УДК 004.056:004.78
DOI: 10.26102/2310-6018/2021.35.4.023

Оценивание эффективности информационных карт защищаемого киберпространства

А.Л. Сердечный
Воронежский государственный технический университет,
Воронеж, Российская Федерация

Резюме: Актуальность исследования вытекает из насущности защиты киберпространства, подвергающегося тотальным информационным атакам вредоносными кодами и деструктивными контентами. Одним из эффективных средств обеспечения безопасности глобального и национальных киберпространств является картография протекающих в них процессов, включая мониторинг и противодействие в условиях информационного противоборства, неуклонно обостряющегося в государственных, корпоративных и социальных сетях. Основным назначением информационных карт следует считать повышение эффективности работы экспертов (лиц, принимающих решение) на основе разрешения противоречия между необходимостью получения объективных количественных оценок влияния информационной карты на скорость и качество решаемых с ее помощью задач и субъективными факторами, влияющими на вышеперечисленные характеристики. В этой связи в работе для картографических методов рассматриваются: скорость решения задачи, точность решения задачи; трудоемкость построения информационной карты; трудоемкость актуализации информационной карты; объем новых знаний, полученных в ходе решения задач. При этом анализируется эффективность визуализации, включая количество пересечений и изгибов ребер графа, их общая длина, метрики формы, динамическая стабильность, метрики достоверности изменения кластеров и расстояний. Дается оценка эффективности информационной карты на примере поиска публикаций по теме «Компьютерные преступления», включая графическое сравнение результатов. В заключительной части работы намечаются перспективы дальнейших исследований по разработке методик оценки эффективности информационных карт защищаемого киберпространства.

Ключевые слова: информационная карта, эффективность визуализации, скорость решения задачи, точность решения задачи, защищаемое киберпространство, картография киберпространства

Для цитирования: Сердечный А.Л. Оценивание эффективности информационных карт защищаемого киберпространства. *Моделирование, оптимизация и информационные технологии.* 2021;9(4). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=1056 DOI: 10.26102/2310-6018/2021.35.4.023

Evaluating the effectiveness of protected cyberspace information maps

A.L. Serdechniy
Voronezh State Technical University,
Voronezh, Russian Federation

Abstract: The relevance of the study stems from the urgency of protecting cyberspace, which is subjected to total information attacks by malicious codes and destructive content. One of the effective means to ensure the security of global and national cyberspace is to map the processes occurring in it, including monitoring and counteraction under the conditions of information confrontation, steadily increasing in the state, corporate and social networks. The main purpose of information maps should be seen as increasing the efficiency of experts' (decision-maker's) work based on resolving the contradiction

between the need to obtain objective quantitative estimates of the information map influence on the speed and quality of tasks solved using it and the subjective factors affecting the aforementioned characteristics. In this regard, the paper considers the following cartographic methods: speed of problem solving, accuracy of problem solving; labor intensity of building an information map; laboriousness of updating the information map; the amount of new knowledge gained through problem solving. Concurrently, the effectiveness of the visualization is analyzed, including the number of intersections and bends of the graph edges, their total length, shape metrics, dynamic stability, cluster and distance change reliability metrics. The effectiveness of the information map is assessed using a search for publications on "Computer Crime" as an example, including a graphical comparison of the results. The conclusion outlines the prospects for further research on the development of methodologies to assess the effectiveness of protected cyberspace information maps.

Keywords: information map, visualization efficiency, problem-solving speed, problem-solving accuracy, protected cyberspace, cyberspace cartography

For citation: Serdechnyi A.L. Evaluating the effectiveness of information maps of protected cyberspace. *Modeling, Optimization and Information Technology*. 2021;9(4). Available from: https://moitvivt.ru/ru/journal/pdf?id=1056 DOI: 10.26102/2310-6018/2021.35.4.023 (In Russ).

Введение

Целью настоящей работы является определение возможности количественного оценивания эффективности информационных карт защищаемого киберпространства. Для этого были решены следующие задачи:

- анализ и обобщение существующих подходов количественного оценивания эффективности визуализации и географических карт;
- разработка способа количественного оценивания эффективности информационных карт на основании существующих подходов;
- практическое подтверждение реализуемости предложенного способа количественного оценивания эффективности информационных карт.

Проблема оценивания эффективности информационных карт лежит в области междисциплинарных исследований и связана с изучением когнитивных способностей человека. Для ее решения требуется привлечение соответствующих специалистов. В настоящей работе обозначены лишь возможные подходы к разрешению противоречия, лежащего в основе частной задачи оценивания эффективности информационных карт: между необходимостью получения объективных количественных оценок влияния информационной карты на скорость и качество решаемых с ее помощью задач и субъективными факторами, оказывающими воздействие на исход экспериментов, в ходе которых могут быть получены такие количественные оценки.

Введем термин «информационная карта» для обозначения цифрового объекта, позволяющего представить в двухмерном или трехмерном пространстве исследуемое множество объектов, субъектов и процессов многомерного киберпространства с учетом следующих требований:

- наличия меры близости между всеми объектами киберпространства в многомерном пространстве признаков;
- сохранения пропорций расстояний между изображениями объектов в двухмерном (трехмерном) пространстве и их расстоянием в многомерном пространстве признаков;
- одновременного изображения объектов исследования и контекста (представленного ландшафтом информационной карты), в котором они находятся;
- воспроизводимости операций построения информационной карты различными исследователями.

Основным назначением информационных карт является повышение эффективности работы экспертов, поэтому необходимо иметь четкое представление о том, насколько эксперт может быстрее и качественнее решить ту или иную задачу с использованием данного инструмента.

Для решения практических задач с помощью информационных карт важно оценивать следующие показатели:

- скорость решения задачи;
- точность решения задачи;
- трудоемкость построения информационной карты;
- трудоемкость актуализации информационной карты;
- объем новых знаний, полученных в ходе решения задачи.

Методики оценки эффективности способов визуализации, а также географических карт позволяют оценивать первые четыре показателя. Для оценки объема новых знаний в настоящей момент не известно удовлетворительное решение, в первую очередь, из-за неоднозначности самого понятия «новое знание» и измерения его ценности.

Скорость решения задачи может быть достаточно просто оценена с помощью обычных временных замеров. При этом для рутинных задач важно понимать не абсолютное значение данного показателя, а динамику изменения скорости по мере изменения состояния исследователя. Удобный и интуитивно понятный способ визуализации, который обеспечивается информационной картой, может способствовать удержанию концентрации на достаточно длительные промежутки времени. Также для оценки скорости решения задачи важно знать, как на значение данного показателя влияет опыт исследователя.

Неотъемлемым свойством информационной карты является наличие различного вида искажений. Искажения могут быть обусловлены как объективными причинами (эффектом снижения размерности, точностью алгоритмов построения и анализа информационных карт), так и субъективными (недостаточным качеством исходных данных, ошибками реализации информационно-картографической системы, ошибками построения информационных карт). Искажения негативно влияют на точность решения задачи. Одновременно компенсирующими свойствами информационной карты, позволяющими повысить точность решения задачи и выявить возможные ошибки, являются:

- отображение объекта исследования одновременно с контекстом исследования (данное свойство позволяет выявлять противоречия объекта исследования и среды, в котором он функционирует, что, во-первых, способствует выявлению ошибок, вызванных искажениями, а во-вторых, позволяет учитывать факторы влияния среды, которые могли бы остаться без внимания при использовании другого способа анализа данных);
- одновременное изображение различных объектов в едином контексте (с помощью информационной карты достаточно просто сравнить различные результаты одного и того же объекта, но полученные независимыми исследователями, благодаря чему могут быть выявлены и устранены недостатки таких результатов).

Трудоемкость построения и актуализации информационной карты напрямую связана со степенью автоматизации методов, используемых при выполнении соответствующих процедур, а также с качеством исходных данных. Так, например, если имеются необходимые исходные данные, формат которых соответствует формату, воспринимаемому информационно-картографической системой, в которой все процедуры построения карты выполняются автоматически, то трудоемкость создания такой карты незначительна. С другой стороны, если для задачи имеется высокая степень

неопределенности как в отношении состава исходных данных, так и методов их получения, то потребуется продолжительная процедура сбора данных. В этом случае формирование подходящего ландшафта может потребовать осуществление нескольких итераций сбора и анализа графов связей. Каждая итерация требует полную перестройку карты, до тех пор, пока не будут обеспечены достаточная полнота и качество ландшафта и собранных исходных данных.

Материалы и методы

Интегральный показатель эффективности может быть сформирован с учётом приведённых выше показателей, для расчёта которых применимы методы оценки эффективности визуализации (а также методы оценки эффективности географических карт, как их частная реализация, наиболее близкая к рассматриваемому объекту исследования).

Наиболее распространенным способом оценки эффективности визуализации является использование метрик качества изображений. Определение данного показателя связано с проблемой критериев восприятия визуализации. Во-первых, само понятие качества визуализации зависит от конкретных стандартов изображения объектов. Во-вторых, каждый человек по-своему воспринимает и оценивает качество изображаемых данных. В первую очередь это связано с имеющимся опытом анализа визуальных изображений. Человек интуитивно имеет разумное представление о том, как элементы диаграммы могут быть расположены так, чтобы они были приятны глазу. Тем не менее, часто бывает трудно формализовать такое представление, а также понять, помогает ли интуитивное расположение лучше воспринимать диаграмму для более эффективного решения задачи.

Попытки решения данной проблемы предпринимаются многими исследователями. В работе [1] проанализированы метрики качества для различных типов визуализируемых данных (многомерных данных, данных высокой размерности, связанных данных, порядковых данных, геопространственных данных и текстовых данных), а также техник визуализации (точечных диаграмм, параллельных координат, радиальных графиков, диаграмм связей, облаков тэгов и др.). На основании результатов анализа авторами [1] предложен интегральный показатель качества, оптимизация которого позволяет выбрать наилучший для визуализируемых данных тип диаграммы.

Также можно отметить работу [2], в которой рассматриваются метрики качества визуализации динамических графов. Для оценки качества визуализации графов могут применяться следующие метрики:

- количество пересечений ребер (каждое пересечение ребер графа создает иллюзию наличия перекрестка с узлом в центре, поэтому для повышения качества визуализации стараются уменьшить значение данного показателя);
- количество изгибов ребер (уменьшение количества пересечений достигается за счет удлинения и изгиба ребер, что искажает восприятие расстояния между узлами, соединенными такими ребрами);
- общая длина ребер (силовые способы укладки графов обеспечивают минимизацию расстояния между наиболее связанными узлами, что позволяет уменьшить общую длину ребер);
- метрики на основе формы (используются для оценки больших графов, где традиционные метрики, такие как пересечение ребер, дают плохой результат);
- динамическая стабильность (разница расстояний между соответствующими узлами графа для двух его состояний, позволяющая оценивать изменчивость положений

узлов для динамического графа. Чем меньше изменение, тем проще воспринимать такой граф);

- метрика достоверности изменения кластера (показывает, насколько хорошо формы динамических графиков отображают его структурные изменения);

- метрика достоверности изменения расстояния (показывает, насколько хорошо расстояния между узлами графа в пространстве более высокой размерности сохраняются при переходе к двухмерному изображению. По сути, данный показатель выполняет роль функции стресса).

При этом необходимо отметить, что метрики качества оценивают лишь «эстетические свойства» и удобочитаемость научных визуализаций и позволяют лишь отбросить неподходящие варианты построения графиков, диаграмм и различных схем. Однако оценка качества задач, решаемых с использованием соответствующих визуальных изображений, такими показателями оценить нельзя (несмотря на наличие корреляции между значениями некоторых показателей и результатами решения ряда простых задач) [2].

Возможность оценки эффективности визуализации на основании качества решения практических задач появляется в рамках экспериментальных исследований. Для таких исследований определенным образом формируются тестовые задачи и организуется работа испытуемых. В ходе эксперимента обычно количественно оцениваются скорость и достоверность получаемых результатов с помощью того или иного способа визуализации. В работе [3] представлен обзор источников, содержащих результаты экспериментальных исследований эффективности восприятия различных способов отображения графов. Отмечается, что при восприятии графов большое значение имеют размеры узлов и плотные структуры. При этом необходимо уделять должно внимание расположению узлов и изображению их связей, так как кластерная структура лучше воспринимается, чем граф, представленный в виде «комка волос» (граф, для которого узлы распределены по всей площади и связаны с большим количеством других узлов). Также в данной работе делается вывод о недостаточной исследованности вопросов когнитивного восприятия графов большой размерности и динамических графов.

Также имеются исследования по оценке эффективности визуализации в краудсорсинговых проектах, одной их которых является работа [4]. В ней представлены результаты использования возможностей сообщества для проведения экспериментальных исследований качества визуализации. Рассматриваются возможные проблемы и их решения, в том числе за счет создания специализированных инструментальных средств, позволяющих контролировать ошибки и целенаправленные ложные результаты, предоставляемые членами такого сообщества.

Одной из важных работ для количественного оценивания эффективности визуализаций является [5], в которой предлагает количественный подход оценки эффективности решения задач с помощью визуализаций (в том числе интерактивных). Подход основан на измерении времени принятия правильного решения экспертами. Он применим и к картам киберпространства, так как позволяет определить, какая из карт лучше подходит для экспертной поддержки решения той или иной задачи. Оценка эффективности основана на следующих показателях [5]:

- теоретическая оценка искажения ($SvEm_d$);

- теоретическая оценка времени ($SvEm_t$).

Теоретические оценки искажения и времени рассчитываются по формулам (1) и (2) соответственно [5]:

$$SvEm_g = \frac{(\omega * h)/S_V}{Cl * t_{me} * n_{clicks}} > 50\%, \quad (1)$$

$$SvEm_t = \frac{(Cl * t_{me})}{n_{clicks} * S_V/d} \leq 0{,}25, \quad (2)$$

где

$\omega * h$ – размеры рабочей поверхности устройства;

S_V – количество визуальных элементов, отображаемых на карте (например, инфицированный IP-пакет, метка времени и др.);

Cl – когнитивная нагрузка (количество идентифицируемых признаков во время предварительного ознакомления с картой);

t_{me} – нагрузка на рабочую память (усилие, основанное на временных оценках рабочей памяти);

n_{clicks} – количество взаимодействий с визуализацией.

Данный подход является перспективным для оценки эффективности с учетом возможностей инструментальных средств визуализации.

Оценка эффективности географических карт основывается на результатах экспериментальных исследований, в ходе которых испытуемые решают пространственные задачи [6, 7, 8, 9, 10, 11, 11, 13]. Изменение скорости решения задачи в результате выбора той или иной формы представления геопространственных данных часто выступает в качестве показателя эффективности. При выборе формы могут варьироваться как какой-либо отдельный параметр (например, цвет объектов) [6], так и выбор определенной картографической проекции. В диссертации [13] рассматриваются вопросы выявления лучших практик создания географических карт для обучения.

В ходе подобных исследований также изучаются когнитивные способности человека и особенности принятия им решений на основании анализа картографической информации [7, 8, 9, 10, 11, 12].

В работе [7] представлены результаты анализа и обобщения научных публикаций по теме исследований зрительного внимания при наблюдении за картами. В работах [8, 9] рассматривается широкий спектр вопросов восприятия географических карт, начиная от частных деталей изображения отдельных элементов, заканчивая выбором наилучших подходов к генерализации и композиции данных. Также можно отметить работу [10], в которой делается вывод о том, что скорость решения простых пространственных задачах, решаемых новичками и профессиональными картографами, отличается друг от друга незначительно.

Имеется ряд работ, в которых авторами в качестве показателя эффективности рассматривается качество принимаемых решений, основаниями для которых служат пространственно-временные данные. Например, в [11] сообщается об исследованиях влияния неопределенности в отношении пространственно-временных данных, отображаемых на карте, в контексте принятия решения в экстренных ситуациях (когда время принятия решения существенно ограничено). В [12] авторы исследуют вопросы культурного различия при восприятии пространственных данных.

Таким образом, подходы, основанные на экспериментальных оценках скорости и качества решения задач (принятия решений), которые используются в картографии, также могут быть применены для оценивания эффективности информационных карт.

Оценка эффективности информационной карты на примере поиска публикаций по теме «Компьютерные преступления»

В настоящем разделе представлены результаты практического подтверждения применимости рассмотренных выше подходов для оценки эффективности информационных карт. Для этого были проведены исследования эффективности картографического поиска сведений по заданной теме.

Суть картографического поиска заключается в выявлении необходимых сведений в результате рассмотрения тематических областей информационной карты. В отличие от классического поиска, по ключевым словам, картографический поиск ориентирован на обнаружении информационных источников, благодаря их расположению в тематическом пространстве. Такой способ позволяет искать данные даже в отсутствии знания конкретных терминов, которые могут быть использованы в качестве поисковых запросов. Благодаря изучению ландшафта информационной карты (который отражает тематическую близость публикаций), исследователь лучше представляет предметную область и может более точно определиться с критериями поиска.

В качестве объекта исследований был использован метод картографического поиска (являющийся результатом обобщения метода картографического поиска научных публикаций, описанного в приложении). Данный метод реализован на базе интерактивной информационной карты, в основе которой лежит граф связей публикаций с ключевыми словами, отражающими их тематику. Тематические кластеры образуются благодаря эффекту «стягивания» ключевыми словами близких по смыслу публикаций.

Для оценки эффективности картографического поиска был поставлен эксперимент, в ходе которого студенты осуществляли поиск информации двумя различными методами:

- методом классического поиска, по ключевым словам, (который проводился при помощи глобальных поисковых систем, а также встроенной поисковой системы конкретного информационного ресурса);
- методом картографического поиска.

Каждый участник эксперимента в разные промежутки времени решал 4 задачи, случайно выбранные из 10 типов заданий. Первые две задачи решались с использованием классического метода поиска, вторые – картографического. Участниками эксперимента были 10 человек. Таким образом, каждая из 10 задач решалась двумя способами двумя различными студентами.

В качестве показателей оценки эффективности использовались:

- средняя скорость получения ответа, вычисляемая как отношение общего времени решения задачи к количеству полученных ответов;
- качество решения задачи (отношение количества правильных ответов, к общему количеству предоставленных ответов).

Дополнительно была получена оценка времени построения информационной карты, использованной для поиска.

Темой поиска были выбраны задания в области защиты от компьютерных преступлений. В качестве исходных данных использованы статьи по данной теме, опубликованные на платформе для ведения блогов Хабр [14] (поиск был ограничен именно этим ресурсом с целью повышения точности результатов эксперимента и упрощения расчетов). Сведения о построенной информационной карте приведены в Таблице 1, а ее интерфейс показан на Рисунке 1.

Таблица 1 – Сведения об информационной карте «Публикации по теме «Компьютерные преступления»
Table 1 – Information about the information map «Publications on «Cybercrimes»

Тип сведений	Характеристика информационной карты
Уровень	Уровень тематических публикаций, относящийся к информационному уровню киберпространства
Решаемые задачи	Систематизация и поиск сведений о компьютерных преступлениях и мерах борьбы с ними
Исходные данные	1099 статей по теме «Компьютерные преступления», опубликованные на платформе для ведения блогов Хабр [14] и связанные с ними дополнительные данные, в том числе 2712 тематических меток, отмеченных авторами публикаций
Модель данных	*Узлы*: «Статья» (p), «Тематическая метка» (t); *Связи*: [p] ← [t] («Связь, характеризующая наличие у статьи соответствующей тематической метки»); *Свойства*: «Название», «Текс статьи», «Тема», «Автор», «Дата публикации», «Адрес», «Доменное имя» (p)
Операции построения	В ходе построения карты осуществлены следующие операции: - сбор сведений о публикациях по теме «Компьютерные преступления» с платформы для ведения блогов Хабр и их загрузка в СУБД Neo4j с помощью разработанного Python-скрипта; - построение графа связей ([p] ← [t]); - укладка графа в двухмерном пространстве с помощью силового алгоритма ForceAtlas2 (LinLog = true, «Влияние весов рёбер» = 1, «Запрет перекрытия» = false, «Устойчивость» = 1, Theta = 1.2, «Разрежённость» = 2, «Гравитация» = 1); - построение интерактивной карты (интерактивные панели PowerBI)
Ландшафты	Интерактивная тепловая карта на основе графа связей [p] ← [t]
Слои	Тематический слой публикаций
Форматы карты	.pbix (интерактивная панель для программы PowerBI)

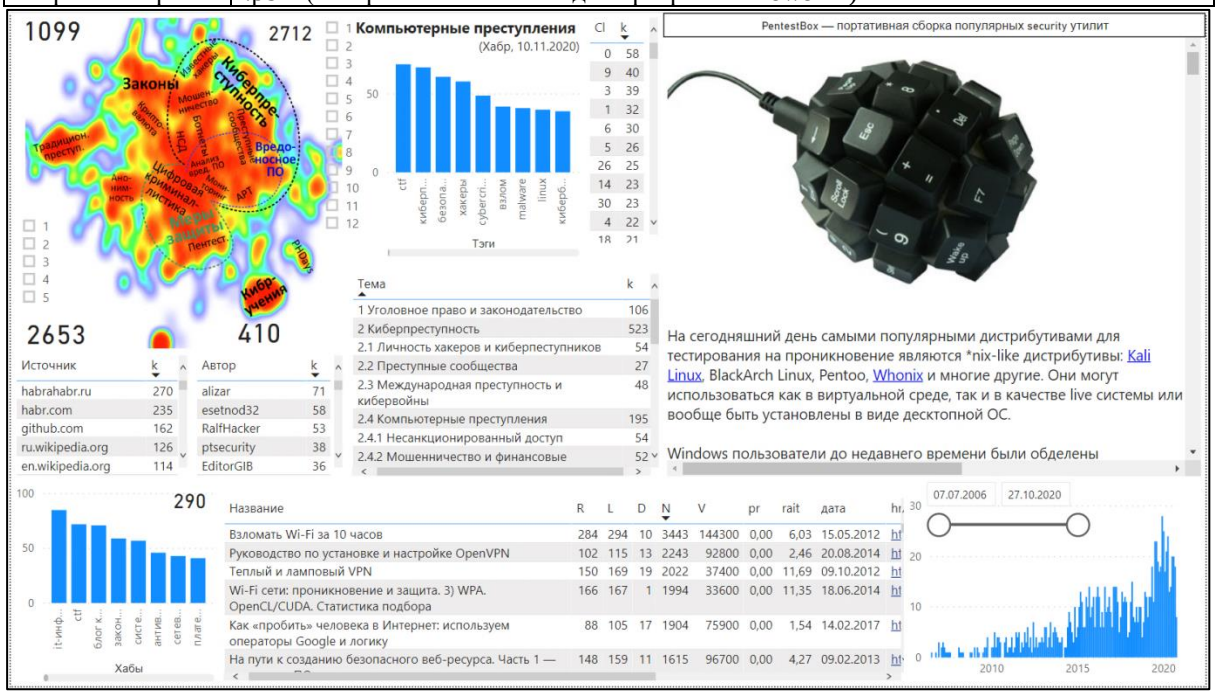


Рисунок1 – Интерфейс интерактивной информационной карты «Публикации по теме «Компьютерные преступления)», используемой для поиска сведений по теме
Figure 1 – Interface of the interactive information map «Publications on «Cybercrimes» used to retraival for information on the topic

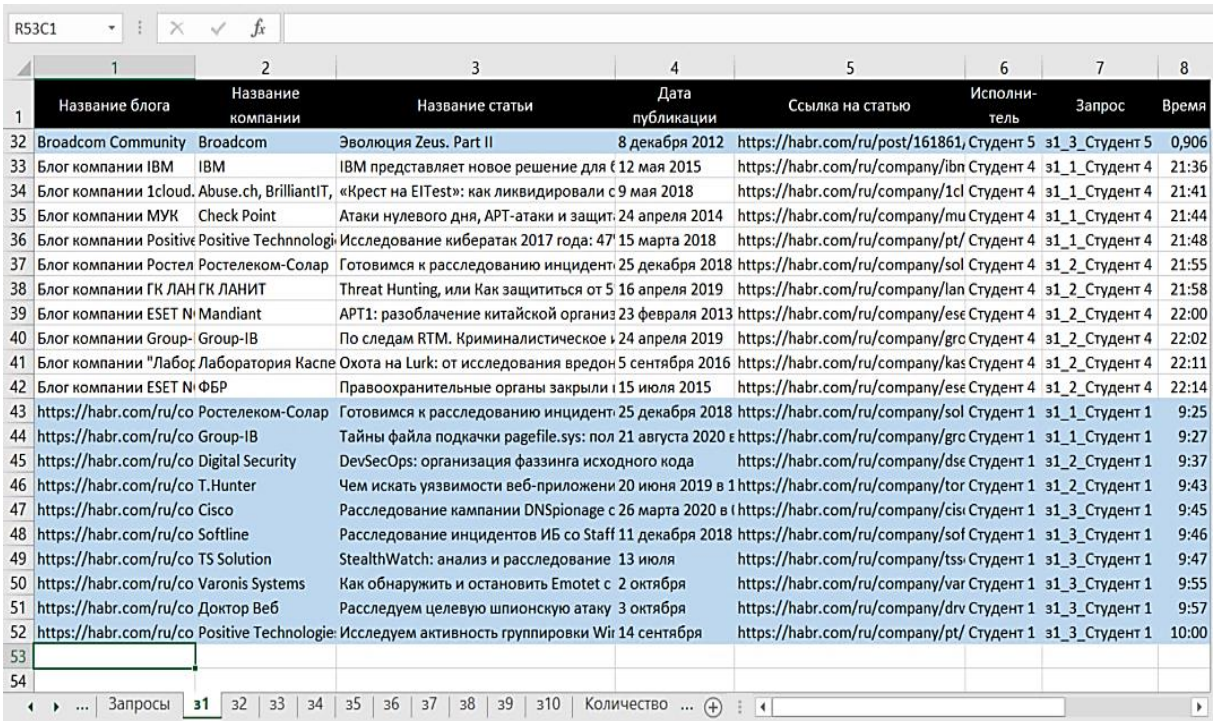
В ходе эксперимента студентами решались следующие задачи:

- поиск блогов компаний, занимающихся расследованием компьютерных преступлений (задача № 1);
- формирование перечня программных и программно-аппаратных средств, используемых для расследования компьютерных преступлений (задача № 2);
- поиск названий методов, используемых для расследования компьютерных преступлений (задача № 3);
- поиск статей, в которых представлено описание процесса расследования компьютерных преступлений (задача № 4);
- формирование перечня хакерских торговых площадок (задача № 5);
- определение названий нормативных документов, имеющих отношение к противодействию компьютерным преступлениям (задача № 6);
- поиск названий методов определения личности компьютерного преступника (задача № 7);
- поиск информационных ресурсов, публикующих сведения о расследовании компьютерных преступлений (задача № 8);
- формирование перечня баз данных, используемых при расследовании компьютерных преступлений (задача № 9);
- формирование словаря терминов и определений в области расследования компьютерных преступлений (задача № 10).

Большинство задач (задачи 1, 2, 4, 6 и 10) связано с поиском фактологической информации, которую достаточно просто получить из текста (а для задачи № 1 из заголовка и сведений об авторе). Задачи № 3 и № 7 требовали от участника эксперимента определенных знаний в области расследования компьютерных преступлений и умения их выявления в тексте публикаций независимо от состава используемых терминов. Задачи 5, 8 и 9 в большинстве случаев требовали от исследователя перехода по ссылкам, содержащимся в тексте статей с целью подтверждения достоверности найденных фактов. Причем задача № 9 вызвала наибольшие затруднения по причине достаточно малого количества статей, содержащих сведения о базах данных, которые используются при расследовании компьютерных преступлений.

В ходе решения каждой задачи (на выполнение каждой отводилось 45 минут) участниками эксперимента формировалась таблица с результатами поиска (пример обобщенной таблицы результатов выполнения задачи № 1 показан на Рисунке 2). По условиям эксперимента испытуемые также должны были сохранять найденные статьи.

Расчет скорости выполнения традиционного поиска осуществлялся на основании временных отметок файлов сохраненных публикаций. Для картографического поиска была использована видеозапись процесса решения задания (которая также использовалась для анализа поисковых стратегий использования информационных карт). В результате обработки результатов эксперимента рассчитывалась оценка рассмотренных выше показателей эффективности поиска. Также определялись индивидуальные поисковые стратегии.



R53C1

	1	2	3	4	5	6	7	8
1	Название блога	Название компании	Название статьи	Дата публикации	Ссылка на статью	Исполни-тель	Запрос	Время
32	Broadcom Community	Broadcom	Эволюция Zeus. Part II	8 декабря 2012	https://habr.com/ru/post/161861/	Студент 5	з1_3_Студент 5	0,906
33	Блог компании IBM	IBM	IBM представляет новое решение для б	12 мая 2015	https://habr.com/ru/company/ibn	Студент 4	з1_1_Студент 4	21:36
34	Блог компании 1cloud.	Abuse.ch, BrilliantIT,	«Крест на EITest»: как ликвидировали с	9 мая 2018	https://habr.com/ru/company/1cl	Студент 4	з1_1_Студент 4	21:41
35	Блог компании МУК	Check Point	Атаки нулевого дня, APT-атаки и защит	24 апреля 2014	https://habr.com/ru/company/mu	Студент 4	з1_1_Студент 4	21:44
36	Блог компании Positive	Positive Technnologi	Исследование кибератак 2017 года: 47	15 марта 2018	https://habr.com/ru/company/pt/	Студент 4	з1_1_Студент 4	21:48
37	Блог компании Ростел	Ростелеком-Солар	Готовимся к расследованию инцидент	25 декабря 2018	https://habr.com/ru/company/sol	Студент 4	з1_2_Студент 4	21:55
38	Блог компании ГК ЛАН	ГК ЛАНИТ	Threat Hunting, или Как защититься от 5	16 апреля 2019	https://habr.com/ru/company/lan	Студент 4	з1_2_Студент 4	21:58
39	Блог компании ESET N	Mandiant	APT1: разоблачение китайской организ	23 февраля 2013	https://habr.com/ru/company/esc	Студент 4	з1_2_Студент 4	22:00
40	Блог компании Group-	Group-IB	По следам RTM. Криминалистическое и	24 апреля 2019	https://habr.com/ru/company/grc	Студент 4	з1_2_Студент 4	22:02
41	Блог компании "Лабор	Лаборатория Каспе	Охота на Lurk: от исследования вредон	5 сентября 2016	https://habr.com/ru/company/kas	Студент 4	з1_2_Студент 4	22:11
42	Блог компании ESET N	ФБР	Правоохранительные органы закрыли	15 июля 2015	https://habr.com/ru/company/esc	Студент 4	з1_2_Студент 4	22:14
43	https://habr.com/ru/co	Ростелеком-Солар	Готовимся к расследованию инцидент	25 декабря 2018	https://habr.com/ru/company/sol	Студент 1	з1_1_Студент 1	9:25
44	https://habr.com/ru/co	Group-IB	Тайны файла подкачки pagefile.sys: пол	21 августа 2020 г	https://habr.com/ru/company/grc	Студент 1	з1_1_Студент 1	9:27
45	https://habr.com/ru/co	Digital Security	DevSecOps: организация фаззинга исходного кода		https://habr.com/ru/company/dse	Студент 1	з1_2_Студент 1	9:37
46	https://habr.com/ru/co	T.Hunter	Чем искать уязвимости веб-приложени	20 июня 2019 в 1	https://habr.com/ru/company/tor	Студент 1	з1_2_Студент 1	9:43
47	https://habr.com/ru/co	Cisco	Расследование кампании DNSpionage с	26 марта 2020 в	https://habr.com/ru/company/cis	Студент 1	з1_3_Студент 1	9:45
48	https://habr.com/ru/co	Softline	Расследование инцидентов ИБ со Staff	11 декабря 2018	https://habr.com/ru/company/sof	Студент 1	з1_3_Студент 1	9:46
49	https://habr.com/ru/co	TS Solution	StealthWatch: анализ и расследование	13 июля	https://habr.com/ru/company/tss	Студент 1	з1_3_Студент 1	9:47
50	https://habr.com/ru/co	Varonis Systems	Как обнаружить и остановить Emotet с	2 октября	https://habr.com/ru/company/var	Студент 1	з1_3_Студент 1	9:55
51	https://habr.com/ru/co	Доктор Веб	Расследуем целевую шпионскую атаку	3 октября	https://habr.com/ru/company/drv	Студент 1	з1_3_Студент 1	9:57
52	https://habr.com/ru/co	Positive Technologie	Исследуем активность группировки Wi	14 сентября	https://habr.com/ru/company/pt/	Студент 1	з1_3_Студент 1	10:00
53								
54								

... | Запросы | з1 | з2 | з3 | з4 | з5 | з6 | з7 | з8 | з9 | з10 | Количество ...

Рисунок 2 – Пример результатов выполнения участниками эксперимента задачи № 1 («Поиск блогов компаний, занимающихся расследованием компьютерных преступлений»)
Figure 2 – Example of the results of experiment participants' performance of task №1 («Retraivaling for computer crime investigation companies' blogs»)

Их визуальное представление в виде временной шкалы (Рисунок 3) позволяло достаточно быстро проанализировать динамику поиска, а также сравнить различные подходы в рамках однотипных задач.

Обсуждение

В ходе анализа стратегий поиска было установлено, что в большинстве случаев при использовании интерактивной карты испытуемые полагались на «проверенные временем» стратегии просмотра списка заголовков публикаций, без учета их положения в какой-либо зоне ландшафта. Лишь в некоторых испытаниях анализ ландшафта учитывался при выборе системы фильтров для сокращения множества названий в таком списке. Данное обстоятельство, а также недостаточное количество испытуемых, не позволяет сделать обоснованное заключение в отношении эффективности картографического метода (несмотря на более лучшие значения показателей скорости и качества для картографического метода, которые были рассчитаны по итогам эксперимента и составили 9,6 % снижения среднего времени поиска и 5,2 % прироста средней точности ответов). Тем не менее, полученные результаты имеют обнадеживающее значение для организации более надежного эксперимента с большим числом участников.

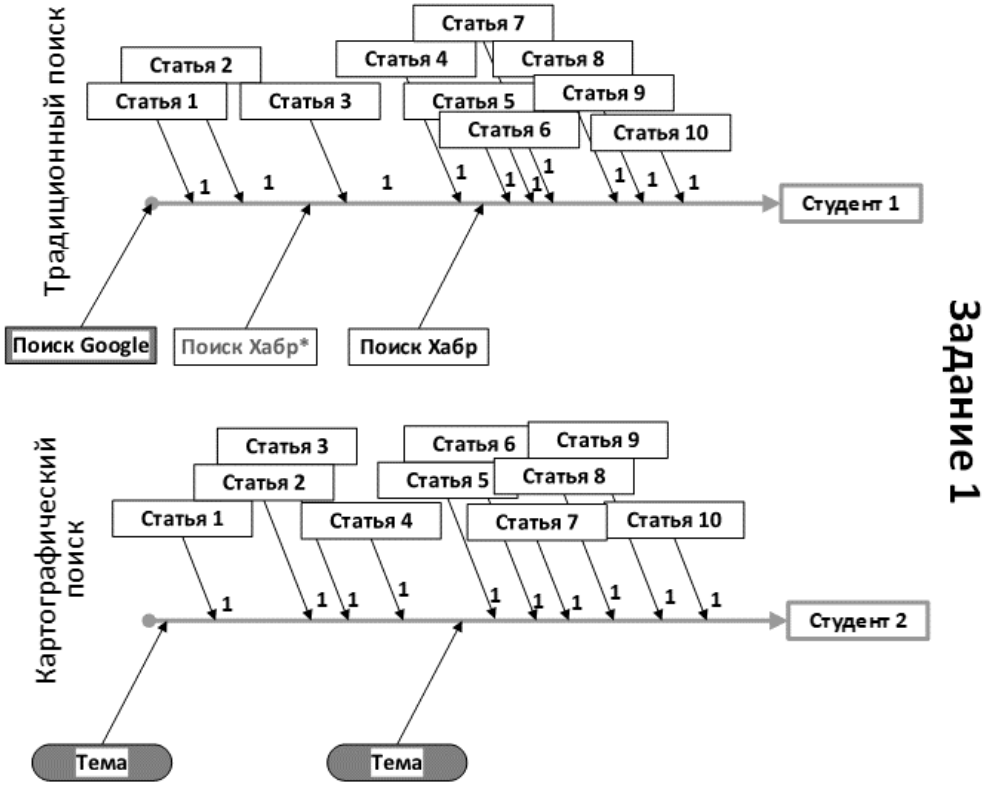


Рисунок 3 – Графическое сравнение результатов двух участников, использовавших для выполнения задания № 1 (поиск блогов компаний, занимающихся расследованием компьютерных преступлений) методы традиционного поиска (верхний график) и картографического поиска (нижний график)

Figure 3 – Graphical comparison of the results of two participants who used traditional retraival (top graph) and mapping retraival (bottom graph) methods to complete task №1 (retraivaling for computer crime investigation companies' blogs)

Заключение

Таким образом, на сегодняшний день тема исследования эффективности информационных карт изучена недостаточно. В настоящем приложении рассмотрены лишь основные направления, в рамках которых можно проводить соответствующие исследования. Основной идеей количественного оценивания эффективности информационных карт является использование показателя скорости получения правильного ответа на решаемые задачи. Пример реализации данной идеи продемонстрирован в ходе оценки эффективности информационной карты поиска публикаций по теме «Компьютерные преступления». Полученный опыт позволил выявить ряд существенных моментов, влияющих на достоверность результатов экспериментальных исследований, которые необходимо учитывать при проведении оценок эффективности. Кроме того, предлагаемый подход оценки эффективности не учитывает возможность оценки «озарений» (количество и качество новых знаний), получаемых благодаря использованию информационных карт. Данное направление требует дальнейших исследований.

СПИСОК ИСТОЧНИКОВ

1. Behrisch M., Blumenschein M., Kim N.W. Quality metrics for information visualization. *Computer Graphics Forum*. 2018;37(3):625–662.
2. Meidiana A., Hong S.H., Eades P. New Quality Metrics for Dynamic Graph Drawing. *arXiv preprint arXiv:2008.07764.* 2020:1–17.
3. Yoghourdjian V., Archambault D., Diehl S. et al. Exploring the limits of complexity: A survey of empirical studies on graph visualization. *Visual Informatics*. 2018;2(4):264–282.
4. Borgo R., Lee B., Bach B. Crowdsourcing for information visualization: Promises and pitfalls. *Evaluation in the crowd. Crowdsourcing and human-centered experiments*. Springer, Cham. 2017:96–138.
5. Garae J, Ko R. K. L., Apperley M. Full-scale security visualization effectiveness measurement and presentation approach. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE*. 2018:639–650.
6. Sherman-Morris K., Antonelli K.B., Williams C.C. Measuring the effectiveness of the graphical communication of hurricane storm surge threat. *Weather, climate, and society*. 2015;7(1):69–82.
7. Krassanakis V., Cybulski P. A review on eye movement analysis in map reading process: The status of the last decade. *Geodesy and Cartography*. 2019;68(1):191–209.
8. Griffin A.L. Cartography, visual perception and cognitive psychology. *The Routledge handbook of mapping and cartography*. Routledge. 2017:44–54.
9. Montello D.R., Fabrikant S.I., Davies C. Cognitive perspectives on cartography and other geographic information visualizations. *Handbook of behavioral and cognitive geography. Edward Elgar Publishing.* 2018:177–196.
10. Gilhooly K.J. et al. Skill in map reading and memory for maps. *The Quarterly Journal of Experimental Psychology Section A.* 1988;40(1):87–107.
11. Korporaal M., Ruginski I.T., Fabrikant S.I. Effects of uncertainty visualization on decision making with map-based geographic data under time pressure. *Frontiers in Computer Science.* 2020;2:32.
12. Stachoň Z., Šašinka Č., Čeněk J. Cross-cultural differences in figure-ground perception of cartographic stimuli. *Cartography and Geographic Information Science*. 2019;46(1):82–94.
13. Stenliden L. Visual Analytics in K12 Education-Emerging Dimensions of Complexity. *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering.* 2015;9(2):663–671.
14. Сердечный А.Л., Гончаров А.А., Остапенко А.Г. Технология построения и использования поисковых карт в образовательном процессе на примере поисковой карты по учебной дисциплине «Компьютерные преступления». *Интеллектуальные информационные системы. труды Международной научно-практической конференции: в 2 ч. Воронеж*. 2021:94–98.

REFFERENCES

1. Behrisch M., Blumenschein M., Kim N.W. Quality metrics for information visualization. *Computer Graphics Forum*. 2018;37(3):625–662.
2. Meidiana A., Hong S.H., Eades P. New Quality Metrics for Dynamic Graph Drawing. *arXiv preprint arXiv:2008.07764.* 2020:1–17.
3. Yoghourdjian V., Archambault D., Diehl S. et al. Exploring the limits of complexity: A survey of empirical studies on graph visualization. *Visual Informatics*. 2018;2(4):264–282.

4. Borgo R., Lee B., Bach B. Crowdsourcing for information visualization: Promises and pitfalls. *Evaluation in the crowd. Crowdsourcing and human-centered experiments*. Springer, Cham. 2017:96–138.
5. Garae J, Ko R. K. L., Apperley M. Full-scale security visualization effectiveness measurement and presentation approach. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE*. 2018:639–650.
6. Sherman-Morris K., Antonelli K.B., Williams C.C. Measuring the effectiveness of the graphical communication of hurricane storm surge threat. *Weather, climate, and society*. 2015;7(1):69–82.
7. Krassanakis V., Cybulski P. A review on eye movement analysis in map reading process: The status of the last decade. *Geodesy and Cartography*. 2019;68(1):191–209.
8. Griffin A.L. Cartography, visual perception and cognitive psychology. *The Routledge handbook of mapping and cartography*. Routledge. 2017:44–54.
9. Montello D.R., Fabrikant S.I., Davies C. Cognitive perspectives on cartography and other geographic information visualizations. *Handbook of behavioral and cognitive geography. Edward Elgar Publishing.* 2018:177–196.
10. Gilhooly K.J. et al. Skill in map reading and memory for maps. *The Quarterly Journal of Experimental Psychology Section A.* 1988;40(1):87–107.
11. Korporaal M., Ruginski I.T., Fabrikant S.I. Effects of uncertainty visualization on decision making with map-based geographic data under time pressure. *Frontiers in Computer Science.* 2020;2:32.
12. Stachoň Z. Šašinka Č., Čeněk J. Cross-cultural differences in figure-ground perception of cartographic stimuli. *Cartography and Geographic Information Science*. 2019;46(1):82–94.
13. Stenliden L. Visual Analytics in K12 Education-Emerging Dimensions of Complexity. *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering.* 2015;9(2):663–671.
14. Serdechnyi A.L., Goncharov A.A., Ostapenko A.G. Technology of construction and use of retraival maps in the educational process on the example of the search map for the academic discipline «Computer Crimes». *Intellektual'nyye informatsionnyye sistemy. trudy Mezhdunarodnoy nauchno-prakticheskoy konferentsii: v 2 ch. Voronezh = Intelligent Information Systems. Proceedings of the International Scientific and Practical Conference: in 2 p. Voronezh.* 2021:94–98. (In Russ.)

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Сердечный Алексей Леонидович, кандидат технических наук, старший научный сотрудник Воронежского государственного технического университета, Воронеж, Российская Федерация
email: alex-voronezh@mail.ru

Serdechnyi Alexey Leonidovich, Cand. Sc (Technical), senior researcher of Voronezh State Technical University, Voronezh, Russian Federation

Статья поступила в редакцию 24.09.2021; одобрена после рецензирования 25.11.2021; принята к публикации 29.12.2021.

The article was submitted 24.09.2021; approved after reviewing 25.11.2021; accepted for publication 29.12.2021.