ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 24.1.206.01, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ НАУКИ «САНКТ-ПЕТЕРБУРГСКИЙ ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР РОССИЙСКОЙ АКАДЕМИИ НАУК» МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ, ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 22.12.2022 г. № 2

О присуждении Жерновой Ксении Николаевне, гражданке Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Оценивание защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности» по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность» принята к защите 20 октября 2022 г., протокол заседания № 2 диссертационного совета 24.1.206.01, созданного на базе Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук», Министерства науки и высшего образования Российской Федерации, 199178, Россия, Санкт-Петербург, 14 линия ВО, дом 39, утвержден приказом Минобрнауки России №105/нк от 11 апреля 2012 г. (с изменениями согласно приказам №574/нк от 15 октября 2014 г., № 386/нк от 27 апреля 2017 г., №748/нк от 12 июля 2017 г., №301/нк от 23 ноября 2018 г., №467/нк от 4 августа 2020 г., №804/нк от 16 декабря 2020 г., 561/нк от 03 июня 2021г., №384/нк от 19 апреля 2022г.).

Соискатель Жернова Ксения Николаевна, 07 июля 1994 года рождения, в 2022 г. окончила очную аспирантуру в Федеральном государственном бюджетном учреждении науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), диплом № 107805 0010490. В настоящее время Жернова Ксения Николаевна работает научным сотрудником лаборатории проблем компьютерной безопасности в Федеральном

государственном бюджетном учреждении науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН) Министерства науки и высшего образования Российской Федерации.

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

Научный руководитель — кандидат технических наук, доцент ЧЕЧУЛИН Андрей Алексеевич, основное место работы: Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН), Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), лаборатория проблем компьютерной безопасности, ведущий научный сотрудник.

Официальные оппоненты:

СИНЕЩУК Юрий Иванович, доктор технических наук, профессор, Федеральное государственное казённое образовательное учреждение высшего образования «Санкт-Петербургский университет Министерства внутренних дел Российской Федерации», кафедра специальных информационных технологий, профессор;

ЛАУТА Олег Сергеевич, доктор технических наук, Федеральное государственное бюджетное образовательное учреждение высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова», кафедра комплексного обеспечения информационной безопасности, профессор.

дали положительные отзывы на диссертацию.

Ведущая организация — Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)», г. Санкт-Петербург в своем положительном отзыве, подписанном

Воробьёвым Евгением Германовичем, доктором технических наук, доцентом, заведующим кафедрой информационной безопасности СПбГЭТУ «ЛЭТИ», отзыв утвердил Тупик Виктор Анатольевич, доктор технических наук, профессор, проректор по научной работе СПбГЭТУ «ЛЭТИ», указала, что в целом диссертационная работа К.Н. Жерновой является завершенной научно-исследовательской работой, выполненной автором самостоятельно и на хорошем научном уровне, работа выполнена на актуальную тему, отличается научной новизной и практической значимостью полученных результатов. Автором в диссертации сформулирована и решена важная научно-техническая задача разработки комплекса моделей, алгоритмов и методики оценивания человеко-компьютерных интерфейсов, повышающих их защищённость.

В диссертации Жерновой К.Н. предложена аналитическая модель уязвимостей человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, позволяющая задать исходные данные, необходимые для оценивания этих интерфейсов. Основным отличием этой модели от существующих является расширенное множество учитываемых параметров уязвимостей человеко-компьютерных интерфейсов (урон оператору и канал восприятия).

Для оценивания защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, в диссертационной работе был разработан алгоритм, использующий новые правила расчёта оценки уязвимости. Основным отличием этих алгоритмов от уже существующих аналогов является учёт характеристик участников обмена информацией в человеко-компьютерных интерфейсах. Данный алгоритм позволит обеспечить повышение показателей защищённости по сравнению с предложенными ранее алгоритмами.

Методика оценивания защищенности человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, объединяет полученные ранее модели и алгоритмы и описывает способ их применения. Также разработанная методика предполагает возможность интеграции предложенного подхода с существующими системами оценки защищённости хоста, что позволит реализовать комплексный подход к защите компьютерных сетей и систем.

На основе предложенной методики был создан программно-аппаратный прототип, отличающийся расширенной функциональностью по расчёту оценок уязвимостей и уровня защищённости интерфейса. Данный прототип позволит выбрать интерфейс с минимальной уязвимостью и тем самым повысить защищённость системы в целом.

Результаты, полученные в данной работе, рекомендуется внедрить в образовательные учреждения, специализирующиеся на телекоммуникациях, такие как Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, а также имеющие направление информационной безопасности, такие как Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В. И. Ульянова. Текст автореферата полностью соответствует содержанию диссертации. Диссертационная работа Жерновой Ксении Николаевны «Оценивание защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности» удовлетворяет требованиям, пп. 9-14 «Положения о присуждении ученых степеней», утвержденного постановлением Правительства Российской Федерации 24.09.2013 года № 842 (в редакции Постановления Правительства РФ от 26.09.2022 года № 1690), предъявляемым к кандидатским диссертациям. Автор работы Жернова Ксения Николаевна заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

Соискатель имеет 27 опубликованных работ, в том числе по теме диссертации опубликовано 26 работ, из них в рецензируемых научных изданиях опубликовано 9 работ, из них опубликованных в изданиях, рекомендуемых ВАК – 5, индексируемых в WoS/Scopus – 4, имеется 9 свидетельств о государственной регистрации программы для ЭВМ.

Основные научные результаты опубликованы в 26 научных трудах общим объемом 18,7 п.л., из которых объем личного вклада соискателя составляет 9,5 п.л. Наиболее значимые работы по теме диссертации:

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. *Личный вклад соискателя – 65%.*

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. *Личный вклад соискателя – 35%.*
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. *Личный вклад соискателя – 35%.*
5. **Жернова К.Н.** Использование интерфейсов виртуальной реальности в области информационной безопасности // Информатизация и связь. – 2021. – №2. – С. 118-127.
6. **Zhernova Ksenia,** Kolomeets Maxim, Kotenko Igor, Chechulin Andrey. Adaptive Touch Interface: Application for Mobile Internet Security // Communications in Computer and Information Science. – 2020. – С. 53-72. *Личный вклад соискателя – 65%.*
7. 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. – С. 395-408. *Личный вклад соискателя – 35%.*
8. **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. – С. 400-409. *Личный вклад соискателя – 85%.*

Оригинальность содержания диссертации составляет не менее 85% от общего объёма текста; цитирование оформлено корректно; заимствованного материала, использованного в диссертации без ссылки на автора либо источник заимствования, не обнаружено; научных работ, выполненных соискателем учёной

степени в соавторстве без ссылок на соавторов не выявлено. Недостоверные сведения об опубликованных соискателем ученой степени работах в диссертации отсутствуют.

На диссертацию и автореферат поступило 6 отзывов, все отзывы положительны:

1. ФГБОУ ВО «Санкт-Петербургский государственный университет промышленных технологий и дизайна». Отзыв составил проректор по научной работе, заведующий кафедрой интеллектуальных систем и защиты информации, д.т.н. Макаров А.Г. Замечания: «Для расчета удобства использования после принятия контрмер используются только формальные показатели точности и скорости, без оценки других показателей удобства использования интерфейса, например, цветовой гаммы, расположения элементов и т.д. Кроме того, предложенная модель позволяет учесть только визуальные и аудиоинтерфейсы».

2. ФГАОУ ВО «Национальный исследовательский университет ИТМО». Отзыв составил заведующий лабораторией валидации программного обеспечения к.ф.-м.н., доцент Комаров И.И. Замечания: «При изложении результатов в контексте оценивания защищённости автор постоянно акцентирует внимание на повышение показателей защищённости, что вызывает естественное недоумение. Очень интересный результат, связанный с предыдущим вопросом и действительно призванный изменять исследуемый интерфейс в сторону повышения показателей защищённости, - предложение/выбор возможных контрмер - в автореферате только упоминается, хотя он является необходимым условием достижения заявленной цели исследования «повышение защищённости человеко-компьютерных интерфейсов». Кроме того, в автореферате имеют место стилистические и методические огрехи изложения, которые затрудняют восприятие материала.

3. ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого». Отзыв составил заместитель директора ИКиЗИ по научной работе, д.т.н., профессор Калинин М.О. Замечания: «Чем определяется представление в методике оценивания защищённости человеко-компьютерных интерфейсов этапа 3, указывающего на необходимость оценки удобства использования интерфейса, и как в этой оценке учитывается субъективность этого показателя? В предложенной

методике оценивания защищённости человеко-компьютерных интерфейсов (рис. 3, 4) не показана обратная связь в расчете уровня защищённости интерфейсов после принятия контрмер. Не описаны принципы измерения/подбора количественных показателей уязвимости человеко-компьютерных интерфейсов, хотя оценка защищённости интерфейсов является основной решаемой задачей».

4. ООО «ДИДЖИТАЛ ДИЗАЙН ИТ». Отзыв составил руководитель Центра информационной безопасности, к.т.н. Миняев А.А. Замечания: «В работе не рассмотрены уже известные бесконтактные атаки на сенсорные экраны, какие как GhostTouch, соответственно, не в полной мере представляется возможным оценить практическую применимость результатов работ. В автореферате есть ряд недостатков, связанных с понятийным аппаратом, а именно: по тексту автореферата прослеживается путанность в понятиях уязвимостей, угроз безопасности информации и негативных последствиях при реализации угроз безопасности информации. Например, в таблицу 1 виртуальная реальность никак не может быть типом интерфейса, возможность подмены ИК-сигнала базовых станций – это не уязвимость, а угроза безопасности информации, которая потенциально возможна в технических каналах утечки информации, и реализация которой возможна с помощью уязвимостей, способов и методов получения доступа к указанным каналам. В работе не использовались сведения из международных и российских баз данных уязвимостей и угроз безопасности информации (БДУ ФСТЭК России, MITRE ATT&CK, NVD и т.д.)».

5. ФГБОУ ВО «Первый Санкт-Петербургский государственный медицинский университет имени академика И.П. Павлова» Министерства здравоохранения Российской Федерации. Отзыв составил заведующий кафедрой физики, математики и информатики, к.ф.-м.н., доцент Тишков А.В. Замечания: «К недостаткам данной работы можно отнести то, что не приведено обоснование выбранных требований к системам оценки защищенности человеко-компьютерных интерфейсов. Кроме того, в автореферате ставится задача поиска варианта интерфейса I0, обеспечивающего минимизацию возможных рисков для безопасности, и пример такого интерфейса приводится в таблице 4. Однако,

представленные на рис. 1, 3 и 4 фрагменты системы оценивают риски, но не предъявляют в явном виде интерфейс I_0».

6. ФГБОУ ВО «Санкт-Петербургский Государственный университет». Отзыв составил доцент кафедры Математического моделирования энергетических систем, директор Центра искусственного интеллекта и науки о данных, д.ф.-м.н., Петросян О.Л. Замечания: «Отсутствие учета времени эксплуатации уязвимости. Отсутствие описания существующих подходов к аналитическому моделированию уязвимостей. Кроме того, рисунок 3 слишком перегружен для понимания. Описание таблицы 2 дано слишком кратко. В описании формулы 4 расшифровки некоторых аббревиатур повторяются. Отсутствует детальное описание группы тестируемых (отсутствует распределение по возрасту и полу)».

Выбор официальных оппонентов и ведущей организации обосновывается тем, что д.т.н., профессор Синещук Ю.И. является известным ученым в области методов защиты информации и оценки графических пользовательских интерфейсов, предложил методологию математического моделирования сложных объектов безопасности, разработал ряд методов, алгоритмов и технологических средств моделирования и оценки свойств структурной устойчивости информационных систем; д.т.н. Лаута О.С. – известный специалист в области обеспечения информационной безопасности и моделирования кибернетических атак, его основным научным направлением является поиск и внедрение способов противодействия информационным воздействиям на информационно-телекоммуникационную сеть военного назначения, кроме того, результаты его работ внедряются в образовательный процесс по учебным дисциплинам защита информации, защита инфокоммуникационных систем специального назначения; ведущая организация, СПбГЭТУ «ЛЭТИ», является известным в России образовательным учреждением, проводящим подготовку специалистов по информационной безопасности, кроме того, широко известны достижения ее специалистов в области проектирования систем информационной безопасности, а также поиска уязвимостей в компьютерных сетях и критически важных инфраструктурах.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработана новая методика, основывающаяся на оригинальных моделях и алгоритме оценивания защищённости человеко-компьютерных интерфейсов, обогащающая научную концепцию оценивания человеко-компьютерных интерфейсов и позволяющая расширить границы применимости методов оценивания защищённости;

предложены:

нетривиальный подход к оцениванию человеко-компьютерных интерфейсов, предполагающий оценивание их защищённости с последующей проверкой удобства использования после принятия контрмер и отличающийся таким образом комплексностью оценки человеко-компьютерного интерфейса;

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;

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;

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;

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.

доказана перспективность использования предложенной методики оценивания защищённости человеко-компьютерных интерфейсов, основывающейся на разработанных моделях и алгоритме;

введены:

- новые типы уязвимостей, типичных для человеко-компьютерных интерфейсов;
- новые параметры безопасности, специфичные для человеко-компьютерных интерфейсов, такие как урон оператору и канал восприятия.

Теоретическая значимость исследования обоснована тем, что:

доказаны применимость предложенной в работе методики с использованием экспериментальных исследований, вносящей вклад в расширение представлений об оценивании человеко-компьютерных интерфейсов, поскольку данная методика расширяет ряд оцениваемых свойств человеко-компьютерных интерфейсов;

применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов) использован метод и подход аналитического и имитационного моделирования, теории графов, дискретной математики, теории множеств, формальной оценки эффективности, информационной безопасности;

изложены методологические и методические основы оценивания человеко-компьютерных интерфейсов, тенденции использования средств информационной безопасности для повышения защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности;

раскрыты

проблемные аспекты применения имеющихся подходов в области оценивания человеко-компьютерных интерфейсов к оцениванию защищённости человеко-компьютерных интерфейсов;

основные вопросы, связанные с поиском и устранением различных типов уязвимостей человеко-компьютерных интерфейсов;

несоответствие человеко-компьютерным интерфейсам существующих подходов к оцениванию защищённости ввиду того, что они не учитывают параметры безопасности, характерные именно для человеко-компьютерных интерфейсов;

изучены существующие методы оценивания человеко-компьютерных интерфейсов, при этом отдельное внимание уделено рассмотрению связи данного явления с оцениванием защищённости, также изучены существующие подходы к оцениванию уязвимостей;

проведена модернизация существующих методов оценивания человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, обеспечивающих получение новых результатов по теме диссертации.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

разработаны и внедрены следующие результаты диссертационной работы:

• модель уязвимостей человеко-компьютерных интерфейсов ТСЭиВР (основанных на технологиях сенсорных экранов и виртуальной реальности), которая позволит расширить множество уязвимостей, учитываемых при оценивании уровня защищённости хоста;

• алгоритм оценивания защищённости человеко-компьютерных интерфейсов ТСЭиВР по комплексному показателю, который позволит учесть параметры безопасности, специфичные для человеко-компьютерных интерфейсов, такие как «урон оператору» и «канал восприятия»;

• методика оценивания защищённости человеко-компьютерных интерфейсов ТСЭиВР, которая позволит оценивать защищённость с помощью разработанных модели и алгоритма и удобство использования после принятия контрмер;

• архитектура и программная реализация системы оценивания уровня защищённости человеко-компьютерных интерфейсов ТСЭиВР, которая позволит интегрировать предложенную методику с уже существующими системами оценивания защищённости хоста,

которые были использованы при выполнении работ в СПб ФИЦ РАН по следующим темам:

- «Модели, методы, методики и алгоритмы человеко-машинного взаимодействия для поддержки визуальной аналитики сетевой безопасности критических инфраструктур с использованием сенсорных мультитач-экранов», выполненных по гранту РФФИ № 18-07-01488 А;

- «Разработка методов поиска уязвимостей интерфейсов взаимодействия человека с искусственным интеллектом транспортной среды “умного города”», выполненных по гранту РФФИ № 19-29-06099 мк;

- «Модели, алгоритмы и методики человеко-компьютерного взаимодействия в области информационной безопасности», выполненных по гранту РФФИ № 20-37-90130 Аспиранты;

а также внедрены в работу коммерческой организации ООО «Жасмин» для оценивания качества пользовательского интерфейса.

определены возможности и перспективы практического использования полученных результатов диссертации при исследовании конкретных технологий оценивания человеко-компьютерных интерфейсов и оценивания уязвимостей;

создана методика оценивания защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, позволяющая существенно расширить возможности известных систем оценки защищённости;

представлены предложения и направления для дальнейших научных исследований, в основу которых могут быть положены разработанные модель, алгоритм и методика.

Оценка достоверности результатов исследования выявила:

для экспериментальных работ достоверность полученных результатов подтверждается проведением многостороннего сравнительного анализа работ по исследуемой проблеме, корректным использованием научно-методического аппарата в виде применяемых подходов и теорий, а также тем, что основные результаты диссертации были опубликованы в печатных трудах и обсуждались на международных и всероссийских конференциях, кроме того, результаты работы были внедрены в рабочий процесс научных и коммерческих организаций;

теория базируется на известных принципах формирования человеко-компьютерных интерфейсов, проверенных данных с использованием современных апробированных методов оценивания защищённости и эффективности, согласуется с опубликованными ранее частными результатами других исследователей в области обеспечения безопасности человеко-компьютерных интерфейсов;

идея базируется на анализе работ отечественных и зарубежных исследователей в области оценивания человеко-компьютерных интерфейсов, а также поиска и закрытия уязвимостей человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности;

использованы полученные характеристики для сравнения с данными, приведенными в современной научной литературе по оцениванию уязвимостей и оцениванию человеко-компьютерных интерфейсов (так, например, при оценке интерфейсов не оценивается защищённость, а при оценке уязвимостей не учитываются показатели безопасности интерфейсов, такие как урон оператору и канал восприятия);

установлено качественное и количественное соответствие результатов решения задачи разработки комплекса моделей, алгоритмов и методики оценивания человеко-компьютерных интерфейсов, повышающих их защищённость. При этом подтверждено преимущество предложенного подхода к оцениванию человеко-компьютерных интерфейсов перед методами, использованными другими авторами.

использованы современные методики сбора, обработки, классификации исходной информации, методы и подходы к анализу гетерогенных данных, методы

формальной оценки эффективности, методы и подходы управления информацией и событиями информационной безопасности.

Личный вклад соискателя состоит в:

- постановке задачи разработки методики оценивания защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности. разработке и обосновании методики оценивания защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности;
- разработке модели уязвимостей человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, использующейся в предложенной методике;
- разработке алгоритма оценивания защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, использующегося в предложенной методике;
- разработке архитектуры программно-аппаратного прототипа, реализующего предложенную методику.

В ходе защиты диссертации были высказаны следующие критические замечания: при оценивании удобства использования интерфейса используется расчёт формальных показателей – точность и скорость, при этом не учитываются более субъективные показатели, такие как физическая усталость, или классические для интерфейса показатели, такие как цветовая гамма, расположение элементов интерфейса и т.п., которые также могут влиять на самочувствие оператора и эффективность его работы, в то время как в работе самочувствие оператора также является важным для оценивания защищённости интерфейса. В работе использован термин «оценивание», хотя чаще всего применяется термин «оценка». Чем обоснована такая терминология?

Соискатель Жернова К.Н. ответила на задаваемые ей в ходе заседания вопросы и привела собственную аргументацию: в работах по оцениванию эффективности и удобства использования чаще всего эти свойства оцениваются по формальным показателям, обычно используются точность и скорость. Кроме того,

точность и скорость выполнения заданий оператором позволяют оценить также и уровень усталости оператора при работе с интерфейсом, поскольку при накоплении усталости, а также при неудачной цветовой гамме и расположении элементов интерфейса точность и скорость работы снижаются. Выбор термина «оценивание» обусловлен тем, что в работе рассматривается процесс получения количественных показателей защищённости интерфейса, в то время как «оценка» – это полученное количественное значение.

На заседании 22.12.2022 г. диссертационный совет принял решение за решение научной задачи разработки комплекса моделей, алгоритмов и методики оценивания человеко-компьютерных интерфейсов, повышающих их защищённость, имеющей существенное значение для развития страны в области информационной безопасности, присудить Жерновой К.Н. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 18 человек, из них 7 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 25 человек, входящих в состав совета, проголосовали: за 18, против нет, недействительных бюллетеней нет.

Заместитель председателя диссертационного совета
доктор технических наук,
профессор Смирнов Александр Викторович

Ученый секретарь диссертационного совета
кандидат технических наук Абрамов Максим Викторович
22.12.2022 г.