АННОТАЦИЯ

диссертационной работы докторанта PhD по специальности
6D070400 – «Вычислительная техника и программное обеспечение»
Жекамбаевой М.Н.
на тему «Методы анализа и оценивания рисков безопасности информационных ресурсов»

Актуальность темы исследования. Стремительное развитие IT-инфраструктуры предприятий влечет за собой неконтролируемый рост количества угроз и уязвимостей информационных ресурсов (ИР). В этих условиях анализ и оценивание рисков является необходимым условием создания системы управления рисками и менеджмента информационной безопасности (ИБ) объекта защиты.

На сегодняшний день существует множество средств анализа и оценивания риска (САОР), начиная нормативными документами (стандартами) и заканчивая конкретными программными приложениями. При их выборе для использования в практической деятельности, эксперт сталкивается с множеством вопросов таких как «Какие использовать параметры?», «Какой математический аппарат применять?», «Как оценить без статистических данных?», «Как провести анализ и оценивание рисков в условиях нечеткости?» и т.д. Эти и другие факторы создают ряд трудностей при выборе соответствующих средств оценивания.

Также следует отметить, что в основном для анализа и оценивания рисков используются статистические данные об инцидентах и угрозах ИБ. Во многих странах, в том числе и в Казахстане, нет соответствующей государственной политики относительно регистрации и применения подобной статистики. Это ограничивает возможности существующих САОР для национального использования. Кроме того, в подобных средствах имеются определенные ограничения на используемый набор параметров, что приводит к снижению их гибкости, то есть не дает возможности их применения для оценивания более широкого спектра величин. Также мало изучены вопросы формирования экспертных оценок, сделанных в нечетко определенной, слабо формализованной среде, с учетом периода времени, отрасли, экономической специфики предприятия и других факторов.

Поэтому необходимо разрабатывать и исследовать методы и средства, позволяющие создавать более гибкие в использовании САОР ИБ как на основе статистических данных, так и на основе экспертных оценок, сделанных в нечетко определенной, слабо формализованной среде, что и определяет ***актуальность темы научного исследования и ее цель.***

Основные задачи исследования:

1. Проанализировать и исследовать базовые понятия, связанные с риском, существующие стандарты, методы, методики, методологии и программные САОР, с целью определения набора базовых характеристик,

используемых для создания и выбора наиболее эффективного инструментария решения соответствующих задач ЗИ;

2. На основе полученных базовых характеристик разработать модель кортежной модели базовых характеристик КМР, позволяющую динамически определять наборы величин и таким образом обеспечить гибкость соответствующих разрабатываемых САОР ИБ;

3. На основе предложенной модели КМР разработать методы анализа и оценивания рисков ИБ, что позволит создавать эффективные средства оценивания, использующие в качестве входных данных динамически изменяемые наборы детерминированных и нечетко определенных базовых характеристик;

4. Разработать методы, которые позволяет эквивалентно переопределять порядок (число термов) лингвистической переменной (ЛП), базирующихся на эталонных параметрических трапециевидных нечетких числах (НЧ) с *n*-кратным инкрементированием при решении задач анализа и оценивания рисков ИБ.

5. С использованием предложенных методов и модели разработать методологию синтеза систем анализа и оценивания рисков ИБ, позволяющую формализовать и обобщить процесс построения как программных, так и программно-аппаратных систем, предназначенных для эффективного оценивания рисков;

6. На основе предложенных методов, модели и методологии разработать новые структурные решения систем в области анализа информационных рисков;

7. На основе предложенной методологии и структурных схем соответствующих систем, разработать программное обеспечение (ПО) САОР и осуществить ее экспериментальное исследование с целью верификации разработанных методов, модели и структурных решений.

Объект исследования – процесс анализа и оценивания рисков информационной безопасности;

Предмет исследования – модели, методы, системы, методики и программные средства анализа и оценивания рисков в сфере информационной безопасности.

Методы исследования. Проведенные исследования базируются на современных методах теории нечеткой логики (разработка методов анализа и оценивания рисков, а также методов *n*-кратного инкрементирования числа терм лингвистических переменных), принятия решений, алгоритмов, объектно-ориентированного программирования (разработка ПО САОР ИБ), имитационного моделирования информационных процессов и структур (моделирование различных условий и среды состояния информационной системы при проведении экспериментального исследования), а также мягких вычислениях.

Научная новизна исследования заключается в следующем:

- *впервые* разработана кортежная модель базовых характеристик риска, которая за счет обобщения базовых характеристик, отображенных шестикомпонентным кортежем, позволяет строить более гибкие и эффективные методы анализа и оценивания рисков, учитывающих возможность формирования требуемого множества наборов характеристик;
- *получили дальнейшее развитие* методы анализа и оценивания рисков, которые за счет кортежной модели базовых характеристик риска и логико-лингвистического подхода в обработке динамически изменяемых наборов детерминированных и нечетко определенных базовых параметров, позволяют создавать эффективные средства оценивания с интегрированными возможностями;
- *впервые* разработаны методы реализации функции n-кратного инкрементирования числа термов с использованием частного расширения базы, в котором за счет модификации n-кратным расширением функции инкрементирования термов на один порядок, расширяется возможность формализации процесса эквивалентного трансформирования числа эталонных термов лингвистической переменной на n порядков без привлечения экспертов соответствующей предметной области;
- *получила дальнейшее развитие* методология синтеза систем анализа и оценивания рисков информационной безопасности, которая позволяет формализовать процесс создания инструментальных средств с гибкими возможностями использования заданных множеств обрабатываемых величин при анализе и оценивании рисков информационной безопасности;
- *получили дальнейшее развитие* структурные решения систем анализа и оценивания рисков информационной безопасности, которые за счет подсистем обработки базовых характеристик и формирования данных, реализующих предложенные методы, позволяют формировать и преобразовывать данные, как в качественной, так и в количественной интерпретации.

Практическая ценность работы заключается в следующем:

- на основе предложенных структурных решений систем и разработанной методологии синтеза, построен алгоритм для реализации программной САОР ИБ;
- разработаны интегрированные базы данных ИР, угроз и событий нарушения ИБ, которые могут быть использованы при построении САОР;
- на основе предложенного алгоритма и интегрированных баз данных, реализована прикладная программная САОР ИБ, использующая и динамически определяющая различные наборы базовых характеристик, что повышает гибкость, функциональность и удобство ее использования, как в детерминированной, так и в нечеткой слабо формализованной среде.

Результаты диссертационного исследования использовались в учебном процессе кафедры «Информационная безопасность» и «Компьютерная и программная инженерия» КазНИТУ имени К.И.Сатпаева, кафедры

«Безопасность информационных технологий» Национального авиационного университета (Украина, г. Киев), а также в ООО «Безопасность информационных систем «ДЕЛЬТА»». (Украина, г. Киев) и ТОО «QUARES» (Алматы).

Апробация результатов диссертации. Основные положения и результаты диссертационной работы докладывались и обсуждались на различных международных конференциях и семинарах, в том числе на:

– семинарах кафедры «Компьютерная и программная инженерия» КазНИТУ имени К.И. Сатпаева;

– научном семинаре «Современные технологии защиты информации» кафедры «Информационная безопасность» КазНИТУ имени К.И.Сатпаева;

– научном семинаре кафедры «Безопасности информационных технологий» Национального авиационного университета (Украина, г. Киев);

– международных Сатпаевских чтениях «Роль и место молодых ученых в реализации «Казахстан-2050», посвященных 80-летию КазНТУ имени К.И.Сатпаева, Алматы, 2014;

– II международной научно-практической конференции «Информационные и телекоммуникационные технологии: образование, наука, практика». – Алматы, КазНИТУ имени К.И. Сатпаева, 2014;

– международном Форуме «Инженерное образование и наука в XXI веке: проблемы и перспективы», посвященного 80-летию КазНТУ имени К.И.Сатпаева, Алматы, 2014;

– III Международной научно-практической конференции «Информационная безопасность в свете Стратегии «Казахстан-2050», Астана, ЕНУ имени Л.Н.Гумилева, 2015;

– XV Международной научно-технической конференции «Проблемы информатики в образовании, управлении, экономике и технике», Пенза, 2015;

– Second International Scientific-Practical Conferenc «Problems of Infocommunications. Science and Technology», Kharkiv, 2015;

– II Международная научно-практическая конференция «Актуальні питання забезпечення кібернетичної безпеки та захист інформації», Киев, Европейский университет, 2016 р.;

– Международная научно-практическая конференция «Математические методы и информационные технологии макроэкономического анализа и экономической политики» (к 80-летию академика А. Ашимова), Алматы, 2017.

Диссертационная работа проводилась в рамках научно-исследовательского проекта КазНТУ имени К.И. Сатпаева № 757.МОН.ГФ.15.ИИТ.6 «Исследование, гармонизация, модификация и постановка на учет группы стандартов по биометрической поддержке информационной безопасности» и научно-исследовательской работы Национального авиационного университета Украины «Методология

оценивания рисков безопасности информационных систем» (регистрационный номер 105 /14.01.05).

Публикации. По теме диссертационной работы опубликовано 20 научных работ, в том числе 6 статей в изданиях, рекомендованных Комитетом по контролю в сфере образования и науки МОН РК; 1 статья опубликована в изданиях, индексируемых в базе данных Scopus (Elsevier); 11 статей опубликовано в материалах международных конференций; 2 статьи опубликованы в международных журналах.

Личный вклад соискателя. Основные положения и результаты диссертационной работы, выносимые к защите, полученные автором самостоятельно. В работах, написанных в соавторстве, личный вклад соискателя заключается в следующем: [20, 58, 59, 63] – проведен анализ понятий риска и разработана модель КМР; [77, 78] – проведены исследования средств анализа и оценивания рисков с использованием предложенной модели; [79] – предложены два метода анализа и оценивания рисков ИБ First-САОР и Second-САОР; [80, 81] – предложен метод n-кратного инкрементирования числа термов ЛП; [82, 83, 84] – разработаны методология синтеза систем анализа и оценивания рисков ИБ и структурные решения First-САОР и Second-САОР систем; [85] – разработаны программные САОР на основании представленных методологии и структурных решений, а также проведено экспериментальное исследования этих систем. Из работ, опубликованных в соавторстве, в диссертационной работе используются результаты, полученные лично соискателем.

Структура и объем диссертации. Диссертация состоит из введения, четырех разделов, заключения, списка использованных источников из 83 наименований, приложения. Общий объем работы 147 страниц и содержит 43 рисунок и 57 таблицу.