АННОТАЦИЯ

диссертационной работы докторанта PhD специальности 6D070400 – «Вычислительная техника и программное обеспечение» Бекетовой Г.С. на тему «Модели и методы интеллектуального распознавания киберугроз в критически важных компьютерных системах»

Актуальность темы исследования. Повсеместное применение компьютерных систем и информационно-коммуникационных технологий способствует повышению производительности труда, снижению материально-сырьевых затрат и улучшению качества продукции и уровня жизни. Компьютерные системы и ИТ играют ключевую роль в развертывании, эксплуатации и техническом обслуживании критически важных инфраструктур, ответственных за своевременную доставку потребителям энергоресурсов, воды, продуктов питания, предоставление транспортных услуг и связи. Важнейшим элементом таких критически важных инфраструктур являются компьютеризированные системы, нарушение работы которых может привести к серьезным или даже взрывоопасным социальным и экономическим последствиям в масштабах государства или отдельного региона, что обуславливается сильной системной взаимосвязью между различными компонентами критически важных компьютерных систем (КВКС) и комплексами жизнеобеспечения. Чтобы гарантировать высокую работоспособность, надежность и безопасность КВКС, необходимо превентивно решать проблемы, связанные с их информационной безопасностью (ИБ) и киберзащитой.

Активное расширение сфер применения КВКС, особенно в сегменте мобильных, распределенных и беспроводных информационных технологий, сопровождается возникновением новых угроз для ИБ, о чем свидетельствует стремительный рост числа инцидентов, связанных с ИБ и киберзащитой КВКС, а также выявленных уязвимостей в их программном обеспечении (ПО). Угрозы вполне реальны, поскольку преступники могут получить возможность перехватывать пароли, отдельные файлы, геолокационную информацию, транслировать аудио- и видеоданные, контролировать Wi-Fi сети, веб-камеры, информационные табло и т.п. О серьезности проблемы можно судить хотя бы по неоднократно имевшим место фактам, когда один или несколько злоумышленников, получив доступ к данным КВКС, за незначительное время смогли полностью парализовать работу крупных предприятий или компаний.

Таким образом, актуальность исследований, направленных на дальнейшее развитие моделей и методов защиты на основе интеллектуального распознавания угроз КВКС и обеспечения их ИБ, является одной из ключевых проблем киберзащиты критической инфраструктуры государства.

Цель и задачи исследования. Целью диссертационной работы является развитие моделей и методов защиты критически важных компьютерных систем на основе интеллектуального распознавания киберугроз в условиях постоянного увеличения количества дестабилизирующих воздействий на конфиденциальность, целостность и доступность информации.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Разработать метод интеллектуального распознавания угроз, аномалий и кибератак, позволяющий обеспечить кибербезопасность КВКС на основе применения инновационных интеллектуальных систем киберзащиты для повышения устойчивости КВКС к кибератакам.

2. Разработать модель интеллектуального распознавания с использованием логических процедур выявления аномалий и кибератак, базирующуюся на покрытиях матриц признаков (МП) и понятии элементарного классификатора (ЭК).

3. Минимизировать количество обучающих выборок для признаков, расположенных в репозитории интеллектуальной системы распознавания угроз, аномалий и кибератак.

4. Усовершенствовать модели определения структурно-технологического резерва программного и информационного обеспечения КВКС с учетом критичности их модулей для повышения уровня ИБ, а также модель, позволяющую выбрать рациональный состав системы защиты информации (СЗИ) с учетом ее влияния на функциональные параметры КВКС.

5. Выполнить имитационное моделирование основных компонентов КВКС и подсистемы киберзащиты, основанной на предложенных моделях интеллектуального распознавания угроз, аномалий и кибератак в КВКС.

Объект исследования – процессы интеллектуального распознавания киберугроз для КВКС.

Предмет исследования – методы и модели защиты критически важных компьютерных систем.

Методы исследования. В ходе исследования, учитывая особенности предметной области и сформулированные задачи, использовались: булевая алгебра и теория нечетких множеств для разработки модели интеллектуального распознавания и выявления аномалий, кибератак и киберугроз; метод дискретной оптимизации – для эффективного решения задач обеспечения киберзащиты КВКС; методы и средства имитационного моделирования для имплементации разработанных моделей; принципы и методы объектно-ориентированного программирования для создания прикладных программных продуктов.

Научная новизна результатов исследований.

1. *Впервые разработаны:*

– метод интеллектуального распознавания киберугроз, базирующийся на определении конъюнкций по покрытиям матриц, содержащих бинарные информативные характеристики признаков для классов угроз, аномалий и кибератак, и отличающийся от существующих применением логических функций и нечетких множеств признаков кибератак, что позволяет создавать эффективные аналитические, схемотехнические и программные решения СЗИ для КВКС;

– модель распознавания и формирования решающего правила для логических процедур идентификации киберугроз и атак, основанная на

процедуре анализа критичности отдельных компонентов КВКС, покрытиях матриц бинарных признаков и понятии элементарного классификатора, и в отличие от существующих, обеспечивающая возможность интеллектуального распознавания с минимальным количеством ошибок, а также учитывать трудно объяснимые признаки аномалий, угроз и кибератак;

2. *Усовершенствованы:*

– оптимизационные модели структурно-технологического и виртуально-восстановительного резервирования, а также программно-информационного обеспечения КВКС, которые отличаются от существующих использованием критерия максимальной вероятности успешного препятствования системы распознавания угроз, аномалий и кибератак действиям атакующей стороны, что позволяет оценить функциональность и устойчивость СЗИ к различным классам кибернападений на этапе проектирования.

3. *Получили дальнейшее развитие:*

– имитационные модели кибератак на элементы КВКС, позволяющие осуществлять выбор рациональных способов препятствования и нейтрализации их последствий, выполнять анализ сложных, комбинированных видов кибернападений на КВКС.

Научные результаты в рамках требований к диссертациям

Во введении раскрыты актуальность, конкретизированы проблемы, связанные с исследуемой проблемой. Приведены идея работы, цели и задачи исследования, научная новизна и практическая ценность работы.

В первом разделе проведен анализ научных трудов, посвященных исследованию кибератак на критически важные компьютерные систем. Рассмотрены наиболее распространенные классы и типы кибератак на КВКС, проведен обзор и анализ их предшествующих исследований, а также выполнены работы в направлении синтеза систем распознавания вторжений на основе интеллектуальных технологий распознавания.

Во втором разделе показано, что применение компонентов интеллектуальной адаптивной защиты информации КВКС может быть основано на использовании логических процедур и понятии элементарного классификатора для аномалий, киберугроз и уязвимостей КВКС. Предложена модель поиска угроз, аномалий и кибератак в КВКС, базирующаяся на построении покрытий классов и элементарных классификаторах. Изложены основные подходы к конструированию логических процедур распознавания угроз (ЛПРУ) с использованием аппарата логических функций, что позволит на практике создавать эффективные аналитические, схемотехнические и программные решения СЗИ для КВКС. Разработана методика составления решающего правила для ЛПРУ, которое позволяет выполнять распознавания угрозы в рамках определенного класса, с минимальным числом ошибок.

В третьем разделе предложены уточнения к моделям, используемым для решения задач оптимизации состава комплексов СЗИ для КВКС. При этом уточнения моделей затрагивают аспект предварительной декомпозиции СЗИ для КВКС на критичные и некритичные составляющие, для которых предусмотрена процедура резервного копирования. Рассмотрены задачи

оптимизации состава комплексов СЗИ КВКС. Уточнена оптимизационная модель структурно-технологического резерва информационных и программных массивов для КВКС и рассмотрены особенности применения методов дискретной оптимизации для решения задач обеспечения кибербезопасности КВКС.

В четвертом разделе проанализирована возможность написания и подключения собственных модулей в среде MATLAB и Simulink для реализации моделей, описывающих вероятностные состояния системы в ходе реализации атакующей стороной различных сценариев кибератак на КВКС. Разработанные модели в MATLAB и Simulink позволяют на 25–30% уменьшить время отладки проектов системы киберзащиты за счет имитационного моделирования кибератак на модули КВКС.

В заключении отражены основные результаты диссертационной работы и информация о практическом применении результатов исследования.

Апробация результатов исследования

Основные результаты диссертационного исследования докладывались и обсуждались на семинарах кафедры «Компьютерная и программная инженерия» Казахского национального исследовательского технического университета имени К.Сатпаева; семинарах кафедры «Безопасность информационных технологий» Национального авиационного университета Украины; международных Сатпаевских чтениях «Роль и место молодых ученых в реализации новой экономической политики Казахстана» (Алматы, 2015); II Международной научно-практической конференции «Актуальные вопросы обеспечения кибербезопасности и защиты информации», (Киев 2016); Международной научно-практической конференции ITSEC (Киев, 2016); Международной научно-практической конференции «Состояние и совершенствование безопасности информационно-телекоммуникационных систем». SITS-2016 (Украина, 2016); X Международной научно-практической конференции «Современные информационные и коммуникационные технологии на транспорте, в промышленности и образовании», (Днепро, 2016); Международной научно-практической online конференции «Энерго- и ресурсосберегающие технологии: опыты и перспективы» (Кызылорда, 2017); Международной научно-практической конференции «Интеграция науки, образования и производства – основа реализации Плана нации», Сагиновские чтения №9 (Караганда, 2017).

Результаты диссертационного исследования были высоко оценены ТОО Лаборатории Касперского по странам Центральной Азии и Монголии; используются в учебном процессе кафедр «Вычислительная техника и информационные системы» Кызылординского государственного университета имени Коркыт Ата и «Безопасность информационных технологий» Национального авиационного университета Украины; апробированы в ТОО «Сайфер БІС» (Киев) и ТОО «QUARES» (Алматы).

Диссертация выполнена на кафедре «Компьютерная и программная инженерия» Института информационных и телекоммуникационных технологий

Казахского национального исследовательского технического университета имени К.Сатпаева.

Публикации. По теме диссертации опубликовано 21 работа, из которых 8 опубликованы в изданиях, рекомендованных Комитетом по контролю в сфере образования и науки МОН РК, 3 статьи опубликованы в изданиях, входящих в базу данных Scopus, 1 статья опубликована в зарубежном журнале, 9 статей опубликованы в сборниках международных научно-практических конференций.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, библиографического списка и приложений, содержит 135 страниц основного текста (64 рисунка, 14 таблиц). Библиографический список содержит 90 наименования литературы.