Материалы конференции

«Кругозор современного студента: Научные интересы»

24 декабря 2021 г.

Ивановский государственный политехнический университет

Кафедра информационных технологий и сервиса

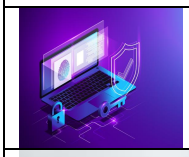
Настоящий сборник является экспериментальным изданием.

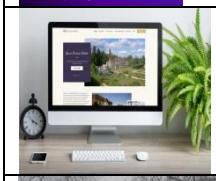
В сборнике собраны результаты научно-исследовательских работ, выполненных студентами группы ИСТД-31 в рамках изучения дисциплины «Основы проведения НИР».

Темы работ выбраны студентами самостоятельно без каких-либо ограничений. Выбор тем оказался весьма интересен: здесь и традиционные IT-технологии, и Web-дизайн, и макроэкономика, и психология, и инновации. Объем статьи не ограничивался.

Каждая статья, кроме стандартных составляющих, содержит Graphic abstract – графическую аннотацию, в которой кратко отражается основной смысл статьи. Graphic abstract, обычно сопровождающий иностранные статьи, в российских журналах пока не применяется. Это отличительная особенность данного сборника.

Все статьи прошли проверку на наличие заимствований. Оригинальность текста у всех статей не менее 60 %.





Оглавление

ИНДИКАТОР СВЕЖЕСТИ МОЛОКА

Н.С. Кудряшова, Л.А. Петросян, Я.Е. Игнатьичев

Ивановский государственный политехнический университет

Аннотация. В статье описана разработка упрощения механизма контроля качества изготавливаемой продукции на протяжении всего пути: от производителя до потребителя, а также отслеживания целостности упаковки во время перевозок и реализации. Планируется внедрение концептуального решения, прототипа.

Ключевые слова: контроль качества, молочная продукция, умная упаковка.

На данный момент не существует точных способов определить свежесть молочной продукции. Срок годности, указанный на упаковке, является расчетным и не всегда отражает истинное состояние продукта. Так же если обратиться к результатам мониторинга «Общественной потребительской инициативы» можно сделать вывод, что более 45% молочных товаров на прилавках стоят уже в просроченном виде [1]. Магазины по всему миру ежегодно выбрасывают около 2 млн. тонн продуктов питания, срок годности которых подходит к концу.

Данные проблемы будут актуальны для производителей, реализаторов и покупателей, а также для людей с ограничениями по зрению, ведь надписи на упаковке написаны очень мелким шрифтом, что усложняет прочтение информации о сроке годности.

В данной работе непосредственным решением данных проблем является создание «Умной упаковки» с функцией отслеживания общего состояния продукта.

Создание упаковки — это неотъемлемая часть планирования продукции, в ходе которой фирма изучает, разрабатывает и производит свою упаковку. При этом производитель не всегда занимается вопросами разработки и производства упаковки своих товаров, что делает «Умную упаковку» еще актуальнее [2].

Умная упаковка сможет, путём изменения своего цвета, указывать на свежесть продукта, то есть при скисании молока, коробка будет постепенно по бокам становится более тёмного цвета. Так эргономичный дизайн упаковки поможет потребителю без дополнительных усилий определить свежесть молока (рис. 1). Также планируется создание приложения для более лёгкого чтения текста. Отсканировав QR-код на упаковке, потребитель сможет получить подробную информацию о приобретаемом товаре.

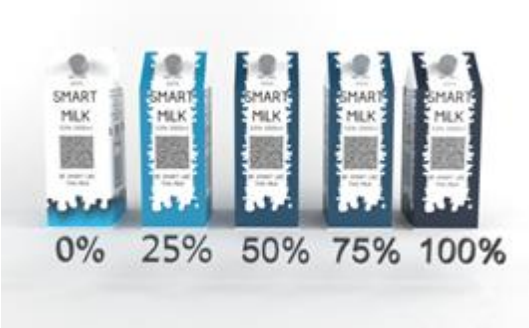


Рис.1 – Этапы изменения цвета упаковки при скисании молока

В настоящее время в секторе «Умной упаковки» в основном доминируют оболочки и пленки с кислород-адсорбирующим слоем, влагопоглотителями и барьерные оболочки [3].

Применение микро- и нано биотехнологий в пищевой упаковке включает использование новых композитных материалов, обладающих улучшенными механическими, теплофизическими, функционально технологическими, барьерными и антимикробными свойствами, а также внедрение датчиков мониторинга и прослеживаемости мясной продукции в течение всего технологического цикла ее хранения, транспортировки и реализации [3].

«Умная упаковка» будет состоять из семи слоев (рис. 2). Второй слой – мембранный, на котором будет расположен индикатор, отслеживающий активную кислотность продукта.

Рис. 2 – Структура упаковки

Активная кислотность – уровень ионов водорода, измеряется он в единицах pH (potentia hydrogeni, что означает сила водорода). Уровень активности ионов водорода в свежем молоке находится в пределах 6,4-6,7pH. В случае если уровень активности водорода опускается ниже 6,3pH можно абсолютно точно говорить о том, что молоко прокисло [4].

Принцип работы индикаторов свежести основывается на прямом взаимодействии молочного продукта и индикатора. Все изменения, которые происходят в продуктах и влияют на состояние их свежести, могут привести к росту микроорганизмов и связанному с этим процессу обмена веществ. Как правило, все индикаторы свежести определяют наличие таких продуктов обмена веществ, как диоксид углерода, диоксид серы, аммиак, этанол, некоторые токсины и органические кислоты [3].

Таким образом, несмотря на то что на рынке, можно найти много реализованных или идейных «Умных упаковок» с использованием передовых технологий и специализированных материалов, не все учитывают внешний вид упаковки. Важно создавая концепцию усовершенствования продукта, увязать её с концепцией и дизайном упаковки, потому что она помогает человеку сделать выбор среди множества других аналогичных товаров.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Мало половины: 45% молочной продукции в магазинах оказались просрочкой. [Электронный ресурс] https://iz.ru/1139434/maksim-khodykin-tatiana-baikova/malo-poloviny-45-molochnoi-produktcii-v-magazinakh-okazalis-prosrochkoi
2. Упаковка и тара / Д.Ф. Ханлон. - СПб.: Профессия, 2008 .- 632 с.
3. Иванова Т., Розанцев Э. Активная упаковка: реальность и перспектива XXI века.
4. Приборы для измерения кислотности молока. [Электронный ресурс] https://cheasy.ru/content/84-pribor-dlya-izmereniya-kislotnosti-moloka

IT – технологии

В. В. Иванов

Ивановский государственный политехнический университет

Аннотация. В статье проанализированы глубокие преобразования, происходящие в нашем обществе, более остро выдвигающие на первый план проблемы развития педагогики, экономики, производства, финансов, систем, искусства, культур, производственных отношений и т.д. Стремительно развивающийся процесс информатизации всех сфер жизни общества делает возможным поднять на новый уровень организацию и качество исследовательской работы в различных сферах.

Ключевые слова: информатизация, информационные технологии, периоды сменяемости.

В условиях развития современного общества информационные технологии глубоко проникают жизнь людей (рис. 1). Они очень быстро превратились в жизненно важный стимул развития не только мировой экономики, но и других сфер человеческой деятельности. Сейчас трудно найти сферу, в которой не используются информационные технологии (рис. 2). Так, в промышленности информационные технологии применяются не только для анализа запасов сырья, комплектующих, готовой продукции, но и позволяют проводить маркетинговые исследования для прогноза спроса на различные виды продукции, находить новых партнеров и многое другое.

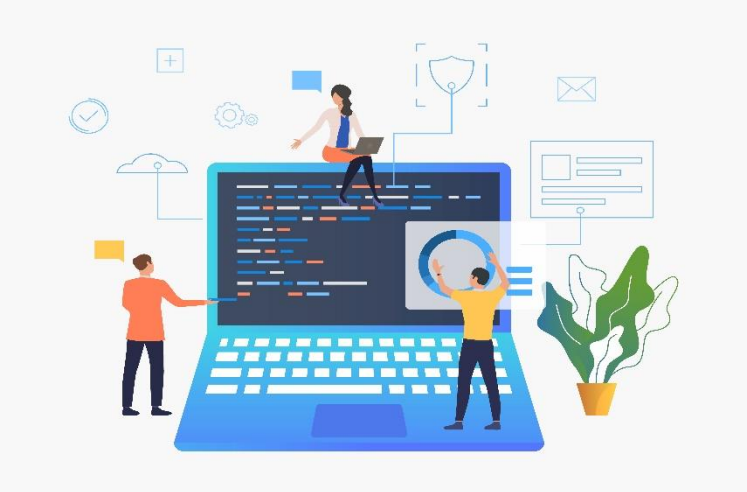


Рис. 1. Место, занимаемое IT-технологиями в жизни современного человека

Применение информационных технологий в научной сфере и в сфере образования сложно переоценить. Сейчас трудно представить себе школу, в которой бы не было компьютерного класса. В наши дни существует масса электронных библиотек, воспользоваться которыми, можно не выходя из дома, что значительно

облегчает процесс обучения и самообразования. Кроме того, информационные технологии способствуют развитию научных знаний.

Рис. 1. Сферы применения IT-технологий

Информационные технологии – это совокупность методов, производственных процессов и программно-технических средств, объединенных в технологическую цепочку, обеспечивающих работу с информацией, с целью снижения трудоемкости процессов использования информационных ресурсов (рис. 3).

Несколько иначе под информационными технологиями подразумевается процесс, использующий совокупность средств и методов сбора, обработки и передачи данных для получения информации передового качества.

Для информационных технологий является вполне естественным то, что они устаревают и заменяются новыми. Так, например, телеграф передал все свои функции телефону. Телефон постепенно вытесняется службой экспресс доставки. Телекс передал большинство своих функций факсу и электронной почте.

Рис. 3. Иллюстрация тесной взаимосвязи IT-технологий

При внедрении новой информационной технологии в организации необходимо оценить риск отставания от конкурентов в результате ее неизбежного устаревания со временем, так как информационные продукты, как никакие другие виды материальных товаров, имеют чрезвычайно высокую скорость сменяемости новыми видами или версиями. Периоды сменяемости колеблются от нескольких месяцев до одного года. Если в процессе внедрения новой информационной технологии этому фактору не уделять должного внимания, возможно, что к моменту завершения перевода фирмы на новую информационную технологию она уже устареет и придется принимать меры к её реанимированию.

Такие неудачи с внедрением информационной технологии обычно связывают с несовершенством технических средств, тогда как основной причиной неудач является отсутствие или слабая проработанность использования информационной технологии.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Лекция 5. Информационные технологии в научной деятельности https://tsput.ru/res/informat/aosit/Lection5.htm
2. Информационные технологии https://bank.nauchniestati.ru/primery/referat-na-temu-informacionnye-tehnologii/
3. Нанотехнологии и информационные технологии - технологии XXI века https://www.elibrary.ru/item.asp?id=19567314

КРИПТОГРАФИЯ И МЕТОДЫ ЕЕ ПРАКТИЧЕСКОГО ПРИМЕНЕНИЯ

В.А. Назаров, В.М. Юзбашян, А.А.Баусина

Ивановский государственный политехнический университет

Аннотация. В статье проанализированы и рассмотрены история криптографии и способы защиты информации. Исследованы методы шифрования. Рассмотрен список интернет-угроз информации и методы противодействия ее похищению.

Ключевые слова: криптография, защита, шифрование информации, интернет-угрозы.

Криптография (от др.-греч. κρυπτός «скрытый» + γράφω «пишу») — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), шифрования (кодировка данных) [1].

Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифровывание и расшифровывание проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Криптография не является защитой от обмана, подкупа или шантажа законных абонентов, кражи ключей и других угроз информации, возникающих в защищённых системах передачи данных.

Криптография — одна из старейших наук, её история насчитывает несколько тысяч лет [2,3].

За наукообразным словом «криптография» скрывается древнее желание человека спрятать важную информацию от посторонних глаз. Можно сказать, что сама письменность в самом начале уже была криптографической системой, так как принадлежала узкому кругу людей, и с помощью нее они могли обмениваться знаниями, недоступными неграмотным. С распространением письма возникла потребность в более сложных системах шифрования. Со времен древних цивилизаций криптография верно служила военным, чиновникам, купцам и хранителям религиозных знаний.

Самым древним свидетельством применения шифра (около 4000 до н.э.) ученые считают древнеегипетский папирус с перечислением монументов времен

фараона Аменемхета II. Безымянный автор видоизменил известные иероглифы, но, скорее всего, не для сокрытия информации, а для более сильного воздействия на читателя [2].

Еще один известный шифр – древнесемитский атбаш, приблизительно 600 г. до н.э. Здесь информацию запутывали самым простым способом − с помощью подмены букв алфавита. Криптограммы на атбаше встречаются в Библии.

А в Древней Спарте пользовались скиталой – шифром из цилиндра и обвивающей его полоски пергамента. Текст писали в строку на пергаменте. После разматывания ленты текст превращался в шифр, прочитать который было возможно, только имея цилиндр такого же диаметра [3]. Можно сказать, что спартанская скитала стала одним из первых криптографических устройств.

В IV столетии до н.э. автор военных трактатов Эней Тактик придумал шифровальный диск, названный впоследствии его именем. Для записи сообщения в отверстия диска с подписанными рядом с ними буквами последовательно продевалась нить. Чтобы прочитать текст, нужно было всего лишь вытягивать нить в обратной последовательности. Это и составляло основной минус устройства – при наличии времени шифр мог быть разгадан любым грамотным человеком. Зато, чтобы быстро «стереть» информацию с диска Энея, нужно было всего лишь вытянуть нить или разбить устройство [3].

Одним из первых документально зафиксированных шифров является шифр Цезаря (около 100 г. до н.э.) [2]. Его принцип был очень прост: каждая буква исходного текста заменялась на другую, отстоящую от нее по алфавиту на определенное число позиций. Зная это число, можно был разгадать шифр и узнать, какие тайны Цезарь передавал своим генералам.

Шифрованием пользовались многие древние народы, но особенного успеха в криптографии уже в нашу эру достигли арабские ученые. Высокий уровень развития математики и лингвистики позволил арабам не только создавать свои шифры, но и заниматься расшифровкой чужих. Это привело к появлению первых научных работ по криптоанализу – дешифровке сообщений без знания ключа. Эпоха так называемой наивной криптографии, когда шифры были больше похожи на загадки, подошла к концу.

Работы арабских ученых способствовали появлению полиалфавитных шифров, более стойких к расшифровке, в которых использовались сразу несколько алфавитов. Однако люди Средневековья продолжали пользоваться простыми шифрами, основанными на замене букв другими буквами или цифрами, неправильном написании букв и т.д. В Средние века в Европе считалось, что криптография была тесно связана с магией и каббалой.

Интересно, что в Древней Руси тоже были свои способы тайнописи, например литорея, которая делилась на простую и мудрую. В мудрой версии шифра некоторые буквы заменялись точками, палками или кругами. В простой литорее, которая еще называлась тарабарской грамотой, все согласные буквы кириллицы располагались в два ряда. Зашифровывали письмо, заменяя буквы одного ряда буквами другого [3].

В эпоху Возрождения криптография переживает подъем. Начинается период формальной криптографии, связанный с появлением формализованных, более

надежных шифров. Над некоторыми загадками ученых Ренессанса криптографы последующих лет бились столетиями.

Около 1466 года итальянский ученый Леон Альберти изобретает шифровальный диск, состоящий из двух частей: внешней и внутренней. На неподвижном внешнем диске был написан алфавит и цифры. Внутренний подвижный диск также содержал буквы и цифры в другом порядке и являлся ключом к шифру. Для шифрования нужно было найти нужную букву текста на внешнем диске и заменить ее на букву на внутреннем, стоящую под ней. После этого внутренний диск сдвигался, и новая буква зашифровывалась уже с новой позиции. Таким образом, шифр Альберти стал одним из первых шифров многоалфавитной замены, основанных на принципе комбинаторики. Кроме того, Леон Альберти написал одну из первых научных работ по криптографии − «Трактат о шифрах».

Здесь стоит упомянуть такое явление, как стеганография, которому в работе Альберти также было уделено внимание. Если с помощью шифра пытаются утаить смысл информации, то стеганография позволяет скрыть сам факт передачи или хранения данных. То есть текст, спрятанный с помощью этого метода, вы примите за картинку, кулинарный рецепт, список покупок или, например, кроссворд. Или вообще не увидите его, если он будет написан молоком, лимонным соком или с помощью особых чернил. Часто методы стеганографии и криптографии объединялись в одном послании.

Прорывом в криптографии стала книга «Полиграфия» аббата Иоганеса Тритемия 1518 года, рассказывающая в том числе о шифрах с полиалфавитной заменой. Самым известным шифровальщиком XVI века считается дипломат и алхимик из Франции Блез де Виженер, придумавший абсолютно стойкий шифр, в котором использовалось 26 алфавитов, а порядок использования шифра определялся знанием пароля. Можно сказать, что шифр Виженера представлял собой комбинацию нескольких уже упоминавшихся шифров Цезаря.

Промышленная революция не обошла вниманием и криптографию. Около 1790 года один из отцов – основателей США Томас Джефферсон создал дисковый шифр, прозванный позже цилиндром Джефферсона. Этот прибор, основанный на роторной системе, позволил автоматизировать процесс шифрования и стал первым криптоустройством Нового времени. Большое влияние на шифровальное дело оказало изобретение телеграфа. Прежние шифры вмиг перестали работать, при этом потребность в качественном шифровании только возрастала в связи с чередой крупных военных конфликтов. В XIX-XX веках основные импульсы для развития криптографии давала именно военная сфера. С 1854 года британские военные применяют шифр Плейфера, в основе которого – шифрование биграмм, или пар символов. Этот шифр использовался до начала Второй мировой войны.

Во Второй мировой войне противники уже использовали мобильные электромеханические шифраторы, шифры которых считались нераскрываемыми. Устройства были роторными или на цевочных дисках. К первым относилась знаменитая машина «Энигма», которой пользовались нацисты, ко вторым – американская машина М-209.

Принцип работы «Энигмы» заключался в следующем: при каждом нажатии на клавишу с буквой алфавита в движение приходили один или несколько роторов.

Буква изменялась несколько раз по принципу шифра Цезаря, и в окошке выдавался результат. Шифры «Энигмы» считались самыми стойкими для взлома, так как количество ее комбинаций достигало 15 квадриллионов. Однако код «Энигмы» все же был расшифрован, сперва польскими криптографами в 1932 году, а затем английским ученым Аланом Тьюрингом, создавшим машину для расшифровки сообщений «Энигмы» под названием «Бомба». Комплекс из 210 таких машин позволял англичанам расшифровывать до 3 тыс. военных сообщений нацистов в сутки и внес большой вклад в победу союзников.

О советских шифровальных машинах известно мало, так как до последнего времени информация о них была засекречена. Например, до 1990-х годов в СССР и союзных странах использовалась роторная шифровальная машина «Фиалка». В отличие от «Энигмы» и других устройств, в ней использовались 10 роторов, а информация выводилась на бумажную ленту.

В 1949 году Клод Шеннон пишет работу «Теория связи в секретных системах», и криптография окончательно переходит в сферу математики. К концу 1960-х роторные шифровальные системы заменяются более совершенными блочными, которые предполагали обязательное применение цифровых электронных устройств. В 1967 году ученый Дэвид Кан издал популярную книгу «Взломщики кодов», которая вызвала большой интерес к криптографии.

С распространением компьютеров криптография выходит на новый уровень. Мощности новых устройств позволяют создавать на порядки более сложные шифры. Шифр или код становится языком общения между компьютерами, а криптография становится полноценной гражданской отраслью. В 1978 году разрабатывается стандарт шифрования DES, который стал основой для многих современных криптографических алгоритмов.

Сфера использования криптографии расширяется, при этом власти различных стран пытаются удержать контроль над использованием шифров. Разработки криптографов засекречиваются, от производителей шифровальных машин требуют оставлять в продуктах «черные ходы» для доступа спецслужб.

Параллельно независимые криптоаналитики разрабатывают способы шифрования, которыми могли бы пользоваться все желающие – так называемую открытую криптографию. Особенно актуально это стало с развитием интернета, где вопрос конфиденциальности информации встал очень остро. Первой криптосистемой с открытым ключом считается созданный в 1977 году алгоритм RSA, название которого является акронимом имен создателей – Риверста, Шамира и Адельмана. А в 1991 году американский программист Филипп Циммерман разрабатывает популярнейший пакет PGP с открытым исходным кодом для шифрования электронной почты.

Распространение доступного интернета по всему миру невозможно представить без криптографии. С появлением мессенджеров, социальных сетей, онлайн-магазинов и сайтов государственных услуг передача персональной информации в сети происходит без остановки и в огромных количествах. Сегодня мы сталкиваемся с криптографией ежедневно, когда вводим пароль от почтового сервиса, узнаем статус покупки онлайн или делаем денежный перевод через приложение банка. Криптография прошла гигантский путь от простых шифров древности к сложнейшим криптосистемам. Будущее этой науки творится на наших

глазах – очередная революция в шифровании произойдет с появлением квантовых суперкомпьютеров, разработка которых уже ведется.

Защита данных с помощью шифрования – одно из возможных решений проблемы безопасности. Зашифрованные данные становятся доступными только тем, кто знает, как их расшифровать, и поэтому похищение зашифрованных данных абсолютно бессмысленно для несанкционированных пользователей.

Наукой, изучающей математические методы защиты информации путем ее преобразования, является **криптология** [4,5]. Криптология разделяется на два направления – **криптографию** и **криптоанализ.**

Криптография изучает методы преобразования информации, обеспечивающие ее конфиденциальность и аутентичность.

Под **конфиденциальностью** понимают невозможность получения информации из преобразованного массива без знания дополнительной информации (ключа).

Аутентичность информации состоит в подлинности авторства и целостности.

Криптоанализ объединяет математические методы нарушения конфиденциальности и аутентичности информации без знания ключей.

Существует ряд смежных, но не входящих в криптологию отраслей знания. Так обеспечением скрытности информации в информационных массивах занимается стеганография. Обеспечение целостности информации в условиях случайного воздействия находится в ведении теории помехоустойчивого кодирования. Наконец, смежной областью по отношению к криптологии являются математические методы сжатия информации.

Современная криптография включает в себя четыре крупных раздела: симметричные криптосистемы, криптосистемы с открытым ключом, системы электронной подписи, управление ключами.

Основные направления использования криптографических методов – передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

В качестве информации, подлежащей шифрованию и расшифрованию, а также электронной подписи будут рассматриваться тексты (сообщения), построенные на некотором алфавите. Под этими терминами понимается следующее.

Алфавит – конечное множество используемых для кодирования информации знаков.

Текст (сообщение) – упорядоченный набор из элементов алфавита. В качестве примеров алфавитов, используемых в современных ИС, можно привести следующие:

− алфавит Z33 – 32 буквы русского алфавита (исключая "ё") и пробел;

− алфавит Z256 – символы, входящие в стандартные коды ASCII и КОИ 8;

− двоичный алфавит – $Z2 = \{0, 1\}$;

− восьмеричный или шестнадцатеричный алфавит.

Коды и шифры использовались задолго до появления ЭВМ. С теоретической точки зрения не существует четкого различия между кодами и шифрами. Однако в современной практике различие между ними является достаточно четким. Коды

оперируют лингвистическими элементами, разделяя шифруемый текст на такие смысловые элементы, как слова и слоги.

В шифре всегда различают два элемента: алгоритм и ключ.

Алгоритм позволяет использовать сравнительно короткий ключ для шифрования сколь угодно большого текста.

Определим ряд терминов, используемых в криптологии. Под шифром понимается совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, заданных алгоритмом криптографического преобразования.

Шифр – это совокупность инъективных отображений множества открытых текстов во множество шифрованных текстов, проиндексированная элементами из множества ключей: $\{Fk : X \rightarrow S, K \in K\}$.

Криптографическая система, или **шифр** представляет собой семейство T обратимых преобразований открытого текста в шифрованный. Членам этого семейства можно взаимно однозначно сопоставить число k, называемое ключом. Преобразование Tk определяется соответствующим алгоритмом и значением ключа k.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного варианта из совокупности всевозможных для данного алгоритма. Секретность ключа должна обеспечивать невозможность восстановления исходного текста по шифрованном.

Пространство ключей K – это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита.

Следует отличать понятия "ключ" и "пароль". Пароль также является секретной последовательностью букв алфавита, однако используется не для шифрования (как ключ), а для аутентификации субъектов.

Криптосистемы подразделяются на симметричные и асимметричные , или с открытым (публичным) ключом.

В симметричных криптосистемах для зашифрования и для расшифрования используется один и тот же ключ.

В системах с открытым ключом используются два ключа открытый (публичный) и закрытый (секретный), которые математически связаны друг с другом. Информация зашифровывается с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Термины распределение ключей и управление ключами относятся к процессам системы обработки информации, содержанием которых является выработка и распределение ключей между пользователями.

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и целостность сообщения.

Зашифрованием данных называется процесс преобразования открытых данных в зашифрованные с помощью шифра, а **расшифрованием** данных – процесс преобразования закрытых данных в открытые с помощью шифра [6]. Вместо

термина "открытые данные" часто употребляются термины "открытый текст" и "исходный текст", а вместо "зашифрованные данные" – "шифрованный текст".

Дешифрованием называется процесс преобразования закрытых данных в открытые при неизвестном ключе и, возможно, неизвестном алгоритме, т.е. методами криптоанализа.

Шифрованием называется процесс зашифрования или расшифрования данных. Также термин шифрование используется как синоним зашифрования. Однако неверно в качестве синонима шифрования использовать термин "кодирование" (а вместо "шифра" – "код"), так как под кодированием обычно понимают представление информации в виде знаков (букв алфавита).

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию. Обычно эта характеристика определяется периодом времени, необходимым для дешифрования.

Гаммирование – процесс наложения по определенному закону гаммы шифра на открытые данные.

Гамма шифра – псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму, для зашифрования открытых данных и расшифрования зашифрованных данных.

Имитозащита – защита от навязывания ложных данных. Для обеспечения имитозащиты к зашифрованным данным добавляется имитовставка, представляющая собой последовательность данных фиксированной длины, полученную по определенному правилу из открытых данных и ключа.

Криптографическая защита – это защита данных с помощью криптографического преобразования, под которым понимается преобразование данных шифрованием и (или) выработкой имитовставки.

Синхропосылка – исходные открытые параметры алгоритма криптографического преобразования.

Уравнение зашифрования (расшифрования) – соотношение, описывающее процесс образования зашифрованных (открытых) данных из открытых (зашифрованных) данных в результате преобразований, заданных алгоритмом криптографического преобразования [6,7].

Стандартные шифры

ROT1

Этот шифр известен многим. Ключ прост: каждая буква заменяется на следующую за ней в алфавите. Так, А заменяется на Б, Б — на В, и т. д.

Шифр транспонирования

В транспозиционном шифре буквы переставляются по заранее определённому правилу. Например, если каждое слово пишется задом наперед, то из hello world получается dlrow olleh. Другой пример — менять местами каждые две буквы. Таким образом, предыдущее сообщение станет eh ll wo ro dl.

Ещё можно использовать столбчатый шифр транспонирования, в котором каждый символ написан горизонтально с заданной шириной алфавита, а шифр создаётся из символов по вертикали. Примером может служить азбука Морзе (рис. 1).

h	e	l	l
o	w	o	r
l	d		

Рис. 1. Азбука Морзе

В азбуке Морзе каждая буква алфавита, цифры и наиболее важные знаки препинания имеют свой код, состоящий из череды коротких и длинных сигналов:

А •–	И ••	Р •–•	Ш ––––
Б –•••	Й •–––	С •••	Щ ––•–
В •––	К –•–	Т –	Ъ ––•––•
Г ––•	Л •–••	У ••–	Ы –•––
Д –••	М ––	Ф ••–•	Ь –••–
Е •	Н –•	Х ••••	Э ••–••
Ж •••–	О –––	Ц –•–•	Ю ••––
З ––••	П •––•	Ч –––•	Я •–•–

Чаще всего это шифрование передаётся световыми или звуковыми сигналами.

Моноалфавитная замена

Коды и шифры также делятся на подгруппы. Например, ROT1, азбука Морзе, шифр Цезаря относятся к моноалфавитной замене: каждая буква заменяется на одну и только одну букву или символ. Такие шифры очень легко расшифровываются с помощью частотного анализа.

Например, наиболее часто встречающаяся буква в английском алфавите — «E». Таким образом, в тексте, зашифрованном моноалфавитным шрифтом, наиболее часто встречающейся буквой будет буква, соответствующая «E». Вторая наиболее часто встречающаяся буква — это «T», а третья — «A».

Однако этот принцип работает только для длинных сообщений. Короткие просто не содержат в себе достаточно слов.

Представим, что есть таблица по типу той, что на рисунке (рис. 2), и ключевое слово «CHAIR». Шифр Виженера использует принцип шифра Цезаря, только каждая буква меняется в соответствии с кодовым словом.

В нашем случае первая буква послания будет зашифрована согласно шифровальному алфавиту для первой буквы кодового слова «C», вторая буква — для «H», etc. Если послание длиннее кодового слова, то для (k*n+1)-ой буквы, где n — длина кодового слова, вновь будет использован алфавит для первой буквы кодового слова.

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

Рис. 2. Шифр Виженера

Чтобы расшифровать шифр Виженера, для начала угадывают длину кодового слова и применяют частотный анализ к каждой n-ной букве послания.

Цифровые шифры

В отличие от шифровки текста алфавитом и символами, здесь используются цифры.

Двоичный код

Текстовые данные вполне можно хранить и передавать в двоичном коде. В этом случае по таблице символов (чаще всего ASCII) каждое простое число из предыдущего шага сопоставляется с буквой: 01100001 = 97 = «a», 01100010 = 98 = «b».

Шифр A1Z26

Это простая подстановка, где каждая буква заменена её порядковым номером в алфавите.

Основные способы шифрования (в кибербезопасности) [7-9]**:**

- Симметричное
- Асимметричное
- Хеширование
- Цифровая подпись

Симметричное шифрование — это способ шифрования данных, при котором один и тот же ключ используется и для кодирования, и для восстановления информации. До 1970-х годов, когда появились первые асимметричные шифры, оно было единственным криптографическим методом.

Принцип работы симметричных алгоритмов

В целом симметричным считается любой шифр, использующий один и тот же секретный ключ для шифрования и расшифровки.

Например, если алгоритм предполагает замену букв числами, то и у отправителя сообщения, и у его получателя должна быть одна и та же таблица соответствия букв и чисел: первый с ее помощью шифрует сообщения, а второй — расшифровывает.

Однако такие простейшие шифры легко взломать — например, зная частотность разных букв в языке, можно соотносить самые часто встречающиеся буквы с самыми многочисленными числами или символами в коде, пока не удастся получить осмысленные слова. С использованием компьютерных технологий такая задача стала занимать настолько мало времени, что использование подобных алгоритмов утратило всякий смысл.

Поэтому современные симметричные алгоритмы считаются надежными, если отвечают следующим требованиям:

Выходные данные не должны содержать статистических паттернов исходных данных (как в примере выше: наиболее частотные символы осмысленного текста не должны соответствовать наиболее частотным символам шифра).

Шифр должен быть нелинейным (то есть в шифрованных данных не должно быть закономерностей, которые можно отследить, имея на руках несколько открытых текстов и шифров к ним).

Большинство актуальных симметричных шифров для достижения результатов, соответствующих этим требованиям, используют комбинацию операций подстановки (замена фрагментов исходного сообщения, например букв, на другие данные, например цифры, по определенному правилу или с помощью таблицы соответствий) и перестановки (перемешивание частей исходного сообщения по определенному правилу), поочередно повторяя их. Один круг шифрования, состоящий из этих операций, называется раундом.

Виды алгоритмов симметричного шифрования

В зависимости от принципа работы алгоритмы симметричного шифрования делятся на два типа:

- блочные;
- потоковые.

Блочные алгоритмы шифруют данные блоками фиксированной длины (64, 128 или другое количество бит в зависимости от алгоритма). Если все сообщение или его финальная часть меньше размера блока, система дополняет его предусмотренными алгоритмом символами, которые так и называются дополнением.

К актуальным блочным алгоритмам относятся:

- AES
- ГОСТ 28147-89
- RC5
- Blowfish
- Twofish

Потоковое шифрование данных предполагает обработку каждого бита информации с использованием гаммирования, то есть изменения этого бита с помощью, соответствующего ему бита псевдослучайной секретной последовательности чисел, которая формируется на основе ключа и имеет ту же длину, что и шифруемое сообщение. Как правило, биты исходных данных сравниваются с битами секретной последовательности с помощью логической операции XOR (исключающее ИЛИ, на выходе дающее 0, если значения битов совпадают, и 1, если они различаются).

Потоковое шифрование в настоящее время используют следующие алгоритмы:

- RC4
- Salsa20
- HC-256
- WAKE

Достоинства и недостатки симметричного шифрования

Симметричные алгоритмы требуют меньше ресурсов и демонстрируют большую скорость шифрования, чем асимметричные алгоритмы. Большинство симметричных шифров предположительно устойчиво к атакам с помощью квантовых компьютеров, которые в теории представляют угрозу для асимметричных алгоритмов.

Слабое место симметричного шифрования — обмен ключом. Поскольку для работы алгоритма ключ должен быть и у отправителя, и у получателя сообщения, его необходимо передать; однако при передаче по незащищенным каналам его могут перехватить и использовать посторонние. На практике во многих системах эта проблема решается шифрованием ключа с помощью асимметричного алгоритма.

Область применения симметричного шифрования

Симметричное шифрование используется для обмена данными во многих современных сервисах, часто в сочетании с асимметричным шифрованием. Например, мессенджеры защищают с помощью таких шифров переписку (при этом ключ для симметричного шифрования обычно доставляется в асимметрично зашифрованном виде), а сервисы для видеосвязи — потоки аудио и видео. В защищенном транспортном протоколе TLS симметричное шифрование используется для обеспечения конфиденциальности передаваемых данных.

Асимметричное шифрование — это метод шифрования данных, предполагающий использование двух ключей — открытого и закрытого. Открытый (публичный) ключ применяется для шифрования информации и может передаваться по незащищенным каналам. Закрытый (приватный) ключ применяется для расшифровки данных, зашифрованных открытым ключом. Открытый и закрытый ключи — это очень большие числа, связанные друг с другом определенной функцией, но так, что, зная одно, крайне сложно вычислить второе.

Асимметричное шифрование используется для защиты информации при ее передаче, также на его принципах построена работа электронных подписей.

Принцип действия асимметричного шифрования

Схема передачи данных между двумя субъектами (А и Б) с использованием открытого ключа выглядит следующим образом:

Субъект А генерирует пару ключей, открытый и закрытый (публичный и приватный).

Субъект А передает открытый ключ субъекту Б. Передача может осуществляться по незащищенным каналам.

Субъект Б шифрует пакет данных при помощи полученного открытого ключа и передает его А. Передача может осуществляться по незащищенным каналам.

Субъект А расшифровывает полученную от Б информацию при помощи секретного, закрытого ключа.

В такой схеме перехват любых данных, передаваемых по незащищенным каналам, не имеет смысла, поскольку восстановить исходную информацию возможно только при помощи закрытого ключа, известного лишь получателю и не требующего передачи.

Применение асимметричных алгоритмов

Асимметричное шифрование решает главную проблему симметричного метода, при котором для кодирования и восстановления данных используется один и тот же ключ [10]. Если передавать этот ключ по незащищенным каналам, его могут перехватить и получить доступ к зашифрованным данным. С другой стороны, асимметричные алгоритмы гораздо медленнее симметричных, поэтому во многих криптосистемах применяются и те и другие.

Например, стандарты SSL и TLS используют асимметричный алгоритм на стадии установки соединения (рукопожатия): с его помощью кодируют и передают ключ от симметричного шифра, которым и пользуются в ходе дальнейшей передачи данных.

Также асимметричные алгоритмы применяются для создания электронных подписей для подтверждения авторства и (или) целостности данных. При этом подпись генерируется с помощью закрытого ключа, а проверяется с помощью открытого.

Асимметричные алгоритмы

Наиболее распространенные алгоритмы асимметричного шифрования:

- RSA (аббревиатура от Rivest, Shamir и Adelman, фамилий создателей алгоритма) — алгоритм, в основе которого лежит вычислительная сложность факторизации (разложения на множители) больших чисел. Применяется в защищенных протоколах SSL и TLS, стандартах шифрования, например в PGP и S/MIME, и так далее. Используется и для шифрования данных, и для создания цифровых подписей.
- DSA (Digital Signature Algorithm, «алгоритм цифровой подписи») — алгоритм, основанный на сложности вычисления дискретных логарифмов. Используется для генерации цифровых подписей. Является частью стандарта DSS (Digital Signature Standard, «стандарт цифровой подписи»).
- Схема Эль-Гамаля — алгоритм, основанный на сложности вычисления дискретных логарифмов. Лежит в основе DSA и устаревшего российского стандарта

ГОСТ 34.10–94. Применяется как для шифрования, так и для создания цифровых подписей.

- ECDSA (Elliptic Curve Digital Signature Algorithm) — алгоритм, основанный на сложности вычисления дискретного логарифма в группе точек эллиптической кривой. Применяется для генерации цифровых подписей, в частности для подтверждения транзакций в криптовалюте Ripple.

Надежность асимметричного шифрования

Теоретически приватный ключ от асимметричного шифра можно вычислить, зная публичный ключ и механизм, лежащий в основе алгоритма шифрования (последнее — открытая информация). Надежными считаются шифры, для которых это нецелесообразно с практической точки зрения [11]. Так, на взлом шифра, выполненного с помощью алгоритма RSA с ключом длиной 768 бит на компьютере с одноядерным процессором AMD Opteron с частотой 2,2 ГГц, бывшем в ходу в середине 2000-х, ушло бы 2000 лет.

При этом фактическая надежность шифрования зависит в основном от длины ключа и сложности решения задачи, лежащей в основе алгоритма шифрования, для существующих технологий. Поскольку производительность вычислительных машин постоянно растет, длину ключей необходимо время от времени увеличивать. Так, в 1977-м (год публикации алгоритма RSA) невозможной с практической точки зрения считалась расшифровка сообщения, закодированного с помощью ключа длиной 426 бит, а сейчас для шифрования этим методом используются ключи от 1024 до 4096 бит, причем первые уже переходят в категорию ненадежных.

Что касается эффективности поиска ключа, то она незначительно меняется с течением времени, но может скачкообразно увеличиться с появлением кардинально новых технологий (например, квантовых компьютеров). В этом случае может потребоваться поиск альтернативных подходов к шифрованию.

Хеширование информации

Хеширование, в отличие от симметричного и асимметричного шифрования, является односторонней функцией. Можно создать хеш из некоторых данных, но нет никакого способа, чтобы обратить процесс. Это делает хеширование не очень удобным способом хранения данных, но подходящим для проверки целостности некоторых данных.

Функция в качестве входных данных принимает какую-то информацию и выводит, казалось бы, случайную строку, которая всегда будет одинаковой длины. Идеальная функция хеширования создает уникальные значения для различных входов. Одинаковый ввод всегда будет производить одинаковый хеш. Поэтому можно использовать хеширование для проверки целостности данных.

Цифровая подпись

Цифровая подпись представляет собой комбинацию хеширования и асимметричного шифрования. То есть сообщения сначала хешируется, а после шифруется с помощью приватного ключа отправителя.

Получатель использует открытый ключ отправителя для извлечения хеша из подписи, затем сообщение снова хешируется для сравнения с извлеченным хешем.

Если вы точно знаете, что открытый ключ принадлежит отправителю и расшифровка открытого ключа прошла успешно, можете быть уверены, что сообщение действительно пришло от отправителя. Совпадение хешей говорит о том, что сообщение не было никак изменено.

Но не стоит забывать, что цифровая подпись не обязательно делает сообщение конфиденциальным. Цифровые подписи будут работать с зашифрованными сообщениями, но шифрование самого сообщения должно выполняться отдельно.

Интернет-безопасность: определение и описание

Интернет-безопасность – это безопасность действий и транзакций, совершаемых в интернете [12]. Интернет-безопасность входит в более широкие понятия, такие как кибербезопасность и компьютерная безопасность, и включает безопасность браузера и сети, а также правильное поведение в сети. Проводя значительное время в сети, можно столкнуться со следующими угрозами интернет-безопасности:

- Взлом – получение неавторизованными пользователями доступа к компьютерным системам, учетным записям электронной почты и веб-сайтам.
- Вирусы и вредоносные программы, которые могут повредить данные и сделать системы уязвимыми для других угроз.
- Кража личных данных, например, личной и финансовой информации злоумышленниками.

Частные лица и организации могут защититься от подобных угроз, используя приемы интернет-безопасности.

Распространенные угрозы интернет-безопасности

Чтобы сохранить конфиденциальность и безопасность в интернете, важно знать о различных типах интернет-атак. Ниже описаны распространенные угрозы интернет-безопасности.

Фишинг

Фишинг – это кибератака с использованием поддельных писем. Злоумышленники пытаются обмануть получателей электронной почты, убедив их в подлинности и актуальности сообщения. Например, они маскируют письма под запросы из банка или сообщения от коллег, чтобы пользователи переходили по ссылкам или открывали вложения. Цель атаки состоит в том, чтобы обманным путем заставить пользователей раскрыть личную информацию или загрузить вредоносные программы.

Взлом и удаленный доступ

Злоумышленники всегда стремятся использовать уязвимости частной сети или системы для кражи конфиденциальной информации и данных. Технология удаленного доступа предоставляет им дополнительные возможности. Программное обеспечение для удаленного доступа позволяет пользователям получать доступ к компьютеру и управлять им удаленно.

Протокол, позволяющий пользователям удаленно управлять компьютером, подключенным к интернету, называется RDP – протокол удаленного рабочего стола.

Многие компании, независимо от размера, широко используют RDP, поэтому высоки шансы недостаточно надежной защиты сети. Злоумышленники используют различные методы выявления и эксплуатации уязвимостей RDP, чтобы получить полный доступ к сети и ее устройствам.

Вредоносные программы и вредоносная реклама

Термин вредоносные программы охватывает все программы: вирусы, черви, трояны и прочие, которые злоумышленники используют для нанесения ущерба и кражи конфиденциальной информации. Любое программное обеспечение, предназначенное для повреждения компьютера, сервера или сети, может расцениваться как вредоносное.

Термин «вредоносная реклама» описывает онлайн-рекламу, распространяющую вредоносные программы. Интернет-реклама – это сложная экосистема, включающая веб-сайты рекламодателей, рекламные биржи, рекламные серверы, сети ретаргетинга и сети доставки контента. Злоумышленники используют эту сложность для размещения вредоносного кода там, где рекламодатели и рекламные сети не всегда могут его обнаружить. Пользователи, взаимодействующие с вредоносной рекламой, могут загрузить вредоносные программы на свое устройство или перейти на вредоносные веб-сайты.

Программы-вымогатели

Программы-вымогатели – это вредоносные программы, блокирующие использование компьютера или доступ к определенным файлам на компьютере, пока не будет уплачен выкуп. Они часто распространяются как троянские программы – вредоносные программы, замаскированные под легальные. После установки программа-вымогатель блокирует экран системы или определенные файлы до тех пор, пока злоумышленники не получат выкуп.

Ботнеты

Термин ботнет означает сеть компьютеров, специально зараженных вредоносным ПО с целью выполнения автоматических задач в интернете без разрешения и ведома владельцев этих компьютеров.

Когда компьютер управляется ботнетом, он может использоваться для выполнения злонамеренных действий. К ним относятся:

- Создание фальшивого интернет-трафика на сторонних веб-сайтах с целью получения прибыли.
- Использование компьютера для участия в распределенных атаках типа «отказ в обслуживании» (DDoS), вызывающих сбои в работе веб-сайтов.
- Рассылка спама миллионам пользователей интернета.
- Совершение мошеннических действий и кража личных данных.
- Атаки на компьютеры и серверы.

Компьютеры становятся частью ботнета так же, как и заражаются любой другой вредоносной программой: например, при открытии вложений электронной почты, загрузке вредоносных программ, посещении веб-сайтов, зараженных вредоносными программами. Ботнеты также могут передаваться с одного

компьютера на другой по сети. Количество ботов (зараженных компьютеров) в ботнете зависит от способности заражать незащищенные устройства.

Опасности в публичных и домашних сетях Wi-Fi

Использование публичных сетей Wi-Fi – в кафе, торговых центрах, аэропортах, отелях и ресторанах – сопряжено с определенными рисками, поскольку уровень безопасности в этих сетях часто низкий или защита полностью отсутствует. Это означает, что киберпреступники могут отслеживать действия пользователей в интернете и красть пароли и личную информацию. Другие опасности использования публичных сетей Wi-Fi включают:

- Прослушивание сети – злоумышленники отслеживают и перехватывают незашифрованные данные при передаче по незащищенной сети.
- Атаки типа «человек посередине» – злоумышленники взламывают точку доступа Wi-Fi и подключаются к процессу передачи данных между пользователем и точкой доступа с целью перехвата и изменения данных в процессе передачи.
- Мошеннические сети Wi-Fi – злоумышленники создают приманку в виде бесплатной сети Wi-Fi для сбора личных данных. Точка доступа злоумышленника служит каналом для всех данных, передаваемых по сети.

Слежка за домашней сетью Wi-Fi не должна вызывать столько беспокойства, поскольку сетевое оборудование принадлежит вам. Но опасность, тем не менее, существует: в США провайдерам интернет-услуг разрешено продавать данные о пользователях. Хотя эти данные являются анонимными, сам факт сбора данных может вызывать беспокойство у тех, кто ценит конфиденциальность и безопасность в интернете. Использование VPN в домашней сети значительно усложняет отслеживание вашей онлайн-активности.

Чтобы обеспечить безопасность в интернете и защитить свои данные, можно следовать перечисленным ниже рекомендациям.

Использование многофакторной аутентификации везде, где возможно

Многофакторная аутентификация – это способ проверки подлинности, при котором для доступа к учетной записи используется два или более метода проверки. Например, вместо простого запроса имени пользователя или пароля при многофакторной аутентификации запрашивается дополнительная информация:

- Дополнительный одноразовый пароль, который серверы аутентификации веб-сайта отправляют на телефон или адрес электронной почты.
- Ответы на личные вопросы безопасности.
- Отпечаток пальца или другая биометрическая информация, например голосовые данные или лицо.

Многофакторная аутентификация снижает вероятность кибератаки. Чтобы защитить онлайн-аккаунты, рекомендуется по возможности использовать многофакторную аутентификацию.

Использование сетевого экрана

Сетевой экран исполняет роль барьера между вашим компьютером и сетью, например интернетом. Сетевые экраны блокируют нежелательный трафик, а также помогают предотвратить заражение компьютера вредоносными программами. Часто сетевой экран входит в состав операционной системы или системы безопасности.

Для обеспечения максимальной безопасности в интернете рекомендуется убедиться, что сетевой экран включен и настроено автоматическое обновление.

Внимательное отношение к выбору браузера

Браузер – это основной инструмент для выхода в интернет, он играет ключевую роль в обеспечении безопасности в интернете. Хороший веб-браузер должен быть безопасным и обеспечивать защиту от утечки данных.

Создавайте надежные пароли и используйте менеджер паролей

Надежный пароль помогает обеспечить безопасность в интернете. Он обладает следующими свойствами:

- Длинный: минимум 12 символов, в идеале, даже больше.
- Содержит заглавные и строчные буквы, а также специальные символы и цифры.
- Не очевидный: в пароле не используются комбинации последовательных цифр (1234) и личная информация, которую может угадать тот, кто вас знает, например, дата рождения или имя домашнего животного.
- Не содержит запоминающихся сочетаний клавиш.

Замена букв и цифр похожими символами, например, “P@ssw0rd” вместо “password”, сейчас уже не является эффективной мерой – злоумышленники умеют обходить такую замену. Чем сложнее ваш пароль, тем сложнее его взломать. Использование менеджера паролей позволяет создавать, хранить и управлять всеми паролями с помощью единой защищенной учетной записи.

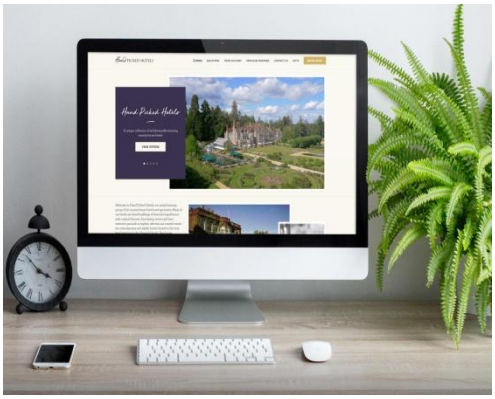
Пароли необходимо хранить в секрете, никому не сообщать и нигде не записывать. Рекомендуется не использовать один пароль для всех учетных записей, а также регулярно менять пароли.

В мире, где большая часть жизни проходит онлайн, безопасность в интернете и защита информации очень важна. Понимание того, как преодолевать угрозы интернет-безопасности и противостоять различным типам интернет-атак, является ключом к обеспечению безопасности и защите данных в интернете.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Википедия. Криптография
2. https://rostec.ru История шифровального дела
3. Википедия. История криптографии
4. https://kartaslov.ru Развитие криптографии, связанные понятия
5. https://sitekid.ru .Основные термины криптографии
6. https://intuit.ru Стандартные методы шифрования и криптографические системы
7. Википедия. Шифрование
8. https://wiki.hostpro.ua Типы методов шифрования
9. https://encyclopedia.kaspersky.ru Симметричное и Асимметричное шифрование
10. https://proglib.io Криптография и главные способы шифрования информации
11. kaspersky.ru Интернет-безопасность
12. Бабаш, А. В. История криптографии. Ч.1 - Изд-во Гелиос АРВ, 2002. 240с.

13. Баричев, С. Г. Основы современной криптографии - ». – М.: «Горячая линия – Телеком», 2001 – 120 с.
14. Кузьмин, Т. В. Криптографические методы защиты информации - Новосибирск: НГУ, 1997. — 44 с.



ВЕБ-ДИЗАЙН В ПРОФЕССИОНАЛЬНОЙ КУЛЬТУРЕ СОВРЕМЕННОГО ДИЗАЙНЕРА

К. М. Юнусова, С. М. Росин

Ивановский государственный политехнический университет

Аннотация. Рассмотрена актуальность преподавания основ дизайна сетевого информационного ресурса в системе современного художественного образования, анализируется состав основных его функций и задач. Перечислены основные стадии проектирования веб-сайта, кратко раскрыто их содержание. Феномен веб-дизайна рассмотрен в контексте культурной и профессиональной деятельности современного специалиста по художественному проектированию эстетического облика элементов предметной среды. На взгляд авторов, веб-дизайн оказывает существенное влияние на уровень эстетической культуры различных категорий современной Internet-аудитории, их визуальное мышление и мировосприятие.

Ключевые слова: дизайн, веб-сайт, стадии проектирования, Интернет-аудитория, эстетическая культура, визуальное мышление.

В настоящее время дизайн является востребованной и неотъемлемой частью любого проекта, изделия, упаковки и сайта [1]. В современной научной литературе дизайн рассматривается как «вид проектно-художественной деятельности, связанный с разработкой предметного окружения человека, систем визуальной коммуникации и информации, организацией жизни и деятельности человека на функциональных, рациональных началах». Как показывает практика, в структуре профессиональной деятельности дизайнер пользуется широким инструментарием проектных средств: техническое конструирование, композиционное формообразование, стилеобразование, функциональный анализ и разработка организационных, концептуальных моделей предметной среды. При этом арсенал проектных практик подчиняется выявлению общекультурного, художественно-образного понимания дизайнером всего комплекса проблем предметного мира и мира коммуникации.

Творческие умения, навыки и знания в сфере культуры и искусства являются основой в таких профессиональных отраслях как графический дизайн, цифровой дизайн, дизайн архитектурной среды и интерьера.

Одним из актуальных направлений цифрового дизайна является веб-дизайн, представляющий отрасль веб-разработки, основу которой составляет проектирование и создание пользовательских интерфейсов для различных сайтов и приложений. Цель современного дизайнера – научиться гармонично и эстетично визуализировать структуру сайта, максимально эргономично расположить информацию в удобной, доступной и понятной для пользователя форме.

В реализации творческих идей в веб-проектировании необходимы специальные базовые художественные навыки и знания в области

профессиональной и современной проектной культуры. Для формирования визуальной культуры дизайнеру необходимо знать современные информационные технологии, владеть специальными базовыми графическими программами: Adobe Photoshop, Adobe Illustrator, Corel Drow. При создании веб-сайта необходимо владение инструментарием проектной деятельности: композиция и ее средства, стиль, психология цвета, знаковая система, инфографика. Отсутствие данных знаний способствует неправильной подаче информации, некорректному размещению знаков навигации, в результате чего пользователю будет трудно найти нужную информацию и, соответственно, уменьшится посещаемость веб-страницы.

Профессиональный поиск в веб-проектировании связан с факторами стилеобразования. С точки зрения Т.Ю. Китаевской [2], стиль для веб-сайта представляет систему визуальных элементов, призванную обеспечить целостность восприятия как веб-сайта в целом, так и отдельной его страницы. Любой сайт должен быть единым по стилю, его блоки должны быть взаимосвязаны и представлять собой целостную картину. Одним из основополагающих нюансов стиля является эстетичное и логическое сочетание шрифтов, форм и цветовых сочетаний. В процессе проектирования веб-сайта также важно композиционное решение, грамотное размещение текста, изображений и элементов навигации.

В веб-дизайне проектирование принято разделять на определенные стадии: концептуальная стадия (выявление противоречия, формулирование и определение проблематики, определение целей, выбор критериев); стадия моделирования (построение, оптимизация моделей, выбор модели (принятие решения); стадия конструирования системы, стадия технологической подготовки.

При этом на концептуальной стадии проектирования необходимо учитывать целевую аудиторию пользователей, их возрастную категорию и возможные профессиональные интересы.

Создание веб-сайта требует глубокого изучения аналогов, траектории взаимодействия пользователей с интерфейсом, механизма построения и использования модульных сеток, а также исследования трендов и стилей современного дизайна. Для развития творческого мышления, культуры восприятия и успешного воплощения идей на практике дизайнеру нужно постоянно развивать навыки в создании различных аналогий образных решений в искусстве и дизайне. Так, на стадии моделирования происходит построение модульной сетки с учетом размеров разрешения нужных экранов (для компьютеров, планшета, мобильных телефонов), что требует профессиональных умений. Профессиональные компетенции дизайнера реализуются в композиционном размещении элементов, их цветовом сочетании, выборе шрифта, компоновке графических изображений, а также в выборе стиля. Дизайнер занимается разработкой новых композиционных приемов и поиском новых средств выразительности. На стадии конструирования системы все элементы объединяют в единую систему, выстраивают в определенном порядке, с учетом всевозможных отступов, размеров и форм. Также могут вноситься некоторые изменения, правки. На стадии технологической подготовки идет проверка дизайнерского макета сайта и подготовка его к верстке, в соответствии с определенными нормами и требованиями.

В связи со стремительным развитием информационных технологий возникает потребность в формировании знаний, умений и навыков посредством

визуализационных методов обучения [3]. В веб-дизайне одной из основных областей коммуникативного дизайна является инфографика.

Основу инфографики составляет графический способ четкой и быстрой подачи информации, что позволяет в упрощенной форме сделать акцент на важных моментах и фактах. В современных условиях инфографика направлена на решение таких задач как стремление к выразительности минимальными средствами, организация визуально-эстетической составляющей. Целью инфографики является оперативное информирование пользователей о фактах, проблемах, событиях.

Также в задачи инфографики входит: организация больших объемов информации, акцентуализация визуальных данных, визуальное представление различных фактов, ключевых моментов, наглядное пояснение трудного в восприятии материала, соотношение фактов и предметов во времени и пространстве, демонстрация конструкции предметов.

Существует два вида инфографики: статичная и динамичная. Статичная – самый распространенный вид графики (рисунок, схема, таблица). Динамичная – графика с применением анимированных элементов, позволяющая уместить больше информации в одном изображении. В основе любого вида инфографики лежит структурирование и схематизация, созданная в результате тщательной обработки информации и сочетающая в себе текст и графику.

Одним из современных и актуальных направлений в создании веб-графики сайта является анимационная графика. Анимированные эффекты часто применяют в рекламных целях, заставках, для создания движущихся композиций. Это делает сайт живым и более привлекательным. Для этого необходимо владеть такими графическими программами, как After Effects, Premiere Pro, 3ds Max.

В структуре современного веб-проектирования существуют три вида анимации в создании сайтов:

1. Gif-анимация – один из простых видов веб-анимации, где для отображения графических элементов браузеру не нужно подгружать сторонние плагины и расширения. Этот вид анимации является внедрением в структуру сайта графических элементов с последовательно сменяющимися картинками, каждая из которых имеет свой временной интервал.

Gif-анимации имеют небольшой размер и практически не влияют на скорость загрузки сайта, то есть загружаются всего один раз и не требуют постоянной связи с сервером. Минусом является невысокий уровень качества и плавности анимации.

2. Flash-анимация – реализуется с помощью средства Adobe Flash. Ее целью является привлечение внимания, акцент на стиль и динамическую визуализацию образа сайта.

Примером Flash-анимации служат flash-баннеры, открытки, электронные каталоги продукции, презентации и прочие элементы. Данный вид анимации требует установки библиотеки Flash-плеера.

3. Web-анимация с помощью java-скриптов, html5 и css3. Для её реализации на сайте не требуется установка дополнительных плагинов на компьютер, так как она реализуется движком браузера и не требует установки библиотеки flash-плеера. Сайты с данной анимацией намного быстрее загружаются и менее затратны в финансовом плане в сравнении с flash-анимацией.

Общие плюсы применения анимационной графики в создании сайтов: динамичность и подвижность, визуальное выделение из общей информации, акцентирование внимания на определенных элементах, активное взаимодействие пользователя с сайтом. Также существуют некоторые минусы при использовании flash-анимации: снижение скорости загрузки веб-страницы, для просмотра некоторых анимации требует установки flash-плеера в браузере. Но уже в настоящее время данный первый вид анимации утрачивает свою актуальность и постепенно заменяется третьим видом.

Интернет-культура является одной из моделей культуры общества, которая выражает систему ценностей современного общества. Веб-дизайн оказывает непосредственное воздействие на культуру пользователей, на их визуальное мышление и мировосприятие, на формирование целей и вкуса. В монографии «Дизайн как он есть» В.Л. Глазычев [4] отмечает: «Восприятие продукта дизайна включает эмоциональную реакцию не только от созерцания самого продукта, но и от собственных переживаний индивидуального потребителя по поводу продукта дизайна.

В то же время восприятие произведения массового искусства также включает целый комплекс эстетических, этических и иных эмоциональных реакций». Р. Арнхейм характеризовал визуальную культуру, как культуру восприятия и представления визуальной информации через художественное творчество. По его мнению, источником визуального мышления и восприятия является художественное творчество.

Развитию творческого мышления способствует обогащение культурного и художественного опыта посредством восприятия произведений искусства, дизайнерских работ высокого уровня, а также развитие способности переживать и «вживаться» в объекты искусства и дизайна, развитие способности креативно мыслить, генерировать интересные идеи и воплощать их посредством творчества на практике [3]. Для освоения визуальной культуры дизайнеру необходимо развивать умение анализировать визуальные образы, интерпретировать, оценивать, сопоставлять, представлять, создавать на этой основе индивидуальные художественные образы. Создаваемые дизайн-проекты призваны благоприятно влиять на психику человека, развивать уровень культуры человека, быть привлекательными с эстетической точки зрения, легко восприниматься, чтобы пользователю было удобно и приятно работать с веб-сайтом. Для любого дизайнера очень важна культурная составляющая его профессиональной деятельности, он должен быть компетентен и ответственен при выполнении дизайнерских проектов.

Рассмотрим типичный жизненный цикл веб-сайта:

1. Формирование идеи веб-сайта — на этом этапе происходит разработка концепции ресурса, определение аудитории, формируются общие принципы контентного наполнения.
2. Разработка бета-версии (или прототипа веб-сайта).

На этом этапе апробируются концепции и идеи первого этапа. Одной из наиболее важных задач данного этапа, является быстрое создание системы, выполняющей базовые и наиболее важные для разрабатываемого сайта функции. Предполагаемая, на этом этапе, нагрузка на систему — невысока, инвестиции на

данном этапе так же скромные, поэтому, как правило используются бесплатные системы разработки, системы хранения данных и т. п.

3. Продвижение созданного веб-сайта (рекламные усилия, продвижение через социальные сети и т. п.). Наращивание функционала, устранение существующих проблем и ошибок

4. Успех веб-сайта, резкое повышение нагрузки. Как следствие, редизайн системы хранения данных и доступа к данным, с сохранением пользовательских интерфейсов (модернизация подсистем хранения данных и подсистемы реализации бизнес — логики)

5. Модернизация визуальной подсистемы в соответствии с последними трендами. Все вышеперечисленные этапы в некоторой степени являются идеализированной моделью.

При этом разделение не три независимых функциональных части позволяет оптимальным образом разделять работы между различными группами разработчиков [4]. Так, обычно разделяют разработчиков, занимающихся пользовательскими интерфейсами (front side) и разработкой серверной части — бизнес-логикой и хранением данных (server side). В наиболее нагруженных проектах, так же отдельно выделяются группы разработчиков ответственные за поддержание и оптимизацию баз данных. Описанная выше модель дизайна веб-ресурсов сегодня используется повсеместно, как в коммерческих веб-проектах, так и в многочисленных решениях предназначенных для создания индивидуальных веб-ресурсов, например, таких, как система ведения блогов WordPress и многих других.

Проблемам создания “идеального” визуального дизайна веб-интерфейсов, посвящено, множество статей. Поэтому здесь мы не будем касаться данного аспекта. Поскольку на наш взгляд, сегодня, на первое место выходит не проблема создания “правильного” визуального дизайна веб-ресурса, а скорее проблема создания дизайна учитывающего новации пользовательского опыта доступа к веб-ресурсам с использованием множества новых устройств, таких как планшеты, смартфоны, смарт-телевизоры и другие устройства. Ключевой особенностью пользовательского опыта доступа в сеть интернет с этих устройств, является, то, что пользователи находятся в сети постоянно, в любое время суток. В пределе можно говорить о том, что они находятся в сети все 24 часа в сутки. Эта особенность коренным образом меняет пользовательское поведение, поскольку если раньше, активным пользователем сети интернет считался тот, кто, хотя бы раз в неделю проверял свою почту, то теперь это тот, кто проводит в сети все свободное время. Таким образом, визуальный дизайн современных успешных веб-ресурсов, в первую очередь должен быть ориентирован на инновационные устройства.

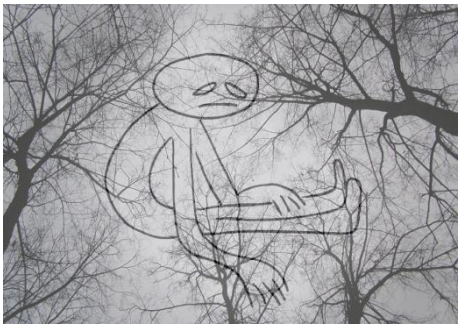
И должен учитывать, как существующие ограничения, так и имеющиеся возможности (высокое разрешение экранов устройств, наличие фото и видеокамер высокого разрешения, наличие различных датчиков и т. п.).

Таким образом, одно из ключевых требований к дизайну современных веб сайтов — размещение всей важной функциональности, в крайне ограниченном объеме, и максимально полная поддержка инновационных возможностей устройств [5]. При этом важно отметить, что сегодня в наличии у веб-разработчиков имеются подходящие инструментальные средства, позволяющие реализовывать предъявляемые к веб-ресурсам требования. Например, язык HTML 5 — позволяет

реализовать все вышеперечисленное и к тому же является гибкой и расширяемой спецификацией, что гарантирует добавление новых возможностей, появляющихся вследствие развития технологий в сфере пользовательских устройств.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Лаврентьев, А. Н. История дизайна. – Москва : Гардарики, 2007. – 303 с.
2. Китаевская, Т. Ю. Альтернативные стили в веб-дизайне // Вестник Томского государственного университета. – 2014. – № 2. – С. 569–570.
3. Батышев С. Я. Профессиональная педагогика / С. Я. Батышев, А. Н. Новиков. – Москва : Эгвес, 2009. – 456 с.
4. Глазычев, В. Л. Дизайн как он есть. – Москва : Европа, 2006. – 320 с.
5. Арнхейм, Р. Искусство и визуальное восприятие / сокращ. пер. с англ. В. Н. Самохина ; Прогресс, 1974. – 392 с.



КАК АПАТИЯ ВЛИЯЕТ НА УЧЕБНЫЙ ПРОЦЕСС

Корец С.

Ивановский государственный политехнический университет

Аннотация. Апатия часто возникает при учебном процессе. Оно затрагивает как студентов, так и преподавателей. Апатия — это безразличие и отсутствие эмоций. Само слово «апатия» происходит от греческого слова «pathos» — «эмоция, чувство, страдание», к которому добавляется префикс «а», вносящий значение отрицания. Часто апатия идет рука об руку с ангедонией — отсутствием радости и удовольствия от занятий, которые раньше радовали.

Ключевые слова: апатия, студенты, учителя, академическое выгорание.

Апатию рассматривают как одну из важных составляющих академического выгорания. Это хроническое заболевание, явление, когда человек не может сосредоточиться на учебе, постоянно отвлекается и не интересуется своими задачами. Это своего рода отрицательная кульминация многих недель или месяцев изучения одного и того же материала, или работы над одним и тем же проектом, или непрерывных лет обучения. Его не следует путать с однократным упадком сил, когда вы занимаетесь часами напролет, или с усталостью от бессонницы. Симптомы академического выгорания проявляются не только в усталости и ощущении, что вы не можете заставить себя пойти на очередное занятие — выгорание может вызвать настоящие психосоматические проблемы, такие как головные боли, бессонница и депрессия. К симптомам академического выгорания относятся:

- чувство истощения независимо от того, сколько вы спите, что приводит к усталости и бессоннице;
- отсутствие мотивации посещать занятия или начинать выполнение заданий;
- повышенная раздражительность;
- утрата уверенности в своих академических способностях;
- неспособность уложиться в важные сроки;
- головные боли, болезненные ощущения в мышцах или напряжение челюсти;
- более высокая частота заболеваний из-за стресса;
- увеличение количества вредных привычек, таких как переедание, слишком поздний отход ко сну, кусание ногтей и т.д;
- неспособность сосредоточиться на учебной работе;
- чувство скуки или отсутствие интереса к тем аспектам учебы или досуга, которые вам раньше нравились;

- тревожность или депрессия.

Социологическое исследование, проведенное среди самарских студентов, показало, что респонденты знают о социальной апатии и единодушны в том, что она существует среди студентов. [2] Однако не все участники исследования считают такое состояние типичным для студентов. Так несколько человек считают, что апатия – это временное психологическое состояние, обычно не свойственное студентам. У других позиция сводится к тому, что апатия среди студентов – это личная проблема. Третья позиция характеризует апатию как общественно-социальную проблему.

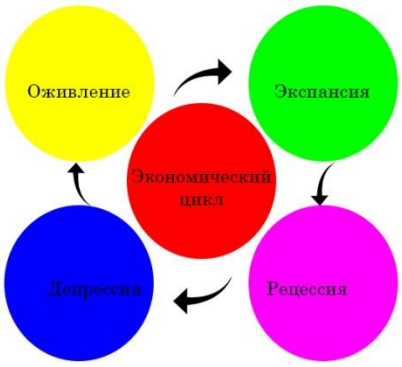
На вопрос о том, чем отличается поведение апатичного человека от неапатичного, были получены разнообразные ответы. [2] В обобщенном виде поведенческие черты апатичного человека, по мнению студентов, определяются эгоистическими устремлениями, замкнутостью, пониженным уровнем притязаний.

Но как я уже говорил, не только студенты склонны к апатии. Безынициативность и инфантилизм большинства учителей, связанные с профессиональными особенностями российских педагогов. Многочисленные исследования психологов показали, что постоянное выполнение своих профессиональных обязанностей накладывает сильный отпечаток на личность человека, который проявляется как специфическая профессиональная черта характера. [3] Современные российские учителя, по мнению исследователей, отличаются высокой исполнительностью и патерналистскими установками, однако при этом проявляют склонность к безразличному отношению к профессии и отсутствию самокритичности.

Вопрос о лечении апатии остается нерешенным. Применяемые для лечения депрессии антидепрессанты, по мнению ряда авторов, могут оказывать негативное влияние на апатические расстройства. В лечении апатии при когнитивных расстройствах применяются симптоматические противодементные препараты (ингибиторы ацетилхолинэстеразы и мемантин), а также психостимуляторы и агонисты дофаминовых рецепторов. Нефармакологические методы лечения также могут быть эффективны. [1]

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Вознесенская Т.Г. Синдром апатии //Научно-исследовательский отдел неврологии НИЦ Первого МГМУ им. И.М. Сеченова
2. Аргунова В.Н., Русь А.А. Проявления социальной апатии у студенческой молодежи // Вестник ПНИПУ. Социально-экономические науки. 2019. № 4. С.89-99. DOI: 10.15593/2224-9354/2019.4.7
3. Быкова Е.Ю. Специфика социальной апатии учителей // Вестник Томского государственного университета. – 2015. – № 394. – С. 84–91. DOI: 10.17223/15617793/394/14
4. Золотарева А.А. Диагностика предрасположенности к скуке: адаптация русскоязычной версии BPS-SR



ОСОБЕННОСТИ ЦИКЛИЧЕСКОГО РАЗВИТИЯ ЭКОНОМИКИ РОССИИ

А. А. Опарин

Ивановский государственный политехнический университет

Аннотация. Исследование цикличности развития российской экономики имеет свои особенности, поскольку хозяйственный опыт нашей страны содержит примеры формирования конъюнктурных колебаний в весьма специфических условиях системных трансформаций, в которых эволюционные изменения сочетаются с революционными преобразованиями социально-экономической сферы. В статье рассмотрены сущность и характер цикличности. Перечислены типы, виды и фазы (стадии) циклов, которые к настоящему времени различает экономическая наука; особое внимание уделено кризису. Исследована эволюция динамики экономических колебаний. Показано становление и развитие экономической теории циклов. Проанализировано влияние набирающего обороты экономического кризиса на экономику России.

Ключевые слова: развитие экономики, кризис, колебания, цикличность.

На первоначальном этапе необходимо отметить, что информационный обзор экономической учебной и научной литературы в сфере изучения сущности развития экономических циклов предоставляет два наиболее распространенных определения данного термина:

1) экономический цикл представляет собой колебания уровня экономической активности, когда периоды подъема сменяются периодами спада в экономике;

2) экономический цикл представляет собой процесс прохождения экономики от одной фазы до следующей и аналогично.

С точки зрения экономики, цикл – это периодические колебания уровня деловой активности, представленного реальным ВВП.

Рыночная экономика склонна к повторению из-за того, что экономика развивается ни как прямая линия, а постоянно отклоняясь от прямой, через спады и падения. Экономисты заметили это еще в первой половине 19 века. Исследуя различные процессы экономики, например такие, как: перепроизводство, кризисы. Ученые-экономисты выявили, что экономический цикл представляет собой периодические спады и подъемы в экономике, колебания деловой активности.

Обычно под цикличностью понимают периодичность повторяющихся отклонений в экономической системе, приводящих к упадку хозяйственной деятельности или же к спаду и кризису. Цикличность особенна чувствительна к воздействию со стороны государства на социально-экономические процессы. Циклический характер экономического развития в основном обусловлен нарастанием, обострением и разрешением внутренних противоречий экономической системы. К настоящему времени экономическая наука различает несколько типов циклов.

1. Годовые (самые элементарные), которые связаны с сезонными колебаниями под воздействием изменения природно-климатических условий и фактора времени.
2. Краткосрочные циклы, длительность которых, по оценкам, составляет 40 месяцев, то есть немногим более 3 лет, обусловлены якобы колебаниями мировых запасов золота. Этот вывод был сделан применительно к условиям господства золотого стандарта.
3. Среднесрочные, или промышленные, циклы могут иметь продолжительность в рамках 7–12 лет, хотя классический их тип охватывает примерно 10-летний период. Он сопряжен с многофакторной моделью нарушения и восстановления экономического равновесия, пропорциональности и сбалансированности народного хозяйства.
4. Строительные циклы охватывают 15–20-летний период и определяются продолжительностью обновления основного капитала. Данные циклы имеют тенденцию к сокращению под воздействием факторов НТП, вызывающих моральный износ оборудования и проведение политики ускоренной амортизации.
5. Большие циклы имеют продолжительность 50–60 лет; они вызываются главным образом динамикой НТП.

В анализе экономических систем активно используется «матрешечная» организация циклических процессов, при которой более короткие циклы включаются в состав более длинных циклов и, наоборот, из длинных циклов извлекаются короткие.

Экономический цикл делят на четыре фазы:

1. Рецессия. В этой стадии производство сокращается, темпы прироста становятся отрицательными, растет безработица и снижается совокупный спрос.
2. Депрессия. Национальный доход продолжает снижаться, но темпы падения замедляются, поэтому кривая темпов прироста «поворачивается» вверх.
3. Оживление. Переход от падения производства к его увеличению, постепенное возвращение экономики к состоянию, соответствующему равновесному росту.
4. Экспансия. Национальный доход растет, несмотря на полную занятость. Увеличивается спрос на инвестиции, безработица снижается ниже естественного уровня. Повышаются уровень цен, ставка заработной платы и ставка процента.

Наиболее сокрушительной и критической фазой промышленного цикла является кризис. Прежде всего, из-за неожиданности. До этого момента экономика находилась в фазе подъема, когда она процветала во всех отношениях.

Невозможность гарантированно спрогнозировать момент наступления кризиса обуславливается его разрушительностью. Обычные предприниматели, как правило, не бывают готовы к нему, поэтому протекание фазы кризиса носит обвальный, сокрушительный характер. Нарушается равновесие не в одной отдельной отрасли, а во всей экономике.

Следует подчеркнуть, что рынок оказывается переполненным товарами, спрос стремительно уменьшается, а производство продолжается, хотя товарные запасы опасно растут. Естественно, следует стремительное падение цен, разрушается механизм кругооборота капитала. Возникают кризис неплатежей и гигантский дефицит наличных денег. Производство хотя и запоздало, но быстро сворачивается. Курс ценных бумаг падает, они обесцениваются, векселям уже никто не верит. Начинается период крахов, ликвидации предприятий.

Естественно, резко возрастает ссудный процент. Возрастает безработица, достигая критической черты, а заработная плата падает. Когда прибыль падает, даже у крупнейших предприятий никто не думает о капитальных вложениях – их масштабы падают. Такую нерадостную картину представляет собой фаза кризиса.

Фаза депрессии следует за кризисом, для нее характерно «замораживание» экономики в том состоянии, в котором она оказалась в итоге кризиса. Эта фаза носит продолжительный характер, иногда бывает самой длительной по времени. При депрессии стремительно меняется на фоне общего застоя только величина ссудного процента. Она падает, поскольку у «выживших» капиталистов появляются свободные денежные средства в результате низких издержек производства, ведь заработная плата застыла на самой низкой точке.

Диалектика экономического развития заключается в том, что факторы кризиса становятся в фазе депрессии факторами перехода экономики на третью фазу – оживления. Дело в том, что в состоянии депрессии стабилизируются товарные запасы, цены. Низкие цены стимулируют потребление, спрос. И не только на предметы потребления. Кризис показал технологическую и техническую несостоятельность основного капитала. Начинается его замена – обновление капитала, которое означает, что началась фаза оживления, и производство берет медленный разгон.

Фаза оживления характеризуется, прежде всего, расширением производства средств производства. Следовательно, импульс оживления начинается с предприятий, производящих оборудование, элементы основного капитала. Производство расширяется вслед за ростом спроса, уменьшается безработица, растет заработная плата. Экономика берет стремительный разбег и переходит в фазу подъема. Критерием перехода экономики от оживления к подъему является достижение предкризисного уровня производства. Именно за ним начинается подъём.

Диагностика фаз экономического цикла является одной из наиболее сложных задач макроэкономического прогнозирования, разрешение которой связано с необходимостью совершенствования сбора и обработки статистической информации, построения комплексных индексов, а также с развитием методов экономико-математического моделирования.

В зависимости от характера экономических спадов, охвата ими различных сфер или отраслей народного хозяйства необходимо различать следующие виды экономических кризисов:

1. циклические кризисы — это периодически повторяющиеся спады общественного производства, вызывающие парализацию деловой и трудовой активности во всех сферах народного хозяйства и дающие начало новому циклу хозяйственной деятельности;

2. промежуточные кризисы — это спорадически возникающие спады общественного производства, которые на время прерывают стадии оживления и подъема национальной экономики. В отличие от циклических кризисов они не дают начало новому циклу, носят локальный характер и непродолжительны;
3. структурные кризисы связаны с постепенным и длительным нарастанием межотраслевых диспропорций в общественном производстве и характеризуются несоответствием сложившейся его структуры изменившимся условиям эффективного использования ресурсов. Такие кризисы вызывают долговременные потрясения и требуют для своего разрешения относительно длинного периода адаптации к изменившимся условиям процесса общественного воспроизводства;
4. частичные кризисы сопряжены с падением экономической активности в крупных отраслях. В частности, речь идет о денежном обращении и кредитах, банковской системе, фондовом и валютном рынках. Мировой валютный кризис 70-х годов, как известно, обусловил переход от Бреттон-Вудской валютной системы к Ямайскому (Кингстонскому) соглашению 1976 года, в соответствии с которым золото перестало играть роль мировых денег и превратилось в один из товаров. Хорошо известен и крупнейший кризис банковской системы в Германии 1932 года;
5. отраслевые кризисы характеризуются спадами производства и свертыванием хозяйственной деятельности в одной из отраслей промышленности, народного хозяйства;
6. сезонные кризисы обусловлены влиянием природно-климатических факторов, которые нарушают принятый ритм хозяйственной деятельности;
7. мировые кризисы охватывают как отдельные отрасли и сферы хозяйственной деятельности в планетарном масштабе, так и все мировое хозяйство.

В экономической теории по-разному объясняются причины цикличности развития:

- неоклассическое направление рассматривало кризисы как случайное, быстро проходящее явление;
- концепция недопотребления объясняла экономические кризисы перепроизводства бедностью трудящихся масс;
- в конце XIX века появилась кредитно-денежная концепция цикла, согласно которой кризисы — результат нарушений в области денежного спроса и предложения;
- марксистская концепция видит причину кризиса в противоречиях капитализма, в основном — между общественным характером производства и частнокапиталистической формой присвоения;
- кейнсианская теория объясняла причины отклонения системы от равновесия слабостью рыночного механизма и давала рецепты для государственного вмешательства в регулирование производства.

У современных экономистов существует три подхода к определению причин циклов.

Первый подход объясняет цикличность внешними (экзогенными) факторами. Внешние факторы — это явления, происходящие вне экономической системы. К ним относятся: изменения численности населения, изобретения и инновации, войны и другие политические события.

Второй подход ставит во главу угла внутренние (эндогенные) факторы. Внутренние факторы — это явления, происходящие внутри системы. К ним относятся: потребление, инвестирование и деятельность правительства.

Третий подход к определению причин цикличности синтезирует внутренние и внешние факторы. Авторы этой концепции считают, что внешние (экзогенные) факторы дают первоначальный толчок циклу, а внутренние (эндогенные) приводят к пофазным колебаниям. Это направление наиболее продуктивно.

Различные взгляды на причины циклических колебаний обуславливают и различные подходы к решению задачи их регулирования. Несмотря на многообразие точек зрения на проблему антикризисного регулирования, их можно свести к двум основным концепциям: кейнсианской и классической.

1. Сторонники кейнсианства, ориентируясь на совокупный спрос, основное внимание уделяют регулированию роли государства с его финансово-бюджетными инструментами, которые используются либо для сокращения или увеличения расходов, либо для манипулирования налоговыми ставками, сжатия или расширения системы налоговых льгот. Денежно-кредитная политика при этом играет вспомогательную роль.
2. Сторонники классиков концентрируют свое внимание на предложении. Речь идет об освоении имеющихся ресурсов и создании условий для эффективного производства, отказе в поддержке низкоэффективным производствам и секторам экономики и поощрении свободы действия рыночных сил.

Антициклическое регулирование представляет собой систему способов и методов влияния на хозяйственную конъюнктуру и экономическую деятельность, направленных на смягчение циклических колебаний. При этом государство действует в направлении, противоположном складывающейся экономической ситуации, на каждом этапе экономического цикла.

Несмотря на это, преодолеть циклический характер экономического развития государству не под силу; оно в состоянии только сглаживать циклические колебания в целях поддержания экономической стабильности.

Важнейшие мероприятия антикризисной политики в периоды бумов:

1) денежно-кредитная политика: повышение учетной ставки, продажа государственных ценных бумаг на открытом рынке;
2) фискальная политика: сокращение расходов госбюджета, повышение налоговых ставок;
3) политика заработной платы и тарифов: понижение заработной платы;
4) политика государственных инвестиций: затормаживание государственного строительства.

Важнейшие мероприятия антикризисной политики в периоды депрессий:

1) денежно-кредитная политика: понижение учетной ставки, покупка государственных ценных бумаг на открытом рынке;

2) фискальная политика: дополнительные расходы госбюджета, понижение налоговых ставок;
3) политика заработной платы и тарифов: повышение заработной платы;
4) политика государственных инвестиций: ускорение осуществления инвестиционных программ.

Можно сделать вывод, что в период подъема государство в целях предотвращения «перегрева» экономики проводит политику сдерживания деловой активности. А в период спада все мероприятия государства, напротив, направлены на ее стимулирование.

Рассмотрим особенности экономического кризиса, происшедшего в России в конце 80 — начале 90-х годов XX века. Оценивать данный кризис и пути выхода из него очень трудно, так как российская проблема экономического цикла «не вписывается» в известные теории.

Кризис в России сформировался по причине краха коммандитной системы в условиях рыночной недостаточности. На рубеже 80-90-х годов действовал рынок продавца, в котором покупатели конкурировали между собой за право приобретения товаров. Развал тоталитарной системы означал разрушение режима командной координации хозяйственных связей, который не был автоматически заменен координацией рыночного типа. Все это вызвало в стране хаос и, как следствие, спад производства.

Кризис 1992–1998 года в России — это самая крупная в истории человечества экономическая катастрофа отдельно взятой страны в мирное время. В годы Великой депрессии ни одна страна не потерпела такого ущерба от действительного циклического кризиса, как Россия от кризиса, порожденного государственной властью. Не углубляясь в анализ, укажу только на тот факт, что в течение двух лет (1992 и 1993) было приватизировано 70 % собственности государства. Причем приватизировались наиболее рентабельные предприятия, которые вскоре пополнили ряды убыточных. В последнее время много говорят о кризисе экономики в России, но положение теории о циклических кризисах к нему не относится. Данный кризис порожден распадом СССР и сообщества социалистических стран, разрывом производственных связей и единого хозяйственного комплекса; разрушением существовавших экономических форм, институтов до развертывания новых; оставшейся в наследство от социализма устаревшей морально и изношенной физически материально-технической базой производства; отсутствием политики защиты отечественного товаропроизводителя; перекосами в макроэкономических пропорциях бывшего СССР; непомерными налогами. В период снижения экономического роста обычно учащаются кризисные годы, соответствующие среднесрочному циклу, наблюдается более резкий и длительный спад производства. Современная волна понижения, как и предыдущие, сопровождается необходимостью структурной перестройки в традиционных отраслях и секторах мирового хозяйства, находящихся в состоянии длительного упадка и застоя.

В первой половине 1990-х годов темпы прироста ВВП и промышленного производства также оставались на более низком, чем в предыдущие, 1980-е годы, уровне, что подтверждает тенденцию отрицательной экономической динамики.

Несмотря на периодически проходившие среднесрочные циклические колебания, прослеживается положительная тенденция в экономическом развитии, характеризующаяся увеличением темпов роста ВВП.

Середина 1990-х гг. вплоть до 1997 года, характеризовалась небольшим приростом (в среднем 3%), но в целом картина не менялась. В 1998 году под воздействием международного финансового кризиса темпы прироста экономики оказались значительно ниже, чем в предыдущем году, и лишь в начале 1999 года было отмечено незначительное улучшение.

Для устойчивого развития страны Правительство Российской Федерации разработало «План первоочередных мероприятий по обеспечению устойчивого развития экономики и социальной стабильности». Этот план был направлен на активизацию структурных изменений в российской экономике, стабилизацию работы системообразующих организаций в ключевых отраслях и достижение сбалансированности рынка труда, снижение инфляции и смягчение последствий роста цен на социально значимые товары и услуги для семей с низким уровнем доходов, достижение положительных темпов роста и макроэкономической стабильности в среднесрочной перспективе.

Несмотря на столь значительный спад, уже в 1999 году российская экономика начала восстанавливаться. Главным стимулом экономического роста стал очень низкий курс рубля по отношению к ведущим мировым валютам, что очень положительно сказалось на производстве внутри страны и экспорте. Затем для страны наступила эра стабильного экономического роста. Стабильный экономический рост в эти годы стал возможен, в первую очередь, благодаря высоким ценам на нефть, в сочетании со структурными реформами, проведенными Правительством России в 2000–2001 годах. Рост ВВП стал причиной роста уверенности деловых кругов и простых потребителей в более благоприятном экономическом будущем России, вследствие чего, существенно увеличился приток иностранных инвестиций в экономику и практически прекратился отток капитала из страны. В 2017 году российская экономика после двух непростых лет вошла в новую фазу. На сегодняшний день темпы роста ВВП страны приближаются к 2%. Эксперты объясняют восстановление не только особенностями экономической политики последних лет, но и более глубинными процессами. В первую очередь, некоторые специалисты отмечают «затухание» переходного периода от планового к рыночному развитию, который стартовал в конце 1980-х – начале 1990-х годов прошлого века.

Итак, ВВП в расчёте на душу населения определяет уровень экономического развития государства. Рост ВВП на душу населения сигнализирует присутствие экономического роста, а также рост производительности труда.

Таким образом, можно сделать вывод, что циклические колебания в российской экономике могут влиять на показатели как положительно, осуществляя их рост, так и отрицательно, что показывает снижение рейтинга.

Объективно обусловленный переход к модели инвестиционно-интенсивного роста экономики России допустимо рассматривать как переход к завершающему циклу системных социально-экономических преобразований, начатых в 1990-х гг., как продолжение дезинвестиционного цикла 1991–1999 гг. и реконструктивного цикла 2000–2008 гг. в рамках понижательной, трансформационной волны большого

цикла. Весь период длительного системно-структурного кризиса российской экономики начиная с 1990-х гг. можно рассматривать как единый долгосрочный трансформационный цикл, состоящий из трех циклов: дезинвестиционного цикла, реконструктивного цикла и цикла перехода к новой модели экономического роста. Методологически подобный подход оправдан. В условиях социально-экономических трансформаций цикличность экономического развития модифицируется, приобретает переходный характер. Соответственно, модифицируется осуществление циклов конъюнктуры. В переходные периоды модифицируется реализация больших и среднесрочных циклов: изменяются хронологические параметры (длительность, стадийность - состав и последовательность протекания фаз цикла), набор и приоритетность взаимодействия факторов циклического экономического развития, форма осуществления цикла.

Цикличность экономического развития в современных условиях представляет собой совокупность макроэкономической, технологической и институциональной составляющих. Программные меры антициклического регулирования в экономике России должны включать в себя подходы, выработанные на основе анализа настоящего глобального кризиса и накопленного опыта развитых стран [1, с. 238].

Для перехода непосредственно к анализу антикризисной политики правительства последних лет необходимо рассмотреть особенности кризиса в России:

- падение суммы реально располагаемого дохода россиян: по данным Росстата, в 2015 году реально располагаемые доходы сократились на 7,7% по сравнению с 2014 годом [2, с. 96];
- реальные заработные платы россиян в 2015 году сократились на 9,8% по отношению к 2014 году [3];
- рост численности малоимущих граждан составил 8,3 млн человек: к концу первого квартала 2016 года насчитывалось 22,7 млн человек с доходами ниже прожиточного минимума, в то время как на конец 2015 года их число равнялось 14,4 млн человек [4, с. 43];
- ключевая ставка ЦБ РФ повысилась в декабре 2014 года с прежних 10,5% до 17%, что привело к обвалу валютного рынка и увеличению стоимости кредита;
- имел место сверхвысокий уровень инфляции цен: 15–16% в 2015 году. При этом саму инфляцию можно охарактеризовать как инфляцию издержек, при которой происходит одновременный рост цен и падение производства [5, с. 62].

При анализе сложившейся экономической конъюнктуры можно предположить, что именно неэффективная экономическая политика государства является источником проблем для экономики России.

Отметим, что под государственным антикризисным регулированием понимают государственную политику в сфере регулирования кризисных ситуаций, которая заключается в выработке и реализации стратегии развития государства и общества, направленной на преодоление кризисных ситуаций и обеспечение равновесного состояния институтов экономической и государственной системы. [6]

Государственное антикризисное регулирование предполагает проведение экономической политики по различным направлениям.

Антикризисная политика будет тогда эффективна и полезна только тогда, когда будет достигнут максимальный баланс между всеми её направлениями. Необходимо, чтобы между направлениями не возникало противоречий, а происходило активное взаимодействие друг с другом. Грамотная антикризисная политика требует ответственного подхода, взвешенности и трезвого расчета. Но, к сожалению, в полной мере реализовать такую модель невозможно. Например, при желании стимулировать средний и малый бизнес государство будет снижать налоговое бремя, однако при этом начнут сокращаться бюджетные ресурсы государства, тем самым и его возможности по оказанию адресной помощи другим субъектам экономики и бедствующим группам населения. Поддержка стратегически важных предприятий смягчает безработицу и другие социальные последствия кризиса, но может противоречить задачам реструктуризации и повышения эффективности производства. Рациональное и грамотное распределение ресурсов между тремя направлениями антикризисной политики зависит от ряда обстоятельств, наиболее важными из которых являются: экономический потенциал страны, объем наличных ресурсов, а также ожидания общества.

В экономике России необходима корректировка политики в плане смещения акцента с мер, которые нацелены на антикризисную поддержку отраслей, предприятий и населения, на меры, которые ориентируются на формирование нового промышленного потенциала, модернизацию, повышение качества человеческого капитала и в инфраструктуру России.

В России необходимо развивать «экономику предложения» и адекватную ей институциональную среду, предпринимая шаги по представленным направлениям:

- переход на расчеты с зарубежными партнерами в российских рублях за поставки углеводородного сырья [7];
- создание с другими развивающимися странами крупных фондовых и сырьевых бирж и, соответственно, сопутствующую им информационную инфраструктуру в виде собственных институтов профессиональной оценки;
- переориентировать процессы накопления золотовалютных резервов на целевое финансирование инновационной деятельности;
- обеспечивать проведение модернизации производственных мощностей и разработку новых видов деятельности с участием зарубежных партнеров [8].

Данные шаги поспособствуют продуктивности и эффективности в проведении в нашей стране антициклической политики. В результате проведения грамотной деятельности удастся достичь намеченных целей и встать на новый уровень развития.

Заключение. Итак, на основании изученных материалов можно сделать следующие выводы.

Экономические циклы — это важная составляющая экономического развития. Они существуют во взаимосвязи с объективными условиями. В связи с этим каждый цикл воссоздает те экономические условия, в которых он развивается.

В современных условиях изменяются также формы проявления циклов и кризисов. Это выражается, прежде всего, в синхронизации циклического движения в разных странах, в учащении циклических кризисов и сокращении

длительности цикла, в уменьшении глубины кризисов, а также в неустойчивости фаз оживления и подъема

Особенности циклических кризисов в современной экономике связаны с кризисом государственного регулирования, выразившимся в несостоятельности антициклической политики государства и недостатках практики государственного воздействия на циклическое воспроизводство.

Кризис государственного регулирования заставил развитые страны искать выход из сложившейся ситуации. Решение данной проблемы возможно было осуществить посредством перестройки форм кризиса и его методов.

Несмотря на разнообразие теорий о природе цикличности, на данный момент не выделены единые причины циклического развития экономики в разных странах.

Необходимо изучать причины цикличности и ее проявления в конкретной стране для того, чтобы суметь прогнозировать возможные экономические явления и вовремя предотвратить неблагоприятные последствия для дальнейшего развития экономики.

Таким образом, можно сделать вывод о том, что цикличность требует незамедлительного контроля и проведения антициклической политики со стороны государства. Только таким образом наша страна может выйти на новый уровень развития, повысив качество и уровень жизни своих граждан, а также предоставив все условия для нормального осуществления предпринимательской деятельности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1) Лавров С. Ю. Макроэкономическая технологическая и институциональная составляющие современного цикла Мир-системы // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2012. — № 51. — С. 236–241

2) Куркина Е. С., Куретова Е. Д. Математические модели эволюции мир-системы // Известия высших учебных заведений. Прикладная нелинейная динамика. – 2013. — Т. 21. – № 6. — С. 88–107.

3) Крючкова Е. Реальные зарплаты продолжат снижение. – URL: https://www.kommersant.ru

4) Лелюк Ю. Н. Особенности антициклического регулирования в контексте взаимосвязей экологической кривой кузнеца // Шумпетеровские чтения. – 2013. — № 1. — С. 41–44.

5) Жариков В. Д., Жариков Р. В., Жариков В. В. Формирование кластенов в инновационной экономике // Организатор производства. – 2013. — № 4. — С. 60–64

6) Потемкина И. А., Братушева В. А., Молдован А. А. Антикризисная политика правительства РФ за последние 5 лет. – URL: https://sibac.info (дата обращения 10.05.2019)

7) Приказчикова Ю. В. О необходимости инноваций на современном этапе развития государства. – URL: http://stroymnogo.com/2015 (дата обращения 12.05.2019).

8) Лавров С. Ю. Направления развития антициклической политики регулирования экономики России. – URL: http://stroymnogo.com

ДОМИНИРУЮЩИЕ ОШИБКИ МЫШЛЕНИЯ

Минеева А.А.

Ивановский государственный политехнический университет

Аннотация. В современном мире люди всё чаще задумываются о работе мозга, о возникновении мыслей, о том, как незаметно для себя раз за разом мы совершаем ошибки, которых могло бы и не быть, владея большей информацией. Именно поэтому необходимо знать как минимум о доминирующих когнитивных искажениях, которые могут стать отправной точкой для изменения мышления, а также о способах, применяемых для стабилизации восприятия и принятию конструктивных решений**.**

Ключевые слова: мышление, когнитивные искажения, стабилизация восприятия принятие конструктивных решений.

Для полноценного взаимодействия с обществом индивиду необходима оптимальная степень развития мышления. Востребованность формирования высокого психологического уровня в профессиональной, социальной и личностной сферах актуален в психологической практике, так как напрямую влияет на качество жизнедеятельности человека.

Анализ различных форм патологии мыслительной деятельности показывает правомерность признания специфичности человеческого мышления. Проблема мышления возникла как предмет психологии в начале 20-х гг. нашего века в вюрцбургской психологической школе. До нашего столетия Господствовавшая до этого ассоциативная психология не ставила перед собой проблемы анализа мыслительной деятельности. Мышление сводилось к "сцеплению" ассоциаций. Мышление являлось следствием развития: памяти, внимания, логики, а также природных компонентов.

Именно в современном мире люди начали изучать и анализировать работу мозга, появились теории о причинах возникновения мыслей, причинно-следственных связей. Тогда появляется самый актуальный вопрос: «Почему в эру компьютерных технологий и переполненности информацией, люди незаметно для себя совершают одни и те же ошибки, владея огромными объемами информации»? Возникновение данного вопроса в когнитивном психоанализе является отправной точкой и ключевым компонентом в решении множества потаенных ошибок в сознании человечества.

Целью работы будет являться выявление основных нарушений в психике человека, в частности патологий мышления, которые сопровождают индивида в повседневной жизни. Влияние подсознательных установок на качество психологического здоровья личности.

В качестве объекта исследования определим ошибки неразвитой системы суждений и оценки ситуации, изменение личности, а также воздействие на мировоззрение ложных когнитивных установок.

Предметом исследования являются внедрение когнитивных стратегий в повседневную жизнь, развитие стабильного психологического фона и способ устранения нежелательных функций мышления.

1. Мышление как понятие. В современном мире огромное количество курсов по изменению мышления. Кто-то относится к этому скептически, отрицая наличие проблем, кто-то понимает важность изменений, но не принимает никаких действий, чтобы изменить положение, а кто-то берет дело в свои руки и замечает изменения в своей жизни.

Более 50 лет назад, израильские психологи Амос Тверски (1937 – 1996) и Даниэль Канеман (1934) впервые ввели термин «когнитивное искажение», которому дали определение, что это своего рода систематические отклонение в поведении, восприятии и мышлении, обусловленное субъективными убеждениями, предубеждениями и стереотипами, сбоями в обработке и анализе информации, а также физическими ограничениями и особенностями строения человеческого мозга. Следует отметить, что из определения нельзя опускать слово «систематически», так как зачастую люди совершают одни и те же ошибки в различных ситуациях [1].

В отечественной психологии Лев Семенович Выготский изучал взаимосвязь между мышлением и речью. Основная суть данного исследования заключалась в том, что мысль зарождается в сознании, которое акцентирует свое «внимание» на важной для него сфере деятельности, по этой причине следует устранить тех или иных идей из ниоткуда. Немаловажно понимать, что в общении каждый человек интерпретирует смысл по-своему, а собеседник осознает сказанное со своей точки зрения, из этого возникают противоречия [2].

2. Патология мышления. Патологии мышления считаются одними из наиболее часто встречающихся признаков наличия психологических заболеваний. Нарушения мышления, встречающиеся в психиатрической практике, носят разнообразный характер. Некоторые из них характеризуются типичными для той или другой формы болезни. Однако общей классификации либо общего принципа рассмотрения данных расстройствотсутствуют. Вследствие этого при рассмотрении патологий мышления психологи основываются на разных теориях мышления, в различных методологических положениях.

Б.В.Зейгарник выделяла три типа патологии мышления [3]:

1. Нарушение операциональной стороны мышления
2. Нарушение динамики мышления.
3. Нарушение личностного компонента мышления.

В каждом отдельном случае могут быть определены несколько видов нарушения. Часто диагностируются наблюдаются сложные сочетания различных типов патологий. Они рассматриваются в легкой, умеренной или выраженной форме.

Нарушения операционной стороны мышления основываются на концепции определений, которые отражают действие в общих и абстрактных формах. Обобщение – результат анализа, отражающий существенные взаимосвязи между явлениями и объектами. Оно обозначает другой подход, вероятность определения

иных связей между объектами. С другой стороны, оно дает возможность определения взаимосвязи между самими понятиями.

При уменьшении степени обобщений оперирование общими свойствами заменяется установлением исключительно определенных связей между предметами. Клинически это выражается предрасположенностью к конкретизации мышления. Снижению уровня обобщений при искажении процесса обобщения соответствует отстранение суждений человека от, частных, отдельных связей. В суждениях отражаются только случайные и несущественные (латентные) признаки предметов или явлений. Процесс мышления представляет собой безосновательное рассуждение согласно определенным вопросам. Речь при этом становится вычурной.

Нарушения операциональной стороны мышления принимают различные формы. При всем их многообразии они могут быть сведены к двум крайним вариантам:

1. Снижение уровня обобщения
2. Искажение процесса обобщения.

К нарушениям динамики мыслительной работы причисляют лабильность и инертность мышления. При первом замечается непостоянность способа выполнения мыслительных операций, трансформация от одного к другому; при втором - тугоподвижность мышления, ригидность, трудности переключения.

Нарушения личностного компонента мышления выражаются разноплановостью мышления, уменьшением критичности и саморегуляции. Происходит потеря целенаправленности мыслительного процесса.

Общего принципа рассмотрения данных расстройств не существует. Основываясь на характеристики, вокруг которых группируются различные виды искажения мышления, обозначенные Б.В. Зейгарник.

В повседневной жизни, люди, не страдающие психическими отклонениями, сталкиваются с подобными патологиями. Для лечения данных нарушений не прописываются лекарства, а нужны действенные методы, помогающие с преодолением патологий.

3. Основные ошибки и их классификация. Ошибки в мышлении – это неверные методы оценки, рассмотрения, синтеза действительности. Данные ошибки препятствуют справедливому оцениваю действительности, совершению заключений, что приводит к отрицательным чувствам, неправильным поступкам.

К ошибкам мышления в современном психоанализе можно отнести: долженствование, ужастификация (катастрофикация), сверхобобщение, черно-белое мышление, атрибуция(сверхатрибуция).

Рассмотрим каждый термин по отдельности для полного понимания сути данного вопроса.

Долженствования. Оценивание действительности в стиле «Мне все должны» снимает ответственность с субъекта, поэтому, когда человек мыслит в таком стиле, он учитывает только один вариант событий. А так как мир многогранен, то, не учитывая другие возможности, человек не может проявить правильную реакцию на происходящие события. Это приводит к негативным эмоциям, неправильным поступкам, к напряжению и обострению отрицательных сторон личности. Здоровой альтернативой долженствования считается принятие изменчивости мира, который

не подчиняется правилам одного человека. В данном мышлении предусматриваются другие исходы событий и, как следствие, человек может рационально реагировать на события, которые идут не так, как он планировал.

Ужастификация. Данная ошибка приводит к завышенной оценке событий и, как следствие, психологическому напряжению и нерациональным решениям, которые могут усугубить ситуацию. Наличие данного мышлении у человека обозначает две градации для оценки: очень плохо (негативное) или нормально (нейтральное), и нет переходных делений. Альтернативой ужастификации является адекватная шкала оценивания условий события. Концентрация на уже произошедшем инциденте и осознанные действия, помогают справиться со сложившейся проблемой.

Сверхобобщения. Данный критерий основывается на способности человека из одной конкретной части события делать вывод, что и вся ситуация в целом аналогичная. При таком мышлении личность не способна смотреть на «картину» в общем, не владеет достаточным количеством информации, а обращает внимание на детали, препятствующие сосредоточению на полномерной оценке действительности, что приводит к поспешным выводам и неправильным действиям. Иной подход к свехобобщению является системное мышление, то есть анализ всех частей события.

Черно-белое мышление. Мышление, при котором индивид видит только черное, или только белое, и не способен заметить переходные тона. Принимая решение, личность выбирает всё или ничего, что является когнитивным искажением. Следствиями подобного мышления являются либо состояния уныния, депрессии, когда не видно ничего позитивного, либо наоборот, эйфории, когда игнорируются и не решаются трудности. Зрелая личность отличается способностью видеть в ситуации как положительные, так и негативные стороны, обретая равновесие и контроль над проблемой.

Сверхатрибуция (приписывание причин). Ошибкой данного мышления считается то, что личность по какому-то внешнему показателю сразу делает вывод о причине. Данная фундаментальная ошибка, приводит к переоцениванию личностных качеств и недооцениванию внешних факторов.Таким образом, индивид, оказавшись перед сложившейся трудностью, начинает оценивать субъективно ситуацию, основываясь на своем личном мировоззрении.Человек со зрелым мышлением не делает умозаключения о причине на основании одного случая, а если ему необходимо понимать первопричину, он ее устанавливает.

4**. Правило «ООО».** При выявлении данных ошибок, мешающих критическому мышлению, существует правило «ООО». В практической деятельности для корректировки мышления может помочь принцип «Осознанность, Ответственность, Оценка». Осознанность – следует лучше понять свою личность путем самоанализа, изучить свои слабые и сильные сторон, а также особенности внутреннего состояние личности. Ответственность – взять ответственность за свое мышление на себя. Оценка – провести анализ рисков, дать оценку подобного мышления в данной конкретной ситуации, неправильность данного мышления, и какое мышление будет максимально разумным в условиях конкретной ситуации. Пользуясь данной техникой, можно избежать доминирующих ошибок в мышлении

[4]. Примеры осознанных действий при преобладающих ошибках мышления указаны в таблице 1.

Таблица 1

Альтернативная реакция на совершаемые ошибки

Доминирующие ошибки мышления	Примеры неправильного мышления	Примеры зрелого мышления
Атрибуция	У меня ничего не получается, значит я плохой.	Если сейчас что-то не получается, это не означает я плохой.
	Я бросил пагубные привычки уже месяц, значит я уже выздоровел.	То, что у меня нет тяги и мыслей о зависимости, еще ничего не означает.
Черно-белое мышление	В том, что я закончил этот ВУЗ нет ничего хорошего.	Возможно, я не буду работать по специальности, зато я приобрёл знания в другой сфере.
Черно-белое мышление	У меня никогда не получится это сделать	Я могу обратиться за помощью к профессионалу, который поможет сделать мне это.
Утверждения долженствования	Ты должна закончить университет с красным диплом.	Ты имеешь право закончить университет как с красным диплом, так и с синим.
	Ты не можешь себя так вести и так одеваться.	Я другая. Я имею право делать так как лучше мне, не нанося вреда другим.
Катастрофизация/ ужастификация	Я случайно порвал куртку, меня мама убьёт за это.	Мама меня даже ругать не будет, ведь это всего лишь вещь, которую можно купить.
	Со мной случилось нечто ужасное.	Произошедшее мало приятно, но на самом деле не смертельно.
Обобщение	У меня получилось выиграть в игре, значит в следующий партии победа будет ещё легче.	Мне не стоит делать предположений о следующей игре, только потому что мне удалось выиграть эту партию.
	Я уже пробовал научиться плавать и у меня ничего не вышло, значит я никогда не смогу научиться плавать.	В прошлый раз у меня ничего не вышло, но если я приложу усилия и наберусь терпения, то обязательно научусь плавать.

В результате проделанной работы были выявлены доминирующие ошибки мышления. Классифицируя данные ошибки, были выявлены пять компонентов, которые подавляли психологическую стабильность и развитие личности в целом.

На основании полученных данных была разработана стратегия оптимального развития и устранения нежелательных особенностей мышления, посредством практики правила «ООО», которая направлена на улучшение качества жизни человека, вне зависимости от специфичности мышления.

Проанализировав доминирующие ошибки мышления, были выявлены ключевые моменты, препятствующие рациональному осмыслению ситуации, грамотной оценки проблемы и комплексному решению поставленного вопроса

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Добелли Р. Искусство ясно мыслить. М.: МИФ, 2020. 244 с.
2. Выготский Л.С. Мышление и речь. М.: Лабиринт, 1999. 352 с.
3. Зейгарник Б.В. Патопсихология: Учеб. Пособие для студ. Высш. Учеб. заведений. - 2-е изд., стереотип. - М.: Академия, 2002
4. Кобанкова А.А. Доминирующие ошибки мышления / Пятигорский государственный университет – URL: https://www.elibrary.ru/download/elibrary_46400081_75443856.pdf (дата обращения 23.12.2021)