

В области интернета вещей интеллектуальный мониторинг помогает обнаруживать аномалии в работе устройств и предотвращать возможные сбои. Он позволяет отслеживать и анализировать данные, поступающие от устройств, чтобы выявлять необычное поведение или отклонения от нормы. Такой мониторинг может быть полезен для предотвращения сбоев в работе устройств и обеспечения более надежной работы интернета вещей.

Примеры использования интеллектуального мониторинга в интернете вещей [4,5]:

- Отслеживание и анализ данных, поступающих от устройств, чтобы выявлять аномалии и предотвращать возможные сбои.

- Обнаружение необычного поведения устройств, которое может указывать на проблемы или угрозы безопасности.

- Предупреждение о потенциальных проблемах или отклонениях от нормы, чтобы принять меры по их устранению до возникновения серьезных проблем.

- Оптимизация работы устройств и повышение их эффективности на основе анализа данных.

- Улучшение надежности и безопасности системы интернета вещей путем раннего обнаружения и предотвращения возможных сбоев.

В данной статье были рассмотрены основные аспекты интеллектуального мониторинга для анализа сетей. Интеллектуальный мониторинг является эффективным инструментом для обнаружения и предотвращения сетевых угроз, а также для оптимизации работы сети. Он позволяет проводить анализ данных в режиме реального времени, а также прогнозировать и предотвращать возможные проблемы. Примеры успешной реализации интеллектуального мониторинга в различных сферах подтверждают его важность и актуальность. В заключении делается вывод о необходимости использования интеллектуального мониторинга для обеспечения безопасности и эффективности работы сетей.

#### Список литературы

1. Артюшевский Р.В. О возможностях интеллектуализации в системах связи // Интеллектуальные информационные системы: тенденции, проблемы, перспективы: сборник научных статей 8-й Международной научно-практической конференции «ИИС-2020», Курск, 18 декабря 2020 г. Курск: Юго-Западный государственный университет, 2020. С. 17-19.

2. Двуреченская Е.О. Проблемы обработки информации в распределенных интеллектуальных системах // Интеллектуальные информационные системы: тенденции, проблемы, перспективы: сборник научных статей 8-й Международной научно-практической конференции «ИИС-2020», Курск, 18 декабря 2020 г. Курск: Юго-Западный государственный университет, 2020. С. 51-53.

3. Львович Я.Е. Проблемы интеллектуализации сетей нового поколения // Интеллектуальные информационные системы: тенденции, проблемы, перспективы: сборник научных статей 8-й Международной научно-практической конференции «ИИС-2020», Курск, 18 декабря 2020 г. Курск: Юго-Западный государственный университет, 2020. С. 136-139.

4. Белых В.С., Ткаченко А.В. Современные методы тестирования программных продуктов на основе искусственно-

го интеллекта // Интеллектуальные информационные системы: тенденции, проблемы, перспективы: сборник научных статей 8-й Международной научно-практической конференции «ИИС-2020», Курск, 18 декабря 2020 г. Курск: Юго-Западный государственный университет, 2020. С. 25-26.

5. Загоруйко Д.А., Ткаченко А.В. Искусственный интеллект // Интеллектуальные информационные системы: тенденции, проблемы, перспективы: сборник научных статей 8-й Международной научно-практической конференции «ИИС-2020», Курск, 18 декабря 2020 г. – Курск: Юго-Западный государственный университет, 2020. С. 67-68.

### ВЛИЯНИЕ ТИПОГРАФИКИ НА ВОСПРИЯТИЕ ИНФОРМАЦИИ В ЦИФРОВОЙ СРЕДЕ

Попов Т.И.

*Мелитопольский государственный университет,  
Мелитополь, e-mail: mr4bread263@gmail.com*

В современном мире, самым распространённым способом восприятия информации всё ещё является чтение текста. По этой причине, важно уметь правильно оформлять текст для удобства навигации в массивах информации. Это также жизненно необходимо для сайтов и рекламы в интернете, если пользователю будет некомфортно читать текст на сайте, то повышается вероятность, что он уйдёт с него.

Целью данной работы является исследование влияния типографики на восприятие информации в цифровой среде. Была поставлена задача – узнать, как сильно влияет соблюдение правил типографики на комфорт чтения и желание остаться на сайте у пользователей.

Актуальность темы обусловлена тем, что понимание влияния типографики может помочь создателям контента, дизайнерам и другим специалистам в области цифровых технологий улучшить качество и доступность информационных продуктов, а также удержать внимание читателей.

#### Методология

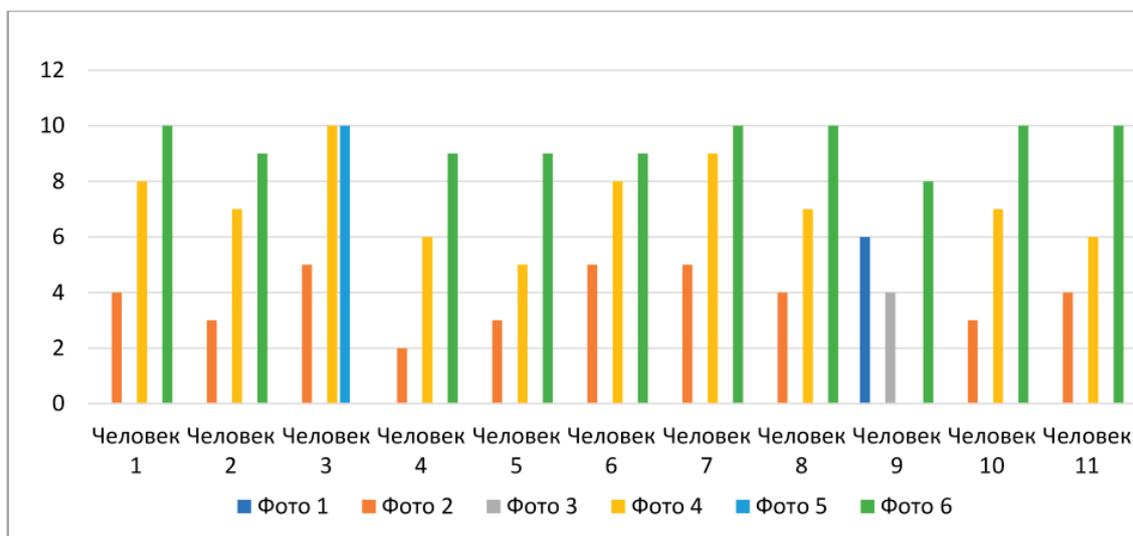
Исследование будет базироваться на базовых типографических правилах и их влияний на самом тексте. Для исследования будет составлен текст, что изменяется в ходе эксперимента, а контрольная группа будет оценивать его по нескольким критериям:

- 1) Скорость чтения;
- 2) Оценка комфорта чтения;
- 3) Понимание содержания текста.

Для обеспечения достоверности результатов, каждый участник контрольной группы будет оценивать один и тот же текст с различными типографическими параметрами. Это позволит нам увидеть, как изменения в типографике влияют на восприятие информации каждым конкретным участником.

В исследовании будут использоваться правила близости и схожести, принципы иерархии, шрифтовой пары и понятие ритма.





Статистика выбора испытуемыми

1) Правила близости и схожести: Правило Близости гласит, что элементы, расположенные рядом, воспринимаются как связанные. Схожесть, с другой стороны, относится к визуальному сходству элементов, таких как шрифт, цвет или размер.

2) Принципы иерархии: Иерархия в типографике упорядочивает текстовые элементы в зависимости от их важности. Основной подход состоит из трех уровней: доминирующий заголовок, подзаголовок и основной текст.

3) Шрифтовая пара: Шрифтовая пара – это два шрифта, которые используют в дизайне для оформления текстов на одном пространстве: для заголовка и основного текста. Они должны гармонично сочетаться друг с другом и решать дизайнерские задачи.

4) Понятие ритма: В контексте типографики, ритм относится к повторяющимся элементам в тексте, которые создают визуальное движение или “поток”.

### Исследование

Опрашиваемые в 3 парах фотографий выбирают фото с самым комфортным текстом.

1) Изначальное фото 1 представляет не отредактированный текст, написанный шрифтом Roboto, что идёт одним потоком размером 12px.

2) Текст на фото 2 разделён на части и заголовки, что связаны с текстом, появляется слабая иерархия.

3) Во второй паре, испытуемые выбирают между прошлым вариантом и 4-м фото, здесь мы усилили иерархию с помощью увеличения веса заголовков, повысив размер до 14px, изменив жирность на Bold. Также, мы подобрали к Roboto шрифтовую пару подвида Serif – Playfair Display. Этот популярный вариант

комбинации строгого геометрического и шрифта с заческами, создают контраст между заголовками и основным текстом повышая уровень порядка в тексте.

4) 3-я пара: выбор между фото 5 и фото 6. На фото 6 мы задействовали правило схожести, близости и ритма. Пробелы между текстом стали одинаковы, а заголовки приблизились к тексту.

### Результаты исследования

В опросе участвовало 11 человек, на основе выбора этих людей, мы получили статистику (рисунок).

Результаты исследования подтвердили значимость соблюдения правил в типографике. Совместив оценки из категорий: Скорость чтения, оценка комфорта чтения, понимание содержания текста. Мы получили оценки каждого фото, что было выбрано из пары. Большинство людей придают большое значение комфорту чтения и не станут читать запутанные и некомфортные текста, это можно убедиться по выбору фотографий, где мы больше соблюдали правила типографики.

### Вывод

Для создателей контента, дизайнеров и других специалистов в области цифровых технологий важно уделить должное внимание типографике при оформлении текста. Это поможет не только улучшить восприятие информации, но и увеличить вероятность того, что пользователь останется на сайте, что особенно важно в условиях современного информационного пространства. Это подчеркивает необходимость дальнейшего изучения этой темы и разработки новых подходов к оформлению текста с учетом типографических правил.

### Список литературы

1. Правило близости и схожести [Электронный ресурс]. URL: <https://typographyhandbook.com/> (дата обращения: 15.10.2023).
2. Иерархия [Электронный ресурс]. URL: <https://vansedesign.com/web-design/visual-hierarchy/> (дата обращения: 25.10.2023).
3. Шрифтовая пара [Электронный ресурс]. URL: <https://www.learnui.design/blog/guide-pairing-fonts.html> (дата обращения: 18.10.2023).
4. Ритм [Электронный ресурс]. URL: <https://www.thoughtco.com/rhythm-design-principle-3470054#:~:text=As%20a%20principle%20of%20design%2C%20rhythm%20is%20also,Our%20senses%E2%80%94and%20therefore%2C%20the%20brain%E2%80%94respond%20to%20rhythm%20positively> (дата обращения: 17.10.2023).

## ПОДХОД К РЕАЛИЗАЦИИ ВЕБ-ПРИЛОЖЕНИЙ НА ОСНОВЕ КЛИЕНТ-СЕРВЕРНОЙ АРХИТЕКТУРЫ, ОБЕСПЕЧИВАЮЩИЙ ЗАЩИЩЕННЫЙ ОБМЕН ДАННЫМИ

Сверчков Р.В.

*ФГБОУ ВО «Российский экономический  
университет имени Г.В. Плеханова»,  
Москва, e-mail: rvsverchkov@gmail.com*

В настоящее время в работе бизнеса различных отраслей стали очень распространены веб-приложения [2, с. 39], которые во многом повторяют логику и устройство аналогичных продуктов компаний, разработанных для какой-либо конкретной операционной системы. Такая ситуация также наблюдается во многих сферах, особенно там, где требуется обеспечение доступа к разработанному программному обеспечению практически с любого устройства, имеющего выход в интернет. Однако из-за такого подхода по созданию полностью аналогичных приложений не учитываются многие особенности работы интернет-браузеров, которые в свою очередь создают множество потенциальных возможностей для воздействия на данные со стороны злоумышленников [1, с. 60], а также необходимость создания корректного контроля доступов, тем самым ограничивая область действий потенциального пользователя. Данная проблема является как никогда актуальной сейчас, поскольку теперь практически любое программное обеспечение имеет свой аналог в виде веб-приложения и многие из них подвержены воздействию злоумышленников.

### Текущие проблемы при использовании и разработки веб-приложений

Из-за того, что при разработке веб-приложений зачастую не учитывают их ключевые особенности, а именно то, что в силу своего строения доступ к ним может быть получен буквально с любого устройства, имеющего интернет-браузер, и у компаний, которые решают проводить полномасштабную интеграцию та-

ких решений в свою корпоративную сеть, может возникнуть множество неочевидных проблем.

Одной из таких проблем является некорректная настройка маршрутизации в итоговом продукте, позволяющая потенциальным пользователям, не имеющим необходимого уровня доступа с помощью прямых ссылок просматривать ресурсы, доступ к которым для них не предусмотрен. Такие ошибки в проектировании практически всегда достаточно дорого обходятся компании, если доступ к таким ресурсам был получен недобросовестным пользователем, который в свою очередь можем поделиться данной уязвимостью с третьими лицами и тем самым подвергнуть колоссальному риску расположенную там информацию.

Вместе с этим также стоит упомянуть, что немаловажную опасность представляет собой недостаточная фильтрация входящей информации в базу данных, расположенную на сервере. Это связано в первую очередь с тем, что потенциальный нарушитель способен ввести в форму какой-либо SQL-запрос и получить в ответ необходимую конфиденциальную информацию из базы. Такая атака называется инъекцией, и она может причинить большой ущерб практически любому продукту, в частности если соответствующая фильтрация или валидация данных вовсе отсутствует.

Также имеется риск некорректной проектировки архитектуры веб-приложения, как пример разрешение пользователям загружать файлы любого формата без какой-либо проверки со стороны клиента, тем самым повышается шанс эксплуатации такой уязвимости со стороны злоумышленников, способных развернуть на стороне сервера исполняемый файл с каким-либо вредоносным кодом.

Стоит также упомянуть, что в большинстве случаев во время разработки веб-приложений редко уделяется достаточное время построению безопасной конфигурации самого приложения и из этого как раз вытекает множество проблем, напрямую связанных с общим уровнем безопасности. В такой ситуации, когда текущие настройки веб-приложения или же сервера не отвечают должным требованиям безопасности, колоссальным образом возникает риск утечки данных или же вовсе компрометации связей логинов и паролей для доступа к административным панелям со стороны серверной части или чего-либо еще.

Использование уязвимых или же вовсе устаревших компонентов также может сильно повлиять на общий уровень веб-приложения. Такая проблема возникает, когда в разработке применяются непроверенные фреймворки или же сторонние решения, уже имеющие в своем исходном коде ошибки безопасности. Злоумышленники же могут воспользоваться достаточно распространенными инструментами, позволяющими