К. Н. ЖЕРНОВА
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук,
Санкт-Петербург

# КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ЧЕЛОВЕКО-КОМПЬЮТЕРНЫХ ИНТЕРФЕЙСОВ, ОСНОВАННЫХ НА ТЕХНОЛОГИЯХ ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ И СЕНСОРНЫХ ЭКРАНОВ

*Человеко-компьютерные интерфейсы являются постоянно развивающейся областью. В то же современные типы интерфейсов начинают применяться в приложениях информационной безопасности, и поэтому данные типы интерфейсов требуется защищать от третьих лиц. По этой причине требуется разрабатывать модели человеко-компьютерных интерфейсов, на основе которых можно проектировать алгоритмы и методики защиты интерфейсов от угроз информационной и компьютерной безопасности. В данном докладе предлагается концептуальная модель человеко-компьютерных интерфейсов на основе сенсорных экранов и виртуальной реальности.*

**Введение.** Угрозы человеко-компьютерным интерфейсам делятся на два типа:

1) атаки на интерфейс, использующие пути, типичные для интерфейса: атака на видеоканал интерфейса – обман системы распознавания лиц [1], атака на аудиоканал – использование команд, записанных в ультразвуковом диапазоне [2];

2) атаки на пользователя через интерфейс. Некоторые атаки могут наносить ущерб здоровью пользователя [3, 4].

Исследования, посвящённые проблеме защищённости интерфейса, рассматривают методы защиты от конкретной угрозы безопасности человеко-компьютерного интерфейса [5, 6, 7]. Однако для того, чтобы оценить защищённость интерфейса, требуется разработать модели интерфейсов, их уязвимостей, а также алгоритмы для оценивания защищённости интерфейсов. Интерфейсы обладают большим разнообразием, однако, несмотря на разнообразие, имеют общие характеристики. Поэтому была разработана концептуальная модель человеко-компьютерного интерфейса, которая позволит оперировать интерфейсом как набором входных данных для алгоритмов оценивания интерфейсов.

**Описание концептуальной модели.** Концептуальная модель взаимодействия внутри интерфейса «система-оператор» предполагает взаимодействие оператора с интерфейсом и интерфейса с оператором. Интерфейс состоит из компонента визуализации (который отображает обработанные данные) и компонента управления (который позволяет взаимодействовать с этими данными через визуализацию).

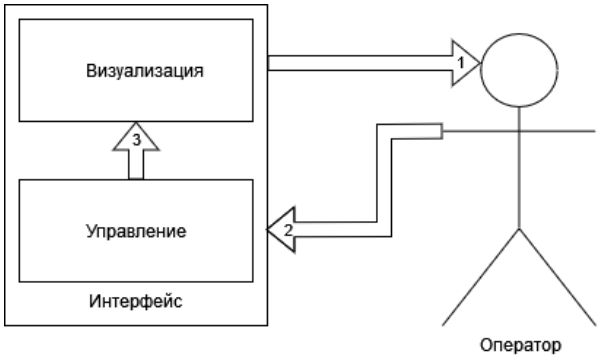


Рис. 1. Кольцо взаимодействия оператора с интерфейсом

Концептуальная модель описывает три основных потока данных при взаимодействии оператора с компьютерной системой: (1) компонент визуализации → оператор, (2) оператор → компонент управления, (3) компонент управления → компонент визуализации.

Процесс циркуляции данных при взаимодействии с интерфейсом выглядит следующим образом.

1. Данные, собранные системой, отображаются в виде модели визуализации, которую оператор воспринимает своими органами чувств.

2. Далее оператор принимает решение, и на основе этого решения вносит изменения в систему с помощью компонента управления интерфейса.

3. Внесённые изменения отображаются с помощью модели визуализации.

Концептуальная модель интерфейсов может применяться для разных типов визуальных интерфейсов. Ниже будут рассмотрены интерфейсы на основе виртуальной реальности и сенсорных экранов. Данные интерфейсы были выбраны, поскольку они достаточно новые и всё ещё активно развиваются, визуальные интерфейсы выбраны по той причине, что большую часть информации человек воспринимает через зрительный канал.

В ходе работы построена схема петли взаимодействия между оператором и системой. На основе этой схемы может быть выработана модель угроз, которая включает в себя угрозы для пользователя, угрозы для системы и угрозы при их пересечении. Затем на основе этой модели угроз возможно построить вектора атак, которые будут учитывать взаимосвязанность элементов схемы между собой.

***Интерфейс виртуальной реальности.*** На рис. 2 представлена схема взаимодействия основных элементов интерфейса виртуальной реальности.

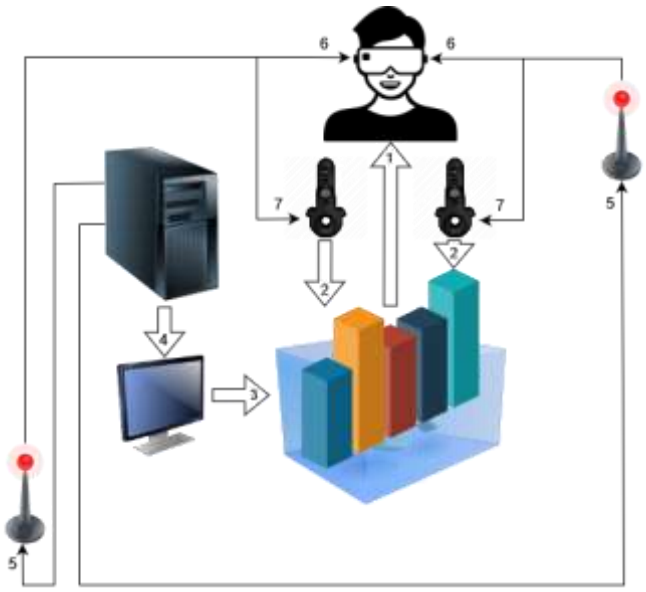


Рис. 2. Схема взаимодействия основных элементов интерфейса виртуальной реальности

Потоки информации на данной схеме обозначены следующим образом.

1. Визуализация → очки виртуальной реальности. При помощи очков виртуальной реальности оператор может видеть представляемые системой модели визуализации.

2. Контроллеры → визуализация. С помощью контроллеров оператор взаимодействует с визуализацией.

3. Монитор → визуализация. Визуализация чаще всего отображается не только очками виртуальной реальности, но и на мониторе.

4. Память устройства → монитор. Обработанные данные приложения отображаются на мониторе в виде моделей визуализации.

5. Память устройства → базовые станции. Обработанные данные приложения передаются с устройства базовым станциям.

6. Базовые станции → очки виртуальной реальности. Базовые станции отслеживают местоположение очков виртуальной реальности для правильного отображения местоположения аватара пользователя.

7. Базовые станции ↔ контроллеры. Базовые станции отслеживают местоположение контроллеров и принимают команды оператора, отданные с помощью контроллеров.

Соответствие потоков информации в концептуальной модели и потоков информации интерфейса виртуальной реальности представлено в табл. 1:

Таблица 1

**Потоки информации в интерфейсе, основанном на технологии виртуальной реальности**

| Концептуальная модель | Интерфейс виртуальной реальности |
|---|---|
| Компонент визуализации → оператор | Визуализация → очки виртуальной реальности<br>Базовые станции → очки виртуальной реальности |
| Оператор → компонент управления | Контроллеры → визуализация |
| Компонент управления → компонент визуализации | Монитор → визуализация<br>Память устройства → монитор<br>Память устройства → базовые станции<br>Базовые станции ↔ контроллеры |

***Интерфейс виртуальной реальности.*** На рис. 3 представлена схема взаимодействия основных элементов интерфейса для сенсорных экранов.


Рис. 3. Схема взаимодействия основных элементов интерфейса для сенсорных экранов

Потоки информации интерфейса сенсорных экранов обозначены следующим образом.

1. Визуализация → оператор. Оператор воспринимает визуализацию на экране сенсорного устройства.

2. Контроллеры → визуализация. В качестве контроллеров могут выступать стилус или рука оператора. Оператор вносит изменения и взаимодействует с данными визуализации.

3. Монитор → визуализация. Визуализация отображается на мониторе после изменений, вносимых оператором.

4. Память устройства → монитор. Обработанные данные приложения отображаются на мониторе в виде моделей визуализации.

Соответствие потоков информации в концептуальной модели и потоков информации интерфейса сенсорных экранов представлено в табл. 2:

Таблица 2

**Потоки информации в интерфейсе, основанном на технологии сенсорных экранов**

| Концептуальная модель | Интерфейс сенсорных экранов |
|---|---|
| Компонент визуализации → оператор | Визуализация → оператор |
| Оператор → компонент управления | Контроллеры → визуализация |
| Компонент управления → компонент визуализации | Память устройства → монитор<br>Монитор → визуализация |

На примере интерфейсов виртуальной реальности и сенсорных экранов можно видеть, что данная концептуальная модель подходит для различных видов визуальных интерфейсов. Каждый поток может подвергаться угрозам информационной безопасности. Однако знание о том, каким потокам в концептуальной модели соответствуют потоки данных рассматриваемого интерфейса, поможет идентифицировать угрозы, которым подвержен интерфейс.

**Заключение.** В данном докладе представлена концептуальная модель человеко-компьютерного интерфейса, которая позволит оперировать интерфейсом как входными данными для алгоритмов оценки человеко-компьютерного интерфейса. Также данная модель рассмотрена на примерах современных типов интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности. Использование предложенной модели в алгоритмах оценки защищённости интерфейсов позволит повысить осведомленность оператора о состоянии информационной и компьютерной безопасности используемой компьютерной системы.

*Работа проводилась при поддержке гранта РФФИ 20-37-90130 Аспиранты.*

ЛИТЕРАТУРА

1. **Zhong Y., Deng W**. Towards transferable adversarial attack against deep face recognition. *IEEE Transactions on Information Forensics and Security*. 2020. V. 16. Pp. 1452-1466.
2. **Song, L., Mittal P**. Poster: inaudible voice commands. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2583–2585 (2017).
3. **Sproul J., Ledger S., MacCallum J**. A review of digital media guidelines for students with visual light sensitivity. *International Journal of Disability, Development and Education*. 2021. V. 68. №. 2. Pp. 222-239.
4. **South L., Saffo D., Borkin M.A**. Detecting and Defending Against Seizure-Inducing GIFs in Social Media/ *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 2021. Pp. 1-17.
5. **Rafique M.U., Sen-ching S.C**. Tracking Attacks on Virtual Reality Systems. *IEEE Consumer Electronics Magazine*. 2020. V. 9. №. 2. Pp. 41-46.
6. **Mathis F. et al.** Fast and Secure Authentication in Virtual Reality using Coordinated 3D Manipulation and Pointing. *ACM Transactions on Computer-Human Interaction (ToCHI)*. 2021. V. 28. №. 1. Pp. 1-44.
7. **De Guzman J.A., Thilakarathna K., Seneviratne A**. Security and privacy approaches in mixed reality: A literature survey. *ACM Computing Surveys (CSUR)*. 2019. V. 52. №. 6. Pp. 1-37.

K.N.Zhernova, (St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg)

**Conceptual model of human-computer interfaces based on virtual reality technologies and touch screens**

Human-computer interfaces are a constantly evolving area. At the same time, modern interface types are beginning to be used in information security applications, and therefore these interface types need to be protected from third parties. For this reason, it is required to develop models of human-computer interfaces, on the basis of which it is possible to design algorithms and methods for protecting interfaces from threats to information and computer security. This report proposes a conceptual model of human-computer interfaces based on touch screens and virtual reality.

Авторы готовы представить текст на английском языке для сборника материалов мультиконференции, который будет подан для индексирования в Scopus.