A. V. Yelizarov, D. Y. Gamayunov

Adaptive Security Event Visualization for Continuous Monitoring

Keywords: adaptive user interfaces, event visualization, information security

The field of information security routinely produces the need for a security information and event management system operator who would be capable of durable and extensive (e.g., workday-long) monitoring of the system in his control with well-timed decision making in emergencies. The obvious concern is that such continuous exertion is bound to lead to the operator's increased fatigue, reduced attention span, and flawed decision making. This paper proposes methods of the visualization system's adaptation to these changes for improving the operator's efficiency in terms of speed and accuracy.

А. В. Елизаров, Д. Ю. Гамаюнов

АДАПТИВНАЯ СИСТЕМА ВИЗУАЛИЗАЦИИ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ПРОДОЛЖИТЕЛЬНОГО МОНИТОРИНГА

Введение

Программно-аппаратные комплексы или системы, обеспечивающие информационную безопасность (СОИБ), можно описать как средства сбора, агрегации, корреляции и последующей визуализации событий информационной безопасности, получаемых из различных источников. Источниками событий для СОИБ являются устройства безопасности (системы обнаружения атак (СОА), системы предотвращения атак, межсетевые экраны), сетевые устройства (маршрутизаторы, коммутаторы), операционные системы, базы данных и различные приложения. В архитектуре СОИБ принято выделять систему визуализации, задачами которой являются отображение получаемых событий и данных о состоянии подконтрольных устройств в режиме реального времени, отображение прошедших атак, предоставление интерфейса для работы с базой данных и возможностей для оперативного управления и разрешения инцидентов.

Увеличить эффективность человеко-компьютерного взаимодействия любой компьютерной системы можно двумя способами: во-первых, можно лучше подготовить человека для работы с конкретной системой (за счет обучения и наращивания опыта), а во-вторых, можно лучше приспособить саму систему под конкретного пользователя и его цели. При этом особое внимание уделяется тем частям системы, которые непосредственно ответственны за прием и передачу информации (иначе говоря, где происходит человеко-компьютерное взаимодействие). Такими частями являются не только система визуализации, монитор, мышь, клавиатура и т. п., но и сам человек, так как именно он, воспринимая полученную информацию и затем взаимодействуя с компьютером, передает ему свое решение. Другими словами, следует также учитывать и свойства человека как «информационного канала».

В условиях возрастающего числа киберпреступлений все чаще на уровнях как корпоративной, так и государственной безопасности возникает потребность в человеческом операторе СОИБ (далее — оператор). Зачастую, такой оператор должен непрерывно в течение длительного времени (например, восьмичасового рабочего дня) наблюдать за состоянием подконтрольных ему сетей и сервисов, взаимодействуя с системой визуализации СОИБ, а при необходимости — принимать своевременные решения для их защиты. Такими решениями могут быть: блокировка внешних узлов и подсетей; запуск или отключение сервисов на подконтрольных хостах; настройка параметров СОА для изменения логики ее работы в соответствии с текущей ситуацией.

Со временем у такого оператора будет накапливаться усталость, притупляться реакция и падать качество восприятия[1] одного и того же объема когнитивной нагрузки (при этом после отдыха, например, эти свойства могут улучшаться). Можно утверждать, что психофизическое состояние[2] (далее — состояние) такого оператора будет с течением времени меняться (подтверждение этого факта — тема отдельного исследования).

Так как именно оператор ответственен за принятие решений, можно предположить, что учет его текущего психофизического состояния и индивидуальных особенностей восприятия благотворно скажется на своевременности и качестве принятых решений. Однако существующие системы визуализации (например, системы визуализации СОИБ от Symantec, HP, IBM и др.) представляют собой средства, рассчитанные на «среднего» оператора. Несмотря на то что зачастую они позволяют самому пользователю настраивать элементы интерфейса, у них отсутствуют какие-либо механизмы определения текущего состояния пользователя.

В данной статье будут предложены методы адаптации (изменения функциональности и отображения) системы визуализации событий информационной безопасности к текущему психофизическому состоянию оператора. Состояние оператора будет определяться на основе данных о характеристике его взаимодействия посредством мыши и клавиатуры с системой. Иные устройства определения состояния оператора (такие, как камеры, айтрекеры, биомедицинские сенсоры и т. п.) в данной работе не рассматриваются. Представленные далее рассуждения будут вестись в контексте систем визуализации событий информационной безопасности, однако их можно обобщить до любой событийно-ориентированной системы визуализации с непрерывно работающим человеком-оператором.

1. Система визуализации событий информационной безопасности

Визуализация в сфере информационной безопасности является относительно молодой темой, посвященной изучению, разработке новых и применению уже существующих методик визуализации для отображения информации о событиях информационной безопасности. Обзоры последних исследований в этой области представлены в работах [6] и [10], а работа [3] рассматривает различные методы эксплуатации уязвимостей существующих систем визуализации и человеческого зрительного восприятия.

Система визуализации получает всю необходимую для отображения информацию в виде сообщений от модуля корреляции событий, который занимается обработкой обнаруженных событий и определением наличия связей между ними. Каждое такое сообщение содержит информацию об IP-адресах цели и источника, типе события (например, сканирование или попытка получения удаленных прав root'а), уровне опасности события (низкий, средний, высокий и иногда отдельный информационный), времени его обнаружения и связях с другими событиями. Последняя информация критична для отображения комплексных (состоящих из более чем одного события) атак (подробнее о визуализации комплексных атак можно прочесть в работе [16]).

1.1. Пример использования

Система визуализации, отображающая состояние сети, например, в 1000 хостов, может в течение 10 секунд получить сообщения о тысячах событий. Такая ситуация возможна, например, в случае нескольких параллельных, не связанных между собой, комплексных атак. Предположим, что всего было обнаружено три атаки, две из которых являются распределенными атаками типа «отказ в обслуживании» (DDoS), нацеленными на определенные, но разные сегменты наблюдаемой

[1] Под «восприятием» в данной статье будет подразумеваться биологический и психический процесс осмысления оператором полученной визуальной информации (когнитивной нагрузки) для ее интерпретации и создания представления о состоянии наблюдаемой сети.
[2] Под «психофизическим состоянием» в данной статье будет подразумеваться способность оператора адекватно реагировать на стимулы со стороны системы визуализации.

сети, а третья – многошаговая атака, состоящая из предварительного сканирования сегмента сети, последующего получения привилегий root'а на одном из наблюдаемых хостов и DoS-атаки с захваченного хоста на еще один наблюдаемый хост. В описанной ситуации система визуализации получит сообщения следующих типов: сканирование (низкий уровень опасности), попытка получения привилегий root'а (средний уровень опасности), DoS (средний уровень опасности) и успешное получение привилегий root'а (высокий уровень опасности). Оператор при этом должен принять следующие решения как можно быстрее: заблокировать отдельные внешние хосты и/или подсети, задействованные в распределенных атаках сканирования и DDoS; перенастроить захваченный хост и/или перенести его сервисы на нескомпрометированный хост и восстановить функциональность хостов задетых DoS'ами. В типичной СОИБ оператору только лишь на реализацию каждого перечисленного решения потребуется не менее 10 нажатий клавиш (как минимум, ему нужно будет задать целевые IP-адреса и выбрать тип действия).

Далее в статье будет показано, как с помощью предлагаемых методов можно уменьшить время восприятия оператором сложившейся ситуации и увеличить скорость реализации принятых им решений. Предлагаемые в статье подходы будут продемонстрированы на примере разработанного в рамках данного исследования прототипа системы визуализации (далее — система).

1.2. Отображение обнаруженных событий

Мы решили, что к наиболее приоритетной для оператора информации относятся IP-адреса целей и источников событий, уровень опасности событий и связи между событиями. Точное время обнаружения события для оператора (непрерывно работающего) не столь важно, так как его основной целью является разрешение самой вредоносной атаки, а не выявление времени ее наступления. В то же время оператор не нуждается в глубоком и доскональном анализе ситуации, сложившейся в наблюдаемой сети, поэтому тип события не обязателен для непосредственного отображения, так как оператору достаточно воспринять уровень опасности событий. С другой стороны, именно тип события определяет набор действий, который оператор может произвести для разрешения данного инцидента (подробнее об этом см. в п. 1.3 и на рис. 2).

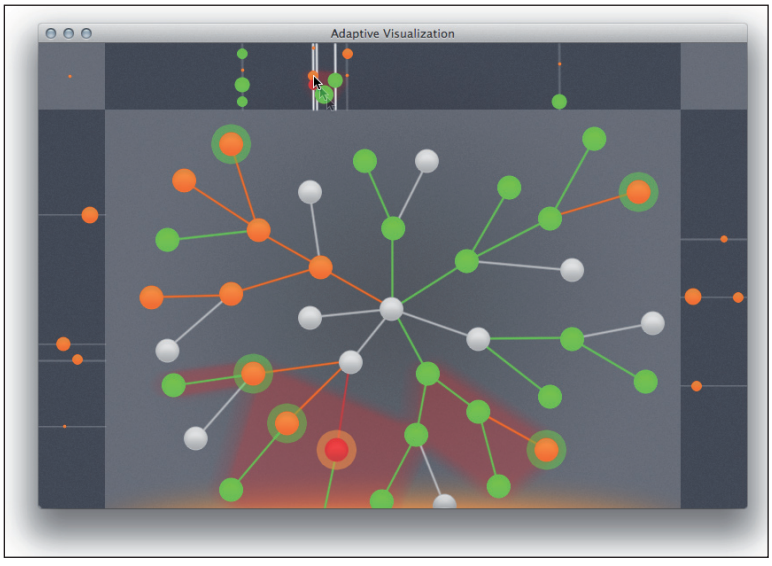

Рис. 1. Отображение системой визуализации описанного примера

Можно считать [15], что наиболее легким для совместного восприятия набором измерений для визуализации различных параметров данных является комбинация цвета, элементов формы (размера и ориентации), расположения в 2D-пространстве и простого движения (анимации).

На основе этих наблюдений под отображение хостов наблюдаемой сети было выделено 2D-пространство, а под отображение уровня опасности — цвет (красный соответствует самому высокому уровню опасности, затем желтый, а затем зеленый). Каждый хост окрашивается в цвет самого опасного неразрешенного события, обнаруженного на нем, и подсвечивается цветом его второго по опасности события. По наведению курсора мыши на любое событие какой-нибудь атаки система подсвечивает все хосты, на которых были обнаружены другие события этой же атаки. Обнаружение новых событий отображается посредством временного выделения хоста, на котором новое событие было обнаружено. Если этот хост находится за границами окна системы визуализации, то тогда подсвечивается соответствующая граница (как видно на рис. 1). Этот прием позволяет оператору отслеживать ситуацию сети в целом. Напомним, что так как работа оператора непрерывная и продолжительная, то он постоянно имеет общее представление о состоянии подконтрольной сети.

Внешние хосты система визуализации отображает вне пространства, занимаемого наблюдаемой сетью. При этом пространство внешних хостов можно представить в виде «полосы», где по оси X отложены первые два байта IP-адреса, а по оси Y — последние. Чем больше в одной атаке задействовано внешних хостов с близкими IP-адресами, тем больше их отображаемый размер. Система визуализации позволяет оператору разделить всю «полосу» внешних хостов на части, соответствующие различным атакам. Также система отдельно отображает внешние хосты, задействованные сразу в нескольких атаках.

1.3. Взаимодействие с системой

Поскольку цвет и положение в 2D-пространстве — наиболее простая для восприятия пара, оператор может легко определить, какие хосты нуждаются в действиях с его стороны. Следует заметить, что самая большая угроза для сети может исходить не от событий с самыми высокими уровнями опасности, а, например, от событий среднего уровня опасности, но обнаруженных на критически важных участках сети. Определив инцидент, который требует наиболее срочного разрешения, оператор может передвинуть курсор на соответствующий хост, после чего около курсора отобразится круговое меню (рис. 2) [2] с самыми опасными событиями, обнаруженными на данном хосте. На основе закона Фиттса [8] для быстроты взаимодействия был сделан выбор именно в пользу кругового меню.

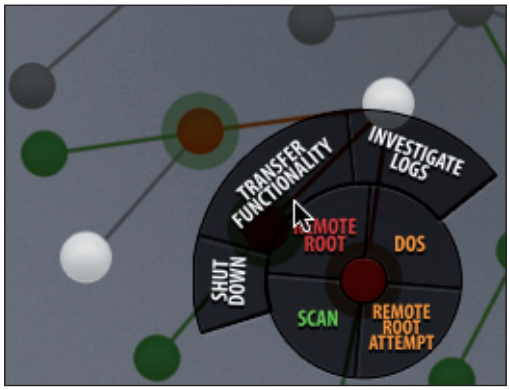

Рис. 2. Взаимодействие с использованием кругового меню

После перемещения курсора на элемент кругового меню, соответствующий определенному событию, визуально выделяются все хосты, на которых обнаружены события, связанные с выбранным. При перемещении курсора группа выделенных хостов меняется. Если оператор кликает по элементу кругового меню, то система предлагает ему набор решений, возможных для принятия, основываясь на типе выбранного события. Для сравнения различных атак оператор может сохранять выделенные группы хостов, зажав любую цифровую клавишу на

клавиатуре. Теперь, когда ему необходимо выделить уже сохраненную атаку, он может нажать соответствующую цифровую клавишу.

2. Адаптация для продолжительного мониторинга

Человеко-компьютерное взаимодействие зависит как от факторов, относящихся к компьютеру (например, от оборудования, быстродействия или программного обеспечения), так и от факторов, относящихся к человеку (например, от предварительного обучения работе с данной системой, уровня владения ею или индивидуальных особенностей) [9]. При этом под «индивидуальными особенностями» подразумеваются не столько личные данные пользователя (пол, возраст и т. п.), сколько его персональные когнитивные особенности. Последние исследования показали, что такие когнитивные особенности, как объем рабочей памяти (working memory capacity [7, 12]), скорость восприятия (perceptual speed [13]), пространственное мышление (spatial ability [14]) и локус контроля (locus of control [17]), влияют на скорость и точность работы пользователя. При этом некоторые когнитивные особенности могут быть достоверно определены самой системой автоматически, например, с использованием технологий айтрекинга (анализа потока взгляда) [11, 13].

Под «адаптивным интерфейсом» принято подразумевать такой интерфейс, который изменяет порядок и набор отображаемых элементов в зависимости от контекста, состояния и целей пользователя. Зачастую адаптивные интерфейсы ограничиваются лишь адаптацией под текущую задачу, что возможно без какого-либо представления о состоянии пользователя. Хотя уже показано, что в некоторых областях применения имеет смысл адаптация системы под пользовательский уровень знаний [1, 13] или под шаблоны его поведения [5]. Представленная в данной статье система визуализации имеет механизмы адаптации под текущую задачу, под уровень усталости оператора, под уровень владения системой, а также возможности регулирования уровня когнитивной нагрузки отображаемой информации.

2.1. Адаптация под задачу

Вообще говоря, любая система визуализации позволяет оператору реализовывать только те его решения, которые предопределены в системе. Можно считать, что оператор, взаимодействуя с системой, выбирает, какую предопределенную последовательность команд запускать и с какими параметрами, например, какому хосту (как параметру) блокировать доступ к сети (как предопределенную последовательность команд).

Оператор может принимать решения относительно события, отображенного либо на внутреннем хосте, либо на внешнем. В первом случае оператор просто выбирает актуальное для разрешения в данный момент времени событие из кругового меню (появляющегося после наведения курсора на соответствующий внутренний хост). В зависимости от типа события система предлагает оператору набор возможных команд для разрешения данного инцидента и изменяет отображение сети таким образом, чтобы показать оператору подходящие параметры. Оператор может, например, перенести функциональность скомпрометированного хоста ровно в два клика, при этом система сама выделит подходящие для данной функциональности хосты (рис. 2).

Оператор также может производить операции непосредственно с внешними хостами. По наведению курсора на внешний хост система выделяет все внутренние хосты, на которых возникли события, связанные с данным хостом. В случае, если нужно заблокировать определенную группу внешних хостов, оператору достаточно зажать кнопку мыши и повести курсор в направлении к другим хостам группы. Система сама добавит к группе для блокирования только те хосты, которые относятся к соответствующей комплексной атаке (как показано на рис. 1).

2.2. Адаптация под уровень усталости

Текущее психофизическое состояние оператора определяется системой на основе данных о его взаимодействии с системой: числа действий за различные промежутки времени, скорости реакции на отображаемые события и точности попадания по элементам интерфейса (в соответствии с моделью Фиттса [4]). Система следит за нажатиями оператором клавиш клавиатуры и кнопок мыши, а также за перемещением курсора (например, попадание по элементу интерфейса считается точным, если курсор перед тем, как на нем остановиться, пересек его границы только один раз). С ростом усталости оператора система замечает изменения характеристик взаимодействия с ним и адаптирует следующие параметры: размер элементов интерфейса, насыщенность цветовой палитры, интенсивность анимации, а также может сама доводить курсор до наиболее важных элементов в его окрестности.

2.3. Адаптация уровня когнитивной нагрузки

Зачастую оператору требуется дополнительное время для принятия решения не из-за его усталости, а из-за большого объема информации для восприятия. Система определяет уровень когнитивной нагрузки предоставляемой оператору информации, основываясь на количестве отображенных хостов, событий и элементов интерфейса. По продолжительности непрерывной работы оператора система определяет предполагаемый уровень его усталости, выявляя ситуации, когда ей следует адаптировать уровень когнитивной нагрузки. Для варьирования этого уровня система может масштабировать карту сети, менять количество элементов кругового меню, изменять уровень прозрачности незначительных хостов (тех, на которых не обнаружено наиболее опасных событий или приоритет которых при настройке топологии сети был указан как низкий), а также агрегировать на узле более высокого уровня информацию о его подсетях.

2.4. Адаптация под уровень владения системой

Под «уровнем владения системой» здесь подразумевается характеристика ознакомленности пользователя с интерфейсом и функциональностью системы. Основываясь на предопределенных в системе шаблонах активности «среднего» оператора (например, после отображения нового события и при отсутствии других инцидентов для разрешения оператор наводит на это событие курсор в течение фиксированного промежутка времени) и отклонениях от этих шаблонов текущего оператора, система может адаптировать уже упомянутый уровень когнитивной нагрузки, а также уровень поддержки (в системе поддержка реализована как всплывающие подсказки, направляющие оператора к наиболее критическим отображенным элементам).

Заключение

Данная статья посвящена системе визуализации событий информационной безопасности, способной адаптировать свои функциональность и методы отображения под текущего оператора, основываясь на характеристиках взаимодействия с ним. В работе представлены возможные методы адаптации (под текущую задачу оператора, под уровень его усталости, под уровень его когнитивной загруженности и под уровень его владения системой), которые могут применятся не только для целей информационной безопасности, но и в любой другой событийно-ориентированной системе с продолжительно работающим оператором. Не были затронуты вопросы производительности такой системы и не было проведено тестирование с участием пользователей, что и является следующим этапом данного исследования.

СПИСОК ЛИТЕРАТУРЫ:

1. *Brusilovsky P., Ahn J. W., Dumitriu T., Yudelson M.* Adaptive Knowledge-Based Visualization for Accessing Educational Examples // Information Visualization, 2006. IV 2006. Tenth International Conference. IEEE. 2006. July. P. 142–150.
2. *Callahan J., Hopkins D., Weiser M., Shneiderman B.* An Empirical Comparison of Pie vs. Linear Menus // Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM. 1988. May. P. 95–100.
3. *Conti G., Ahamad M., Stasko J.* Attacking Information Visualization System Usability Overloading and Deceiving the Human // Proceedings of the Symposium on Usable Privacy and Security. ACM. 2005. July. P. 89–100.
4. *Fitts P. M.* The Information Capacity of the Human Motor System in Controlling the Amplitude of Movement // Journal of Experimental Psychology. 1954. June. Vol. 47, № 6. P. 381–391.
5. *Gotz D., Wen Z.* Behavior-Driven Visualization Recommendation // Proceedings of the 14th International Conference on Intelligent User Interfaces. ACM. 2009. February. P. 315–324.
6. *Kohlhammer J., et al.* Visual Analytic Representation of Large Datasets for Enhancing Network Security: D1.1 Analysis of Current Practices. 2011.
7. *Lohse G. L.* The Role of Working Memory on Graphical Information Processing // Behaviour & Information Technology. 1997. Vol. 16, № 6. P. 297–308.
8. *MacKenzie I. S.* Fitts' Law as a Research and Design Tool in Human-Computer Interaction // Human-Computer Interaction. 1992. Vol. 7, № 1. P. 91–139.
9. *Merchant S.* Customizing the Human-Computer Interface to Compensate for Individual Cognitive Attitude: An Exploratory Study // Informing Science. 2002. P. 1043–1049.
10. *Shiravi H., Shiravi A., Ghorbani A. A.* A Survey of Visualization Systems for Network Security // Visualization and Computer Graphics. IEEE Transactions. 2012. Vol. 18, № 8. P. 1313–1329.
11. *Steichen B., Carenini G., Conati C.* User-Adaptive Information Visualization – Using Eye Gaze Data to Infer Visualization Tasks and User Cognitive Abilities // Proceedings of the International Conference on Intelligent User Interfaces. 2013. P. 317–328.
12. *Toker D., Conati C., Carenini G., Haraty M.* Towards Adaptive Information Visualization: On the Influence of User Characteristics // User Modeling, Adaptation, and Personalization. Springer Berlin Heidelberg. 2012. P. 274–285.
13. *Toker D., Conati C., Steichen B., Carenini G.* Individual User Characteristics and Information Visualization: Connecting the Dots through Eye Tracking // Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems. 2013. P. 295–304.
14. *Velez M. C., Silver D., Tremaine M.* Understanding Visualization through Spatial Ability Differences // Visualization. 2005. IEEE. P. 511–518.
15. *Ware C.* Information Visualization: Perception for Design. Morgan Kaufmann Pub., 2012.
16. *Yelizarov, A., Gamayunov D.* Visualization of Complex Attacks and State of Attacked Network // Visualization for Cyber Security. 6th International Workshop. 2009. IEEE. P. 1–9.
17. *Ziemkiewicz C., Crouser R. J., Yauilla A. R., Su S. L., Ribarsky W., Chang R.* How Locus of Control Influences Compatibility with Visualization Style // Visual Analytics Science and Technology (VAST). IEEE Conference. 2011. P. 81–90.

REFERENCES:

1. *Brusilovsky P., Ahn J. W., Dumitriu T., Yudelson M.* Adaptive Knowledge-Based Visualization for Accessing Educational Examples. In Information Visualization, 2006. IV 2006. Tenth International Conference on. IEEE. P. 142–150.
2. *Callahan J., Hopkins D., Weiser M., Shneiderman B.* An Empirical Comparison of Pie vs. Linear Menus. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM. P. 95–100.
3. *Conti G., Ahamad M., Stasko J.* Attacking Information Visualization System Usability Overloading and Deceiving the Human. In Proceedings of the 2005 Symposium on Usable Privacy and Security. ACM. P. 89–100.
4. *Fitts P. M.* The Information Capacity of the Human Motor System in Controlling the Amplitude of Movement. In Journal of Experimental Psychology. 47(6). P. 381–391.
5. *Gotz D., Wen Z.* Behavior-Driven Visualization Recommendation. In Proceedings of the 14th International Conference on Intelligent User Interfaces. ACM. P. 315–324.
6. *Kohlhammer J., et al.* Visual Analytic Representation of Large Datasets for Enhancing Network Security: D1.1 Analysis of Current Practices.
7. *Lohse G. L.* The Role of Working Memory on Graphical Information Processing. Behaviour & Information Technology, 16(6). P. 297–308.
8. *MacKenzie I. S.* Fitts' Law as a Research and Design Tool in Human-Computer Interaction. Human-Computer Interaction, 7(1). P. 91–139.
9. *Merchant S.* Customizing the Human-Computer Interface to Compensate for Individual Cognitive Attitude: An Exploratory Study. Informing Science, 1043-1049.
10. *Shiravi H., Shiravi A., Ghorbani A. A.* A Survey of Visualization Systems for Network Security. Visualization and Computer Graphics, IEEE Transactions on, 18(8), 1313-1329.
11. *Steichen B., Carenini G., Conati C.* User-Adaptive Information Visualization — Using Eye Gaze Data to Infer Visualization Tasks and User Cognitive Abilities. In Int. Conf. on Intelligent User Interfaces.

12. *Toker D., Conati C., Carenini G., Haraty M.* Towards Adaptive Information Visualization: On the Influence of User Characteristics. In User Modeling, Adaptation, and Personalization. Springer Berlin Heidelberg. P. 274–285.
13. *Toker D., Conati C., Steichen B., Carenini G.* Individual User Characteristics and Information Visualization: Connecting the Dots through Eye Tracking. In Proc. of the ACM SIGCHI Conference on Human Factors in Computing Systems.
14. *Velez M. C., Silver D., Tremaine M.* Understanding Visualization Through Spatial Ability Differences. In Visualization, 2005. VIS 05. IEEE. P. 511–518.
15. *Ware C.* Information Visualization: Perception for Design. Morgan Kaufmann Pub.
16. *Yelizarov A., Gamayunov D.* Visualization of Complex Attacks and State of Attacked Network. In Visualization for Cyber Security, 2009. VizSec 2009. 6th International Workshop on. IEEE. P. 1–9.
17. *Ziemkiewicz C., Crouser R. J., Yauilla A. R., Su S. L., Ribarsky W., Chang R.* How Locus of Control Influences Compatibility With Visualization Style. In Visual Analytics Science and Technology (VAST), 2011 IEEE Conference on. IEEE. P. 81–90.