначении доступа к функциональным и ведомственным политикам, что упрощает аудит и мониторинг. Всегда тратьте время на анализ журналов на наличие уязвимостей в системе.

4.7 Политика удаленного доступа

По мере быстрого увеличения числа пользователей модемом, количество уязвимостей также увеличивается. Чтобы позволить администраторам предоставлять контролируемый доступ для коммутируемых пользователей, должен быть реализован сервер удаленного доступа с набором номера (RADIUS). Доступ по SecureID или Safeword Token через брандмауэр обеспечивает однократный сеанс аутентификации доступа к сетям. Если данные передаются удаленно, используйте шифрование данных, чтобы минимизировать вероятность попадания данных.

Пользователь внутренней сети никогда не должен иметь возможность выходить из корпоративной сети, находясь в локальной сети; т.е. избежать сценария взлома публичной и частной сети через модем.

Политика удаленного доступа может предусматривать, чтобы пользователи не передавали номера дозвона неавторизованным пользователям. Аудит, мониторинг и публикация данных, по имени пользователя, тех, кто проводит много времени в Интернете. Это может помочь предотвратить злоупотребление правами доступа в Интернет, чтобы пользователи лучше осознавали, что их действия контролируются. Политика удаленного доступа также должна содержать рекомендации по реализации стандартной конфигурации клиента.

4.8 Политика физической безопасности

Физическая безопасность зданий, серверов, переносимых носителей (дисков, лент), ноутбуков, настольных компьютеров и любых сетевых компонентов, подключенных к внутренним сетям передачи данных, также важна.

Во-первых, обеспечьте доступ к зданию через приемную и разрешите доступ авторизованным пользователям с помощью идентификационных значков и машин доступа к картам. Используйте системы видеонаблюдения или такие инструменты, как радиационная лампа Eck / TEMPEST или электромагнитные импульсы (2). 24-часовой мониторинг авторитетной консультацией по безопасности должен быть рассмотрен. Защитите оборудование, разместив его в специально построенных дата-центрах, контролируемых некоторыми из вышеупомянутых инструментов, контролирующих доступ и контролирующих использование.

Держать коммуникационное оборудование в запираемых шкафах, доступ к которым разрешен только авторизованным пользователям.

При транспортировке носителей, таких как резервные ленты и жесткие диски, необходимо соблюдать осторожность, чтобы использовать специальные герметичные контейнеры, которые защитят носитель от повреждений и не могут быть подделаны. Всегда храните резервные ленты на

месте, а также вне его в безопасных местах.

Жесткие диски ноутбука должны быть зашифрованы и защищены парол м загрузочных протоколов (пароль netbios).

Многие пользователи оставляют печатные материалы на своих столах и мусорных баках. Внутри злоумышленники всегда ищут такие возможности. Храните печатные материалы в запирающихся шкафах или в клочках нежелательных материалов. Обеспечить соблюдение и применение политики «чистого стола». Контролируйте всех посетителей сайта и предупреждайте сотрудников «Социальной инженерии». Люди используют телефон, факс, электронную почту или личное влияние, чтобы попытаться получить то, что они хотят. Люди должны защищать от таких атак.

5. Вывод

Глобальное расширение сетей позволило вести бизнес через Интернет. Современные тенденции показывают, что есть четкие признаки того, что безопасность должна рассматриваться очень серьезно любым бизнесом, имеющим доступ к Интернету.

Физическая безопасность одинаково важна для управления и контроля. Социальная инженерия очень распространена и часто упускается из виду из-за внутренних отношений между сотрудниками или дружеских отношений.

Ни один сайт не является абсолютно защищенным, но предоставление рекомендаций и информирование сотрудников о проблемах безопасности может только помочь защитить его. Политики безопасности позволяют сотруднику знать, что нужно делать, а что нельзя.

Политика облегчает принятие решений и реагирование на чрезвычайные ситуации. Они не должны быть слишком одержимы, чтобы помешать сотрудникам выполнять свою роль. Регулярный пересмотр политик, сохранение бдительности с помощью тестирования, мониторинга, обновления и обновления может только обеспечить более безопасный сайт для их сотрудников и клиентов.

Библиографический список:

1) Руководство по безопасности ИТ – Физическая безопасность – последнее обновление, июнь 2000 г. http://www.boran.com/security/IT1x-8.html

2) Майкл Р. Оверли (1999), Электронная политика, как развивать компьютер, электронную почту и интернет Руководство по защите вашей компании и ее активов, SciTech Publishing Inc. (СОЕДИНЕННЫЕ ШТАТЫ АМЕРИКИ)

3) Как разработать политику безопасности сети Обзор URL ezопасности межсетевого сайта: http://www.sun.com/software

4) URL обзора безопасности: http://www.sun.com/security.

Антонова Виктория Валерьевна
Antonova Viktoriya Valer'yevna
Магистр Воронежского государственного технического университета, факультет архитектуры и градостроительства.

УДК 72.01

АКТУАЛЬНЫЕ КОНЦЕПЦИИ НАУЧНОГО ЗНАНИЯ В АРХИТЕКТУРЕ

CONCEPTS OF SCIENTIFIC KNOWLEDGE IN ARCHITECTURE

Аннотация: в статье рассматриваются актуальные концепции научного знания в архитектуре. Определены основные направления научного знания и инструментарий их внедрения. Приведены варианты применения научного знания в архитектуре на примере зарубежного опыта в проектировании городов будущего (Smart City) и «умной» архитектуры в частности.

Abstract: The article examines the current concepts of scientific knowledge in architecture. The main directions of scientific knowledge and tools for their implementation are determined. Variants of application of scientific knowledge in architecture are given on the example of foreign experience in designing cities of the future (Smart City) and "smart" architecture in particular.

Ключевые слова: научное знание в архитектуре, концепция, умный город, архитектура будущего, экология, устойчивое развитие.

Key words: scientific knowledge in architecture, concept, smart city, architecture of the future, ecology, sustainable development

Определение роли науки в образовании невозможно без раскрытия роли в нём практики как ему современной, так и исторической. Сама же практика на протяжении многих веков истории зодчества занимает ведущее место в триаде «образование – наука – практика». Между тем, развитие науки и технологий привело к тому, что в смежных с искусством областях они играют всё большую роль.

В истории архитектуры представлены всевозможные ситуации взаимодействия в системе «практика–образование»: образование на основе практики (например, творчество в «стилях»), образование с учётом практики (паллиатив «стиля» и технологии), образование вопреки современной практике (авангард XX века) [1].

В процессе анализа архитектуры русского авангарда С.О. Хан-Магомедов отметил динамику взаимоотношений науки и образования, разрешения проблем, которые характеризуют процесс формообразования как пронизывающий триаду «наука–образование–практика», вектор художественного развития, интегрирующий создание формы с достижениями социально-функциональной практики и технологического прогресса. Проблема взаимоотношений практики–образования–науки была представлена как процесс открытия новых законов формообразования[1].

Архитектурная наука и практика проектирования не имеют ярко выраженной, на первый взгляд, связи, но при этом неразрывны. Сегодня ясно, что проблема создания безопасной и комфортной среды обитания не может быть решена без применения новейших достижений науки и техники. Архитектура будущего будет их отражением. Гармония в системе «человек — природа — архитектура» невозможна без их использования: это и компьютерные технологии, создание новейших способов получение энергии, искусственного интеллекта и т.д [1].

На сегодняшний день одним из самых ярких примеров внедрения новых технологий в сферу архитектуры и строительства является оснащение современной практики программным IT-инструментарием. В поддержание устойчивого развития среды на первый план выдвигаются идеи экологичного строительства, преобразования солнечной и ветровой энергии, разработки и реализации интеллектуальных систем автоматического управления строительными объектами на всем протяжении их жизненного цикла.

Управление зданием (сооружением) трактуется на современном этапе развития строительной науки как управление процессами изменения его действительных функциональных и технических характеристик. Целевой функцией такого управления является компенсация или подавление влияния возмущений любого вида и интенсивности на устойчивое состояние строительного объекта (здания или сооружения), т.е. обеспечение его гомеостата.

Город, как организм, способный совершенствоваться - обучаться, развиваться, накапливать и анализировать информацию - уже находит свое проявление в концепциях городов будущего. Концепцию «умный город» (Smart City) впервые выдвинули в 90-х годах 20 века, когда пришло осознания главенства развития IT-технологий [2].

Изначально Smart City рассматривали как концепцию, поддерживающую идеи защиты окружающей среды и способствующей устойчивому развитию. В настоящее время «умный город» сочетает в себе все больше функций, в том числе и высокие технологии, направленные на комфортную работу и интересное проведение досуга, максимальный комфорт пребывания человека в любой среде. Рассмотрим наиболее подробно некоторые из проектов будущих Smart City [2].

Умный город «Karle Town Centre». Бангалор, Индия

Авторы: UNStudio

Проект Karle Town Centre – удачный пример города будущего в концепции «эко». Концепция проекта предполагает решение экологических проблем сразу по нескольким фронтам. Так, ограничение движения транспорта в определенных районах города, просторные пешеходные улицы и большое количество зеленых зон позволят освободить улицы от лишнего автомобильного траффика(рис.1).

Рисунок 1. Визуализация проекта.

В помощь к урегулированию температуры воздуха и экономии потребления энергии здания будут окрашены специальной теплоотражающей краской, а на улицах города для увеличения площади теневых участков будут установлены специальные «навесы». Снижению ветровых нагрузок будут способствовать висячие сады [2].

Smart Forest City Cancun. Пригород Канкуна, Мексика

Авторы: бюро Stefano Boeri Architetti

Smart Forest City спроектирован как город-ботанический сад, расположенный на территории современного города в местах обитания майя. Город также отличается экологической направленностью, а также внедрением высоких технологий в сфере здравоохранения, но при этом с сохранением конфиденциальности данных человека.

Предполагается, что умный город будет самостоятельно обеспечивать себя продуктами питания, энергией, пресной водой. А развитие общественного транспорта позволит оставлять жителям свои автомобили на окраинах города, разгружая центр (рис.2) [2].

Рисунок 2. Визуализация проекта.

«Умный город» в целом подразумевает «умную архитектуру» в частности. Актуальные концепции научного знания позволяют проектировать все более гибкие системы, которые имеют возможность подстраиваться под окружающую среду. Одним из примеров такой системы является так называемый «Кинетический фасад». Это не только интересное решение с точки зрения функционала, оно также отвечает требованиям концепции «эко», уменьшая расход используемой

энергии.

Важность научного знания в целом в сфере новых технологий сложно переоценить. Однако не менее важным является изучение влияния архитектурной среды на психологическое состояние человека. Места, где человек пребывает длительное время, оказывают существенное влияние. Такое сооружение как больница - не основное место для пребывания, однако очень влиятельное в эмоциональном плане. Проектирование с учетом контекста в данном случае не просто важно, а критически необходимо, т.к. от этого напрямую зависит процесс выздоровления человека.

Рассмотрим примеры проектов современных больниц, построенных по принципу положительного психологического влияния.

Реабилитационный центр Мэгги. Манчестер, Великобритания

Авторы: Foster + Partners

Основной концепцией реабилитационных центров Мэгги является психологическая и информационная поддержка онко-больных и их близких в процессе протекания болезни. Одним из таких проектов стал центр в Манчестере, автором которого выступил Норман Фостер. Это небольшое и уютное здание, пропитанное атмосферой дома. Очень важно, что посетители уже с порога испытывают приятные эмоции, что всегда благотворно влияет на здоровье (рис.3) [3].

Рисунок 3. Фото реабилитационного центра.

Медицинский центр Navyas. Бангалор, Индия.

Авторы: Cadence Architects

Основной функцией центра является лечение и оздоровление, но в нем также расположены зал-терраса для йоги и органический ресторан. Одной из проблем проектирования здания стал контекст города – здание находится на оживленной улице. Решением стало создание сада вокруг здания. Зеленая зона не только скрывает проезжую часть из окна, но и является самостоятельным местом для уединения (рис.4) [3].

Рисунок 4. Интерьер палаты.

Заключение

Архитектура будущего неразрывна связана с научным знанием, как и любая другая деятельность, которая развивается вместе с человечеством, находя новые формы существования и взаимодействия с окружающей средой. Проекты, опирающиеся на научное знание в той или иной сфере, безусловно, в несколько раз эффективнее выполняют свою роль. Проектирование с учетом концепций современных научных знаний позволит уж в ближайшие десятилетия значительно повысить качество жизни человека.

Библиографический список:

1. Есаулов Г.В. Архитектурная наука и образование: векторы развития. file:///C:/Users/%D0%92%D0%B8%D0%BA%D1%82%D0%BE%D1%80%D0%B8%D1%8F/Downloads/11-12-PB.pdf Дата обращения: 27.06.2020

2. Леденева Н. Топ-10 «Умных городов» мира. Режим доступа: https://www.architime.ru/specarch/top_10_smart_city/smart_city.htm Дата обращения: 29.06.2020

3. Леденева Н. Топ-10 примеров исцеляющей архитектуры. Режим доступа: https://www.architime.ru/specarch/top_10_hospital/hospitals.htm Дата обращения: 30.06.2020

Научное издание

Коллектив авторов

Сборник материалов LVIII Международной научной конференции «Техноконгресс»

ISBN 978-5-6040934-2-9

Техниконаучный журнал «Техноконгресс»

Кемерово 2020