В диссертационный совет Д212.052.02
ФГБОУ ВО «Дагестанский государственный технический университет»

ОТЗЫВ

официального оппонента доктора технических наук, профессора, заведующего кафедрой информационно-аналитических систем безопасности Института компьютерных технологий и информационной безопасности Инженерно-технологической академии федерального государственного автономного образовательного учреждения «Южный федеральный университет» Целых Александра Николаевича на диссертацию Шувалова Ильи Александровича «Разработка и реализация имитационных и аналитических моделей для исследования актуальных угроз безопасности сложных информационных систем обработки персональных данных», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.18 – «Математическое моделирование, численные методы и комплексы программ»

На отзыв были представлены следующие материалы:

– текст диссертационной работы в объеме 136 страниц машинописного текста;
– автореферат объемом 22 страницы;
– оттиски публикаций соискателя в количестве 8.

1. АКТУАЛЬНОСТЬ ТЕМЫ ИССЛЕДОВАНИЯ

Диссертационная работа И.А. Шувалова посвящена изучению воздействия угроз безопасности на информационные системы с целью выявления среди них таких угроз, защита от которых является недостаточной и нуждается в обновлении. Автором предложено исследовать поведение информационных систем при воздействии на них потока угроз безопасности информации путем построения имитационных моделей их функционирования.

Также И.А. Шуваловым в рамках диссертационной работы предложено прибегнуть к методу экспертных оценок для получения первоначальных

данных, необходимых при построении имитационных моделей. Метод экспертных оценок является популярным при необходимости получения данных различного характера, однако оригинальным является предложение привлечения нескольких групп экспертов для более детального изучения поставленной задачи. Причем одна из групп, состоящая из наиболее компетентных специалистов, является головной и обобщает предложенные варианты. Данный подход позволяет повысить достоверность данных, но, в то же время, требует привлечения большого количества специалистов, что может себе позволить далеко не каждая организация.

Реализацию имитационной модели функционирования информационной системы автором предлагается осуществлять с применением полученных первоначальных данных. Следует отметить, что основной отличительной особенностью предложенной модели является то, что в ней учтены как вероятности наступления угроз, так и вероятности их реализации при разных уровнях защиты. Предусмотренная возможность одновременного рассмотрения всех уровней защиты сразу позволяет провести более детальный анализ поведения информационной системы.

При этом отличительной особенностью предложенной имитационной модели является предусмотренная автором возможность разбиения сложной системы на сегменты для их детального изучения и, в последующем, получения данных по всей информационной системе в целом.

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

Достоверность результатов подтверждается следующими фактами:

– предложенная имитационная модель и методика получения первоначальных данных использованы для изучения информационной системы, применяемой для обработки персональных данных в подразделениях ГИБДД Краснодарского края, о чем свидетельствуют акты использования результатов диссертационной работы.

– результаты диссертационной работы успешно апробированы на всероссийских конференциях по проблемам развития сектора IT-технологий.

– автору выданы свидетельства о государственной регистрации программ для ЭВМ, позволяющих автоматизировать процессы проведения экспериментов с моделями и обработки полученных сведений.

К **научной новизне** можно отнести предложенный автором метод определения перечня угроз безопасности, которые могут воздействовать на информационную систему, и, в месте с ним, метод получения первоначальных данных, необходимых для построения моделей. Привлечение экспертов позволяет определить перечень возможных угроз, которые могут воздействовать на информационную систему, что, в свою очередь, позволяет применять предложенную модель для выявления актуальных угроз безопасности данных, обрабатываемых в любой информационной системе. Данный факт свидетельствует об универсальности предложенной имитационной модели.

3. ПРАКТИЧЕСКОЕ ЗНАЧЕНИЕ РЕЗУЛЬТАТОВ РАБОТЫ

Практическая значимость выполненной работы заключается в следующем:

– предложена методика определения первоначальных данных, необходимых для построения имитационных моделей, описывающих функционирование информационных систем.

– разработана имитационная модель информационной системы, позволяющая изучить воздействие угроз безопасности на функционирование системы, выделяя при этом участи (сегменты), на которых передаваемая или принимаемая информация наиболее уязвима, при этом предложенную модель можно использовать для изучения любой информационной системы;

– предложена методика определения необходимости и целесообразности внедрения дополнительных мер защиты информации;

– разработаны программные продукты, позволяющие автоматизировать процесс обработки результатов, полученных с применением имитационной модели.

По материалам исследования опубликовано 8 работ, в том числе 4 статьи в рецензируемых журналах и изданиях, рекомендованных ВАК РФ, а также получено 4 свидетельства о государственной регистрации программ для ЭВМ.

В ходе рецензирования работы установлено, что в представленных оттисках публикаций в достаточной мере освещены основные научные результаты работы соискателя.

Теоретические положения рассмотренной диссертационной работы и результаты проведенного исследования использованы для определения актуальных угроз безопасности информационной системы обработки и

хранения персональных данных, используемой в служебной деятельности сотрудниками подразделений ГИБДД Краснодарского края, что подтверждается соответствующими актами.

4. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Диссертационная работа общим объемом 136 страниц машинописного текста, включая 47 таблиц, 36 рисунков и список литературы из 120 наименований, состоит из введения, четырех глав, заключения, списка сокращений и условных обозначений.

В первой главе автором рассмотрены проблемы изучения угроз безопасности персональных данных, воздействующих на информационные системы, предложена методика получения исходных данных, основанная на методе экспертных оценок и приведен пример ее применения. Также в первой главе предложена блок-схема алгоритма реализации имитационной модели информационной системы.

Во второй главе приводится подробное описание процесса реализации предложенной имитационной модели. Предложенная имитационная модель предполагает рассматривать процесс функционирования информационной системы с точки зрения прохождения запроса по каналам связи от оператора к серверу обработки баз данных и обратно. Причем изначально предложено информационную систему рассматривать посегментно, выделив типовые участки прохождения сигнала и перечень угроз, которые могут воздействовать на информационную систему на данных участках. Реализация имитационной модели описана на примере ее фактического применения для изучения воздействия угроз на информационную систему, используемую для обработки информации подразделений ГИБДД Краснодарского края.

В третей главе приводится методика анализа воздействия угроз безопасности информации на информационную систему в целом, основываясь на результаты, полученные в ходе экспериментов с имитационными моделями сегментов информационной системы. Приведен пример практической реализация предложенной методики при определении актуальных угроз безопасности информационной системы. Также в третей главе на основании полученных ранее данных предложена методика определения необходимости и целесообразности внедрения дополнительных мер защиты информации.

В четвертой главе предложены аналитические модели определения актуальных угроз безопасности информационных систем. При построении моделей автором предложено рассматривать процесс функционирования

информационной системы в качестве Марковской цепи. Данный подход позволяет рассматривать информационную систему абстрагируясь от большого количества факторов, влияющих на ее работоспособность. Вместе с тем, при использовании предложенной модели для рассмотрения влияния большого количества угроз на информационную систему модель сильно усложняется и требует высоких трудозатрат для проведения расчетов. Данный недостаток скорее показывает превосходство удобства использования предложенной имитационной модели перед математической при изучении информационной системы.

5. ЗАМЕЧАНИЯ ПО РАБОТЕ

1. В работе недостаточно полно представлен сравнительный анализ предложенных моделей (имитационной и математической), и результатов их применения.
2. В первой главе отсутствует сравнение методов получения первоначальных данных, необходимых для построения моделей.
3. Следовало бы более подробно описать предложенную методику определения первоначальных данных и примеры их практической реализации.
4. Большинство представленных в работе таблиц содержат большой объем информации, в связи с чем их тяжело читать. Было бы целесообразно разбить их на несколько таблиц с меньшим объемом информации.

6. ОБЩЕЕ ЗАКЛЮЧЕНИЕ

Замечания по диссертационной работе в основном имеют характер пожеланий и не влияют на положительную оценку результатов работы.

Представленная на отзыв диссертационная работа характеризуется полнотой изложения, а название работы полностью соответствует ее содержанию. Автореферат в целом отражает содержание диссертационной работы и позволяет сделать вывод о качестве проведенных исследований и полученных новых научных результатов.

Диссертация И.А. Шувалова является научной квалифицированной работой, которая по своему содержанию и значимости соответствует требованиям, изложенным в п.9 «Положения о присуждении ученых степеней» ВАК РФ, предъявляемым к кандидатским диссертациям. Они не являются принципиальными и не снижают ценности полученных в работе результатов.

Считаю, что автор представленной диссертации, И.А. Шувалов, заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.18 – «Математическое моделирование, численные методы и комплексы программ».

Официальный оппонент:
Доктор технических наук, профессор
Федеральное государственное автономное
образовательное учреждение
«Южный федеральный университет»,
Инженерно- технологическая академия,
Институт компьютерных технологий
и информационной безопасности,
кафедра информационно-аналитических
систем безопасности
заведующий кафедрой А.Н. Целых

Александр Николаевич Целых
Доктор технических наук (специальность 05.13.18), профессор заведующий кафедрой информационно-аналитических систем безопасности Института компьютерных технологий и информационной безопасности Инженерно-технологической академии федерального государственного автономного образовательного учреждения «Южный федеральный университет»
Адрес: 347900, г. Таганрог, Ростовской области, пер. Некрасовский, 44
Тел.: 8 (8634) 360-450
E-mail: inf@tgn.sfedu.ru

Федеральное государственное автономное образовательное учреждение высшего образования «ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Личную подпись А.Н. Целых
ЗАВЕРЯЮ:
Ведущий специалист по работе с персоналом
30 08 2017 г.