

ОТЗЫВ

на автореферат диссертации Макаровой Ольги Сергеевны на тему «Разработка методик прогнозирования динамики изменения вектора компьютерной атаки с точки зрения нарушителя», представленной на соискание учёной степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Одна из актуальных современных проблем информационной безопасности (ИБ) связана с отсутствием единого подхода к прогнозированию компьютерных атак. Данная ситуация подтверждается как международными («Отчет Всемирного экономического форума по глобальным рискам»), так и российскими экспертами (Паспорт федерального проекта «Информационная безопасность»), а также результатами соревнований по кибербезопасности между командами атакующих, защитников и специалистов в области мониторинга ИБ (например, PHDays), в которых в большинстве случаев победу одерживают атакующие. В этой связи необходимо уметь прогнозировать наиболее вероятные векторы компьютерных атак, используемые нарушителями ИБ. В этой связи тема диссертации, посвящённая разработке подходов по оценке угроз ИБ с учётом экономических интересов нарушителя, является актуальной.

В работе получен ряд новых научных результатов, в том числе: разработана и обоснована математическая модель оценки вероятности реализации нарушителем компьютерной атаки и идентификации её параметров; разработана математическая модель (и ее параметры), описывающая динамику возможности реализации нарушителем компьютерной атаки во времени, получены оценки параметров данной модели и подтверждена ее адекватность результаты натурного моделирования с помощью программно-аппаратного комплекса «Ampire» и статистическими данными из открытых источников о более чем 700 тысяч компьютерных атак различного типа на организации; разработана методика прогнозирования динамики векторов компьютерной атаки с точки зрения нарушителя.

Обоснованность и достоверность научных результатов исследования достигнута благодаря корректной постановке задачи и целей исследования, подтверждена апробацией результатов на пяти международных научных конференциях. По теме диссертации опубликовано десять работ в периодических и научных журналах, в том числе в изданиях, рекомендованных ВАК РФ и Аттестационным советом УрФУ для публикации результатов диссертационных исследований.

Вместе с этим имеют место следующие замечания и вопросы по содержанию автореферата:

1. В автореферате не обнаружено определение вектора компьютерной атаки.
2. Согласно теории диффузии инноваций (стр.10), информация о новых методах компьютерных атак распространяется не только среди нарушителей, но и среди операторов атакуемых систем. Как это учитывается в моделях, представленных в п.1. и п.2 автореферата?

Сделанные замечания носят дискуссионный характер и не снижают научной ценности рецензируемой по автореферату работы.

Представленная работа на тему: «Разработка методики прогнозирования динамики изменения вектора компьютерной атаки с точки зрения нарушителя» изложена грамотным языком и соответствует требованиям п. 9 Положения о присуждении учёных степеней в УрФУ, предъявляемым к кандидатским диссертациям. Автор диссертации Макарова Ольга Сергеевна заслуживает присуждения ей учёной степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Заведующий кафедрой «Защита информации» Высшей школы электроники и компьютерных наук ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)»,
кандидат технических наук, доцент

Адрес: 454080, г. Челябинск, проспект Ленина, д. 87, ауд. 907, 911/3бв

Тел: +7 (351) 267-93-55

E-mail: sokolovan@susu.ru

Соколов Александр Николаевич

08.12.2021

