ОТЗЫВ на автореферат диссертации
КРИБЕЛЯ АЛЕКСАНДРА МИХАЙЛОВИЧА
на тему «Выявление аномалий и классификация компьютерных атак в сети передачи данных на основе применения фрактального анализа и методов машинного обучения», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Современный этап развития общества характеризуется повышением роли информационной сферы, представляющей собой совокупность информации и информационных технологий, что позволило осуществлять сбор, формирование, хранение, обработку и распространение информации в таких объемах и с такой оперативностью, которые были немыслимы ранее.

Именно новые технологии привели к бурному распространению сетей передачи данных (СПД), открывающих принципиально новые возможности международного информационного обмена. Происходит интеграция и конвергенция сетей и служб. Это обеспечивает доступ пользователей к любой услуге, имеющейся во множестве сетей, за счет гибких возможностей по их обработке и управлению.

Несмотря на удобство, экономическую выгоду и эффективность использования СПД, темпы, с которыми развивается современная сфера информационных технологий, подвергают мировое сообщество целому ряду беспрецедентных угроз и факторов уязвимости, которые злоумышленнику открывают возможность реализации компьютерных атак (КА).

Несмотря на то, что киберугрозы отличаются от физических угроз по своей природе, конечный результат может быть одинаково необратимым.

Таким образом, для обоснования направлений защиты необходимо адекватно оценить возможности потенциального злоумышленника по воздействию на СПД, то есть, задача разработки алгоритмов и методов повышения эффективности выявления аномалий и классификации КА в сетевом трафике СПД является на сегодняшний день весьма актуальной.

Автореферат диссертации свидетельствует о том, что автором, который опирался на проведенный анализ, сформулированы противоречия в теории и практике противодействия КА, сформулированы новые научные подходы к вопросам повышения уровня защищенности СПД в условиях тенденции стремительного развития средств и методов КА.

Достоверность, актуальность и обоснованность полученных

Крибелем А.М. научных результатов и выводов основываются на глубоком анализе проводимых ранее научно-исследовательских работ в предметной области (как отечественными, так и ведущими зарубежными учеными), верной постановкой задач исследования и использовании уже известного многократно апробированного научно-методического аппарата. Результаты исследования подтверждены необходимым количеством практических экспериментов, а также верификацией известных теоретических данных.

Теоретическая значимость результатов диссертации определена тем, что разработанные научно-методические положения позволяют определять ранние этапы КА, прогнозировать этапы вскрытия сети, тем самым научно обосновывая пути повышения защищенности СПД за счет ранних мер противодействия.

Практическая значимость работы определяется тем, что разработанные научно-технические предложения, доведенные до реализации в виде программного комплекса, позволяют за счет раннего обнаружения КА и алгоритма противодействия повысить защищенность СПД. Разработанный программный комплекс, на который получено свидетельство о государственной регистрации программ для ЭВМ, может быть использован соответствующими должностными лицами при организации информационной безопасности, а также при разработке перспективных средств и телекоммуникационных комплексов.

Однако, хотелось бы отметить, что, несмотря на положительное впечатление о диссертации Крибеля А.М., в качестве замечаний выделим:

1. Модель угроз недостаточно конкретизирована: каким образом определен злоумышленник и сформулированы его возможности в отношении СПД.

2. В четвертом разделе работы, посвященном описанию разработанных научно-технических предложений, автором не поясняется, как происходит классификация аномалий, то есть не охарактеризован критерий «аномальности» всплесков трафика в СПД.

Несмотря на указанные недостатки, диссертация Крибеля А.М. является завершенной научно-квалификационной работой. Из автореферата объективно ясно, что работа отличается актуальностью, характеризуется полнотой проведенных исследований, в которых решена новая научная задача, имеющая ключевое значение для защиты страны в вопросах обеспечения информационной безопасности. Автореферат написан

технически-грамотным языком, материал изложен в меру лаконично, логично структурирован.

Работа отвечает пп. 9, 10, 11 и 14 требований «Положения о присуждении ученых степеней», а ее автор заслуживает присуждения ему ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Профессор кафедры радиофизики и электроники ФГБОУ ВО «Челябинский государственный университет», Доктор физико-математических наук (специальность 1.3.8. (01.04.07) Физика конденсированного состояния), доцент	**Загребин Михаил Александрович**

Почтовый адрес 454001, г. Челябинск, ул. Братьев Кашириных, 129.
Тел. (351) 799-71-19, e-mail zagrebinm.a.@csu.ru

Доцент кафедры радиофизики и электроники ФГБОУ ВО «Челябинский государственный университет», Кандидат физико-математических наук (специальность 01.04.02 – Теоретическая физика)	**Анзулевич Антон Петрович**

Почтовый адрес 454001, г. Челябинск, ул. Братьев Кашириных, 129.
Тел. (351) 799-71-81, e-mail anzul@list.ru

18.04.2023