Адаптивная под условия продолжительного мониторинга система визуализации событий информационной безопасности

Елизаров Анатолий Валерьевич,
Гамаюнов Денис Юрьевич

Аспирант, С.Н.С.

Лаборатория безопасности информационных систем,
Факультет вычислительной математики и кибернетики,
МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: tolya@lvk.cs.msu.ru, gamajun@seclab.cs.msu.su

В условиях возрастающего числа киберпреступлений все чаще возникает потребность в **человеческом операторе** СОИБ (Системы, Обеспечивающей Информационную Безопасность). Такой оператор должен непрерывно в течение длительного промежутка времени наблюдать за состоянием подконтрольных ему сетей и сервисов и принимать своевременные решения для их защиты, взаимодействуя с системой визуализации СОИБ.

Со временем у такого оператора будет меняться уровень усталости, скорость реакции и качество восприятия когнитивной нагрузки. Можно предположить, что учет текущего психофизического состояния оператора (способности адекватно реагировать на стимулы со стороны системы визуализации) и его индивидуальных особенностей восприятия благотворно скажется на своевременности и качестве принятых решений. Однако у существующих систем визуализации СОИБ (от Symantec, HP, IBM и др.) отсутствуют какие-либо механизмы определения текущего состояния пользователя.

Последние исследования показали, что такие когнитивные особенности человека, как объем рабочей памяти (working memory capacity [2,3]), скорость восприятия (perceptual speed [4]), пространственное мышление (spatial ability [5]) и локус контроля (locus of control [6]) влияют на скорость и точность работы с компьютером. При этом некоторые когнитивные особенности могут быть достоверно определены самой системой автоматически, например, с использованием технологий айтрекинга (анализа потока взгляда) [7,4].

Под **«адаптивным интерфейсом»** принято подразумевать такой интерфейс, который изменяет набор, порядок и вид отображаемых элементов в зависимости от контекста, состояния и целей пользователя. Уже показано, что в некоторых областях применения имеет смысл адаптировать систему под пользовательский уровень зна-

ний [8,4] или под шаблоны его поведения [9].

В докладе будет представлена **система визуализации событий информационной безопасности**, способная адаптировать свой интерфейс и методы отображения под текущее психофизическое состояние оператора, основываясь на таких характеристиках взаимодействия с ним, как *число действий за промежутки времени*, *скорость реакции на отображаемые события*, *точность попадания по элементам интерфейса* и *число ошибок первого и второго уровня*.

Также в докладе будут представлены результаты **исследования с реальными пользователями**. В рамках данного исследования 14 человек взаимодействовали как с разработанной адаптивной системой визуализации, так и с системой визализации OSSIM (открытой и активно применяемой СОИБ). Обе системы визуализации отображали одинаковые тестовые сценарии. В каждой сессии оценивалось количество и качество принятых пользователем решений. Исследование показало, что *состояние непрерывно взаимодействующего с системой пользователя меняется с течением времени*, *адаптация системы визуализации позволяет улучшить скорость и качество принятых пользователем решений*.

Иллюстрации

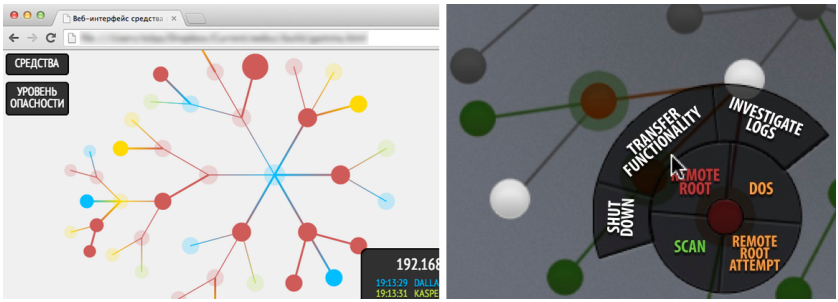

Рис. 1: Веб-интерфейс разработанной адаптивной системы визуализации и пример взаимодействия.

Литература

1. Merchant S. (2002). Customizing the Human-Computer Interface to Compensate for Individual Cognitive Attitude: An Exploratory

Study. Informing Science, 1043–1049.

2. Lohse G. L. (1997). The Role of Working Memory on Graphical Information Processing. Behaviour & Information Technology, 16(6), 297–308.

3. Toker D., Conati C., Carenini G., & Haraty M. (2012). Towards Adaptive Information Visualization: On the Influence of User Characteristics. In User Modeling, Adaptation, and Personalization (pp. 274–285). Springer Berlin Heidelberg.

4. Toker D., Conati C., Steichen B., & Carenini G. (2013). 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,(CHI 2013).

5. Velez M. C., Silver D., & Tremaine M. (2005, October). Understanding Visualization Through Spatial Ability Differences. In Visualization, 2005. VIS 05. IEEE (pp. 511–518). IEEE.

6. Ziemkiewicz C., Crouser R. J., Yauilla A. R., Su S. L., Ribarsky W., & Chang R. (2011, October). How Locus of Control Influences Compatibility With Visualization Style. In Visual Analytics Science and Technology (VAST), 2011 IEEE Conference on (pp. 81–90). IEEE.

7. Steichen B., Carenini G., & Conati C. (2013). User-Adaptive Information Visualization — Using Eye Gaze Data to Infer Visualization Tasks and User Cognitive Abilities. In Int. Conf. on Intelligent User Interfaces.

8. Brusilovsky P., Ahn J. W., Dumitriu T., & Yudelson M. (2006, July). Adaptive Knowledge-Based Visualization for Accessing Educational Examples. In Information Visualization, 2006. IV 2006. Tenth International Conference on (pp. 142–150). IEEE.

9. Gotz D., & Wen Z. (2009, February). Behavior-Driven Visualization Recommendation. In Proceedings of the 14th International Conference on Intelligent User Interfaces (pp. 315–324). ACM.