ОТЗЫВ

официального оппонента
доктора технических наук, профессора
Синещука Юрия Ивановича
на диссертационную работу Жерновой Ксении Николаевны
«Оценивание защищённости человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»

1. АКТУАЛЬНОСТЬ ИЗБРАННОЙ ТЕМЫ

Цифровизация всех сфер экономики и управления, внедрение результатов и технологий четвертой промышленной революции в практическую деятельность, возрастание роли и значимости информации в процессах принятия решений обуславливают необходимость решения проблемы обеспечения информационной безопасности.

Наиболее эффективным способом решения проблем информационной безопасности является обеспечение надлежащего уровня защищенности за счет профилактических(упреждающих) мер выявления и предотвращения опасности. В общем случае, негативные воздействия на информационную систему, по своей природе, могут быть различными: внешние физические деструктивные факторы; внутренние деструктивные факторы, исследуемые в рамках анализа надежности; электромагнитные помехи; программно-информационные воздействия, или кибератаки.

Если про традиционные группы факторов можно сказать, что они в достаточной степени исследованы и рассматриваются во многих сложных электротехнических системах, не только в информационных системах, то последняя группа факторов характерна именно для информационных систем, так как именно компьютерная обработка информации является средой для распространения кибератак.

Эффективность информационных систем во многом зависит от качества их визуальной составляющей - пользовательского интерфейса, который тоже необходимо рассматривать и как объект защиты и как потенциальное средство нарушения информационной безопасности.

Анализ существующих информационных систем показывает, что при реализации элементов пользовательского интерфейса часто нарушаются основные принципы человеко-ориентированного подхода, допускаются логические ошибки в сценариях поведения пользователей, не учитываются их психологические особенности и когнитивные способности, что приводит к увеличению количества атак на человеко-компьютерные интерфейсы.

Современные исследования новых развивающихся типов интерфейсов (сенсорные экраны и виртуальная реальность) в большей степени связаны с эргономикой, чем с информационной безопасностью. 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. В связи с этим проблема обеспечения безопасности взаимодействия с интерфейсами является важной, а задача разработки методики оценивания защищенности человеко-компьютерных интерфейсов, решаемая в рамках представленной диссертационной работы является актуальной.

2. СТЕПЕНЬ ОБОСНОВАННОСТИ НАУЧНЫХ ПОЛОЖЕНИЙ, ВЫВОДОВ И РЕКОМЕНДАЦИЙ, СФОРМУЛИРОВАННЫХ В ДИССЕРТАЦИИ

Автором диссертационного исследования был проведен анализ существующих подходов к оцениванию защищенности человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, что позволило выявить отсутствие комплексных решений, нацеленных на расчет степени защищенности человеко-компьютерных интерфейсов.

Обоснованность результатов проведенного исследования подтверждается тем, что полученные результаты обсуждались на различных научно-технических и научно-практических конференциях всероссийского и международного уровня. Основные результаты диссертации были опубликованы в 26 печатных работах (9 статей и 17 тезисов докладов на конференциях), в том числе на английском языке. Автором были опубликованы 5 статей в научных изданиях из перечня ВАК на соискание ученой степени доктора и кандидата наук («Вопросы кибербезопасности», «Информатизация и связь») и получено 9 свидетельств о государственной регистрации программ для ЭВМ.

3. ДОСТОВЕРНОСТЬ И НОВИЗНА НАУЧНЫХ ПОЛОЖЕНИЙ, ВЫВОДОВ И РЕКОМЕНДАЦИЙ

К основным научным результатам, определяющим новизну и значимость представленной диссертационной работы, можно отнести следующие достижения:

- Модель уязвимостей человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, которая позволяет определить насколько уязвим тот или иной элемент интерфейса, а также выявить возможность злоумышленника атаковать данный элемент интерфейса. Модель уязвимостей человеко-компьютерных интерфейсов отличается от существующих моделей тем, что она учитывает параметры безопасности, характерные для человеко-компьютерных интерфейсов, такие как канал восприятия и урон наносимый оператору. Использование мировых стандартов спецификации уязвимостей и параметров безопасности в качестве основы при разработке этой модели позволяет при оценивании защищённости интерфейса интегрировать разработанную модель

с существующими системами оценивания защищённости хоста.

- Алгоритм расчёта уровня критичности каждой уязвимости и общего уровня защищённости человеко-компьютерного интерфейса. Новизной данного алгоритма являются новые правила расчёта оценки уязвимости, позволяющие учесть характеристики участников обмена информацией в человеко-компьютерных интерфейсах.
- Методика оценивания защищенности человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности, в основе которой лежат разработанные модели и алгоритмы. Основным отличием данной методики от ближайших аналогов является комплексное применение предложенных моделей и алгоритмов как на этапе разработки, так и на этапе эксплуатации интерфейсов, а также возможность оценки степени удобства использования интерфейса, что в совокупности обеспечивает оптимизацию показателей защищённости интерфейса;
- Архитектура и программный прототип системы, автоматизирующий предложенную методику. Данный прототип может быть использован в качестве элемента перспективной системы оценки защищённости человеко-компьютерных интерфейсов в частности и компьютерных сетей в целом.

Достоверность результатов работы подтверждается результатами экспериментальными исследований.

4. ПРАКТИЧЕСКАЯ ЗНАЧИМОСТЬ ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ

В рамках диссертационной работы были разработаны модель, алгоритм и методика, в совокупности представляющие систему оценивания значений показателей защищенности человеко-компьютерных интерфейсов, основанных на технологиях сенсорных экранов и виртуальной реальности. Такая система позволяет повысить осведомленность оператора или разработчика об уровне защищённости используемого или разрабатываемого интерфейса, что предполагает возможность ее использования как на этапе проектирования, так и на этапе эксплуатации. На основе предложенных модели, алгоритма и методики разработан программный прототип оценивания защищённости человеко-компьютерных интерфейсов.

Высокая практическая значимость результатов диссертационной работы подтверждается их успешным внедрением в ряде научных и коммерческих проектов. Также представленные результаты могут быть использованы в высших учебных заведениях при подготовке специалистов по информационной безопасности.

5. ЗАМЕЧАНИЯ К ДИССЕРТАЦИОННОЙ РАБОТЕ

Несмотря на все вышеперечисленные достоинства, представленная диссертационная работа не лишена и некоторых недостатков:

- требует уточнения степень применимости представленных результатов к различным интерфейсам, поскольку на стр. 16,17 указывается, что речь идёт

о «приложениях информационной и компьютерной безопасности,…одним из основных инструментов …которых является визуальная аналитика»;

- не приведено обоснование значений выбранных критериев оценки защищенности человеко-компьютерных интерфейсов;
- при перечислении используемых в работе подходов и методов исследования, в большей степени, приведены не сами методы, а предметные области, затрагиваемые в работе: «методы и подходы к визуализации больших объемов многомерных данных; методы и подходы к анализу гетерогенных данных; методы и подходы контроля и управления доступом; методы и подходы обнаружения и предотвращения утечек информации; ……» и т.д.;
- при анонсировании рассмотрения уязвимостей для каждой категории полученной модели, автор, на самом деле, анализирует не уязвимости, а угрозы(п.п. 1.3.1, 1.3.2);
- в предложенной модели уязвимостей (во второй главе диссертационной работы) в явном виде не указаны конкретные формы компьютерных атак, реализующих потенциальные угрозы путем использования выявленных уязвимостей, и не учитывается время, которое потребуется на эксплуатацию уязвимости;
- при формулировке второго результата утверждается, что « разработан оригинальный алгоритм оценивания защищённости человеко-компьютерных интерфейсов,….обеспечивающий повышение показателей защищённости по сравнению с предложенными ранее алгоритмами», при этом не уточняется: о каких показателях идет речь(поскольку не все из них требуют максимизации);
- при рассмотрении одного из базовых показателей уязвимостей – «Сложность эксплуатации уязвимости – Complexity (C)», приводится спорное утверждение, что «Данный параметр не зависит от злоумышленника»(стр.66);
- некорректное использование термина «подопытные» при обозначении участников эксперимента(стр.90).

Указанные замечания не снижают научной ценности работы и не влияют на общую положительную оценку диссертации.

ВЫВОДЫ

1. Диссертационная работа Жерновой Ксении Николаевны представляет собой законченное научное исследование, содержащее решение актуальной научной задачи разработки подхода, позволяющего оценивать уровень защищенности человеко-компьютерных интерфейсов. Была сформулирована и решена научно-техническая задача повышения защищённости человеко-компьютерных интерфейсов.

2. Содержание автореферата полностью соответствует тексту диссертационной работы.

3. Диссертационная работа Жерновой Ксении Николаевны «Оценивание защищённости человеко-компьютерных интерфейсов, основанных на

технологиях сенсорных экранов и виртуальной реальности» полностью соответствует 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.

4. Жернова К. Н. заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Доктор технических наук, профессор, профессор кафедры специальных информационных технологий ФГКОУ ВО Санкт-Петербургского университета Министерства внутренних дел Российской Федерации

Синещук Юрий Иванович

«28» ноября 2022 года

Рабочий адрес: 198206, Санкт-Петербург, ул. Лётчика Пилютова, дом 1
Тел.: +7 911 213 81 84
E-mail: sinegal53@mail.ru