ВИЗУАЛЬНАЯ АНАЛИТИКА ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ОБЛАСТИ ПРИМЕНЕНИЯ, ЗАДАЧИ И МОДЕЛИ ВИЗУАЛИЗАЦИИ

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

Цель статьи: *выявление и систематизация областей и задач информационной безопасности, решаемых с использованием методов визуальной аналитики, а также анализ применяемых моделей визуализации и их свойств, влияющих на восприятие данных оператором.*

Метод исследования: *системный анализ применения методов визуальной аналитики для решения задач информационной безопасности. Анализ релевантных работ в области информационной безопасности и визуализации данных. Объектами исследования являются: теоретические и практические решения задач информационной безопасности посредством визуального анализа. Визуальная аналитика в статье рассматривается с нескольких сторон: с точки зрения областей применения методов визуального анализа в информационной безопасности, с точки зрения решаемых аналитиком задач, с точки зрения применяемых моделей визуализации и используемых структур данных, а также с точки зрения свойств моделей визуализации данных.*

Полученный результат: *предложена классификация моделей визуализации, отличающаяся тем, что она основана на анализе областей и задач информационной безопасности и соответствующих им моделей визуализации.*

Область применения предложенного подхода – создание моделей визуализации, которые могут использоваться для повышения эффективности взаимодействия оператора с приложениями информационной безопасности. Предлагаемая статья будет полезна как специалистам, разрабатывающим системы защиты информации, так и студентам, обучающимся по направлению подготовки „Информационная безопасность“.

Ключевые слова: *информационная безопасность, визуальная аналитика, анализ данных, поддержка и принятие решений, модель визуализации, визуализация данных.*

DOI:10.21681/2311-3456-2021-4-2-15

1. Введение

Визуальная аналитика является одним из инструментов анализа данных, наряду с методами машинного обучения и статистики. Визуализация используется в тех процессах поддержки и принятия решений, в которых задействован человек, упрощая восприятие информации, и тем самым повышая эффективность анализа информации, в том числе оперативность (своевременность) принятия решений и их обоснованность. Зачастую в системах информационной безопасности задействован оператор или эксперт, на плечи которого ложится задача оперативного (своевременного) и обоснованного принятия решений. Таким образом, возникает необходимость обеспечить оператора арсеналом методов визуальной аналитики по целому ряду решаемых задач безопасности. Для разработки новых средств визуальной аналитики (которые всегда основаны на синтезе уже существующих решений), необходимо понимать возможные способы визуализации, их составляющие, особенности применения тех или иных компонентов визуализации, а также знать методы оценки эффективности разрабатываемых решений.

В данной работе представлен анализ текущего состояния визуальной аналитики в области информационной безопасности. Научная значимость работы состоит в разработке классификации использования методов визуализации для различных задач информационной безопасности. Данная классификация может являться фундаментальной базой для определения областей применения, научной новизны и практической значимости последующих работ по визуализации данных безопасности.

Практическая значимость данной работы состоит в возможности использования предложенной классификации моделей визуализации в процессе разработки

1 Котенко Игорь Витальевич, доктор технических, 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, аспирант, 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

систем визуальной аналитики для различных областей информационной безопасности.

Работа организована следующим образом. Во втором разделе представлен анализ областей применения визуализации данных, на основе которого выделены области применения визуализации для информационной безопасности и решаемые задачи. В третьем разделе рассматриваются графические примитивы, используемые для визуализации. В четвертом разделе приводятся основные свойства моделей визуализации. В пятом разделе представлена классификация моделей визуализации по структуре данных, и выделены показатели визуализации.

2. Области применения и задачи визуализации

Основная область применения визуальной аналитики – это поддержка и принятие решений. Визуализация используется как дополнительный инструмент оператора, позволяющий принимать решения более эффективно.

На верхнем уровне абстракции, вне зависимости от области применения, можно выделить следующие задачи визуальной аналитики, решаемые с использованием средств визуализации: (1) презентация, (2) мониторинг, (3) расследование и (4) управление. Презентация служит для объяснения результатов анализа данных безопасности и включает в себя различные отчеты, графический материал и т.п. Мониторинг, как правило, сводится к отслеживанию динамики событий и инцидентов. Для мониторинга, зачастую, используются различные информационные панели (dashboard), функционирующие в режиме реального времени, или периодические отчеты. Расследование подразумевает поиск событий и инцидентов в наборах данных. Как правило, оно осуществляется на основе визуализации результатов работы узконаправленных программ анализа данных (анализ трафика, кода и т.п.) и выполняется на различных уровнях детализации данных, причем, как правило, применяются развитые возможности по навигации (поиск элементов в изображении) и фильтрации. Управление осуществляется на основе изменения настроек системы, при этом используются различные возможности по детализации, навигации и фильтрации.

Подобная классификация является традиционным представлением задач, решаемых визуальной аналитикой во многих областях - от биоинформатики до журналистики. Несмотря на универсальность, она не отражает в очевидном виде специфику информационной безопасности, которая заключается в решении конкретных задач защиты информации. Кроме того, если попробовать применить данную классификацию к существующим коммерческим системам информационной безопасности, решаемые аналитиком задачи могут совмещаться. Например, как правило, SIEM-системы включают задачи мониторинга и презентации, DLP-системы - мониторинг и расследование, сетевая криминалистика - расследование и презентации, и т.д.. По этой причине, в данной работе предлагается классификация, основанная не на задачах визуальной аналитики, а на задачах информационной безопасности. Под задачей информационной безопасности будет подразумеваться конкретная задача, стоящая перед аналитиком в рамках обеспечения процесса защиты информации, которую он решает с использованием той или иной системы информационной безопасности.

Подобное определение позволяет:

— выбирать модели визуализации для конкретной задачи информационной безопасности, причем одна и та же задача может решаться несколькими методами визуального анализа, которые выражаются в виде используемой модели визуализации; таким образом, можно увидеть зависимость между применяемыми решениями по визуализации данных и задачей информационной безопасности.
— определять область применения для множества задач информационной безопасности, причем одна и та же система защиты информации может решать сразу несколько задач, и по этой причине их целесообразно объединять в области применения, которые будут являться отображением класса систем защиты информации и специализации аналитика, работающего с данной системой; следовательно, можно увидеть применимость тех или иных моделей визуализации в рамках определенного класса систем защиты информации, а также какие именно модели визуализации используются в рамках той или иной специализации аналитика.

Таким образом, классификация базируется на учете задачи информационной безопасности, области применения и модели визуализации. На основе данного подхода производился выбор работ (публикаций) для данного анализа и их классификация. Критерии выбора работ состояли в следующем:

— в работе должна решаться конкретная задача информационной безопасности с помощью средств визуальной аналитики. Работы по визуализации данных, не ориентированные на решение задач, связанных с информационной безопасностью, исключались из обзора;
— работа должна опираться на программную реализацию предлагаемого процесса визуального анализа, выраженную в виде модели визуализации;
— работа должна сопровождаться графическим материалом, представляющим предлагаемую реализацию модели визуализации;
— модель визуализации использует данные, полученные от систем информационной безопасности; работы, включающие инфографику организационных процессов обеспечения защиты информации, и прочие модели, не использующие данные, полученные от конкретных информационных систем, исключались из обзора;
— работа должна быть не старше 2000 года.

Работы группировались по задачам информационной безопасности. В результате было выделено 29 задач, которые представлены в таблице 1.

Исходя из задач, были сформированы следующие области применения:

— контроль доступа и политики безопасности – включают в себя системы контроля и управления доступом, системы обеспечения прав доступа файловых

Таблица 1

Карта использования моделей визуализации данных для различных областей информационной безопасности

Область	Задача	Пример
Контроль доступа и политики безопасности	Анализ политик в иерархических моделях безопасности	Карта деревьев [1][2] Матрица [2] Дерево [2][3]
	Анализ политик в дискреционных моделях безопасности	Граф [4] Матрица [4]
Предотвращение и обнаружение утечек информации	Анализ активности сотрудника	Простейший график [6][7] Граф [6] Матрица [7] Дерево [7] График потока [7] График рассеивания [7] Параллельные координаты [7]
	Анализ данных сессий	Граф [5]
	Анализ перемещения сотрудников	Простейший график [6] Граф [6]
Цифровая криминалистика	Анализ исторических данных трафика	Параллельные координаты [8] Простейший график [8] График рассеивания [8]
	Анализ связей между людьми	Граф [9] Простейший график [9] Дерево [10]
	Анализ логов	Простейший график [9] Граф [9] Матрица [11] Дерево [11] График рассеивания [11] Гео-карта [43]
	Анализ файловых систем	Матрица [11] Дерево [11] График рассеивания [11]
	Анализ транзакций	Граф [12] Простейший график [13]
	Обнаружение мошенничества	Матрица [14] Граф [14]
Сетевая безопасность	Анализ и мониторинг инцидентов в IDS	Граф [15] Параллельные координаты [18] Дерево [16] Тепловая карта [15] Матрица [15][16] Простейший график [15][16] График рассеивания [17] Хордовая диаграмма [35]
	Управление правилами межсетевых экранов	Матрица [19] Граф [19] Дерево [20]
	Мониторинг работы межсетевых экранов	Матрица [19] Граф [19]

Область	Задача	Пример
Сетевая безопасность	Анализ географии атак	Матрица [15] Граф [15] Простейший график [15][22] Тепловая карта [21][23] Гео-карта [22][23] График рассеивания [21] Параллельные координаты [23]
	Анализ трафика сети	Матрица [16] Дерево [16] Простейший график [16][22] Параллельные координаты [18] График рассеивания [24] Гео-карта [22] График потока [24]
	Анализ доменов	Матрица [15] Граф [15] Простейший график [15] Тепловая карта [15] График рассеивания [25]
	Анализ файлов	Гео-карта [21] Тепловая карта [21] График рассеивания [21]
	Обеспечение ситуационной осведомленности	Простейший график [29] График рассеивания [29] Карта деревьев [29] Матрица [29]
Анализ рисков и выработка контрмер	Анализ активов (графы атак и зависимости сервисов)	Простейший график [27][28] Граф [27, 28] Матрица [27] График рассеивания [28]
	Выработка контрмер	Простейший график [27][28] Граф [27][28] Матрица [27] График рассеивания [28]
Защита от информации в социальных сетях	Анализ социальных связей и связи контента	Граф [29, 31] Гео-карта [29] Облако слов [29] Простейший график [31][30] График рассеивания [31] Матрица [30]
	Анализ метрик пользователей	Простейший график [30, 32] Облако слов [32] Граф [32] Матрица [30] Гео-карта [32]
	Анализ текстового контента	Простейший график [32] Облако слов [32] Граф [32] Гео-карта [32]
Вирусология и реверс-инжиниринг	Анализ бинарного представления вредоносного ПО	Матрица [33] График рассеивания [33]
	Анализ графа вызова функций	Граф [35] Дерево [34] График рассеивания [34]

DOI:10.21681/2311-3456-2021-4-2-15

Область	Задача	Пример
Вирусология и реверс-инжиниринг	Анализ уязвимостей	Карта деревьев [36]
	Анализ метрик вредоносного ПО	Матрица [33] График рассеивания [33][34] Дерево [34] Простейший график [37]
	Анализ поведения вредоносного ПО	Простейший график [38] Граф [39] Матрица [40] График потока [40]

систем, настройки приватности (в устройствах, соцсетях и т.д.) и т.п.
- предотвращение и обнаружение утечек информации – составляющие DLP-систем;
- цифровая криминалистика (форензика) – системы анализа трафика, логов и графического представления найденных улик. Кроме того, к данной области относятся системы анализа логов банковских транзакций и обнаружения мошенничества;
- сетевая безопасность – обширный класс систем мониторинга сетевых событий и обнаружения инцидентов безопасности, например, систем SIEM, IDS и IPS;
- анализ рисков и выработка контрмер – системы, использующиеся в процессах моделирования угроз, анализа активов компаний, моделирования атак;
- защита от информации в социальных сетях – обнаружение деструктивных сообществ, ботов и анализ их активности;
- вирусология и реверс-инжиниринг – анализ исходного кода вредоносного ПО и поведения вирусов.

Таким образом, была получена карта использования моделей визуализации данных для различных областей информационной безопасности, которая включает в себя: область информационной безопасности, задачу информационной безопасности и пример в виде используемой модели визуализации и ссылки на публикацию. Данная карта отражает основные тенденции в области визуальной аналитики информационной безопасности. Используя данную карту, можно определить, для каких именно областей и задач уже существуют готовые решения, которые можно использовать для синтеза новых способов визуализации.

3. Графические примитивы для визуализации

В основе любой визуализации лежат графические примитивы — составляющие визуализации, которые используются для компоновки сцены (пространства, в котором отображается информация), задания процесса взаимодействия человека с системой визуализации и отображения метрик визуализации. В качестве примера классификации графических примитивов можно привести „Визуальную грамматику“ [41], которая включает в себя объекты четырёх классов: абстрактные, конкретные, действия и отношения. Так, критерием оценки эффективности способа визуализации может служить количество графических примитивов, которые поддерживает визуализация.

Те графические примитивы, которые могут визуализировать метрики визуализации, подразделяются на количественные и категориальные. Количественные примитивы позволяют сравнивать численные значения различных объектов, в то время как категориальные – лишь искать объект определённой категории среди остальных. Примерами количественных примитивов являются: размер (площадь, объем, радиус и т.п.), цвет (например, по шкале RGB), скорость (вращения, передвижения и т.д.), прозрачность и т.д. Примерами категориальных графических примитивов являются: форма (квадрат, сфера, произвольная фигура и т.д.), медиа (изображение или видео), текстура и т.д. Ключевым отличием между двумя классами является то, что количественные примитивы могут визуализировать как численные, так и категориальные метрики, в то время как категориальные примитивы – только категориальные метрики. Для простоты понимания количественных и категориальных примитивов можно провести эксперимент, используя рис. 1.

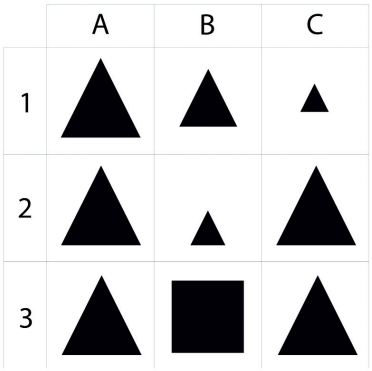


Рис. 1. Примеры графических примитивов: (1) численный графический примитив площади и численная мера, (2) численный графический примитив площади и категориальная мера, (3) категориальный графический примитив формы и категориальная мера

При помощи площади визуализируем три числа в виде треугольников A, B и C и зададим вопрос (см. рис. 1, строка 1): “Во сколько раз треугольник A больше C?”. В данном случае площадь является количественным примитивом и отображает количественную меру.

Теперь при помощи площади визуализируем категории. Первая категория – это большие треугольники, а вторая категория – малые. Зададим вопрос (см. рис. 1,

строка 2): “Сколько больших треугольников вы видите?” В данном случае площадь является количественным примитивом, но уже отображает категорию.

Теперь при помощи формы визуализируем две категории с помощью треугольника и квадрата. Можно задать вопрос (см. рис. 1, строка 3): “Сколько треугольников Вы видите?”. В данном случае форма является категориальным примитивом и отображает категорию.

Однако, при помощи формы невозможно визуализировать численную метрику. Мы не можем задать вопрос (см. рис. 1, строка 3): “Во сколько раз А более треугольный/квадратный, чем В?”

Таким образом, количественные примитивы могут отображать количественные и категориальные метрики, а категориальные примитивы — только категориальные метрики. Понятие количественных и категориальных графических примитивов необходимо для понимания того, какие данные поддерживает та или иная визуализация. Так, можно сопоставить количество и тип примитивов модели визуализации, а также количество и тип метрик данных, из чего сделать вывод о применимости модели к определенному набору данных.

Из графических примитивов формируется модель визуализации — комбинация нескольких графических примитивов, лежащих в основе визуализации. Понятие модели визуализации необходимо для того, чтобы отличать и классифицировать концепции, согласно которым формируется изображение. Например, в основе карт

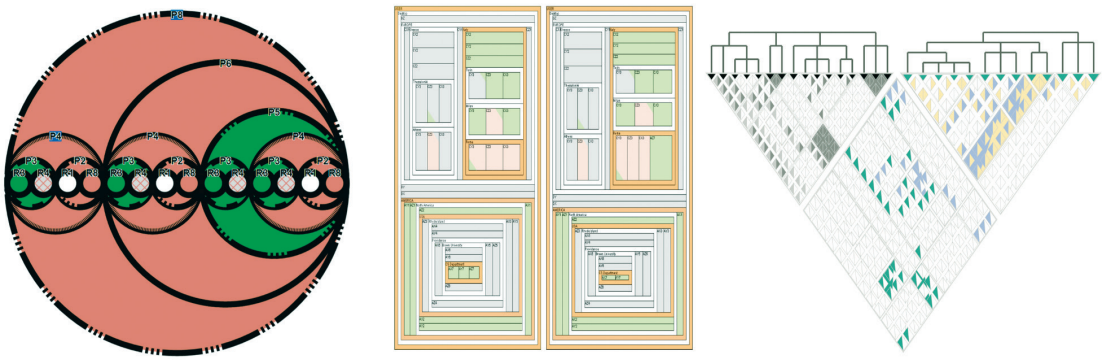


Рис. 2. Три различные реализации иерархии прав доступа с помощью одной модели визуализации — карт деревьев (слева на право: упаковка шаров [3], карты деревьев [1], треугольные матрицы [2])

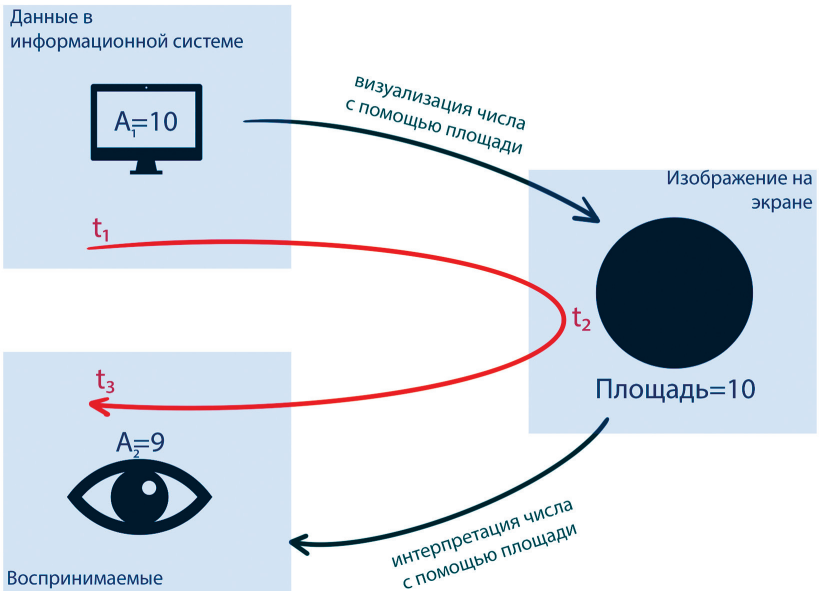


Рис. 3. Процесс анализа: (1) система визуализирует число 10 с помощью круга с площадью в 10 единиц в момент времени t2, при этом система тратит определенное время на рендеринг изображения; (2) пользователь смотрит на круг и интерпретирует площадь круга как 9 в момент времени t3, при этом пользователь тратит время на интерпретацию изображения, а также допускает погрешность в интерпретации значения

DOI:10.21681/2311-3456-2021-4-2-15

деревьев лежит концепция того, что иерархические данные можно отображать вложенностью, когда дочерний объект вложен в родительский. Карты деревьев формируются с использованием примитива площади (через которую выражается метрика объекта) и примитива вложенности (через которую выражаются связи между объектами). Таким образом, несмотря на большое разнообразие реализаций карт деревьев (см. рис. 2), о них можно рассуждать как об одной модели визуализации.

4. Свойства моделей визуализации

Для того чтобы сгруппировать публикации по используемым моделям визуализации, необходимо понимать основные характеристики (свойства), которые этим моделям свойственны. Следует отметить, что представленные характеристики рассматриваются как свойства моделей визуализации и их составляющих, а не человека-аналитика. На основе данных характеристик определяется вид модели (так как визуально принадлежность способа визуализации к той или иной модели не очевидна) и производится оценка эффективности способа визуализации.

Модели визуализации можно охарактеризовать с помощью точности и оперативности (скорости). Точность модели визуализации задает точность интерпретации данных человеком в процессе визуального анализа. Скорость модели визуализации отражает скорость рендеринга и интерпретации данных человеком в процессе визуального анализа. Пример процесса анализа изображен на рис. 3.

Необходимо отметить, что в данном процессе в качестве человека-аналитика подразумевается генеральная совокупность целевых пользователей системы. Таким образом, измерение скорости и точности будет интерпретироваться не как свойство человека, а как фундаментальное свойство графического примитива. Такой подход позволяет разработчику исходить из того, что скорость и точность зависят от модели визуализации и используемых графических примитивов, на которые можно влиять, а не от пользователей.

Точность и скорость являются свойствами графического примитива или графической модели (как совокупности примитивов). Точность выражается как распределение:

$$Accuracy = \left\{ \frac{min\left(A_{i1}, A_{i2}\right)}{max\left(A_{i1}, A_{i2}\right)} \right\}, i \in [1,\ldots,N] \quad (1)$$

где A_{i1} — истинное значение данных *i*-го пользователя; A_{i2} – воспринимаемое *i*-ым пользователем значение данных, полученное в результате интерпретации визуализации; *N* - размер генеральной совокупности целевых пользователей (на практике, чаще всего, это размер репрезентативной выборки пользователей).

Аналогично выражается распределение скорости:

$$Speed = \left\{ t_{i3} - t_{i1} \right\}, i \in [1,\ldots,N] \quad (2)$$

где t_{i3} — момент интерпретации значения пользователем; t_{i1} — момент предшествующий рендерингу изображения (если рендеринг выполняется моментально, t_{i1} заменяют на t_{i2} — момент отображения изображения на экране); *N* - размер генеральной совокупности целевых пользователей (на практике, чаще всего, это размер репрезентативной выборки пользователей).

При достаточно большой выборке распределение будет стремиться к нормальному. Как правило, в качестве критериев для сравнения распределений выступают квантили Q1, Q2 или Q3.

Наиболее известным примером точной и неточной модели (относительно друг друга) являются столбчатый график и круговая диаграмма. При использовании столбчатого графика пользователю намного проще увидеть небольшие различия между столбцами и дать ответ с меньшей погрешностью, в сравнении с секторами круговой диаграммы (см. рис. 4).

Высокая точность может использоваться для того, чтобы подчеркнуть небольшие отличия в данных, если даже малая разница критична для принятия решения. Низкая точность скрывает отличия и может использоваться в случаях, когда решение не должно приниматься на основе небольших отличий в данных. Часто именно критерии скорости и точности являются объектив-

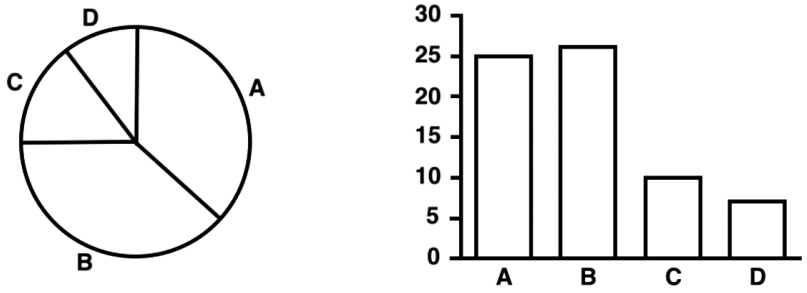
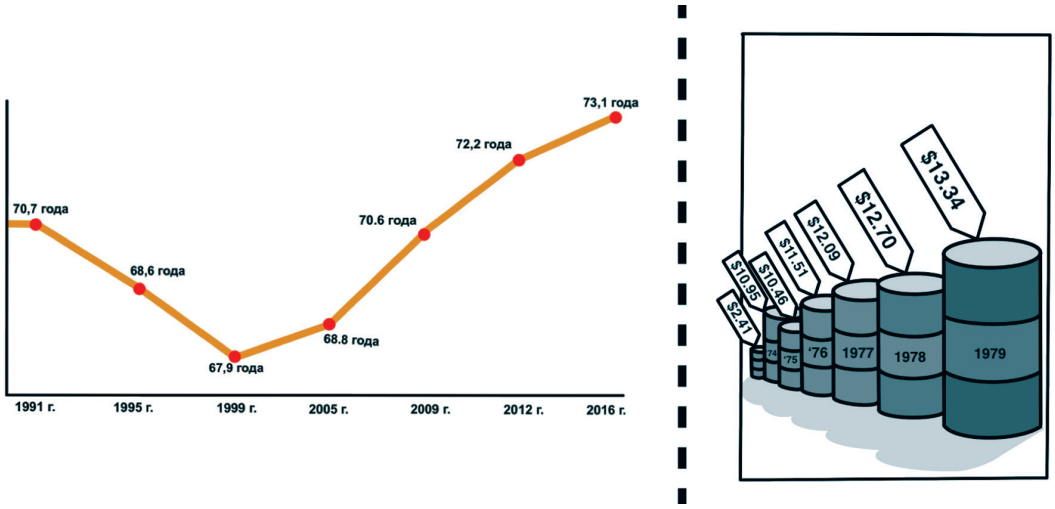


Рис. 4. Пример сравнения точности графиков с одинаковыми данными для круговой диаграммы (которая использует графический примитив площади) и столбчатого графика (который использует графический примитив длины)



а) *б)*

Рис. 5. Виды ошибок: (а) ошибка реализации, (б) ошибка нормализации

ными экспериментально-измеряемыми показателями эффективности визуализации.

Важными понятиями визуализации данных информационной безопасности являются понятия больших данных и ошибки восприятия. В отличие от классического определения, в визуализации под большими данными подразумевают данные с большим количеством метрик, для которых сложно подобрать модель визуализации. Так как количество графических примитивов, с помощью которых можно отображать метрики, ограничено моделью визуализации, а само добавление новых примитивов в модель визуализации снижает точность и скорость модели, возникает проблема оптимизации модели под большие данные. Возможность модели отображать большое количество метрик также часто становится элементом формальной оценки модели визуализации.

Ошибка восприятия модели (также известная как lie factor [42]) возникает, когда метрика численного графического примитива не соответствует метрике данных, что приводит к искажению и неправильной интерпретации метрик. Ошибка восприятия является численной мерой и обозначает, во сколько раз результат анализа с использованием визуализации будет отличаться от результатов анализа данных в численном виде (в условиях идеально точной модели). Искажение происходит на этапе рендеринга (момент времени t2 на рис. 3), и его можно выразить как отношение между разницами метрик графики и метриками данных:

$$PerceptionError = \frac{ValueDiff_{chart}}{ValueDiff_{data}}, \quad (3)$$

где

$$ValueDiff = \frac{|Value_1 - Value_2|}{Value_2}, \quad (4)$$

$ValueDiff_{chart}$ — значение $ValueDiff$ для изображения, $ValueDiff_{data}$ — значение $ValueDiff$ для набора данных, $Value_1$ — значение одного графического примитива (размер, цвет и т.д. при расчете $ValueDiff_{chart}$) или соответствующая графическому примитиву метрика данных (при расчете $ValueDiff_{data}$), $Value_2$ — значение другого графического примитива или соответствующая ему метрика данных.

Как правило, ошибка восприятия возникает при неправильной реализации (рис. 5а - несколько значений не соответствуют отображаемому на графике представлению), или ошибок нормализации графических примитивов (рис. 5б - все значения в равных пропорциях не соответствуют отображаемому на графике представлению, и, скорее всего, была ошибка нормирования). Сам факт присутствия такой ошибки (например, в отчете безопасности для руководства) может свидетельствовать о попытке манипуляции восприятием данных. Ошибки восприятия встречаются крайне редко, поэтому ниже мы приводим два показательных примера из других предметных областей.

Например, на рис. 5а заметно, что значение „68.6 лет“ (2-ое значение) лежит выше значения „68.8 лет“ (4-ое значение) по оси Y. Если допустить, что вертикальная шкала начинается с отметки в 67 лет, тогда можно посчитать, что максимальная ошибка восприятия достигается именно в этих значениях:

$$ValueDiff = \frac{|Value_2 - Value_4|}{Value_4} \Rightarrow ValueDiff_{chart} = \\ = \frac{|190\,px - 125\,px|}{125\,px} = 0.52, \\ ValueDiff_{data} = \frac{|(68.6 - 67) - (68.8 - 67)|}{(68.8 - 67)} = 0.11, \\ PerceptionError = \frac{0.52}{0.11} = 4.68, \quad (5)$$

На рис. 5б ошибку восприятия можно посчитать двумя способами – по площади (как у 2D изображения) или по объему (как у 3D изображения). В первом случае величина ошибки составит 9.4, а в случае объема – 59.4 [42].

5. Структура моделей и показатели визуализации

Структура моделей визуализации опираются на структуры данных, на основе которых осуществляется визуализация. Большинство моделей визуализации могут отображать лишь определённую структуру. Согласно структуре, модели визуализации можно разбить на несвязанные и связанные.

Несвязанные модели являются моделями для визуализации табличных структур данных (набор объектов и их метрик). В зависимости от размера таблицы они подразделяются на:

— маломерные – таблицы с несколькими столбцами (например, круговой график, столбчатая диаграмма, облако слов);
— многомерные – таблицы с множеством столбцов, для которых ярко выражена проблема больших данных (например, параллельные координаты).

Связанные модели являются моделями для визуализации графовых структур данных (набор объектов и их метрик, а также набор связей между объектами и метрики связей). В зависимости от топологии графа эти модели подразделяются на:

— иерархические, например, карты деревьев;
— планарные, например, карты Вороного;
— неструктурированные (не планарные), например, матрицы;
— гибридные – с несколькими структурами, например, хордовые диаграммы, с радиальным деревом, отображающим иерархические данные, и графом, представляющим неструктурированные данные.

Также выделяются географические модели, например, карты местности.

Исходя из структуры и модели визуализации, можно составить карту моделей и поддерживаемых ими данных. Для этого предложена карта (таблица 2), в которой обозначена зависимость модели от структуры данных.

Необходимо отметить, что в данной классификации представлено максимально необходимое соответствие “структура–модель”. Например, максимально поддерживаемая структура картами Вороного – это планарные структуры. Но, в то же время, любое дерево является планарным. Таким образом, карты Вороного могут визуализировать и планарные, и иерархические структуры. Данная особенность справедлива, в том числе, для неструктурированных (графы могут использоваться для планарных данных) и многомерных структур (параллельные координаты могут отображать маломерные данные).

Данная классификация позволяет сгруппировать публикации по моделям визуализации в таблице 1. Кроме того, данная классификация полезна разработчикам, когда необходимо выбирать модель, исходя из имеющейся структуры данных.

Таблица 2

Карта использования моделей визуализации данных для различных областей информационной безопасности

Структура		Модель
Несвязанные	Маломерные	Тепловые карты, облака слов, простейшие графики (линейные, столбчатые, круговое и т.д.), графики рассеивания, матрицы и модели для многомерных структур
	Многомерные	Параллельные координаты (и им подобные радиальные координаты)
Связанные	Иерархические	Карты деревьев (включают упаковки шаров, карты деревьев Вороного), графы (деревья, радиальные деревья) и модели для планарных структур
	Планарные	Карты Вороного и модели для неструктурированных структур
	Неструктурированные	Графы (силовые, радиальные, деревья, радиальные деревья)
	С несколькими структурами	Хордовые диаграммы (радиальный граф и радиальное дерево), а также многие совмещенные модели
Географические		Карты (стран, городов, помещений и т.д.), Диаграммы Вороного

Таким образом, на основе характеристик моделей визуализации и графических примитивов можно выделить следующие показатели, которые могут использоваться в методах оценки эффективности способов визуализации:

— количество графических примитивов – большее количество примитивов модели визуализации позволяет отобразить больше метрик, что может использоваться как оценка гибкости модели;
— количество графических примитивов определённого вида (количественного или категориального) – может использоваться как оценка гибкости модели, которая должна применяться к данным с определённым видом метрик (соответственно, количественных или категориальных);
— скорость – может использоваться для оценки оперативности (своевременности) принятия решений;
— точность – может применяться для оценки обоснованности принятия решений;
— ошибка восприятия – тоже может использоваться для оценки обоснованности принятия решений;
— поддерживаемая структура данных – может использоваться для оценки гибкости модели, которая должна применяться к данным с определённой структурой.

Данные показатели используются в методах оценки эффективности визуализации, чему будет посвящена следующая статья авторов.

6. Заключение

В работе представлен анализ текущего состояния исследований в области визуальной аналитики информационной безопасности и охвачены наиболее важные аспекты, которые могут пригодиться специалистам при внедрении различных способов визуализации в свои системы.

Так, классификация по областям применения и задачам информационной безопасности охватывает основные уже существующие решения визуальной аналитики и поможет сориентироваться в выборе подхода к визуализации, если решается схожая задача. Кроме того, приведенная классификация по моделям визуализации может помочь выбрать модель визуализации при разработке новых решений путем синтеза уже существующих.

В продолжении данного исследования будут рассмотрены методы, которые пригодятся для обоснованного оценивания эффективности разрабатываемого решения по визуализации для задач информационной безопасности, исходя из возможности или невозможности привлечь испытуемых или экспертов. Также будет приведена карта методов визуализации, которая позволит ориентироваться в публикациях, представленных в статье.

Работа выполнена при частичной финансовой поддержке РФФИ (проект № 19-17-50173).

Литература

1. Javed Y., Shehab M. Visual Analysis of Photo Policy Misconfigurations Using Treemaps // arXiv preprint arXiv:1903.02612. 2019.
2. Kolomeets M., Chechulin A., Kotenko I., Saenko I. Access Control Visualization Using Triangular Matrices // Proceedings of the 27th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2019). Pavia, Italy, February 13-15, 2019. Los Alamitos, California. IEEE Computer Society. 2019. P.348-355. DOI: 10.1109/EMPDP.2019.8671578.
3. Morisset C., Sanchez D. On building a visualisation tool for access control policies //International Conference on Information Systems Security and Privacy. - Springer, Cham, 2018. P. 215–239.
4. Gove R. V3SPA: A visual analysis, exploration, and diffing tool for SELinux and SEAndroid security policies // 2016 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2016. P. 1–8.
5. Котенко И. В., Ушаков И. А., Пелёвин Д. В., Преображенский А. И., Овраменко А. Ю. Выявление инсайдеров в корпоративной сети: подход на базе UBA и UEBA // Защита информации. Инсайд. 2019. № 5. С. 26–35.
6. Коломеец М. В. Использование моделей визуализации данных в DLP-системах // X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2017). 1-3 ноября 2017 г. Сборник трудов. Том 3. СПб.: СПОИСУ, 2017.
7. Legg P. A. Visualizing the insider threat: challenges and tools for identifying malicious user activity // 2015 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2015. P. 1–7.
8. Kolomeets M., Chechulin A., Kotenko I., Chevalier Y.A visual analytics approach for the cyber forensics based on different views of the network traffc // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 2018. vol. 9, No. 2. P. 57–73.
9. Tassone C. F. R., Martini B., Choo K. K. R. Visualizing digital forensic datasets: a proof of concept //Journal of forensic sciences. 2017. Vol. 62. №. 5. P. 1197–1204.
10. Qazi N., Wong B. Behavioural & tempo-spatial knowledge graph for crime matching through graph theory //2017 European Intelligence and Security Informatics Conference (EISIC). IEEE, 2017. P. 143–146.
11. Leschke T. R., Nicholas C. Change-link 2.0: a digital forensic tool for visualizing changes to shadow volume data // Proceedings of the Tenth Workshop on Visualization for Cyber Security. 2013. P. 17–24.
12. Novikova E., Kotenko I. Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services // International Cross Domain Conference and Workshops (CD-ARES 2014). September 8nd – 12th, 2014. Fribourg, Switzerland. Lecture Notes in Computer Science (LNCS), vol. 8708. Springer-Verlag. 2014, P.63–78.
13. Oggier F., Phetsouvanh S., Datta A. BiVA: Bitcoin network visualization & analysis //2018 IEEE International Conference on Data Mining Workshops (ICDMW). IEEE, 2018. P. 1469–1474.

14. Webga K., Lu A.Discovery of rating fraud with real-time streaming visual analytics // 2015 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2015. P. 1–8.
15. Cappers B.C.M., Wijk J.J. Understanding the context of network traffc alerts // 2016 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2016. P. 1–8.
16. Hao L., Healey C.G., Hutchinson S.E. Ensemble visualization for cyber situation awareness of network security data // 2015 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2015. P. 1–8.
17. Shi Y., Zhao Y., Zhou F., Shi R., Zhang Y.A novel radial visualization of intrusion detection alerts // IEEE Computer Graphics and Applications. 2018. vol. 38. No. 6. P. 83–95.
18. Theron R., Magan-Carrion R., Camacho J., Fernndez G. Network-wide intrusion detection supported by multivariate analysis and interactive visualization // 2017 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2017. P. 1–8.
19. Kim U., Kang J., Lee J., Kim H., Jung S. Practical firewall policy inspection using anomaly detection and its visualization // Multimedia tools and applications. 2014. vol. 71. No. 2. P. 627–641.
20. Kim H., Ko S., Kim D., Kim HK. Firewall ruleset visualization analysis tool based on segmentation //2017 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2017. P. 1–8.
21. 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. P. 1–8.
22. Ulmer A., Schufrin M., Sessler D., Kohlhammer K. Visual-Interactive Identification of Anomalous IP-Block Behavior Using Geo-IP Data // 2018 Symposium on Visualization for Cyber Security (VizSec). IEEE, 2018. P. 1–8.
23. 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. P. 1–4.
24. Krokos E., Rowden A., Whitley K., Varshney A. Visual Analytics for Root DNS Data //2018 IEГБ Symposium on Visualization for Cyber Security (VizSec). IEEE, 2018. P.18.
25. Romero-Gomez R., Nadji Y., Antonakakis M. Towards designing effective visualizations for DNS-based network threat analysis // 2017 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2017. P. 1–8.
26. Sopan A., Berninger M., Mulakaluri M., Katakam R. Building a Machine Learning Model for the SOC, by the Input from the SOC, and Analyzing it for the SOC // 2018 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2018. P. 1–8.
27. Kolomeec M., Gonzalez-Granadillo G., Doynikova E., Chechulin A., Kotenko I, Debar H. Choosing models for security metrics visualization // Computer Network Security. Lecture Notes in Computer Science, Springer-Verlag, vol. 10446. The 2017 7th International Conference on Mathematical Methods, Models and Architectures for Computer Networks Security (MMM-ACNS-2017). August 28-30, 2017, Warsaw, Poland. P.75–87.
28. Motzek A., Gonzalez-Granadillo G., Debar H., Garcia-Alfaro J., Möller R. Selection of Pareto-efficient response plans based on financial and operational assessments // EURASIP Journal on Information Security. 2017. vol. 2017. No. 1. P. 12.
29. Mrsic L., Zajec S., Kopal R. Appliance of Social Network Analysis and Data Visualization Techniques in Analysis of Information Propagation // Asian Conference on Intelligent Information and Database Systems. – Springer, Cham, 2019. P. 131–143.
30. Ferrara E. Disinformation and social bot operations in the run up to the 2017 French presidential election // arXiv preprint arXiv:1707.00086. 2017.
31. Faris R., Roberts H., Etling B., Bourassa N., Zuckerman E., Benkler Y. Partisanship, propaganda, and disinformation: Online media and the 2016 US presidential election // Berkman Klein Center Research Publication. 2017. vol. 6.
32. Shu K., Mahudeswaran D., Liu H. FakeNewsTracker: a tool for fake news collection, detection, and visualization // Computational and Mathematical Organization Theory. 2019. vol. 25. No. 1. P. 60 -71.
33. Nataraj L., Karthikeyan S., Jacob G., Manjunath B. Malware images: visualization and automatic classification // Proceedings of the 8th international symposium on visualization for cyber security. 2011. P. 1–7.
34. Angelini M., Blasilli G., Borrello P., Coppa E., D'Elia D., Ferracci S., Lenti S., Santucci G. ROPMate: Visually Assisting the Creation of ROP-based Exploits // 2018 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2018. P. 1–8.
35. Santhanam G. R., Holland B., Kothari S., Mathews J. Interactive visualization toolbox to detect sophisticated android malware // 2017 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2017. P. 1–8.
36. Assal H., Chiasson S., Biddle R. Cesar: Visual representation of source code vulnerabilities // 2016 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2016. P. 1–8.
37. Gove R., Saxe J., Gold S., Long A., Labs G., Piper Z. SEEM: a scalable visualization for comparing multiple large sets of attributes for malware analysis // Proceedings of the Eleventh Workshop on Visualization for Cyber Security. – 2014. – P. 72-79.
38. Kartel A., Novikova E., Volosiuk A. Analysis of Visualization Techniques for Malware Detection //2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). IEEE, 2020. P. 337–340.
39. Peryt S., Andre Morales J., Casey W., Volkmann A., Mishra B., Cai Y. Visualizing a malware distribution network // 2016 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2016. P. 1–4.
40. Cappers B., Meessen P., Etalle S., Wijk J. Eventpad: Rapid malware analysis and reverse engineering using visual analytics // 2018 IEEE Symposium on Visualization for Cyber Security (VizSec). IEEE, 2018. P. 1–8.
41. Bestley R., Noble I. Visual research: An introduction to research methods in graphic design. Bloomsbury Publishing, 2016.
42. Angelini M., May T., Santucci G., Schulz HJ. On Quality Indicators for Progressive Visual Analytics //EuroVA@ EuroVis. 2019. P. 25–29.
43. Syamkumar M., Durairajan R., Barford, P.Bigfoot: A geo-based visualization methodology for detecting bgp threats // 2016 IEEE Symposium on Visualization forCyber Security (VizSec). IEEE, 2016. P. 1–8.

VISUAL ANALYTICS FOR INFORMATION SECURITY: AREAS OF APPLICATION, TASKS, VISUALIZATION MODELS

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 the areas and problems of information security that are solved using visual analytics methods, as well as analysis of the applied data visualization models and their properties that affect the perception of data by the operator.*

Research method: *a systematic analysis of the application of visual analytics methods for solving information security problems. Analysis of relevant papers in the field of information security and data visualization. The objects of research are: theoretical and practical solutions to information security problems through visual analysis. Visual analytics in the article is considered from several sides: from the point of view of the areas of application of visual analysis methods in information security, from the point of view of the tasks solved by the security analyst, from the point of view of the visualization models used and the data structures used, as well as from the point of view of the properties of data visualization models.*

The result: *classification of visualization models is prop*osed, which differs from analogs in that it is based on the analysis of areas and tasks of information security and comparison of visualization models to them.

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 specialists who develop information security systems and for students studying in the direction of training "Information Security".

Keywords: *information security, visual analytics, data analysis, support and decision making, visualization model, data visualization.*

References

1. Javed Y., Shehab M. Visual Analysis of Photo Policy Misconfigurations Using Treemaps //arXiv preprint arXiv:1903.02612. – 2019.
2. Kolomeets M., Chechulin A., Kotenko I., Saenko I. Access Control Visualization Using Triangular Matrices // Proceedings of the 27th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2019). Pavia, Italy, February 13-15, 2019. Los Alamitos, California. IEEE Computer Society. 2019. P.348-355. DOI: 10.1109/EMPDP.2019.8671578.
3. Morisset C., Sanchez D. On building a visualisation tool for access control policies //International Conference on Information Systems Security and Privacy. - Springer, Cham, 2018. - P. 215-239.
4. Gove R. V3SPA: A visual analysis, exploration, and diffing tool for SELinux and SEAndroid security policies //2016 IEEE Symposium on Visualization for Cyber Security (VizSec). — IEEE, 2016. — P. 1-8.
5. Kotenko I., Ushakov I., Pelevin D., Preobrazhenskiy A., Ovramenko A. Identification of insiders in the corporate network: an approach based on UBA and UEBA ff Information security. Inside. 2019. no. 5. pp. 26-35.
6. Kolomeec M. Data visualization models usage in DLP systems. X Saint-Petersburg Interregional conference «Information security of regions of Russia (IBRR-2017) Vo1. 3. Saint-Petersburg, November 1-3, 2017. The proceedings of conference, 2017.
7. Legg P. A. Visualizing the insider threat: challenges and tools for identifying malicious user activity // 2015 IEEE Symposium on Visualization for Cyber Security (VizSec). – IEEE, 2015. – P. 1-7.
8. Kolomeets M., Chechulin A., Kotenko I., Chevalier Y.A visual analytics approach for the cyber forensics based on different views of the network traffc // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2018, vol. 9, No. 2, P. 57-73.
9. Tassone C. F. R., Martini B., Choo K. K. R. Visualizing digital forensic datasets: a proof of concept //Journal of forensic sciences. – 2017. – Vol. 62. – №. 5. – P. 1197-1204.
10. Qazi N., Wong B. Behavioural & tempo-spatial knowledge graph for crime matching through graph theory //2017 European Intelligence and Security Informatics Conference (EISIC). – IEEE, 2017. – P. 143-146.

5 Igor 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. E-mail: ivkote@comsec.spb.ru

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

7 Kseniia Zhernova, Ph.D. Graduate student, Junior Research fellow at St. Petersburg Institute for Informatics and Automation of Russian Academy of Science, St. Petersburg, Russia. E-mail: zhernova@comsec.spb.ru

8 Andrey Chechulin, Ph.D., Assistant Professor, 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

11. Leschke T. R., Nicholas C. Change-link 2.0: a digital forensic tool for visualizing changes to shadow volume data // Proceedings of the Tenth Workshop on Visualization for Cyber Security. – 2013. – P. 17-24.
12. Novikova E., Kotenko I. Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services // International Cross Domain Conference and Workshops (CD-ARES 2014). September 8nd – 12th, 2014. Fribourg, Switzerland. Lecture Notes in Computer Science (LNCS), vol. 8708. Springer-Verlag. 2014, P.63-78.
13. Oggier F., Phetsouvanh S., Datta A. BiVA: Bitcoin network visualization & analysis //2018 IEEE International Conference on Data Mining Workshops (ICDMW). – IEEE, 2018. – P. 1469-1474.
14. Webga K., Lu A.Discovery of rating fraud with real-time streaming visual analytics // 2015 IEEE Symposium on Visualization for Cyber Security (VizSec). – IEEE, 2015. – P. 1-8.
15. Cappers B.C.M., Wijk J.J. Understanding the context of network traffc alerts // 2016 IEEE Symposium on Visualization for Cyber Security (VizSec). – IEEE, 2016. – P. 1-8.
16. Hao L., Healey C.G., Hutchinson S.E. Ensemble visualization for cyber situation awareness of network security data // 2015 IEEE Symposium on Visualization for Cyber Security (VizSec). – IEEE, 2015. – P. 1-8.
17. Shi Y., Zhao Y., Zhou F., Shi R., Zhang Y.A novel radial visualization of intrusion detection alerts //IEEE Computer Graphics and Applications. – 2018. – vol. 38. – No. 6. – P. 83-95.
18. Theron R., Magan-Carrion R., Camacho J., Fernndez G. Network-wide intrusion detection supported by multivariate analysis and interactive visualization // 2017 IEEE Symposium on Visualization for Cyber Security (VizSec). – IEEE, 2017. – P. 1-8.
19. Kim U., Kang J., Lee J., Kim H., Jung S. Practical firewall policy inspection using anomaly detection and its visualization // Multimedia tools and applications. – 2014. – vol. 71. – No. 2. – P. 627-641.
20. Kim H., Ko S., Kim D., Kim HK. Firewall ruleset visualization analysis tool based on segmentation //2017 IEEE Symposium on Visualization for Cyber Security (VizSec). – IEEE, 2017. – P. 1-8.
21. 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. - P. 1-8.
22. Ulmer A., Schufrin M., Sessler D., Kohlhammer K. Visual-Interactive Identification of Anomalous IP-Block Behavior Using Geo-IP Data // 2018 Symposium on Visualization for Cyber Security (VizSec). - IEEE, 2018. - P. 1-8.
23. 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. - P. 1-4.
24. Krokos E., Rowden A., Whitley K., Varshney A. Visual Analytics for Root DNS Data //2018 IEГБ Symposium on Visualization for Cyber Security (VizSec). — IEEE, 2018. — P.18.
25. Romero-Gomez R., Nadji Y., Antonakakis M. Towards designing effective visualizations for DNS-based network threat analysis // 2017 IEEE Symposium on Visualization for Cyber Security (VizSec). - IEEE, 2017. - P. 1-8.
26. Sopan A., Berninger M., Mulakaluri M., Katakam R. Building a Machine Learning Model for the SOC, by the Input from the SOC, and Analyzing it for the SOC // 2018 IEEE Symposium on Visualization for Cyber Security (VizSec). - IEEE, 2018. - P. 1-8.
27. Kolomeec M., Gonzalez-Granadillo G., Doynikova E., Chechulin A., Kotenko I, Debar H. Choosing models for security metrics visualization // Computer Network Security. Lecture Notes in Computer Science, Springer-Verlag, vol. 10446. The 2017 7th International Conference on Mathematical Methods, Models and Architectures for Computer Networks Security (MMM-ACNS-2017). August 28-30, 2017, Warsaw, Poland. P.75-87.
28. Motzek A., Gonzalez-Granadillo G., Debar H., Garcia-Alfaro J., Möller R. Selection of Pareto-efficient response plans based on financial and operational assessments // EURASIP Journal on Information Security. — 2017. - vol. 2017. - No. 1. - P. 12.
29. Mrsic L., Zajec S., Kopal R. Appliance of Social Network Analysis and Data Visualization Techniques in Analysis of Information Propagation // Asian Conference on Intelligent Information and Database Systems. – Springer, Cham, 2019. – P. 131-143.
30. Ferrara E. Disinformation and social bot operations in the run up to the 2017 French presidential election // arXiv preprint arXiv:1707.00086. – 2017.
31. Faris R., Roberts H., Etling B., Bourassa N., Zuckerman E., Benkler Y. Partisanship, propaganda, and disinformation: Online media and the 2016 US presidential election // Berkman Klein Center Research Publication. – 2017. – vol. 6.
32. Shu K., Mahudeswaran D., Liu H. FakeNewsTracker: a tool for fake news collection, detection, and visualization // Computational and Mathematical Organization Theory. – 2019. – vol. 25. – No. 1. – P. 60-71.
33. Nataraj L., Karthikeyan S., Jacob G., Manjunath B. Malware images: visualization and automatic classification // Proceedings of the 8th international symposium on visualization for cyber security. – 2011. – P. 1-7.
34. Angelini M., Blasilli G., Borrello P., Coppa E., D'Elia D., Ferracci S., Lenti S., Santucci G. ROPMate: Visually Assisting the Creation of ROP-based Exploits // 2018 IEEE Symposium on Visualization for Cyber Security (VizSec). – IEEE, 2018. – P. 1-8.
35. Santhanam G. R., Holland B., Kothari S., Mathews J. Interactive visualization toolbox to detect sophisticated android malware // 2017 IEEE Symposium on Visualization for Cyber Security (VizSec). – IEEE, 2017. – P. 1-8.
36. Assal H., Chiasson S., Biddle R. Cesar: Visual representation of source code vulnerabilities // 2016 IEEE Symposium on Visualization for Cyber Security (VizSec). – IEEE, 2016. – P. 1-8.
37. Gove R., Saxe J., Gold S., Long A., Labs G., Piper Z. SEEM: a scalable visualization for comparing multiple large sets of attributes for malware analysis // Proceedings of the Eleventh Workshop on Visualization for Cyber Security. – 2014. – P. 72-79.
38. Kartel A., Novikova E., Volosiuk A. Analysis of Visualization Techniques for Malware Detection //2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). – IEEE, 2020. – P. 337-340.

39. Peryt S., Andre Morales J., Casey W., Volkmann A., Mishra B., Cai Y. Visualizing a malware distribution network // 2016 IEEE Symposium on Visualization for Cyber Security (VizSec). – IEEE, 2016. – P. 1-4.
40. Cappers B., Meessen P., Etalle S., Wijk J. Eventpad: Rapid malware analysis and reverse engineering using visual analytics // 2018 IEEE Symposium on Visualization for Cyber Security (VizSec). – IEEE, 2018. – P. 1-8.
41. Bestley R., Noble I. Visual research: An introduction to research methods in graphic design. – Bloomsbury Publishing, 2016.
42. Angelini M., May T., Santucci G., Schulz HJ. On Quality Indicators for Progressive Visual Analytics //EuroVA@ EuroVis. – 2019. – P. 25-29.
43. Syamkumar M., Durairajan R., Barford, P.Bigfoot: A geo-based visualization methodology for detecting bgp threats // 2016 IEEE Symposium on Visualization forCyber Security (VizSec). – IEEE, 2016. – P. 1-8.