ОТЗЫВ

на диссертационную работу
ЖУМАНГАЛИЕВОЙ НАЗЫМ КЕНЖЕГАЛИЕВНЫ
"Технология контроля аномальности состояния параметров
для систем обнаружения вторжений",
представленную на соискание ученой степени доктора философии (PhD)
по специальности 6D070400 – Вычислительная техника и
программное обеспечение

Диссертационная работа направлена на решение важной научно-технической задачи усовершенствования систем обнаружения вторжений, функционирующих по принципу обнаружения аномалий.

Использование современных компьютерных технологий во всех сферах деятельности общества позволило осуществлять автоматизированную обработку больших объемов данных. Сплошная компьютеризация общества предоставила возможность работать с информацией широкому кругу пользователей. Но вместе с этим увеличилась возможность несанкционированного доступа к различным компьютерным ресурсам. Такое положение негативно влияет на состояние безопасности ресурсов информационных систем вследствие возникновения новых видов угроз что приводит к порождению новых кибератак.

Поэтому одной из важных научных проблем в области информационной защиты на сегодняшний день является направление, связанное с идентификацией кибератак на ресурсы компьютерных систем. Одним из распространенных решений этой проблемы является системы обнаружения вторжений, направлены прежде всего на выявление фактов несанкционированного доступа через компьютерные сети. Сетевые системы обнаружения вторжений (которые могут базироваться как на программных, так и на аппаратно-программных средствах) в зависимости от применяемого метода анализа событий можно разделить на два общих класса: те, что используют сигнатуры, и те, которые выявляют аномалии, порожденные атакующими действиями.

Главным преимуществом систем, которые выявляют аномалии, является способность обнаруживать новые, неизвестные ранее типы вторжений, а также прогнозировать и блокировать кибератаки на ранних стадиях (этапах разведки). К недостаткам систем на базе выявления аномального состояния относится, в частности, потребность в сложных и длительных подготовительных процедурах, связанных с получением статистических данных и реализацией процесса обучения системы. Устранить эти недостатки способны подходы, основанные на использовании опыта экспертов, но при реализации таких решений необходимо обрабатывать данные, которые подаются в нечеткой (лингвистической) форме.

Формализовать такую информацию и провести ее обработку позволяет теория нечетких множеств. Поэтому разработка моделей, методов и систем обнаружения вторжений в нечетких условиях аномалий, порожденных атакующими действиями злоумышленника, является важной научной задачей.

В этой связи тема диссертационной работы Жумангалиевой Н.К. является актуальной, а решение вопросов и задач, что в ней сформулированы, имеет теоретическое и прикладное значение для разработки средств защиты информации в компьютерных системах и сетях.

Результаты, полученные в диссертационной работе, могут быть использованы при создании технических решений в виде программных или программно-аппаратных модулей для обнаружения аномалий и применяться автономно или в качестве расширителя функциональности современных систем обнаружения вторжений, а также внедрены в деятельность Национального авиационного университета (Украина, Киев) и ООО "Сайфер БІС" (Украина, Киев).

Диссертация соответствует специальности специальности 6D070400 – Вычислительная техника и программное обеспечение, основные научные положения диссертации достаточно полно изложены в публикациях и автореферате. По диссертационной работе опубликовано 12 научных трудов, среди которых статьи в изданиях, рекомендованных Комитетом по контролю в сфере образования и науки МОН РК, статьи в изданиях, индексируемых базой Scopus, статьи в научных журналах и сборниках научных трудов (Украина), а также статьи в сборниках международных конференций (Казахстан, Украина, Южная Корея). Основные положения диссертационной работы докладывались и обсуждались на научных конференциях и семинарах (Казахстан, Украина).

В целом диссертационная работа является завершенной научной работой, которая нацелена на решение актуальной научной задачи, соответствует требованиям к кандидатским диссертациям по специальности 6D070400 – Вычислительная техника и программное обеспечение, а ее автор, Жумангалиева Назым Кенжегалиевна, заслуживает присуждения ученой степени доктора философии (PhD).

Зарубежный консультант,
заведующий кафедрой безопасности
информационных технологий
Национального авиационного
университета (Украина),
доктор технических наук, профессор Корченко А.Г.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ * м. КИЇВ * ідентифікаційний код 01132339

Корченко А.Г.
Підпис засвідчую
Вчений секретар
Національного авіаційного університету
Г. Сичев