ВИЗУАЛЬНАЯ АНАЛИТИКА ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ОЦЕНКА ЭФФЕКТИВНОСТИ И АНАЛИЗ МЕТОДОВ ВИЗУАЛИЗАЦИИ

Котенко И.В.[1], Коломеец М.В.[2], Жернова К.Н.[3], Чечулин А.А.[4]

Цель статьи: *систематизация методов оценки эффективности визуализации данных информационной безопасности и сравнительная оценка методов визуализации по областям применения.*

Метод исследования: *системный анализ релевантных работ в области оценки эффективности визуализации. Объектами исследования являются: решения задач информационной безопасности посредством визуального анализа и методы оценки эффективности визуализации.*

Полученный результат: *представлена интерактивная карта моделей визуализации и областей их применения, которая позволит исследователям и разработчикам выбирать модели визуализации, наиболее приемлемые для конкретных прикладных задач информационной безопасности. Представлена классификация методов оценки визуализации.*

Область применения предложенного подхода – создание моделей визуализации, которые могут использоваться для повышения эффективности взаимодействия оператора с приложениями информационной безопасности. Визуальный анализ релевантных работ в области визуализации данных информационной безопасности с использованием интерактивной карты.

Ключевые слова: *визуальные средства взаимодействия, модель визуализации, методы оценки эффективности, классификации методов оценки, структуры данных, анализ данных, поддержка и принятие решений.*

DOI:10.21681/2311-3456-2021-6-36-45

1. Введение

В первой части статьи [1] была представлена классификация моделей визуализации по областям применения и задачам информационной безопасности, выполнена классификация моделей визуализации по структурам данных, а также проанализированы свойства моделей визуализации, которые могут применяться в методах оценки визуализации.

В данной работе проводится анализ методов оценки эффективности визуальных средств взаимодействия оператора с приложениями информационной безопасности (далее будем называть их методами оценки эффективности визуализации), а также сравнительная оценка методов визуализации по областям применения в информационной безопасности. Научная значимость работы состоит в разработке классификации методов оценки эффективности визуализации для задач информационной безопасности. Данная классификация может использоваться для выбора метода оценки эффективности визуализации, исходя из потребностей и возможностей разработчика систем визуальной аналитики.

В работе также проводится сравнительная оценка методов визуализации, результатом которой является интерактивная карта моделей визуализации, позволяющая осуществлять навигацию по представленным в данной работе решениям.

Практическая значимость данной работы состоит в возможности использования предложенных результатов в процессе разработки и оценки новых систем визуальной аналитики для решения различных задач информационной безопасности.

Работа организована следующим образом. Во втором разделе анализируются методы оценки эффективности визуализации. В третьем разделе рассматривается предложенная классификация методов оценки эффективности визуализации. В четвертом разделе проводится сравнительная оценка методов визуализации и предлагается разработанная интерактивная карта представленных в публикациях решений.

2. Методы оценки эффективности визуализации

Оценка эффективности средств взаимодействия оператора с приложениями информационной безопасности является важной составляющей при разработке новых решений по визуальной аналитике информа-

1 Котенко Игорь Витальевич, доктор технических наук, профессор, главный научный сотрудник и заведующий лабораторией проблем компьютерной безопасности, ФГБУН Санкт-Петербургский институт информатики и автоматизации Российской академии наук, г. Санкт-Петербург, Россия. E-mail: ivkote@comsec.spb.ru

2 Коломеец Максим Вадимович, младший научный сотрудник, ФГБУН Санкт-Петербургский институт информатики и автоматизации Российской академии наук, г. Санкт-Петербург, Россия. E-mail: kolomeec@comsec.spb.ru

3 Жернова Ксения Николаевна, младший научный сотрудник, ФГБУН Санкт-Петербургский институт информатики и автоматизации Российской академии наук, г. Санкт-Петербург, Россия. E-mail: zhernova@comsec.spb.ru

4 Чечулин Андрей Алексеевич, кандидат технических наук, доцент, ведущий научный сотрудник, ФГБУН Санкт-Петербургский институт информатики и автоматизации Российской академии наук, г. Санкт-Петербург, Россия. E-mail: chechulin@comsec.spb.ru

Таблица 1

Виды методов оценки эффективности визуализации

Степень формализации метода		Методы
Объективные	Сильные	-Веб/Поисковая аналитика -Эвристические оценки
	Относительно сильные	-А/Б и многофакторное тестирование -Контролируемые формализованные эксперименты -Неконтролируемые формализованные эксперименты -Построение маршрутов пользователей -Отслеживание взгляда
Субъективные	Слабые	-Опросы -Фокус-группы -Экспертные оценки -Мнения

ционной безопасности. Тем не менее в большинстве работ по визуальной аналитике информационной безопасности оценка эффективности визуализации либо не используется, либо применяются, в основном оценки, которые были получены экспертным путем [2]. По этой причине в статье рассматриваются методы оценки эффективности визуализации с примерами их применимости в области визуальной аналитики информационной безопасности.

Для оценки эффективности систем визуальной аналитики существует множество методов. Ключевым отличием данных методов является то, что они по-разному определяют само понятие эффективности, которое во многом зависит от используемых для оценки характеристик (свойств) моделей визуализации [3].

Рассмотрим методы, которые применимы для оценки эффективности систем визуальной аналитики данных информационной безопасности. При этом, для того чтобы охватить большинство сценариев применения, методы оценки эффективности выбирались, исходя из следующих критериев:

- применимы для оценки моделей визуализации, которые отображают данные информационной безопасности;
- могут учитывать целевую аудиторию системы визуализации;
- могут учитывать возможности лица, проводящего оценку.

Методы оценки эффективности визуализации можно классифицировать по степени формализации оценивания. Так, оценка эффективности визуализации может быть формализована (то есть, эффективность выражена в виде каких-либо формальных свойств, таких как оперативность (своевременность), точность, количество поддерживаемых графических примитивов и т.п.) или не формализована (то есть, эффективность визуализации определяется в виде текстового описания мнений экспертов, результатов анкетирования пользователей и т.д.). Также оценку эффективности визуализации можно проводить при помощи пользователя или без его участия. Таким образом, в [4] выделяются следующие группы методов оценки:

1) сильные (формализованные, без участия пользователя-испытуемого);

2) относительно сильные (формализованные, с участием пользователя-испытуемого);

3) слабые (не формализованные, с участием пользователя-испытуемого).

Сильные и относительно сильные методы основаны на обработке данных и считаются объективными, причём относительно сильные включают в себя обработку данных, получаемых в ходе проведения экспериментов. Слабые методы полностью основаны на обработке мнений пользователей, получаемых в ходе проведения экспериментов, поэтому считаются субъективными. Неформализованные методы без участия испытуемого невозможны. В таблице 1 представлены примеры методов оценки эффективности визуализации в зависимости от степени формализации.

Объективные сильные методы

Веб/Поисковая аналитика [5]. Этот метод может включать в себя анализ существующих исследований, научных публикаций и мнений о конкретной модели визуализации. Также возможно изучение обзоров и комментариев пользователей коммерческих продуктов на тему использования исследуемой визуализации. Необходимо отметить, что данный метод зачастую объединяют с опросами или интервью [6, 7]. Таким образом, с помощью веб-аналитики оценивается эффективность модели визуализации на основе предыдущих оценок, используя множество работ, в том числе из областей информационной безопасности, отличных от исследуемой [8, 9].

Эвристические оценки [11, 12]. Данный метод позволяет оценить визуализацию с помощью определенного набора формальных требований, выполнимость которых можно оценить без привлечения испытуемых. Набор таких правил может формироваться экспертами, исходя из их представлений о «лучших практиках». Примерами таких правил: высокая критичность может отображаться красным цветом, блок с сообщениями тревоги должен быть всегда на экране, используемые оттенки должны соответствовать корпоративному дизайн-коду компании и т.д. Оценка соответствия таким

правилам осуществляется по заранее определённой экспертом методике в виде баллов за каждое соответствие. Реализация считается хорошей, если оценка преодолевает определенный порог баллов.

Объективные относительно сильные методы

А/Б и многофакторное тестирование [5]. Пользователям предлагается сравнить два варианта модели визуализации, которые отличаются одним графическим примитивом. Таким образом, количественно измеряется то, как изменение того или иного графического примитива визуализации сказывается на восприятии всей графической модели целиком. Данный метод является очень популярным для оценки изменений в коммерческих продуктах с большой целевой аудиторией. Например, компании, разрабатывающие антивирусы, могут проверять на части пользователей, как изменение цвета или размера отдельных компонентов влияет на ситуационную осведомленность оператора. В этом случае можно исследовать различные варианты интерфейса на нескольких группах людей, для которых случайным образом обновили интерфейс системы, либо оставили его прежним. Данный метод позволяет сравнить эффективность небольших изменений в визуализации на этапе, когда у компании сформировалась обширная пользовательская база.

Контролируемые формализованные эксперименты [5, 6]. Представляют собой эксперименты с количественной оценкой скорости и точности с привлечением испытуемых и наблюдателей. В ходе таких экспериментов реализуется сценарий эксперимента – испытуемый решает определенные задачи с использованием тестируемой модели визуализации. Скорость и точность ответов фиксируется. Ход эксперимента записывается на камеру, видеозапись анализируется, и наблюдатели делают вывод о том, насколько корректно был поставлен эксперимент, были ли зафиксированы факторы, вызвавшие затруднения у пользователя и повлиявшие на результат и т.д. [13].

Эксперимент с измерением точности и скорости предполагает количественную оценку. Для достижения большого количества участников эксперимента и построения выборки большего размера привлекаются не только профессионалы, но и неспециалисты. По этой причине задания часто довольно абстрактны, чтобы избежать необходимости знания предметной области (например, задачи могут выглядеть как „выделить красные вершины графа“, а не „найти уязвимые хосты компьютерной сети, которые обозначены красным цветом“). Однако из-за такого абстрагирования задания могут не в полной мере отвечать реальному положению вещей, что может оказать влияние на результат [5].

Из распределений скорости и точности выполнения заданий, полученных в ходе реализации сценария, рассчитываются параметры распределений: среднее, медиана, квантили и т.п. Важно отметить, что параметры распределений имеют практический смысл только в сравнении. Поэтому данный метод может использоваться только в сравнении двух и более вариантов моделей визуализации с одним сценарием.

Неконтролируемые формализованные эксперименты. Представляют собой эксперименты с количественной оценкой скорости и точности выполнения заданий с привлечением испытуемых и без наблюдателей [14, 15]. Ключевым отличием от контролируемых формализованных экспериментов является отсутствие наблюдателей, в результате чего условия проведения эксперимента невозможно проконтролировать. Например, в неконтролируемых экспериментах, модель визуализации можно разместить на веб-сайте, а задания прислать испытуемым по электронной почте. В таком случае, испытуемые могут использовать для прохождения заданий разные устройства, для них может отличаться освещение, некоторые испытуемые могут выполнять задания недоброкачественно и т.д. Недостаток такого подхода состоит в сложности последующей оценки распределений точности и скорости, так как на результаты оказывает влияние множество факторов. Преимущество такого подхода в том, что таким способом значительно проще собрать большую группу испытуемых.

Метод *построения маршрутов пользователей* основан на анализе порядка действий, которые могут быть записаны в логи, после чего можно статистически определить параметры последовательностей [6]. Последовательности образуют маршруты действий, которые можно анализировать на предмет длины (количество действий), частоты (из которой следует востребованность пользователем) и времени, затраченного на выполнение маршрута. При помощи данного метода можно сравнивать маршруты для разных моделей визуализации, а также адаптировать модель визуализации, минимизируя длину и время для часто используемых маршрутов [5].

Например, данный метод актуален для оценки эффективности браузерных интерфейсов (из-за относительно легкого осуществления журналирования действий) и моделей визуализации в системах с большим количеством пользователей (например, публичные базы данных уязвимостей, онлайн инструменты сетевого анализа и т.д.). Данный метод позволяет собрать большое количество записей о действиях пользователя и оптимизировать процессы фильтрации или поиска, основываясь на анализе записанных маршрутов.

Отслеживание взгляда [17]. С помощью камеры можно отследить направление взгляда испытуемого, на основе чего получить тепловую карту, разделённую на зоны интереса. Например, зоны, которым уделялось больше внимания, окрашиваются в тёплые тона, участки, которые практически игнорировались, окрашиваются в холодные.

Данные методы используются для оценки интерфейсов, которые состоят из блоков с различными назначениями, например: блок сообщений тревоги, блок инцидентов, блок визуализации и т.д. Влиять на поведение пользователя можно с использованием расположения блоков, их размеров, цветовых акцентов и т.д. Определить эффективность подобного интерфейса можно при помощи отслеживания взгляда пользователя при взаимодействии с приложением: куда пользователь направляет взгляд в первую очередь, куда движется его взгляд, на каких элементах интерфейса задерживается.

Субъективные слабые методы

Опросы [5]. В процессе опроса пользователь должен дать ответы на заранее подготовленные вопросы о модели визуализации [13]. Такие ответы предполагают субъективную и (часто) эмоциональную оценку визуализации пользователем. Чаще всего при данном методе оценки эффективности визуализации используется определённая численная шкала оценивания. Например, предлагается оценить удобство по шкале от 1 до 5. На основе всего множества оценок высчитывается среднее значение, и реализация считается хорошей, если оценка преодолевает определенный порог баллов.

Опросы позволяют охватить более широкую аудиторию пользователей, в отличие от других методов. Однако сами по себе опросы не дают качественной оценки визуализации и должны использоваться вместе с другими методами оценки [5].

Фокус-группы [5]. Фокус-группы формируются из пользователей, соответствующих каким-то определённым критериям, например, в соответствии с заданной специализацией или опытом работы. Далее пользователи отобранной фокус-группы опрашиваются относительно разработанной модели визуализации. Ключевым отличием от опросов, является то, что опрашиваемым необходимо коллективно сформировать и обосновать свое мнение. Необходимо отметить, что распространено использование фокус-групп на этапе разработки продукта, когда из коллективного мнения опрашиваемых формируются требования к модели визуализации, которые затем учитываются разработчиками.

Экспертные оценки [6]. Для оценки модели визуализации приглашаются эксперты, имеющие опыт в разработке или применении на практике моделей визуализации. Например, в [16] в качестве экспертов выступали социологи, которые проводили оценку динамических графов социальных сетей. Эксперты могут обозначить проблемы, возникающие при эксплуатации модели визуализации в их профессиональной сфере [18][19]. Преимуществом такого подхода является то, что для оценки визуализации достаточно небольшое количество экспертов. Экспертный подход полезен в случаях, когда проблематично собрать большую или репрезентативную выборку из потенциальных пользователей системы.

Мнения друзей, коллег, а также личный опыт [10]. Данный метод подразумевает сбор мнений пользователей вне зависимости от их компетенции и каких-либо других критериев. Распространенными сценариями являются оценка методом сбора мнений в ходе демонстрации прототипа на конференции или анализ отзывов о продукте в сети Интернет. Отдельно можно отметить сбор мнений в ходе прототипирования [16] – пользователям предлагается сравнить несколько разных прототипов модели визуализации. Прототипы создаются с использованием соответствующих программ, например, Adobe XD. После этого прототипы показывают пользователям, высказывающим свои мнения, которые необходимо учесть в последующей разработке. Прототипирование позволяет заранее получить обратную связь от предполагаемого пользователя, еще до этапа разработки самой системы.

3. Классификация методов оценки эффективности визуализации

Разные методы оценки эффективности визуализации могут использоваться на различных стадиях разработки. Например, на стадии проектирования разработчик может собрать предварительные мнения, продемонстрировав прототип, провести поисковую аналитику или собрать фокус-группу. Во время непосредственной разработки могут приглашаться эксперты, проводиться контролируемые эксперименты. Финальная стадия, когда продукт уже присутствует на рынке и у него есть множество пользователей, может включать в себя неконтролируемые эксперименты, А/Б тестирование. При этом на разных этапах могут применяться методы оценки эффективности визуализации с различной степенью формализации.

Выбор методики также зависит от возможностей разработчика, например, возможности оборудовать помещение для контролируемого эксперимента, сформировать большую группу испытуемых, собрать экспертов и т.д.

По этой причине, в данной работе также приводится несколько классификаций методов оценки эффективности визуализации, которые помогут понять, какие методы оценки целесообразнее всего применить в той или иной ситуации. Методы оценки эффективности визуализации были классифицированы по следующим признакам:

1) по графическим примитивам;
2) по квалификации аудитории;
3) по типу эксперимента.

Классификация по графическим примитивам (таблица 2) предполагает, что будут оцениваться отдельные графические примитивы модели визуализации, либо модель визуализации, либо интерфейс программного обеспечения или сайта, который содержит данную модель визуализации. Чаще всего оценка отдельных графических примитивов необходима при разработке массового продукта, когда, например, в антивирусах, даже небольшое изменение в цвете позволит статистически большему числу людей чаще обращать внимание на угрозы. Оценка модели визуализации чаще всего необходима на этапе разработки прототипа, а интерфейса — для оценки готового продукта.

Программный продукт может разрабатываться как для массового пользователя, так и для решения специфических задач узкого круга специалистов или бизнеса. Аудитория, использующая продукт, также может различаться по уровню квалификации. Массовый продукт, скорее всего, будет предназначен для неквалифицированной аудитории, в то время как для решения специфических задач требуется определённая квалификация. В зависимости от того, квалифицирован ли потенциальный пользователь или нет, используются различные методы оценки эффективности моделей визуализации. Таким образом, классификация по тестируемой аудитории (таблица 3) подразделяет методы оценки эффективности модели визуализации на те, которые подходят для неквалифицированных пользователей (используются в случае, если разрабатывается массовый продукт), и те, которые

DOI:10.21681/2311-3456-2021-6-36-45

Таблица 2

Классификация методов оценки эффективности визуализации по графическим примитивам

Признак	Метод
Проверяют определённый графический примитив	-Веб/поисковая аналитика -А/Б и многофакторное тестирование -Контролируемые формализованные эксперименты -Неконтролируемые формализованные эксперименты
Проверяют объект в целом	-Веб/поисковая аналитика -Эвристические оценки -Контролируемые эксперименты -Неконтролируемые формализованные эксперименты -Отслеживание взгляда -Опросы -Фокус-группы -Экспертные оценки -Мнения
Проверяют интерфейс	-Веб/поисковая аналитика -Эвристические оценки -Контролируемые эксперименты -Неконтролируемые формализованные эксперименты -Построение маршрутов пользователей -Отслеживание взгляда -Опросы -Фокус-группы -Экспертные оценки -Мнения

Таблица 3

Классификация методов оценки эффективности визуализации по тестируемой аудитории

Признак	Метод
Для неквалифицированных пользователей	Все методы оценки
Для квалифицированных пользователей	-Веб/Поисковая аналитика -Эвристические оценки -Контролируемые формализованные эксперименты -Отслеживание взгляда -Фокус-группы -Мнения

предназначены для квалифицированных пользователей (используются для решения специфических задач).

Возможности разработчика определяют выбор эксперимента. Если разработчик имеет возможность привлечь испытуемых, в зависимости от их количества и квалификации, разработчик может проводить различные виды экспериментов. Оценку можно получить в абсолютном виде (результаты эксперимента на одной группе), либо в сравнении с другим продуктом/моделью/интерфейсом/т.п. (результаты эксперимента в двух группах сравниваются). Также получение ответов от пользователей может быть осознанным (испытуемому задают вопросы – более субъективная оценка), либо не осознанным, когда разработчик следит за невербальной реакцией испытуемого (например, замеряет скорость и точность выполнения заданий, либо направление взгляда – более объективная оценка).

Таким образом, классификация по типу эксперимента (таблица 4) разделяет методы оценки эффективности модели визуализации на методы с проведением эксперимента и методы без проведения эксперимента. Методы с проведением эксперимента, в свою очередь, классифицируются по количеству групп, участвующих в эксперименте (могут проводиться эксперименты с одной группой или с несколькими группами), и по осознанности ответа (ответ на тестовое задание может даваться осознанно – например, в случае опросов, и не осознанно – например, при отслеживании взгляда пользователя). В некоторых случаях проведение эксперимента не представляется возможным ввиду невозможности привлечения испытуемых, для чего в том числе существуют методы оценки эффективности визуализации.

Выбор необходимого метода оценки может производиться с использованием выделенных классификаций.

Таблица 4

Классификация методов оценки эффективности визуализации по типу эксперимента

Признак			Метод
С проведением эксперимента	По группам	Две группы	-А/Б и многофакторное тестирование -Контролируемые формализованные эксперименты -Неконтролируемые эксперименты -Фокус-группы
		Одна группа	-Построение маршрутов пользователей -Отслеживание взгляда -Опросы -Фокус-группы -Экспертные оценки -Мнения
	По осознанности ответа	Осознанно	-Опросы -Фокус-группы -Экспертные оценки -Мнения
		Не осознанно	-А/Б и многофакторное тестирование -Контролируемые формализованные эксперименты -Неконтролируемые формализованные эксперименты -Построение маршрутов пользователей -Отслеживание взгляда
Без проведения эксперимента			-Веб/Поисковая аналитика -Эвристические оценки

По разработанным классификациям можно определить применимость методов оценки эффективности, исходя из требований и возможностей разработчика:

- что именно оценивается – отдельный графический примитив, модель визуализации в целом или интерфейс программного обеспечения/сайта;
- какой продукт разрабатывается – массовый или специализированный;
- есть ли возможность привлечения группы испытуемых и проведения экспериментов;
- есть ли возможность произвести измерения, например, скорости и (или) точности выполнения заданий (от этого зависит, насколько сильной будет формализация метода оценки эффективности модели визуализации);
- есть ли возможность обратиться к экспертному сообществу.

4. Сравнительный анализ методов визуализации по областям применения в информационной безопасности

В работе [1] было продемонстрировано, что текущее применение визуализации достаточно распространено, и в каждой области безопасности есть сразу несколько задач, которые решают с использованием визуальной аналитики. При этом можно заметить закономерность, что для решения одной и той же задачи часто используется одна и та же модель визуализации, хоть и в различном представлении. В данном разделе представлен анализ работ, исходя из классификации по областям применения [1] и классификации по моделям визуализации [1].

В задаче контроля доступа визуализация в основном используется для анализа иерархических моделей безопасности (RBAC и их производных) или управления доступом к иерархии файловых систем. Для этого применяется модель карты деревьев или модель упаковки шаров, которая весьма похожа на карты деревьев. Для анализа иерархии ролей используются графы-деревья. Для отображения взаимосвязей субъектов и объектов в дискреционных моделях могут применяться графы и матрицы.

В задачах обнаружения и предотвращения утечек информации визуализация сводится к анализу истории событий, но, в зависимости от контекста, для этого применяются различные модели. Так, для анализа сессий используются графы, для перемещений сотрудников – тепловые карты и BandView (разновидность столбчатого графика). Для анализа активности сотрудника используется множество моделей, таких как матрицы, графики рассеивания, параллельные координаты и простейшие графики, такие как круговые диаграммы и потоковые графики.

В форензике основной задачей визуализации является анализ истории событий и подготовка доказательств в легко воспринимаемом графическом виде (например, для суда). Основными сценариями являются: исторический анализ трафика с помощью параллельных координат, матриц и графиков рассеивания; анализ связей между людьми с помощью графов; анализ логов или событий с помощью простейших графиков; обнаружение местонахождения сетевого следа злоумышленника, а также анализ файловых систем с

DOI:10.21681/2311-3456-2021-6-36-45

помощью графов-деревьев и матриц. Также к данной категории относится и анализ логов систем банковских транзакций, которые используют графы и столбчатые графики. Для анализа паттернов поведения пользователей используются диаграммы типа матриц и графов для обнаружения мошенничества.

В сетевой безопасности визуальная аналитика крайне разнообразна и в основном используется для анализа или мониторинга инцидентов безопасности компьютерных сетей в рамках систем предотвращения вторжений. К этим задачам также относятся управление межсетевыми экранами, анализ географии атак, анализ трафика сети, анализ файлов, анализ доменов и ситуационная осведомленность оператора.

Для анализа событий и инцидентов с целью предотвращения вторжений в сети используются графы атак и событий. Карты деревьев или упаковки шаров применяются для визуализации иерархических сетей. Матрицы, хордовые диаграммы – для неструктурированных сетей. Параллельные координаты, столбчатые графики и графики рассеивания – для визуализации сетевых параметров. Цифровой след злоумышленника просматривается и с помощью круговой диаграммы со слоями.

Кроме того, можно отдельно выделить большой пласт работ в области визуализации сетевых экранов, где выделяют две основные функции визуализации – управление правилами, где используются матрицы, деревья и параллельные координаты, а также мониторинг работы – где применяются графы и параллельные координаты.

Визуализация также используется для анализа географии атак. Географические карты, которые часто совмещаются с тепловыми картами, помогают отслеживать степень опасности загружаемых файлов, а также географическое положение источника атаки. С помощью тепловых карт также визуализируют количественные показатели. Географические карты с элементами связей графа используются для изучения анализа поведения пользователей в сети.

Трафик сети изучается с помощью гистограмм, а круговые диаграммы отображают срабатывание сигналов тревоги. Столбчатые графики и закрашенные области применяются, чтобы оценить и визуализировать объем и поведение трафика. Поведение трафика также отслеживается с помощью матриц и линейных графиков, потоковых графиков и графиков рассеивания. Также можно осуществлять мониторинг пакетов, передающихся по сети. Гистограммы показывают промежутки времени между аномалиями трафика, а параллельные координаты используются для визуализации связей между аномалиями. Матрицы показывают различные группы пакетов.

Для анализа доменов используются графики рассеивания, которые могут применяться для визуализации процентного соотношения, например, заблокированных доменов. Карту доменов можно также построить с помощью матриц.

Анализ файлов осуществляется с помощью графиков рассеивания, которые показывают уровень доверенности файлов, а пузырьковая диаграмма применяется для наблюдения за файлами, которые передаются по сети.

Для визуализации тревоги используют пузырьковые диаграммы и карты деревьев.

В случае анализа рисков для обеспечения безопасности сети задача визуальной аналитики, как правило, сводится к анализу активов и выработке контрмер. Для анализа активов используются представления активов в виде различных сетей: вероятностных графов атак (могут быть представлены в виде вариации наложения графа на модель матрицы) и графов зависимостей сервисов. Для выработки контрмер применяются двухмерные геометрические графики для анализа метрик (таких как критичность, доступность, восстанавливаемость и др.), и трехмерные – для наглядной демонстрации того, как контрмера влияет на атаку.

При анализе социальных сетей, как и в форензике, визуализация используется в рамках расследований. Почти всегда применяется анализ графов социальных связей между пользователями или связи контента. К другим сценариям можно отнести анализ метрик пользователей, для отображения которых выбираются линейные, круговые и прочие простейшие графики, а для гео-метрик – карты. Кроме того, распространен анализ текстового содержимого с помощью облака слов.

В вирусологии и реверс-инжиниринге основное применение визуализации – это анализ бинарного представления вредоносного программного обеспечения с использованием матриц, которые позволяют по паттернам изображения определить семейство вредоносного кода. Также для анализа вредоносного кода применяют графы вызова функций, а для анализа найденных в приложении уязвимостей – карты деревьев.

К другим решаемым задачам можно отнести анализ метрик вредоносного кода с помощью графиков рассеивания, матриц и простейших графиков для определения схожести и выявления семейств отдельных фрагментов кода. Такая визуализация используется при проактивном анализе паттернов поведения с помощью столбчатых диаграмм, который в том числе включает анализ поведения вируса в сети с помощью графов и анализ трафика, генерируемого вирусом, с помощью матриц.

Для простоты сравнения методов визуализации и их возможностей применения в задачах информационной безопасности была разработана специальная карта публикаций (рис. 1 и рис. 2). Данная карта доступна по адресу http://comsec.spb.ru/files/cyberVis/.

Данная карта представляет собой силовой граф со скрытыми ребрами, которые связывают публикации по тому или иному параметру. Карта позволяет определить схожесть представленных в данном обзоре работ и группировать имеющиеся публикации по следующим признакам:

- областям применения (столбец “область”);
- задачам (столбец “задача”);
- применяемым моделями визуализации (столбец “модель”).

При наведении на публикацию ребрами отображаются схожие работы.

Публикации также можно фильтровать по областям применения, задачам, моделям визуализации и году. При наведении на публикацию с помощью ребер ука-

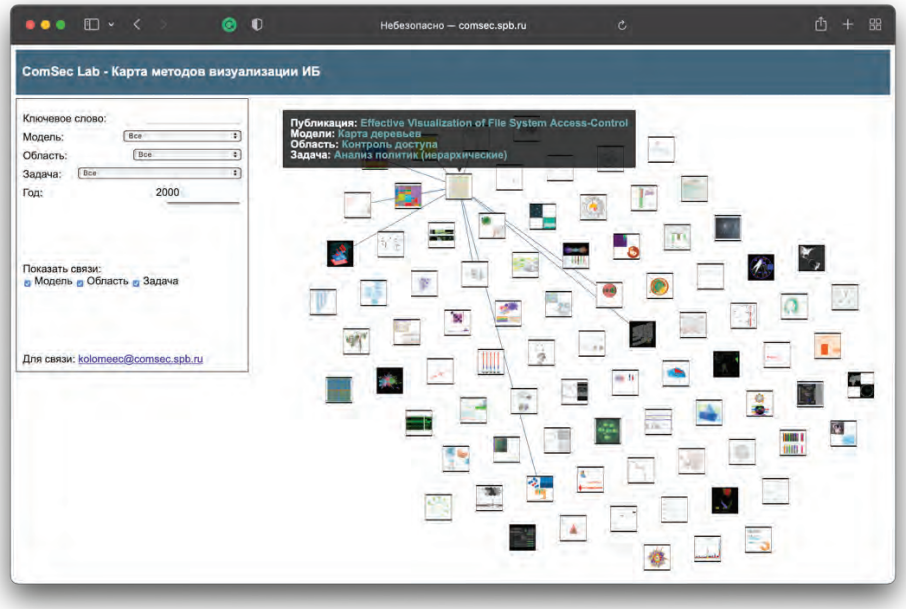

Рис. 1. Карта публикаций. Общее представление

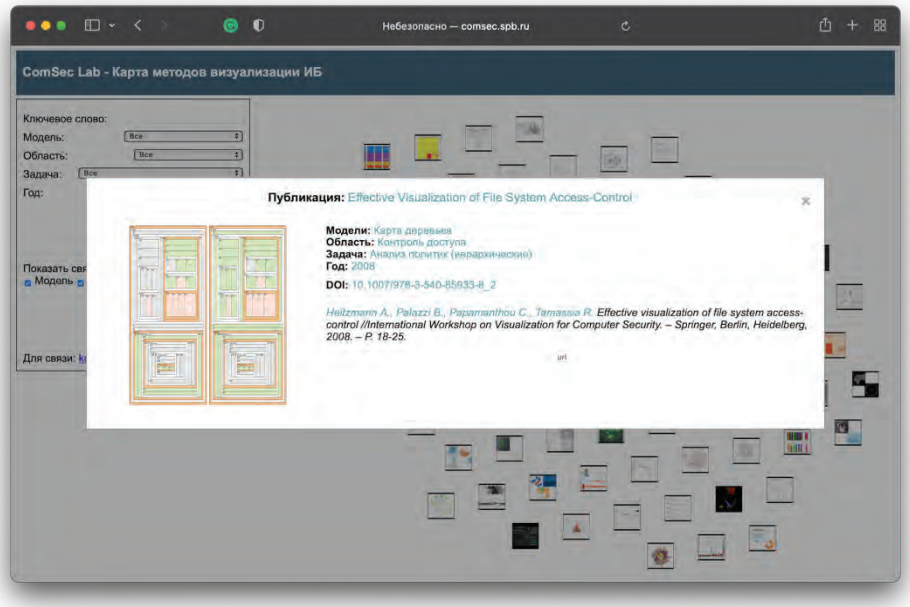

Рис. 2. Карта публикаций. При нажатии на публикацию можно посмотреть дополнительную информацию и перейти на страницу выбранной работы

зываются схожие работы в зависимости от выбранных параметров группировки и фильтрации, а при нажатии на публикацию будет отображена более подробная информация (рис. 2): название публикации, представленные в публикации модели визуализации, изображение моделей из работы, область применения, решаемая задача, год, DOI, цитирование по ГОСТ и кнопка для перехода на страницу публикации в Интернете.

5. Заключение

В работе представлен анализ методов оценки эффективности р визуальных средств взаимодействия оператора с приложениями информационной безопасности, исходя из возможности или невозможности привлечь испытуемых или экспертов. Выделены три группы методов оценки: сильные (формализованные, без участия пользователя-испытуемого); относительно сильные (формализованные, с участием пользователя-испытуемого); слабые (не формализованные, с участием пользователя-испытуемого).

В работе также проведена сравнительная оценка методов визуализации, исходя из классификации по областям применения и классификации по моделям визуализации, и их возможное применение рассмотренных

моделей визуализации для различных задач информационной безопасности. Также представлена карта методов визуализации, которая позволит ориентироваться в публикациях, представленных в статье. Предполагается, что данная карта будет полезна как специалистам в области процессов поддержки и принятия решений, так и разработчикам систем защиты информации, которые желают внедрить визуальную аналитику в свои системы. Кроме того, эта карта может быть полезна студентам, обучающимся по направлению “Информационная безопасность”, как отправная точка в области визуализации данных безопасности.

Будущее направление исследований авторов по использованию моделей визуализации связано с анализом конкретных реализаций систем визуальной аналитики для информационной безопасности и практической реализацией ряда решений по визуализации в системах мониторинга информационной безопасности.

Рецензент: *Саенко Игорь Борисович, доктор технических наук, профессор, ведущий научный сотрудник Санкт-Петербургского Федерального исследовательского центра Российской академии наук, Санкт-Петербург, Россия. E-mail: ibsaen@comsec.spb.ru*

Литература

1. Котенко И.В., Коломеец М.В., Жернова К.Н., Чечулин А.А. Визуальная аналитика для кибербезопасности: области применения, задачи и модели визуализации // Вопросы кибербезопасности, № 4 (44), 2021. С.2-15. DOI: 10.21681/2311-3456-2021-4-2-15
2. Интеллектуальные сервисы защиты информации в критических инфраструктурах / И.В.Котенко, И.Б.Саенко, А.А.Чечулин [и др.]; под общей ред. И.В.Котенко, И.Б.Саенко. СПб.: БХВ-Петербург, 2019. 400 с. ISBN 978-5-9775-3968-5.
3. Коломеец М.В., Чечулин А.А., Котенко И.В. Обзор методологических примитивов для поэтапного построения модели визуализации данных // Труды СПИИРАН. 2015. Вып. 5 (42). С. 232-257.
4. Travis D., Hodgson P. Think Like a UX Researcher: How to Observe Users, Influence Design, and Shape Business Strategy. CRC Press, 2019.
5. Hullman J. et al. In pursuit of error: A survey of uncertainty visualization evaluation // IEEE transactions on visualization and computer graphics. 2018. Vol. 25. №. 1. Pp. 903-913.
6. Song H., Szafir D. A. Where’s my data? evaluating visualizations with missing data // IEEE transactions on visualization and computer graphics. 2018. Т. 25. №. 1. С. 914-924.
7. Cappers B.C.M., Wijk J.J. Understanding the context of network trac alerts // 2016 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2016. P. 1-8.
8. Angelini M., Aniello L., Lenti S., Santucci G., Ucci D. The goods, the bads and the uglies: Supporting decisions in malware detection through visual analytics // 2017 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2017. Pp. 1-8.
9. Chen Si., Chen Sh., Andrienko N., Andrienko G., Nguyen P., Turkay C., Thonnard O., Yuan X. User behavior map: Visual exploration for cyber security session data // 2018 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2018. Pp. 1-4.
10. Staheli D., Yu T., Crouser J., Damodaran S., Nam K., O’Gwynn D., McKenna S., Harrison L. Visualization evaluation for cyber security: Trends and future directions // Proceedings of the Eleventh Workshop on Visualization for Cyber Security. 2014. Pp. 49-56.
11. Dowding D., Merrill J. A. The development of heuristics for evaluation of dashboard visualizations // Applied clinical informatics. 2018. vol. 9. no. 03. Pp. 511-518.
12. Zuk T., Schlesier L., Neumann P., Hancock M., Carpendale S. Heuristics for information visualization evaluation // Proceedings of the 2006 AVI workshop on BEyond time and errors: novel evaluation methods for information visualization. 2006. Pp. 1-6.
13. Arendt D. L., Burtner R., Best D. M., Bos N. D., Gersh J. R., Piatko C. D., Paul C. L. Ocelot: user-centered design of a decision support visualization for network quarantine // 2015 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2015. Pp. 1-8.
14. Arendt D. L., Lyndsey R. F., Yang F., Brisbois B., LaMothe R. Crush Your Data with ViC 2 ES Then CHISSL Away // 2018 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2018. Pp. 1-8.
15. Yang Y., Collomosse J., Manohar A., Briggs J., Steane J. Tapestry: Visualizing interwoven identities for trust provenance // 2018 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2018. Pp. 1-4.
16. Elmqvist N., Yi J. S. Patterns for visualization evaluation //Information Visualization. 2015. vol. 14. No. 3. Pp. 250-269.
17. Fu B., Noy N. F., Storey M. A. Eye tracking the user experience–An evaluation of ontology visualization techniques // Semantic Web. 2017. vol. 8. No. 1. Pp. 23-41.
18. Kim H., Ko S., Kim D., Kim H. Firewall ruleset visualization analysis tool based on segmentation // 2017 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2017. Pp. 1-8.
19. Arendt D., Best D., Burtner R., Lyn Paul C. CyberPetri at CDX 2016: Real-time network situation awareness // 2016 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2016. Pp. 1-4.

VISUAL ANALYTICS FOR INFORMATION SECURITY: EFFICIENCY ASSESSMENT AND ANALYSIS OF VISUALIZATION METHODS

Kotenko I.V.[5], Kolomeec M.V.[6], Zhernova K.N.[7], Chechulin A.A.[8]

The purpose of the article: *to identify and systematize information security problems that are solved using visual analytics methods, applied data visualization models and methods for assessing the effectiveness of visualization models.*

Research method: *a systematic analysis of the application of visual analytics methods for solving information security problems. Analysis of relevant work in the field of information security and data visualization, as well as methods for assessing visualization. The objects of research are: solving information security problems through visual analysis and methods for assessing the effectiveness of visualization models.*

The result obtained: *an interactive map of visualization models and their areas of application is presented, which will allow researchers and developers to choose the visualization models that are most appropriate for specific applied information security problems. A classification of methods for assessing visualization is presented.*

The scope of the proposed approach is the creation of visualization models that can be used to increase the efficiency of operator interaction with information security applications. The proposed article will be useful both for students studying in the direction of training "Information Security", and for specialists who develop information security systems.

Keywords: *visual means of interaction, visualization model, methods of evaluation, classification of evaluation methods, data structure, data analysis, support and decision-making.*

References

1. Kotenko I.V., Kolomeetc M.V., Zhernova K.N., Chechulin A.A. Vizual`naia analitika dlia kiberbezopasnosti: oblasti primeneniia, zadachi i modeli vizualizatcii // Voprosy` kiberbezopasnosti, № 4 (44), 2021. C.2-15. DOI: 10.21681/2311-3456-2021-4-2-15
2. Intellektual`ny`e servisy` zashchity` informatcii v kriticheskikh infrastrukturakh / I.V.Kotenko, I.B.Saenko, A.A.Chechulin [i dr.]; pod obshchei` red. I.V.Kotenko, I.B.Saenko. SPb.: BKHV-Peterburg, 2019. 400 s. ISBN 978-5-9775-3968-5.
3. Kolomeetc M.V., Chechulin A.A., Kotenko I.V. Obzor metodologicheskikh primitivov dlia poe`tapnogo postroeniia modeli vizualizatcii danny`kh // Trudy` SPIIRAN. 2015. Vy`p. 5 (42). C. 232-257.
4. Travis D., Hodgson P. Think Like a UX Researcher: How to Observe Users, Influence Design, and Shape Business Strategy. CRC Press, 2019.
5. Hullman J. et al. In pursuit of error: A survey of uncertainty visualization evaluation // IEEE transactions on visualization and computer graphics. 2018. Vol. 25. №. 1. Pp. 903-913.
6. Song H., Szafir D. A. Where's my data? evaluating visualizations with missing data // IEEE transactions on visualization and computer graphics. 2018. T. 25. №. 1. C. 914-924.
7. Cappers B.C.M., Wijk J.J. Understanding the context of network trac alerts // 2016 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2016. P. 1-8.
8. Angelini M., Aniello L., Lenti S., Santucci G., Ucci D. The goods, the bads and the uglies: Supporting decisions in malware detection through visual analytics // 2017 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2017. Pp. 1-8.
9. Chen Si., Chen Sh., Andrienko N., Andrienko G., Nguyen P., Turkay C., Thonnard O., Yuan X. User behavior map: Visual exploration for cyber security session data // 2018 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2018. Pp. 1-4.
10. Staheli D., Yu T., Crouser J., Damodaran S., Nam K., O'Gwynn D., McKenna S., Harrison L. Visualization evaluation for cyber security: Trends and future directions // Proceedings of the Eleventh Workshop on Visualization for Cyber Security. 2014. Pp. 49-56.
11. Dowding D., Merrill J. A. The development of heuristics for evaluation of dashboard visualizations // Applied clinical informatics. 2018. vol. 9. no. 03. Pp. 511-518.

5 Igor V. Kotenko, Dr.Sc., Professor, Head of Laboratory of Computer Security Problems at St. Petersburg Institute for Informatics and Automation of Russian Academy of Science, St. Petersburg, Russia. Email: ivkote@comsec.spb.ru

6 Maxim V. Kolomeec, Junior Research fellow at St. Petersburg Institute for Informatics and Automation of Russian Academy of Science, St. Petersburg, Russia. Email: kolomeec@comsec.spb.ru

7 Maxim V. Kolomeec, Junior Research fellow at St. Petersburg Institute for Informatics and Automation of Russian Academy of Science, St. Petersburg, Russia. Email: kolomeec@comsec.spb.ru

8 Andrey A. Chechulin, Ph.D., Leading Research fellow at St. Petersburg Institute for Informatics and Automation of Russian Academy of Science, St. Petersburg, Russia. E-mail: chechulin@comsec.spb.ru

12. Zuk T., Schlesier L., Neumann P., Hancock M., Carpendale S. Heuristics for information visualization evaluation // Proceedings of the 2006 AVI workshop on BEyond time and errors: novel evaluation methods for information visualization. 2006. Pp. 1-6.
13. Arendt D. L., Burtner R., Best D. M., Bos N. D., Gersh J. R., Piatko C. D., Paul C. L. Ocelot: user-centered design of a decision support visualization for network quarantine // 2015 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2015. Pp. 1-8.
14. Arendt D. L., Lyndsey R. F., Yang F., Brisbois B., LaMothe R. Crush Your Data with ViC 2 ES Then CHISSL Away // 2018 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2018. Pp. 1-8.
15. Yang Y., Collomosse J., Manohar A., Briggs J., Steane J. Tapestry: Visualizing interwoven identities for trust provenance // 2018 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2018. Pp. 1-4.
16. Elmqvist N., Yi J. S. Patterns for visualization evaluation //Information Visualization. 2015. vol. 14. No. 3. Pp. 250-269.
17. Fu B., Noy N. F., Storey M. A. Eye tracking the user experience–An evaluation of ontology visualization techniques // Semantic Web. 2017. vol. 8. No. 1. Pp. 23-41.
18. Kim H., Ko S., Kim D., Kim H. Firewall ruleset visualization analysis tool based on segmentation // 2017 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2017. Pp. 1-8.
19. Arendt D., Best D., Burtner R., Lyn Paul C. CyberPetri at CDX 2016: Real-time network situation awareness // 2016 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2016. Pp. 1-4.