ОТЗЫВ

на автореферат диссертации Новохрестова А.К.
«Модель угроз информационной безопасности программного обеспечения компьютерных сетей на основе атрибутивных метаграфов»,
представленной на соискание ученой степени кандидата технических наук.
Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Выбранная диссертантом тема «Модель угроз информационной безопасности программного обеспечения компьютерных сетей на основе атрибутивных метаграфов» представляет интерес для всех специалистов, изучающих методы построения моделей угроз безопасности компьютерных сетей. Новая методика составления перечня угроз, с использованием рассмотренных в работе модели компьютерной сети и модели угроз компьютерной сети, позволяют обнаружить большее количество угроз, чем традиционные методики, в связи с чем актуальность работы не вызывает сомнений.

В первой главе автором изучены и критически анализируются известные методики и теоретические положения других авторов по существующим подходам к построению моделей компьютерных сетей, которые применяются для идентификации угроз и оценки защищенности. Кроме того, производится обзор существующих методов идентификации угроз и построения моделей угроз компьютерных сетей.

На основании выводов по первой главе, где был выделены несколько недостатков существующих методик построения моделей угроз компьютерных сетей: отсутствие описания угроз информационной системе в явном виде, отсутствие строгой формализации и математической модели, во второй главе автор предлагает новую модель компьютерной сети и модель угроз информационной безопасности компьютерной сети.

Модель компьютерной сети на основе атрибутивных метаграфов позволяет описывать компоненты программного обеспечения компьютерных сетей и все возможные связи между ними. Предлагаемый подход к классификации угроз и разработанная модель угроз основаны на элементарных операциях над метаграфами. Разработанная автором модель угроз позволяет составлять полные перечни угроз целостности и конфиденциальности компьютерных сетей.

Рассмотренные во второй главе модели были использованы для разработки методики составления перечня угроз информационной безопасности компьютерных сетей. Основным преимуществом данной методики можно считать воспроизводимость, так как она устраняет зависимость получаемого результата от квалификации эксперта. Методика отличается от аналогов использованием матрицы взаимосвязей между элементами и позволяющая увеличить количество идентифицируемых угроз при формировании моделей угроз компьютерных сетей.

Третья глава посвящена сравнению разработанной модели угроз с наиболее полным аналогом, существующим на данный момент – банком данных угроз ФСТЭК России, а также апробации методики составления перечня угроз и моделей на реальном объекте – разрабатываемой автоматизированной системе коммерческого учета энергоресурсов.

Для подтверждения теоретических положений в третьей главе автором были проведены исследования и сравнение полученной модели угроз с банком данных угроз ФСТЭК России. По результатам сравнения установлено, что предложенный подход к построению модели угроз позволяет специалистам по защите информации учесть при построении системы защиты информации на 11 типов угроз информационной безопасности системы больше, чем использование банка данных угроз ФСТЭК России.

В качестве замечаний необходимо отметить следующее:

1. На стр. 12 автореферата утверждается, что модель позволяет составлять полный перечень угроз целостности и конфиденциальности КС. Не ясно, на чем основано такое утверждение и как автор оценивает полноту.
2. Желательно уточнить, какими классами угроз ограничивается автор. Так, на стр. 10 (абзац 3) определено: «под угрозами понимается несанкционированное изменение структуры КС», а ниже: «таким образом, рассматриваются угрозы целостности и конфиденциальности программного обеспечения КС».
3. Базовые операции над атрибутивными метаграфами автор ограничивает изменениями структуры. Как при этом учитывается угроза нарушения целостности ПО? В формуле (1) присутствует только удаляемое ПО, которое, возможно, только модифицируется.

4. Неясно, возможно ли распространить предлагаемый подход на сети с гибкой архитектурой (программно-конфигурируемые сети)
5. Полученная модель опробована только по данным банка ФСТЭК. Есть ли возможность сравнения с другими данными?

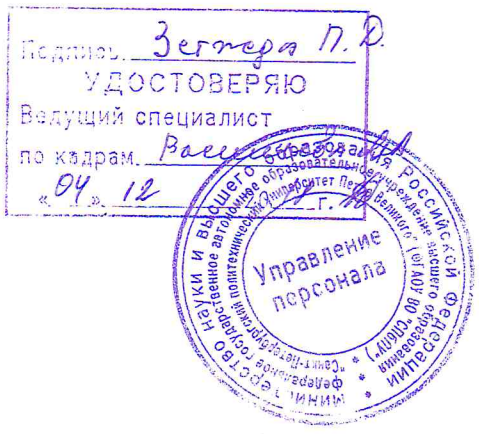
Представленные замечания не носят принципиального характера, связаны со сложностью проблемы, и не снижают общей положительной оценки работы, выполненной на хорошем теоретическом уровне и имеющей практическое занижение для организаций осуществляющих аттестацию КС.

Насколько можно судить по автореферату, представленная работа является законченным научно-квалификационным исследованием на актуальную тему, содержит научные и практические результаты, представляющие интерес для специалистов. Работа удовлетворяет требованиям ВАК, предъявляемым к кандидатским диссертациям, тема исследования соответствует п.п. 3 и 15 паспорта специальности.

Автор работы Новохрестов А.К. заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Профессор кафедры ИБКС
ИПММ ФГАОУ ВО «СПбПУ»
д.т.н., профессор, засл. деятель науки РФ

Петр Дмитриевич
Зегжда
« 04 » декабря 2018 г.



Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (ФГАОУ ВО «СПбПУ»)
195251, Санкт-Петербург,
ул. Политехническая, д.29
тел. (812) 552-76-32
e-mail kafedra@ibks.spbstu.ru