На правах рукописи

Жернова Ксения Николаевна

ОЦЕНИВАНИЕ ЗАЩИЩЁННОСТИ ЧЕЛОВЕКО-КОМПЬЮТЕРНЫХ ИНТЕРФЕЙСОВ, ОСНОВАННЫХ НА ТЕХНОЛОГИЯХ СЕНСОРНЫХ ЭКРАНОВ И ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

Специальность: 2.3.6 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени кандидата технических наук

Санкт-Петербург

2022

Работа выполнена в Федеральном государственном бюджетном учреждении науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН) в лаборатории проблем компьютерной безопасности.

Научный руководитель: **ЧЕЧУЛИН Андрей Алексеевич**
кандидат технических наук, доцент, ведущий научный сотрудник лаборатории проблем компьютерной безопасности ФГБУН СПб ФИЦ РАН.

Официальные оппоненты: **СИНЕЩУК Юрий Иванович**
доктор технических наук, профессор, профессор ФГКОУ ВО «Санкт-Петербургский университет Министерства Внутренних Дел Российской Федерации»

ЛАУТА Олег Сергеевич
доктор технических наук, профессор кафедры комплексного обеспечения информационной безопасности ФГБОУ ВО «Государственный университет морского и речного флота имени адмирала С.О.Макарова»

Ведущая организация: Федеральное государственное автономное образовательное учреждение высшего образования Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова

Защита состоится «22» декабря 2022 г. в 16 часов 00 минут на заседании диссертационного совета 24.1.206.01, созданного на базе Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН) по адресу: 199178, Санкт-Петербург, 14-я линия В.О., 39, каб. 401, e-mail: dc@spcras.ru. Факс: (812) 328-44-50, тел: (812) 328-33-11.

С диссертацией и авторефератом можно ознакомиться в отделе аспирантуры (каб. 402а) Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН) si на сайте http://www.spiiras.nw.ru/dissovet

Автореферат разослан «9» ноября 2022 г.

Ученый секретарь
диссертационного совета 24.1.206.01 АБРАМОВ
кандидат технических наук Максим Викторович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертации. Человеко-компьютерные интерфейсы используются во всех областях человеческой деятельности, где применяются компьютерные системы: информационная безопасность, банковские приложения, образование, персональные компьютеры и т. д. При этом пользователи могут обмениваться с компьютерной системой чувствительными данными, содержащими конфиденциальную информацию. Однако в современных исследованиях мало внимания уделяется защите взаимодействия пользователя с компьютерной системой.

В настоящее время всё чаще применяются человеко-компьютерные интерфейсы, основанные на технологиях сенсорных экранов и виртуальной реальности. Многие персональные устройства пользователей (такие как смартфоны, планшеты или мониторы персональных компьютеров) имеют сенсорный экран. Также стремительно развивается технология виртуальной реальности, которая начинает внедряться в различные области, такие как образование, медицина и военное дело. Следовательно, данные интерфейсы требуют проведения исследований с точки зрения информационной и компьютерной безопасности.

Современные исследования новых развивающихся типов интерфейсов (сенсорные экраны и виртуальная реальность) сосредоточены на изучении конкретных типов уязвимостей и угроз. Небольшое количество обзоров приводит классификацию найденных уязвимостей, большая часть которых связана в большей степени с эргономикой, чем с информационной безопасностью. Однако для того, чтобы определить, насколько защищён данный человеко-компьютерный интерфейс, требуется создать методику оценивания уровня защищённости интерфейса.

Существующие системы оценки уязвимостей применимы к оценке уязвимостей сети и программного обеспечения, однако в них отсутствуют показатели, характерные для человеко-компьютерных интерфейсов, такие как канал восприятия и урон оператору. По этой причине требуется разработать методику создания подобных систем оценивания уязвимостей, пригодных для оценивания защищённости человеко-компьютерного интерфейса.

Решаемая научная задача: разработка комплекса моделей, алгоритмов и методики оценивания человеко-компьютерных интерфейсов, повышающих их защищённость.

Важность и значимость решаемой задачи обусловлены возможностью применения результатов исследования исследователями человеко-компьютерного взаимодействия и информационной безопасности, а также разработчиками человеко-компьютерных интерфейсов.

Степень разработанности темы. Исследования вопросов формирования защищённых интерфейсов, основанных на сенсорных экранах и виртуальной реальности, существуют, однако их крайне мало. При этом исследования в области безопасности интерфейсов подразделяются на две группы: решения конкретных вопросов безопасности с помощью человеко-компьютерных интерфейсов и поиски методов защиты от конкретных угроз безопасности для человеко-компьютерных интерфейсов. Такие российские учёные как Юсупов Р.М., Ронжин А.Л., Карпов А.А., В. Л. Авербух, Байдалин А.Ю. занимались проблемами человеко-компьютерного взаимодействия. Ряд зарубежных учёных (например, Roesner F., Gulhane A., George C., Khamis M.) решал проблемы защищённости интерфейсов от конкретных уязвимостей. Также со стороны иностранных учёных были попытки классифицировать угрозы для человеко-компьютерных интерфейсов (исследования таких авторов, как Kohno T., Thalmann D., Azuma R., Behringer R.). Однако не было выявлено работ, посвящённых оцениванию уязвимостей человеко-компьютерных интерфейсов.

Таким образом, несмотря на сделанный учёными научный задел, проблема оценивания уровня защищённости интерфейсов в области информационной безопасности на данный момент не разрешена, поэтому требуется проведение новых исследований.

Цель диссертационной работы: повышение защищённости человеко-компьютерных интерфейсов. Достижение поставленной цели предусматривало следующие **задачи**:

1) разработку модели человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности и модели уязвимостей человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности.

2) разработку алгоритма оценивания общего уровня защищённости интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности.

3) разработку методики оценивания защищённости интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности.

4) разработку архитектуры системы оценивания человеко-компьютерного интерфейса и её программного прототипа, реализующего разработанные модели и алгоритмы с помощью разработанной методики оценивания защищённости интерфейсов.

Объект исследования: перспективные человеко-компьютерные интерфейсы и присущие им уязвимости.

Предмет исследования: модели человеко-компьютерных интерфейсов и их уязвимостей, а также алгоритмы и методика, используемые для оценивания уровня защищённости человеко-компьютерных интерфейсов.

Научная новизна результатов определяется тем, что:

1) предложена новая аналитическая модель уязвимостей человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, отличающаяся от известных моделей расширенным множеством учитываемых уязвимостей этих человеко-компьютерных интерфейсов и связанных с ними новых параметров (урон оператору, канал восприятия и взаимодействие), обеспечивающая возможность работы с данными, необходимыми для оценивания защищённости интерфейса, и позволяющая учесть специфику технологий сенсорных экранов и виртуальной реальности;

2) разработан оригинальный алгоритм оценивания защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, по комплексному показателю, отличающийся от аналогов новыми правилами расчёта оценки уязвимости, учитывающий характеристики участников обмена информацией в человеко-компьютерных интерфейсах, обеспечивающий повышение показателей защищённости по сравнению с предложенными ранее алгоритмами;

3) предложена методика оценивания защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, отличающаяся от аналогов комплексным применением предложенных моделей и алгоритмов как на этапе разработки, так и на этапе эксплуатации интерфейсов, обеспечивающая повышение показателей защищённости интерфейсов по сравнению с аналогами;

4) разработаны архитектура и программная реализация системы оценивания защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, отличающиеся от аналогов расширенной функциональностью по расчёту оценок уязвимостей и уровня защищённости интерфейса, обеспечивающие оператору или разработчику выбор интерфейса с минимальной уязвимостью и повышение защищённости системы в целом.

Теоретическая и практическая значимость работы обусловлена доведением полученных результатов до уровня программной реализации и возможностью их внедрения в научные проекты, НИР и ОКР, связанные с разработкой новых и совершенствованием существующих систем. Предполагается, что использование полученных в данном диссертационном исследовании результатов позволит повысить общую защищенность как разрабатываемых, так и эксплуатируемых систем, использующих виртуальную реальность и/или сенсорные экраны в качестве интерфейса взаимодействия с пользователем системы. Кроме того, полученные результаты могут быть полезны исследователям в области информационной безопасности и человеко-компьютерного взаимодействия.

Методология и методы исследования. Задача оценивания человеко-компьютерных интерфейсов является междисциплинарной. В рамках диссертационного исследования использовались следующие методы и подходы. Для разработки моделей визуализации использовались методы и подходы к визуализации больших объемов многомерных данных, визуальной обработки информации посредством когнитивной графики, теории графов. Для разработки моделей интерфейсов использовался теоретико-множественный подход. Для разработки алгоритмов взаимодействия оператора с системами информационной безопасности использовались методы и подходы аналитического и имитационного моделирования, управления информацией и событиями информационной безопасности. Для разработки алгоритма оценивания защищённости интерфейсов использовались методы формальной оценки эффективности, экспертного анализа действий пользователя, экспериментальной оценки результатов на основе двойного рандомизированного тестирования.

Положения, выносимые на защиту:

1) модель уязвимостей человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности;

2) алгоритм оценивания защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, по комплексному показателю;

3) методика оценивания защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности;

4) архитектура и программная реализация системы оценивания уровня защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности.

Соответствие диссертации научной специальности. Представленные результаты соответствуют специальности 2.3.6 — «Методы и системы защиты информации, информационная безопасность».

Степень достоверности научных результатов, представленных в настоящем диссертационном исследовании, подтверждается с помощью подробного анализа современных работ и исследований в рассматриваемой области. Также обоснованность подтверждена согласованностью полученных результатов экспериментов, результаты и основные положения успешно прошли апробацию на различных научных и научно-практических конференциях всероссийского и международного уровня. Кроме того, результаты подтверждаются рядом публикаций, описывающих результаты экспериментов и раскрывающих основные положения исследования.

Апробация результатов работы. Результаты научной работы были подтверждены на следующих научно-практических конференциях:

1. 4th International Symposium on Mobile Internet Security (MobiSec 2019), (2019).
2. 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP-2020), (2020).
3. XV Международная конференция по электронике и робототехнике "Завалишинские чтения", (2020).
4. 5th International Scientific Conference “Intelligent Information Technologies for Industry”, Sochi, Russia, (2021).
5. Санкт-Петербургская международная конференция «Региональная информатика», г. Санкт-Петербург, СПб ФИЦ РАН, (2020).
6. Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России», участие с докладом, (2019, 2021).
7. Международная научно-техническая и научно-методическая конференция "Актуальные проблемы инфотелекоммуникаций в науке и образовании" (АПИНО), СПбГУТ им. проф. М.А. Бонч-Бруевича, (2018, 2019, 2020, 2021).
8. Межрегиональная научно-практическая конференция «Перспективные направления развития отечественных информационных технологий», (2019, 2020).

Результаты исследования были использованы в следующих проектах:

1. Модели, методы, методики и алгоритмы человеко-машинного взаимодействия для поддержки визуальной аналитики сетевой безопасности критических инфраструктур с использованием сенсорных мультитач-экранов, 18-07-01488 А, руководитель Котенко И.В., 2018-2020 гг.
2. Разработка методов поиска уязвимостей интерфейсов взаимодействия человека с искусственным интеллектом транспортной среды “умного города”, 19-29-06099 мк, руководитель Чечулин А.А., 2019-2022 гг.
3. Модели, алгоритмы и методики человеко-компьютерного взаимодействия в области информационной безопасности, 20-37-90130 Аспиранты, руководитель Чечулин А.А., 2020-2022 гг.

Публикации. По результатам выполнения диссертационного исследования опубликовано девять статей: пять статей в журналах из перечня ВАК, четыре статьи в трудах конференций, индексируемых в системах цитирования Web of Science и Scopus. Кроме того, полученные результаты представлены в 17 тезисах на международных и всероссийских научно-технических и научно-практических конференциях, в том числе “Parallel, Distributed, and Network-Based Processing” (PDP 2020), «Завалишинские чтения» (2020), “Intelligent Information Technologies for Industry” (IITI 2021), «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО 2018, 2019, 2020, 2021) и др.

Структура и объем диссертационной работы. Диссертационная работа включает введение, три главы, заключение, список использованных источников (147 наименований) и два приложения. Объем работы – 161 страница машинописного текста; включая 37 рисунков и 16 таблиц.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснованы важность и актуальность темы диссертационной работы, определена цель и сформулированы задачи, решение которых необходимо для ее достижения. Показаны научная новизна и практическая значимость работы. Дано краткое описание разработанных моделей представления анализируемых объектов, а также алгоритмов и методики, предназначенных для оценивания общего уровня защищённости человеко-компьютерных интерфейсов на основе моделирования уязвимостей. Представлены основные результаты их реализации в научно-исследовательских проектах.

Первая глава диссертационной работы посвящена исследованию задачи оценивания защищённости человеко-компьютерных интерфейсов, основанных на сенсорных экранах и виртуальной реальности. Определены место и роль этих интерфейсов в области информационной и компьютерной безопасности. Приведены основные определения и обзор действующих в настоящее время нормативных документов (ГОСТ Р ИСО/МЭК 15408-1-2008, ISO/IEC 18045:2005), описаны существующие методы и средства защиты человеко-компьютерных интерфейсов от различных угроз, приведена классификация существующих угроз человеко-компьютерным интерфейсам, основанным на сенсорных экранах и виртуальной реальности. Выделены основные недостатки существующих методик, затрудняющие обеспечение защищённости человеко-компьютерных интерфейсов и её оценку. Обоснована актуальность цели исследования.

Поставлена задача исследования, которая заключается в поиске целесообразного интерфейса с минимальной уязвимостью при определенных условиях. Суть задачи состоит в том, что имеется N различных интерфейсов, каждый из которых характеризуется собственным множеством уязвимостей $VULN_n$ со своими рисками $BS_{in}(I_n)$. Требуется оценить эти риски и найти целесообразный вариант интерфейса I_0, обеспечивающий минимизацию возможных рисков для безопасности $BS_{\Sigma}(I_0)$ (1):

$$BS_{\Sigma}(I_0) = \min_{n \in N} \sum_{i=1}^{VULN_n} BS_{in}(I_n) \quad (1)$$

Также должны учитываться ограничения по оперативности и ресурсопотреблению, предъявляемые к процессам оценивания защищённости человеко-компьютерных интерфейсов (2, 3):

$$TIME_n(I_n) \le TIME_n^{\text{ДОП}}, \quad (2)$$

$$r_n(I_n) \le R_n^{\text{ДОП}}, \quad (3)$$

где $TIME_n$ – время, которое необходимо для получения оценки защищённости интерфейса I_n, $TIME_n^{\text{ДОП}}$ – допустимая величина временных затрат на оценивание защищенности; r_n – ресурсы, необходимые для оценивания защищённости интерфейса, $R_n^{\text{ДОП}}$ – допустимое значение затрачиваемых ресурсов. На основе проведенного анализа литературы и опроса экспертов были выбраны следующие значения: $TIME_n^{\text{ДОП}} = 1$ мин и $R_n^{\text{ДОП}} = 0.3$.

Для реализации этой задачи необходимо наличие соответствующих моделей, алгоритмов и методики.

Во второй главе представлены разработанные модели человеко-компьютерных интерфейсов и их уязвимостей, а также алгоритмы оценивания уязвимостей интерфейсов и общего уровня защищённости интерфейса, необходимые для решения поставленных задач.

Для представления элементов реального интерфейса разработана модель человеко-компьютерных интерфейсов, включающая в себя модели элементов интерфейса и связей между ними. Структура модели описывается с помощью теоретико-множественного подхода. *Модель человеко-компьютерного интерфейса* задается в виде $I = <D, L, P>$, где D – множество элементов интерфейса; L – множество связей между элементами интерфейса, описывающих возможные способы взаимодействия (проводная связь между элементами, беспроводная и встроенная, когда один элемент интерфейса встроен в другой); P – настройки системы защиты интерфейса при её наличии, описывающая каждый хост с точки зрения его защищенности от реализации атак, использующих различные уязвимости. Интерфейсы обладают уязвимостями, некоторые из которых в качестве примеров приведены в таблице 1.

Таблица 1 – Примеры уязвимостей новых типов интерфейсов

Тип интерфейса	**Пример уязвимости**
Сенсорные экраны	Возможность наблюдения за действиями оператора
	Возможность повлиять на самочувствие оператора с помощью изображения
	…
Виртуальная реальность	Возможность подмены ИК-сигнала базовых станций
	Возможность повлиять на самочувствие оператора с помощью изображения
	Возможность сбоя настроек контроллеров
	…

Все примеры уязвимостей можно описать в виде следующей модели. *Модель уязвимостей* представлена в виде v_i =<*pd, ec, pr, ui, ch, c, i, a*>, где *pd* – урон оператору, *ec* – сложность эксплуатации уязвимости, *pr* – требуемые привилегии, *ui* – взаимодействие, *ch* – канал восприятия, *c* – риск для конфиденциальности, *i* – риск для целостности, *a* – риск для доступности. С использованием этой модели оценивание уязвимости осуществляется экспертами при заполнении таблицы, пример которой дан в таблице 2.

Таблица 2 – Пример заполнения таблицы экспертами

Показатель	**Значение, балл**	**Экс.1**	**Экс.2**	**…**	**Экс.N**
Сложность эксплуатации уязвимости	Низкая, 1	Низкая	Низкая	…	Высокая
	Высокая, 2				
Требуемые привилегии	Нет, 0	Нет	Низкие	…	Нет
	Низкие, 1				
	Высокие, 2				
Взаимодействие	Оператор, 1	Оператор	Оператор	…	Оператор
	Злоумышленник, 2				
Канал восприятия	Аудио, 1	Видео	Видео	…	Видео
	Видео, 2				
Конфиденциальность/ Целостность/ Доступность/ Урон оператору	Нет ущерба, 0	Низкий	Нет ущерба	…	Низкий
	Низкий, 1				
	Высокий, 2				

Каждому категориальному значению показателя присваивается целочисленный балл. Баллы значений, выбранных экспертами, суммируются, а затем сумма делится на количество экспертов. В случае если получено дробное число, результат округляется до ближайшего целого. Пусть уязвимость оценивают 3 эксперта. Сложность эксплуатации уязвимости они оценили как «Низкая» (1 балл), «Низкая» (1 балл) и «Высокая» (2 балла). Полученная оценка показателя равна (1+1+2)/3=1,33. В результате округления до ближайшего целого даёт 1. Таким образом, сложность эксплуатации уязвимости следует оценить как низкую.

Для человеко-компьютерных интерфейсов в настоящее время ещё не разработано стандартов, таких как Common Vulnerabilities and Exposures (CVE) и Common Attack Pattern Enumeration and Classification (CAPEC). Однако модель уязвимостей была разработана с учётом Common Vulnerability Scoring System (CVSS), для использования предлагаемой методики оценивания защищённости интерфейса в сочетании с оценкой сетевых уязвимостей хоста, что позволит получить более полные сведения об уровне защищённости хоста. Для оценивания уровня защищённости человеко-компьютерных интерфейсов был разработан соответствующий алгоритм,

использующий разработанные модели. Блок-схема *алгоритма оценивания защищённости интерфейса* представлена на рис. 1.

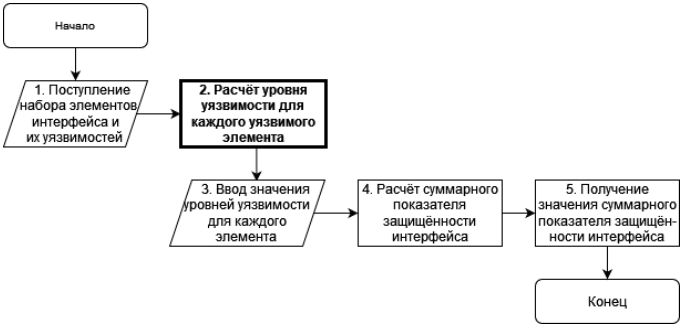


Рисунок 1 – Блок-схема алгоритма оценивания защищённости интерфейса

Для расчёта уровня уязвимости (шаг 2) используются числовые значения показателей уязвимости, представленные в таблице ниже.

Таблица 3 – Числовые значения показателей уязвимости

Показатель	**Значение**	**Числовое значение**
Сложность эксплуатации уязвимости	Низкая	0.65
	Высокая	0.42
Требуемые привилегии	Нет	0.86
	Низкие	0.72 (0.78, если сфера действия уязвимости поменялась)
	Высокие	0.67 (0.6, если сфера действия уязвимости поменялась)
Аудио-канал восприятия	Взаимодействие – оператор	0.72
	Взаимодействие – атакующий	0.68
Видео-канал восприятия	Взаимодействие – оператор	0.73
	Взаимодействие – атакующий	0.69
Конфиденциальность/ Целостность/ Доступность/ Урон оператору	Нет ущерба	0
	Низкий	0.12
	Высокий	0.52

Используя эти показатели, был проведён эксперимент оценки 336 типов уязвимостей, являющихся различными комбинациями данных показателей. Распределение уровня критичности при оценке данных комбинаций с помощью приведённого ниже алгоритма представлено на рис. 2. Из рисунка видно, что наибольшим оказалось количество уязвимостей среднего уровня (жёлтые столбцы), наименьшим – количество уязвимостей низкого (зелёные столбцы) и критического (красный столбец) уровня.

Уязвимости высокого уровня критичности представлены оранжевыми столбцами. Таким образом, распределение уровней критичности уязвимостей близко к нормальному.

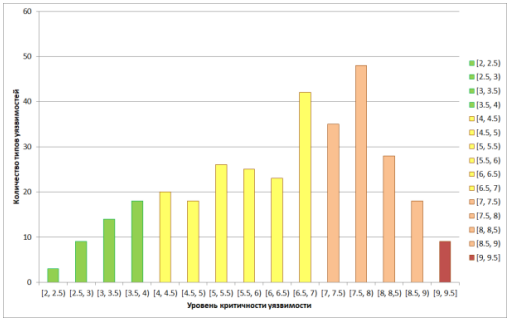


Рисунок 2 – Распределение уровня критичности оцениваемых уязвимостей

При этом уровни критичности уязвимости были следующие:

$$Criticality(v) = \begin{cases} Low, \ \ BS_{in}(I_n) \in (0; 4), \\ Medium, \ \ BS_{in}(I_n) \in [4; \ 7), \\ High, \ \ BS_{in}(I_n) \in [7; \ 9), \\ Critical, \ \ BS_{in}(I_n) \in [9; 10]. \end{cases}$$

Рассмотрим алгоритм более подробно.

1. На вход алгоритма поступает набор элементов интерфейса и их уязвимостей.

2. Производится расчёт уровня каждой уязвимости.

2.1. Вначале оценивается уровень ущерба для конфиденциальности, целостности и доступности данных и физического урона оператору. В отличие от исходной системы оценки (CVSS), здесь добавлен показатель урона оператору (*Damage*):

$$preImpact = 1 - [(1 - Confidentiality) \times (1 - Integrity) \times (1 - Availability) \times (1 - Damage)]. \quad (1)$$

Влияние ущерба в случае, если сфера действия уязвимости – только уязвимый компонент (*Scope* = *Unchanged*):

$$Imp = preImpact \times 6{,}42. \quad (2)$$

Влияние ущерба в случае, если сфера действия уязвимости может распространяться на другие компоненты интерфейса, кроме уязвимого (*Scope* = *Changed*):

$$Imp = 7.52 \times (preImpact - 0.029) - 3.25 \times (preImpact - 0.02)^{15}. \quad (3)$$

2.2. Возможность применения уязвимости, в отличие от исходной системы оценки, включает изменённый параметр «взаимодействие» (*UI*) и новый параметр «канал восприятия» (*CH*):

$$Exp = 8.22 \times EC \times PR \times UI \times CH, \quad (4)$$

где *EC* – сложность использования уязвимости (с двумя возможными значениями), *PR* – требуемые привилегии (с тремя возможными значениями), *UI* – параметр взаимодействия (с двумя возможными значениями), *CH* – параметр «канал восприятия» (с двумя возможными значениями).

2.3. Общая оценка уязвимости (*BS*) *k*-ого элемента интерфейса оставлена без изменений, поскольку для того, чтобы можно было объединять исходную систему с предлагаемой, для расчёта ущерба данным должны сохраняться те же принципы. Общая оценка будет равна нулю ($BS_k = 0$), если *Imp* = 0. Если сфера действия уязвимости не менялась, BS_k рассчитывается по формуле:

$$BS_{in}(I_n) = \min[(Imp + Exp), 10]. \quad (5)$$

Если сфера действия уязвимости поменялась, BS_k имеет вид:

$$BS_{in}(I_n) = \min[1{,}08 \times (Imp + Exp), 10]. \quad (6)$$

3. Вводятся полученные значения уязвимостей каждого элемента интерфейса $BS_{in}(I_n)$.

4. Процесс расчёта суммарного показателя уязвимости интерфейса (*Vulnerability*(I_n)) (с учётом коэффициентов важности групп уязвимостей) можно представить в виде (7):

$$\begin{aligned} BS_{\sum}(I_n) = {} & 0{,}01 \sum_{i=1}^{VULN_{n1}} BS_{in}(I_n)(Low) \\ & + 1 \sum_{i=1}^{VULN_{n2}} BS_{in}(I_n)(Medium) + 124{,}5 \sum_{i=1}^{VULN_{n3}} BS_{in}(I_n)(High) \\ & + 13\,969 \sum_{i=1}^{VULN_{n4}} BS_{in}(I_n)(Critical), \end{aligned} \quad (7)$$

где $VULN_n = VULN_{n1} + VULN_{n2} + VULN_{n3} + VULN_{n4}$ – число уязвимостей низкого, среднего, высокого и критического уровней соответственно. Коэффициенты 0,01, 1, 124,5, 13 969 были подобраны таким образом, чтобы значения различных уровней уязвимостей не пересекались, и можно было однозначно определить, что уязвимость такого уровня существует. Таким образом, значения показателя уязвимости интерфейса следующие:

$$Vulnerability(i) = \begin{cases} None, BS_{in}(I_n) = 0, \\ Low,\ 0 < BS_{in}(I_n) \le 1{,}5, \\ Medium, 1{,}5 < BS_{in}(I_n) \le 870{,}3, \\ High, 870{,}3 < BS_{in}(I_n) \le 125\,720{,}1, \\ Critical, BS_{in}(I_n) > 125\,720{,}1. \end{cases}$$

где *i* – *i*-ая уязвимость *n*-ого интерфейса, $BS_{in}(I_n)$ – базовая оценка уровня критичности уязвимости *n*-ого интерфейса I_n.

5. Тогда расчёт уровня защищённости интерфейса (*Security*(I_n)) производится в соответствии со следующим выражением:

$$Security(I_n) = \begin{cases} Unsafe, Vulnerability(I_n) = Critical, \\ Low, Vulnerability(I_n) = High, \\ Medium, Vulnerability(I_n) = Medium, \\ High, Vulnerability(I_n) = Low, \\ Secure, Vulnerability(I_n) = None. \end{cases}$$

6. Среди оцениваемых интерфейсов выбирается тот, который обладает наибольшим уровнем защищённости.

В третьей главе приведена разработанная методика оценивания защищённости человеко-компьютерного интерфейса (рис. 3 и 4). Также было дано описание архитектуры и программной реализации системы оценки защищённости человеко-компьютерного интерфейса. Также в данной главе представлены результаты экспериментов и сравнение предложенной методики с существующими аналогами.

Рисунок 3 – Методика оценивания защищённости интерфейса, этапы 1-2

Предложенная методика определяет основные стадии использования разработанных моделей и алгоритмов. Методика состоит из трех этапов.

1. Сбор информации: (1) с помощью модулей выбора уже известных уязвимостей и угроз, (2) ручной ввод оператором параметров ещё не известных уязвимостей и угроз для оценивания уровня критичности конкретной уязвимости.

2. Анализ защищённости интерфейса. Ввод информации об уровнях критичности уязвимостей интерфейса, расчёт суммарного показателя его защищённости, предлагаются возможные контрмеры.

3. Анализ удобства использования модифицированного интерфейса происходит с учётом применяемых контрмер против уязвимостей и угроз.

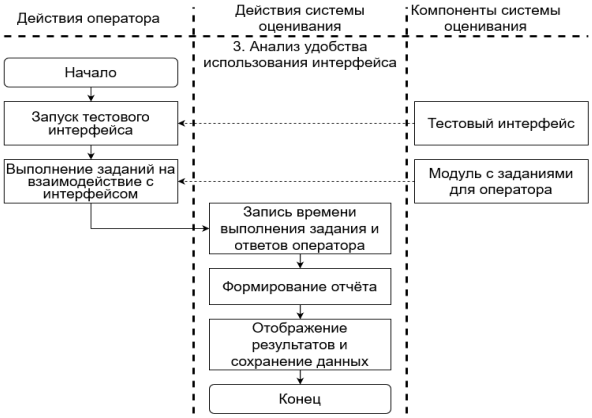


Рисунок 4 – Методика оценивания защищённости интерфейса, этап 3

Для реализации предложенного подхода была построена распределенная архитектура, содержащая модули алгоритмов оценивания уязвимостей и оценивания уровня защищённости интерфейса, графические модули данных алгоритмов, а также база данных уязвимостей, которая будет пополняться (рис. 5). Элементы методики были реализованы как сервисы, запущенные на сервере приложений.

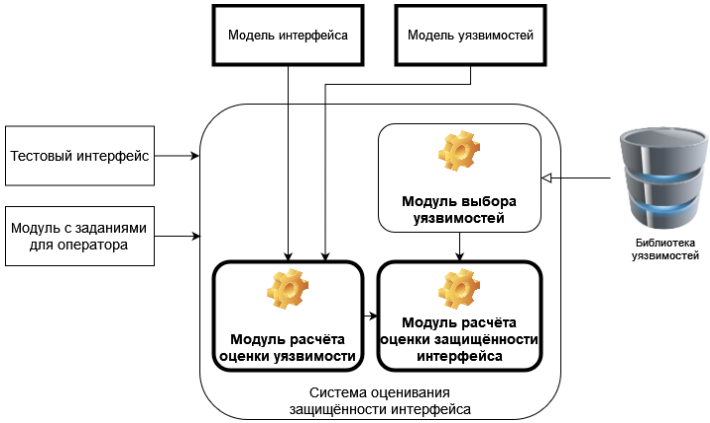
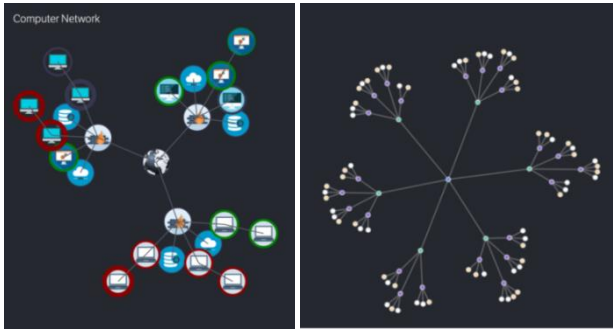


Рисунок 5 – Архитектура системы оценивания защищённости интерфейса

Для оценки использовались свойства, характеризующие приспособленность разработанной методики к выполнению оценивания защищённости интерфейса. В работе рассмотрены такие свойства как оперативность и ресурсопотребление, а также их показатели. При проведении экспериментов по очереди выполнялись этапы методики для

человеко-компьютерных интерфейсов, основанных на сенсорных экранах и виртуальной реальности.

Было проведено 20 тестов по взаимодействию оператора с программным прототипом системы оценивания защищённости человеко-компьютерного интерфейса. По результатам экспериментов, минимальное время оказалось 22 с, максимальное время – 46 с, при среднем времени взаимодействия 29,5 с. Результаты показывают, что требование к оперативности выполняется. Время выполнения методики складывается из продолжительности ее этапов и зависит от скорости работы оператора с приложением системы оценивания защищённости интерфейса. Для экспериментов использовались программные модули, содержащие разработанные модели и алгоритмы. В качестве платформы для проведения экспериментов использовался ЭВМ с установленной ОС Windows 10 x64 на базе четырехъядерного процессора Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz 1.99 GHz с 16 Гб оперативной памяти. Результаты экспериментов представляют собой усредненные величины. Анализ полученных данных позволяет судить о том, что время, необходимое на анализ уровня защищённости человеко-компьютерного интерфейса не превышает 3 минут. Показано, что методика удовлетворяет предъявляемым требованиям к *оперативности*. Данные, полученные в результате экспериментов, также показали, что *ресурсопотребление* соответствует требованиям, предъявляемым к подобным системам.



а) б)

Рисунок 6 – Внешний вид проверяемых интерфейсов: а) интерфейс с уязвимостью, б) исправленный интерфейс

Сравнивались различные типы человеко-компьютерных интерфейсов, основанных на сенсорных экранах и виртуальной реальности, с использованием разработанного подхода. В качестве таких интерфейсов выступают сенсорный интерфейс компьютерной сети с уязвимостью (рис. 6-а) и сенсорный интерфейс компьютерной сети исправленный (рис. 6-б).

Первый интерфейс содержал уязвимость для нарушения конфиденциальности (возможность осуществления атаки через наблюдение): крупные иконки устройств содержали изображение устройства. Кроме того, частота обновления сенсорного экрана причиняла дискомфорт оператору.

Экспертные оценки критичностей уязвимости к данным атакам в соответствии с методикой составили 6,7 и 2,5 соответственно. Расчёт по формуле 7 дал результат суммарной оценки уязвимости $BS_{\sum}(I_n)$ – 6,725.

Во втором интерфейсе исправлены обе уязвимости (рис. 6-б): иконки с изображениями были заменены мелкими разноцветными вершинами, что затрудняет атаку через наблюдение, так как для осуществления атаки злоумышленник теперь должен заранее располагать сведениями о том, какое устройство закодировано определённым цветом. Частота экрана изменена на комфортную. Расчёт по формуле 7 дал результат $BS_{\sum}(I_n)$ – 0 (см. таблицу 4).

Таблица 4 – Пример поиска наименее уязвимого интерфейса, сенсорные экраны

№	**Название интерфейса**	**Тип**	**Кол-во уязв.**	**Тип уязв.**	$\boldsymbol{BS_{in}(I_n)}$	$\boldsymbol{BS_{\sum}(I_n)}$
1	Граф компьютерной сети, с уязвимостью	СЭ	2	Уязвимость к наблюдению	6,7	6,725
				Некомфортная частота обновления экрана	2,5	
2	Граф компьютерной сети, исправленный	СЭ	0	**-**	**0**	**0**
Min уязвимость		**0**				

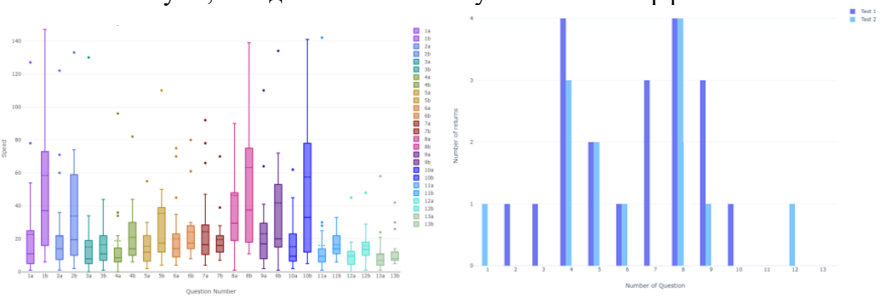
Интерфейс виртуальной реальности также уязвим к атакам через наблюдение. Изображение с головного дисплея может транслироваться на монитор компьютера. В этом случае также есть риск ущерба конфиденциальности. Кроме того, злоумышленник может заменить конфигурационный файл виртуальной среды, а базовые станции подвержены атакам типа спуфинг. Экспертные оценки критичностей уязвимости к данным атакам в соответствии с методикой составили 6,7, 5,4 и 7,1 соответственно. Суммарная оценка уязвимости $BS_{\sum}(I_n)$ – 896,05. Чтобы снизить возможный урон конфиденциальности, требуется сворачивать приложение на главном мониторе персонального компьютера, чтобы не оставить злоумышленнику возможности следить за действиями оператора. Чтобы предотвратить возможность замены конфигурационного файла на устройстве, требуется настройка политик безопасности и аутентификации. Тогда, $BS_{\sum}(I_n)$ будет равна 883,95. Интерфейсом с минимальной уязвимостью будет интерфейс 2 (таблица 5). Таким образом, из двух оцениваемых интерфейсов можно выбрать исправленный интерфейс, так как он обладает

минимальной уязвимостью. В приведённых выше примерах показано, что методика позволяет решить сформулированную задачу.

Таблица 5 – Пример поиска наименее уязвимого интерфейса, виртуальная реальность

№	Название интерфейса	Тип	Кол-во уязв.	Тип уязв.	$BS_{in}(I_n)$	$BS_{\sum}(I_n)$
1	Трёхмерный граф компьютерной сети, с уязвимостью	ВР	3	Уязвимость к наблюдению	6,7	896,05
				Возможность подмены файла конфигурации	5,4	
				Уязвимость ИК-базовых станций к спуфингу	7,1	
2	Трёхмерный граф компьютерной сети, исправленный	ВР	1	Уязвимость ИК-базовых станций к спуфингу	**7,1**	**883,95**
Min уязвимость			**883,95**			

Однако после принятия контрмер показатели удобства использования защищённого интерфейса могут существенно ухудшаться. Проведены эксперименты, оценивающие удобство использования исправленного интерфейса. Эксперименты включали в себя тесты скорости (рис. 7, а) и точности принятия решения оператором (рис. 7, б). Проводилось сравнение уязвимого интерфейса и исправленного интерфейса. Согласно проведённым экспериментам, результаты тестов для исправленного сенсорного интерфейса оказались не хуже, чем для изначального уязвимого интерфейса.



а) б)

Рисунок 7 – Результаты тестов проверяемых интерфейсов: а) тесты на скорость принятия решения оператором в секундах, б) тесты на точность принятия решения оператором, кол-во ошибок

Проверка удобства использования осуществлялась по следующему алгоритму, представленному на блок-схеме (рис. 8).

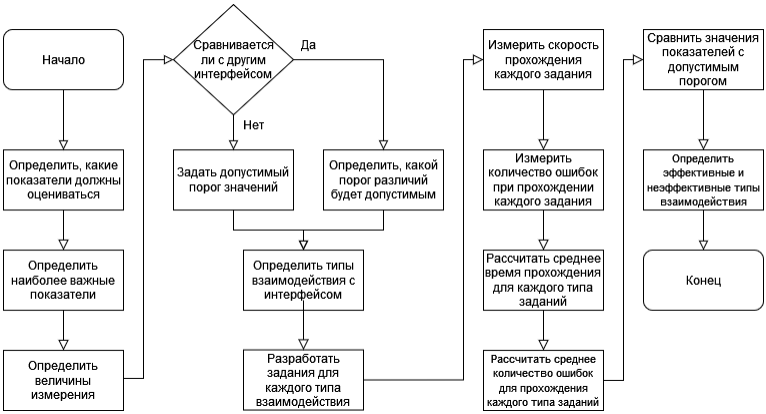


Рисунок 8 – Блок-схема алгоритма оценивания удобства использования

В таблице 6 были использованы следующие обозначения: «+» – система полностью удовлетворяет заданным условиям; «-» – заданное условие не удовлетворяется рассматриваемой системой. Например, система CVSS оценивает уязвимости хоста, но не интерфейса, так как не учитывает параметры, характерные для человеко-компьютерных интерфейсов. Эвристический подход Нильсена оценивает удобство использования интерфейса, однако не учитывает возможные уязвимости.

По результатам сравнения, параметры предлагаемой методики превзошли параметры рассматриваемых ближайших аналогов.

Таблица 6 – Сравнение разработанной методики с ближайшими аналогами

Параметры	**Реализация предлагаемой методики**	**CVSS**	**Nielsen Heuristics**
Оценивает уязвимости	+	+	-
Оценивает защищённость интерфейса	+	-	-
Учитывает урон, наносимый пользователю	+	-	-
Учитывает ущерб, наносимый данным пользователя	+	+	-
Оценивает удобство использования	+	-	+

Результаты экспериментов показали, что предлагаемая методика расширяет знания оператора или разработчика об уязвимостях компьютерной системы и позволяет выбрать интерфейс с минимальной уязвимостью. Таким образом, предлагаемая методика не уступает существующим методикам оценивания уязвимостей и удовлетворяет предъявляемым требованиям.

Таким образом, результаты экспериментальной проверки и сравнение с ближайшими аналогами предлагаемой методики и программного прототипа показали, что методика позволяет достичь поставленную цель

и удовлетворяет предъявляемым требованиям к оперативности и ресурсопотреблению (таблица 7).

Таблица 7 – Выполнение дополнительных требований

Свойство	Показатели	Требования
Оператив-ность	Вероятность того, что время, необходимое для получения результата оценки защищенности не будет превышать допустимое значение.	$P_{\text{ОП}}(TIME_I \le TIME^{\text{ДОП}}) \ge P_{\text{ОП}}^{\text{ДОП}}$ $P_{\text{ОП}}(46\text{ с} < 1\text{ мин}) \ge 0{,}99$ $P_{\text{ОП}} = 0{,}9911 > 0{,}99$ Требование выполняется.
Ресурсо-потребление	Вероятность того, что количество использованных ресурсов не будет превышать допустимое значение.	$P_{\text{РЕС}}(r \le R^{\text{ДОП}}) \ge P_{\text{РЕС}}^{\text{ДОП}}$ $P_{\text{РЕС}}(r \le 0{,}3) \ge 0{,}99$ r складывается из: $R_{ЦП}=0{,}04$, $R_{СЕТЬ}=0{,}01$, $R_{ЖД} \le 0{,}000001$, $R_{ОП}=0{,}08$. $P_{РЕС} = 1$. Требование выполняется.

Таким образом, результаты проведенных экспериментов и теоретической оценки подтверждают, что поставленная задача решена, требования к оперативности и ресурсопотреблению выполнены и, таким образом, цель диссертационного исследования достигнута.

В заключении приведены основные научно-практические результаты, полученные в ходе диссертационного исследования.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ РАБОТЫ

В диссертационной работе решена научная задача разработки комплекса моделей, алгоритмов и методики оценивания человеко-компьютерных интерфейсов, повышающих их защищённость, за счет чего была достигнута поставленная в исследовании цель – повышение защищённости человеко-компьютерных интерфейсов. **Итоги** исследования включают нижеперечисленные научные результаты:

1. Разработана аналитическая модель уязвимостей человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, которая использует теоретико-множественный подход к описанию параметров этих уязвимостей. Также разработаны (1) концептуальная модель человеко-компьютерного интерфейса и (2) теоретико-множественная модель интерфейса, учитывающая параметры безопасности. Теоретико-множественный подход описывает человеко-компьютерный интерфейс и его уязвимости как набор данных, использующихся при выполнении алгоритмов оценивания защищённости человеко-компьютерного интерфейса.

2. Разработан алгоритм оценивания защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, по комплексному показателю, включающий

расчёт показателя его уязвимости, учитывающий показатели, характерные для человеко-компьютерного интерфейса.

3. Разработана методика оценивания защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, в которую входят оценивание общего уровня защищённости человеко-компьютерного интерфейса и оценивание удобства его использования, повышающая осведомленность оператора об уровне защищённости компьютерной системы.

4. Разработана архитектура и программная реализация системы оценивания защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, использующая разработанную методику. Проведённые эксперименты показали, что требования к показателям оперативности и ресурсопотребления выполняются, и методика позволяет выполнить задачу поиска интерфейса с минимальной уязвимостью.

Также были даны **рекомендации** по практическому использованию научных результатов: результаты, полученные при проведении данного диссертационного исследования, могут быть использованы для разработки систем оценивания защищённости человеко-компьютерных интерфейсов, учитывающих удобство использования после принятия контрмер. Таким образом, задача, поставленная в диссертационном исследовании, была успешно решена. Использование предложенной методики позволит повысить защищённость взаимодействия оператора с компьютерными системами, основанными на технологиях сенсорных экранов и виртуальной реальности.

Перспективы дальнейшей разработки темы состоят в улучшении алгоритмов оценивания защищённости интерфейсов, уточнении показателей уязвимости, изучении новых типов интерфейсов.

Полученные результаты соответствуют специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность».

СПИСОК ОСНОВНЫХ ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в ведущих рецензируемы научных журналах и изданиях из списка ВАК:

1. Жернова К.Н., Коломеец М.В., Котенко И.В., Чечулин А.А. Применение адаптивного сенсорного интерфейса в приложениях информационной безопасности // Вопросы кибербезопасности. – 2020. – Т. 1, №35. – С. 18-28.
2. Жернова К.Н. Тенденции и проблемы развития естественности человеко-машинных интерфейсов // Информатизация и связь. – 2020. – №2. – С. 84-95.
3. Котенко И.В., Коломеец М.В., Жернова К.Н., Чечулин А.А. Визуальная аналитика для информационной безопасности: области применения, задачи и модели визуализации // Вопросы кибербезопасности. – 2021. – Т. 4, №44. – С. 2-15.
4. Котенко И.В., Коломеец М.В., Жернова К.Н., Чечулин А.А. Визуальная аналитика для информационной безопасности: оценка эффективности и анализ методов визуализации // Вопросы кибербезопасности. – 2021. – Т. 6, №46. – С. 2-15.
5. Жернова К.Н. Использование интерфейсов виртуальной реальности в области информационной безопасности // Информатизация и связь. – 2021. – №2. – С. 118-127.

Публикации в ведущих российских и иностранных научных журналах, входящих в список WoS/Scopus:

1. Zhernova Ksenia, Kolomeets Maxim, Kotenko Igor, Chechulin Andrey. Adaptive Touch Interface: Application for Mobile Internet Security // Communications in Computer and Information Science. – 2020. – Pp. 53-72.
2. Kolomeets Maxim, Chechulin Andrey, Zhernova Ksenia, Kotenko Igor, Gaifulina Diana. Augmented reality for visualizing security data for cybernetic and cyberphysical systems // 2020 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), Västerås, Sweden. – 2020.
3. Kolomeets Maxim, Zhernova Ksenia, Chechulin Andrey. Unmanned Transport Environment Threats // Proceedings of 15th International Conference on Electromechanics and Robotics "Zavalishin's Readings", Ufa, Russia, 15–18 April 2020 / Smart Innovation, Systems and Technologies. – 2020. – №187. – Pp. 395-408.
4. Zhernova Ksenia, Chechulin Andrey. Overview of Vulnerabilities of Decision Support Interfaces based on Virtual and Augmented Reality Technologies // Proceedings of 5th International Scientific Conference “Intelligent Information Technologies for Industry”, Sochi, Russia, 1 October 2021. – 2021.

Публикации в трудах российских и иностранных научных конференций:

1. Жернова К.Н., Коломеец М.В. Когнитивные особенности цветового восприятия пользователями приложений информационной безопасности // XI Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России» (ИБРР-2019). – 2019. – 596 с. – С. 119-120.
2. Виткова Л.А., Десницкий В.А., Жернова К.Н., Чечулин А.А. Обзор способов человеко-компьютерного взаимодействия для сетевой безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019).

VIII Международная научно-техническая и научно-методическая конференция. – 2019. – Т.1. – С. 218-223.

3. Коломеец М.В., Жернова К.Н. Визуальный анализ ботов социальной сети в дополненной реальности // XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)», Санкт-Петербург, Россия, 28-30 октября, 2020. – 2020. – Т.1. – С. 141-142.

4. Жернова К.Н., Комашинский Н.А., Котенко И.В. Модели визуального человеко-компьютерного взаимодействия с сетью устройств интернета вещей // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция. 26–27 февраля 2020. Санкт-Петербург. – 2020. – Т.1. – С. 466-470.

5. Жернова К.Н., Гайфулина Д.А., Иванов А.Ю., Комашинский В.И. Управление данными визуализации мобильной сети с использованием сенсорных экранов // XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)», Санкт-Петербург, Россия, 28-30 октября, 2020. – 2020. – С. 129-131.

6. Жернова К.Н. Методика проектирования человеко-компьютерных интерфейсов для приложений информационной безопасности // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). X Международная научно-техническая и научно-методическая конференция. 26–27 февраля 2021. Санкт-Петербург. – 2021. – Т.1 – С. 384-387.

7. Жернова К.Н., Коломеец М.В. Уязвимости интерфейсов «оператор – искусственный интеллект» в беспилотной транспортной среде // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). X Международная научно-техническая и научно-методическая конференция. 26–27 февраля 2021. Санкт-Петербург. – 2021. – Т. 1. – С. 387-390.

Свидетельства о государственной регистрации программ для ЭВМ:

1. Жернова К.Н., Котенко И.В. Компонент распознавания мультитач жестов для сенсорного экрана // Свидетельство № 2019666461. Зарегистрировано в Реестре программ для ЭВМ 10.12.2019. // 2019.

2. Жернова К.Н., Котенко И.В. Сенсорный интерфейс взаимодействия для мониторинга безопасности компьютерной сети // Свидетельство № 2019666536. Зарегистрировано в Реестре программ для ЭВМ 11.12.2019. // 2019.

3. Коломеец М.В., Чечулин А.А., Жернова К.Н. Система оценки визуального восприятия пользователя в виртуальной реальности // Свидетельство № 2019664065. Зарегистрировано в Реестре программ для ЭВМ 30.10.2019. // 2019.

4. Жернова К.Н. Компонент распознавания жестов для управления безопасностью компьютерной сети. Свидетельство № 2020665761. Зарегистрировано в Реестре программ для ЭВМ 01.12.2020. // 2020.

5. Жернова К.Н., Котенко И.В. Программный комплекс для оценки эффективности человеко-машинного взаимодействия с помощью сенсорных экранов. Свидетельство № 2020665837. Зарегистрировано в Реестре программ для ЭВМ 01.12.2020. // 2020.

6. Жернова К.Н., Чечулин А.А. Компонент визуализации сети Интернета вещей для приложений безопасности на основе сенсорных экранов. Свидетельство № 2021667922. Зарегистрировано в Реестре программ для ЭВМ 08.11.2021. // 2021.

Автореферат диссертации

Жернова Ксения Николаевна

ОЦЕНИВАНИЕ ЗАЩИЩЁННОСТИ ЧЕЛОВЕКО-КОМПЬЮТЕРНЫХ ИНТЕРФЕЙСОВ, ОСНОВАННЫХ НА ТЕХНОЛОГИЯХ СЕНСОРНЫХ ЭКРАНОВ И ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

Текст автореферата размещен на сайтах:

Высшей аттестационной комиссии Министерства образования и науки Российской Федерации
https://vak.minobrnauki.gov.ru/

Федерального государственного бюджетного учреждения науки Санкт-Петербургского Федерального исследовательского центра Российской академии наук (СПб ФИЦ РАН)
http://www.spiiras.nw.ru/dissovet/