



МИНОБРНАУКИ РОССИИ
федеральное государственное автономное образовательное учреждение
высшего образования
**«Санкт-Петербургский государственный электротехнический университет
«ЛЭТИ» им. В.И. Ульянова (Ленина)»**
(СПбГЭТУ «ЛЭТИ»)

ул. Профессора Попова, д.5, Санкт-Петербург, 197376
Телефон: (812) 346-44-87 Факс: (812) 346-27-58 E-mail: eltech@eltech.ru [http:// www.eltech.ru](http://www.eltech.ru)
ОКПО 02068539 ОГРН 1027806875381 ОКВЭД 80.3, 73.1 ОКТМО 40392000
ИНН/КПП 7813045402/781301001

№ _____
от _____

«Утверждаю»
Проректор по научной работе
СПбГЭТУ «ЛЭТИ»
д.т.н. профессор

В.А. Тупик
_____ 2022 г.

ОТЗЫВ

ведущей организации на диссертационную работу

Жерновой Ксении Николаевны

«Оценивание защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности» на соискание ученой степени кандидата технических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

Актуальность избранной темы

Оценка защищенности человеко-компьютерных интерфейсов в настоящее время является мало исследованной областью. Однако множество атак, направленных на перехват конфиденциальной информации, можно провести именно при взаимодействии оператора и системы. При этом системы взаимодействия оператора с устройством и данными на этом устройстве часто бывают не защищены. Вместе с тем во многие области человеческой деятельности внедряются новые перспективные виды человеко-компьютерных интерфейсов, такие как сенсорные экраны и виртуальная реальность. Для этих типов интерфейсов также постоянно

появляются новые виды неизученных угроз. Таким образом, для того, чтобы повысить защищённость человеко-компьютерного взаимодействия, необходимо разработать подходы к оцениванию перспективных человеко-компьютерных интерфейсов.

Однако, существующие исследования защищённости человеко-компьютерных интерфейсов направлены на устранение отдельных конкретных уязвимостей и угроз, при этом практически не предлагая систематизацию уязвимостей, присущих человеко-компьютерным интерфейсам. Также не было выявлено подходов к оцениванию общего уровня защищённости человеко-компьютерных интерфейсов.

Таким образом, можно сформулировать следующее противоречие: для разработки безопасного человеко-компьютерного интерфейса необходимо выполнять оценку защищённости разрабатываемого интерфейса, но с помощью существующих подходов это сделать практически невозможно. Следовательно, разработка моделей, алгоритмов и методики оценивания защищённости человеко-компьютерных интерфейсов является актуальной и имеет практическую ценность. Актуальность подтверждается также использованием результатов диссертации в ряде научно-исследовательских работ.

Новизна исследования и полученных результатов, выводов и рекомендаций, сформулированных в диссертации

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 защищённости 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.

Новизна и достоверность результатов и выводов, сформулированных в диссертационной работе, подтверждается сравнительным анализом разработанной методики и предшествующих научных разработок в исследуемой области.

Значимость полученных автором диссертации результатов для развития соответствующей отрасли науки

Основными научным достижением автора является разработка подхода к оцениванию защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности.

Теоретические выводы, описанные в диссертационной работе, были подтверждены с помощью разработанного программно-аппаратного прототипа и проведённых на нём экспериментов.

Теоретическая значимость полученных результатов выражается в том, что проведённое исследование вносит вклад в научную область человеко-компьютерного взаимодействия, а также предлагает алгоритмы и методику по его защите. Практическая значимость состоит в том, что предложенные модели, алгоритм и методика могут быть использованы разработчиками человеко-компьютерных интерфейсов для создания защищённых интерфейсов на основе сенсорных экранов и виртуальной реальности, а также разработчиками систем информационной безопасности для усовершенствования подобного рода систем.

Полученные результаты могут использоваться для повышения качества проектирования человеко-компьютерных интерфейсов и оценки защищённости человеко-компьютерного взаимодействия. Кроме того, предложенный подход позволяет оценить эффективность возможных контрмер, а также проверить удобство использования интерфейса после принятия этих контрмер, благодаря чему комплекс разработанных моделей, алгоритмов и методики может быть использован в системах поддержки принятия решений. Высокий уровень полученных результатов подтверждается актами о внедрении в различные проекты, полученными от СПб ФИЦ РАН, а также использованием в коммерческой организации ООО «Жасмин» для оценки пользовательских интерфейсов.

Рекомендации по использованию результатов и выводов, приведенных в диссертации:

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 (Ленина).

Общая оценка диссертационной работы

При оценке диссертации К.Н.Жерновой было отмечено, что данное исследование является завершённой научно-исследовательской работой, выполненной автором самостоятельно и на хорошем научном уровне. В данной работе решена актуальная и практически значимая научная задача – разработка методики оценивания защищённости человеко-компьютерных интерфейсов. Результаты были представлены на ряде российских и международных конференций, основные положения были описаны в нескольких научно-исследовательских работах, опубликованных в российских и зарубежных изданиях. Имеются пять публикаций в рецензируемых журналах из перечня ВАК («Информатизация и связь», «Вопросы кибербезопасности»). Содержание автореферата отражает основные положения диссертации.

В то же время можно выделить и ряд замечаний к диссертационной работе:

1) В первой главе проанализированы существующие способы представления моделей человеко-компьютерных интерфейсов, рассмотрены существующие угрозы человеко-компьютерным интерфейсам, однако описание методик оценки этих угроз практически отсутствует.

2) Недостаточно раскрыта причина употребления термина «человеко-компьютерный интерфейс» вместо более частого термина «человеко-машинный интерфейс».

3) Во второй главе приведены числовые значения показателей уязвимости интерфейса, однако принципы их получения раскрыты недостаточно полно.

4) Понятие «уязвимости», используемое в диссертации, раскрыто недостаточно полно. Необходимо было более четко описать разницу между уязвимостью и угрозой в данном случае. В работе не использована Методика оценки угроз безопасности информации ФСТЭК, утвержденная 5 февраля 2021 года, в результате чего неполно рассмотрен перечень основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации.

5) При проверке удобства использования уделяется недостаточно внимания субъективным ощущениям пользователя при работе с интерфейсом, удобство использования определяется, в основном, по формальным показателям.

Однако отмеченные недостатки не влияют на общую положительную оценку диссертационной работы. Предложенный подход, позволяющий оценивать общий уровень защищенности человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, является существенным вкладом в решение задачи построения систем, предназначенных для защиты информации. Таким образом, автореферат отражает основное содержание диссертационной работы, а научно-техническая задача повышения защищённости человеко-компьютерных интерфейсов сформулирована и решена.

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 от 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».

Доклад Жерновой Ксении Николаевны был заслушан на заседании кафедры ИБ ФГАОУ ВО Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В. И. Ульянова. протокол № 11 от «10» ноября 2022 г.

Заведующий кафедрой информационной безопасности
ФГАОУ ВО Санкт-Петербургского государственного электротехнического
университета «ЛЭТИ» имени В.И.Ульянова (Ленина)
доктор технических наук, доцент

Воробьев Евгений Германович

~~«10»~~ ноября 2022 года

Рабочий адрес: 197022, Санкт-Петербург, ул. Профессора Попова, 5
Тел.: +7 812 234-43-31
E-mail: egvorobiev@etu.ru