АННОТАЦИЯ

диссертационной работы **Жумангалиевой Назым Кенжегалиевны**
на тему: «Технология контроля аномальности состояния параметров
для систем обнаружения вторжений», представленной на соискание степени доктора
философии PhD по специальности 6D070400 –
Вычислительная техника и программное обеспечение

Актуальность темы. Интенсивное развитие информационных технологий позитивно влияет на все сферы деятельности человека, общества, государства. Вместе с тем наблюдаются и побочные эффекты, которые, в первую очередь, связаны с тем, что компьютерные системы и сети все больше подвергаются воздействиям угроз, новые виды которых порождают новые кибератаки, негативно влияющие на состояние безопасности ресурсов информационных систем (ИС). В этой связи существует потребность в системах защиты, позволяющих анализировать, контролировать, прогнозировать и блокировать указанные вторжения. Одним из распространенных решений безопасности ресурсов ИС (РИС), являются системы обнаружения вторжений (СОВ), основанные на программных или программно-аппаратных средствах, ориентированных прежде всего, на выявление фактов несанкционированного доступа через компьютерные сети. Указанные решения базируются на сигнатурном (шаблонном) и аномальном принципах обнаружения вторжений. Современные СОВ аномального принципа в основном основаны на математических моделях, требующих много времени для получения статистических данных, реализацию процесса обучения (для нейросетевых систем) и осуществления других сложных и длительных подготовительных процедур. Более эффективными в этом отношении являются подходы, основанные на формализации суждений экспертов и их использование в процессе принятия решений о возможности осуществления атакующих действий на компьютерные системы и сети.

Известно, что несанкционированные действия на РИС влияют на среду их окружения и порождают в ней определенные аномалии. Она обычно слабоформализована, нечетко определена и для обнаружения вторжений, породивших аномалии в такой среде, нужно использовать специальные модели, методы и системы. Расширить функциональные возможности и повысить эффективность систем сетевого противодействия можно за счет использования новых соответствующих технических решений, ориентированных на функционирование в нечетких условиях.

Формализовать информацию в нечетко определенной слабоформализо-ванной среде и эффективно осуществить ее обработку позволяют методы и модели теории нечетких множеств, а для реализации процесса принятия решений (по выявлению атакующих действий), основанных на упомянутых специальных методах и моделях, необходимы соответствующие средства.

В связи с этим актуальной задачей при разработке средств, расширяющих возможности современных СОВ является создание соответствующих моделей, методов, технологий и систем выявления в нечетких условиях аномалий, порожденных сетевыми несигнатурными кибератаками.

Целью диссертационной работы является разработка моделей и средств идентификации аномального состояния, для расширения возможностей системы обнаружения несигнатурных типов кибератак в компьютерных сетях.

Для достижения поставленной цели было необходимо решить следующие **задачи:**

1. Исследовать современное состояние развития теоретической и практической базы, используемой для обнаружения вторжений в компьютерных сетях;

2. Разработать модель базовых величин и модель эталонных величин для отображения и измерения аномального состояния в среде окружения, характерного для определенного типа кибератак в компьютерных сетях;

3. На основе модели базовых величин и модели эталонных величин построить модель решающих правил выявления аномального состояния для формализации процесса их формирования;

4. Разработать на основе модели базовых величин, модели эталонных величин и модели решающих правил технологию выявления аномальных состояний, порожденных действиями неавторизованной стороны;

5. На основе технологии выявления аномальных состояний разработать структурное решение для расширения функциональных возможностей систем обнаружения вторжений, ориентированных на несигнатурные типы сетевых кибератак;

6. Разработать и провести экспериментальное исследование новых решений, позволяющих выявлять атакующие действия в компьютерных сетях посредством контроля активности в среде окружения.

Объект исследования – процесс выявления аномального состояния, порожденного атакующими действиями в компьютерных сетях.

Предмет исследования – модели, методы, технологии и системы обнаружения аномалий в нечетко определенной слабоформализованной среде, порожденных атакующими действиями в компьютерных сетях.

Научная новизна работы заключается в следующем:

1. Получили дальнейшее развитие модель базовых величин и модель эталонных величин, которые за счет введенных множеств возможных вторжений и величин, и на их основе множеств пар «вторжение : величины» и «вторжение : множество сопряженных пар», позволяют отображать и измерять аномальное состояние в среде окружения и формализовать процесс построения эталонов нечетких переменных, характерных для определенного множества сетевых вторжений;

2. Получила дальнейшее развитие модель решающих правил, которая за счет множества эталонных величин и сформированных методами экспертного оценивания матриц инициализации для сопряженных пар и нечетких идентификаторов, позволяет формализовать процесс формирования множеств решающих правил для выявления экспертным путем аномального состояния в компьютерных сетях;

3. Впервые на основе модели базовых величин и модели эталонных величин разработан метод формирования лингвистических эталонов для систем обнаружения вторжений, который за счет использования множеств идентификаторов лингвистических оценок и идентификаторов интервалов, базовой и производной матрицы частот отображения суждений экспертов. характеризующих относительно вторжений текущие состояния величин, а также процессов формирования на заданных интервалах частот встречаемости экспертных оценок и подмножеств нечетких термов, позволяет формализовать процедуру получения эталонных значений величины заданных групп лингвистических переменных, характеризующих в различных условиях аномальности конкретную гетерогенную параметрическую среду окружения;

4. На основе модели базовых величин, модели эталонных величин и модели решающих правил разработана технология выявления аномальных состояний, порожденных действиями неавторизованной стороны, которая позволяет на основе экспертного подхода и сформированных нечетких текущих величин создавать средства идентификации несигнатурных типов кибератак;

5. Получило дальнейшее развитие структурное решение для систем обнаружения вторжений, которое с помощью реализованной технологии выявления аномальных состояний

за счет модуля нечеткой арифметики и подсистем; формирования нечетких эталонов сетевых величин; формирования решающих правил и первичной обработки позволяет путем контроля активности в среде окружения расширить функциональные возможности современных систем обнаружения вторжений.

Методы исследования базируютсяна теориях нечеткости, множеств, принятия решений, алгоритмов, моделирования информационных процессов и структур, а также методах экспертного оценивания и мягких вычислениях.

Во введении раскрыты актуальность, конкретизированы проблемы, связанные с исследуемой темой. Изложены идея работы, цель и задачи исследования, научная новизна и практическая ценность работы, методы исследования.

В первом разделе проведен анализ методов и средств реализации атак (вторжений) и определено, что они составляют достаточно широкий спектр, непрерывно совершенствуются, обновляются и используются для реализации неавторизованных действий в отношении компьютерных систем и сетей. Наиболее распространенные СОВ в основном ориентированы на использование статистических методов и нейросетевых подходов. Достоверность работы таких систем довольно чувствительна к недостаточной выборке статистических данных, неожиданных изменений в среде окружения, погрешностей в обучении систем, неизвестных атак (например, "нулевого дня") и модификации известных, что приводит к определенным сложностям обнаружения вторжений.

Второй раздел посвящен разработке моделей выявления аномального состояния для СОВ. Для построения модели базовых величин (МБВ) введено множество возможных вторжений (intrusion) модели эталонных величин (МЭВ) На основе предложенной МБВ, с учетом выбранного метода формирования функций принадлежности (МФФП) формируются модели эталонных величин (МЭВ). Процесс идентификации аномалий, порожденных вторжениями на компьютерные системы и сети, требует определения необходимых величин и их свойств. Для построения модели решающих правил (МРП) введено множество нечетких идентификаторов (fuzzy identifiers).

Третий раздел посвящен разработке технологии выявления аномального состояния и новых структурных решений для систем обнаружения аномалий, порожденных сетевыми атаками. Предлагаемая технология основана на разработанных во второй главе математических моделях и проанализированных в первом разделе методах нечеткой логики и определения коэффициента важности (КВ). Оно содержит восемь базовых этапов, раскрывающих процесс выявления аномального состояния, порождаемого определенным типом кибератак.

Четвертый раздел посвящен практическим реализациям и исследованиям средств обнаружения аномалий в компьютерных сетях. На основе предложенного алгоритмического обеспечения и типовой системы обнаружения аномалий, порожденных сканированием портов, было разработан и проведено экспериментальное исследование программной системы обнаружения сканирующих средств и прикладной системы обнаружения аномалий, порожденных атакующими действиями. Также на конкретных примерах проиллюстрирована основная суть работы системы, реализующей предложенный метод. Представлена графическая интерпретация полученных аномальных состояний для разного типа кибератак, а базовый эксперимент проведен путем моделирования 1500 вторжений (атак) на рабочие станции кафедры безопасности информационных технологий Национального авиационного университета.

Эксперимент показал, что выявленные кибератаки в 29,3% случаев были инициированы правилом SR_{15} = «Если $\underset{\sim}{t}_{VCA}$ наиболее близко к $\underset{\sim}{Y}^{e}$, входящего в $\underset{\sim}{T}^{e}_{VCA}$ и

$\underset{\sim}{t}_{NVC}$ наиболее близко к $\underset{\sim}{VB}^{e}$, входящего в $\underset{\sim}{T}^{e}_{NVC}$, то уровень аномального состояния, порожденного *SCANNING* будет LIMITS», а в 38, 7% и 32% соответственно правилам SR_{14} и SR_{13}. По результатам проведенной верификации установлено, что все вторжения (атаки) были обнаружены различными правилами и отражают разную степень уверенности эксперта, а также определено, что реализации предложенных моделей и систем адекватно отражают реакции на моделируемые действия

В заключении отражены основные результаты и выводы диссертационной работы.

Практическая значимость работы заключается в следующем:

- на основе созданных моделей и технологии разработана лабораторная работа и лекционный материал, использованный в учебном процессе подготовки специалистов в области знаний 1701 – «Информационная безопасность». Практическое использование результатов диссертационного исследования подтверждается актами внедрения в учебный процесс Национального авиационного университета (Украина, Киев) от 17.02.2017.
- на основе предложенной технологии выявления аномального состояния разработана компьютерная программа «Выявление сканирования портов на основе нечеткой логики», позволяющая в нечетко определенной слабоформализованной среде выявлять кибератаки на ресурсы информационных систем, что дало возможность улучшить степень защищенности информационной системы и оптимизировать показатели эффективности работы сетевой системы защиты, что подтверждается актом внедрения в деятельность ООО «Сайфер БІС» от 03.02.2017.

Апробация работы. Основные положения диссертационной работы докладывались, а также обсуждались на следующих научно-технических и научно-практических конференциях:

- Международная научно-техническая конференция «Современные информационно-телекоммуникационные технологии» (Украина, Киев, 2015);
- II Международная научно-практическая конференция «Информационные и телекоммуникационные технологии: образование, наука, практика» (Казахстан, Алматы, 2015);
- 16th International Conference on Control, Automation and Systems / ICCAS.2016.7832298 Gyeongju, South Korea, 2016
- II и III Международные научно-практические конференции «Актуальные вопросы обеспечения кибербезопасности и защиты информации» (Украина, Киев, 2016, 2017);
- VI международная научно-техническая конференция ITSEC (Украина, Киев, 2016);
- «Состояние и совершенствование безопасности информационно-телекоммуникационных систем» (SITS-2016) (Украина, Николаев-Коблево 2016).

Публикации. Основные положения диссертационной работы опубликованы в 23 научных работах, из которых 8 статьи опубликованы в изданиях, рекомендованных Комитетом по контролю в сфере образования и науки МОН РК; 4 статьи опубликованы в изданиях, индексируемых в базе Scopus; 4 статьи опубликованы в научных журналах и сборниках научных трудов: 5 статьи опубликованы в сборниках международных конференций (Украина), 2 статья опубликованы в материалах международной конференции (Казахстан).

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, общих выводов, приложений, списка использованных источников и имеет 165 страницы основного текста, 41 рисунок, 23 таблицы, 13 страниц приложений. Список литературы содержит 113 наименований и занимает 14 страниц. Общий объем работы 185 страницы.

По теме диссертации опубликовано 23 публикаций:

1. Ахметов Б.С. Использование методов нечетких множеств в системах обнаружения вторжений / Б.С. Ахметов, А.А. Корченко, Н.К. Жумангалиева // Інформаційна безпека. – 2014. – №1 (13); №2 (14). – С. 42-55.

2. Использование методов експертного оценивания в системах обнаружения вторжений/ Б.С. Ахметов, А.А. Корченко, С.Т. Ахметова, Н.К. Жумангалиева // Інформаційна безпека. – 2014. – №3 (15); №4 (16). – С. 34-43.

3. Ахметов Б.С. Анализ методов нечетких множеств для построения систем обнаружения вторжений /Б.С.Ахметов, А.А.Корченко, Н.К.Жумангалиева //«Современные информационно-телекоммуникационные технологии»: Междунар. науч.-тех. конф. : Матер. конф. – К.: ГУТ, 17-20 ноября 2015 года – С. 38-40.

4. Базовые модели эталонных величин для систем обнаружения вторжений / Б.С. Ахметов, Р.Б.Абдрахманов, А.А.Корченко, Н.К. Жумангалиева // ВестникМеждународногоКазахско-Турецкогоуниверситета. им. А.Ясави. – 2015. – №5-6 (97-98). – С. 15-26

5. Анализ методов экспертного оценивания для систем обнаружения вторжения / Б.С. Ахметов, А.А. Корченко, С.Т. Ахметова, Н.К. Жумангалиева // «Информационные и телекоммуникационные технологии: образование, наука, практика» : II междунар. науч.-практич. конф. : Труды. – Алматы, Казахстан, 3-4 декабря, II том. – 2015 года. – С. 28-31.

6. Ахметов Б.С. Модель базовых величин для контроля аномальности состояния среды окружения / Б.С. Ахметов, А.А. Корченко, Н.К. Жумангалиева// Известия Национальной Академии наук Республики Казахстан. Серия физико-математическая. – 2016. – №1 (305). – С. 26-33.

7. Ахметов Б.С. Модель решающих правил для обнаружения аномалий в информационных системах / Б.С. Ахметов, А.А. Корченко, Н.К. Жумангалиева // Известия Национальной Академии наук Республики Казахстан. Серия физико-математическая. – 2016. – №4 (308). – С. 91-100.

8. Метод построения условных детекционных выражений для систем обнаружения кибератак / Н.П. Карпинский, А.А. Корченко, С.Т. Ахметова, Н.К. Жумангалиева // Актуальні питання забезпечення кібербезпеки та захисту інформації : II міжнар. наук.-практ. конф. : Тези доп. – Київ, 24-27 лютого 2016 року – С. 65-69.

9. Ахметов Б.С. Технология выявления аномального состояния для систем обнаружения вторжений / Б.С. Ахметов, А.А. Корченко, Н.К. Жумангалиева // Вестник КазНУ. Серия математика, механика, информатика. – 2016. – №1 (88). – С. 106-113

10. Akhemtov Bakhytzhan, Korchenko Anna, Akhmetova Sanzira, Zhumangalieva Nazym. Improved method for the formation of linguistic standards for ofintrusion detection systems // Journal of The oreticaland Applied Information Technology, 2016. Vol.87. №.2. – Pp. 221-232.

11. Корченко А.А. Построение лингвистических эталонов для выявления сниффинг атак / А.А. Корченко, Н.К. Жумангалиева, П.А. Викулов // Актуальні питання забезпечення кібербезпеки та захисту інформації : III міжнар. наук.-практ. конф. : Тези доп. – Київ, 22-25 лютого 2017 року – С. 93-97.

12. Ахметов Б.,Иванов А., Алибиева Ж., Мукапил К., Бекетова Г. Prospects for Multiple Reductions in Test Samples with a Multivariate, Multicriteria, The Neural Network Statistical Analysis of Biometric Data // Medwell Journals, 2015 Research Journal Applied Scienses 10(12) 2015 956-967

13. Mikolaj Karpinski, Vasyl Martsenyuk, Iryna Gvozdetska, Bakhytzhan Akhmetov, Zhumangalieva Nazym. Estimation Problem for Network Model at State and Measurements Attacks and Information Cost Criterion// 16th International Conference on Control, Automation and Systems / ICCAS.2016.7832298 Gyeongju, South Korea, 2016, pp. 45-50.doi: 10.1109/

14.Aleksandra Kłos-Witkowska; Bakhytzhan Akhmetov; Volodymyr Karpinskyi; Tomasz Gancarczyk. Bovine Serum Albumin stability in the context of biosensors//2016 16th International Conference on Control, Automation and Systems ICCAS)//Year:016//Pages: 976 80, DOI: 10.1109/ICCAS.2016.7832427EEE Conference Publications
15. Ахметов Б.С., Корченко А.А. Смагулов С.К , Жумангалиева Н:К . Ақпараттық жүйенің жағдайын бақылауға арналған базалық ауытқымалық шаманың модельдері// Семей Қаласының Шәкәрім Атындағы Мемлекеттік Университетінің х а б а р ш ы с ы 2016 № 2 (74) -С . 87 -91
16. Ахметов Б.С., Корченко А.А. Смагулов С.К , Жумангалиева Н.К . Ақпараттық жүйенің аномалиялық жағдайын бақылауға арналған базалық шаманың модельдері// Семей Қаласының Шәкәрім Атындағы Мемлекеттік Университетінің х а б а р ш ы с ы № 1 (77) 2017 С 111-115 ISSN 1607-2774
17. B. Akhmetov, A. Korchenko, J. Kultan, N.Zhumangalieva,. Model decision rules to detect anomalies in Information Systems// Informational Technology Application, Словакия, №1, 2016 126-136 ISSN 13386468
18. Бекетова Г. С., Ахметов Б.С., Абишева Г.К., Жумангалиева Н.К . Жеке биометриялық мәліметтерді қорғаудың нейрожелілік технологиясы//«Қазақстанның жаңа экономикалық саясатын таратуда жас ғалымдардың орны мен рөлі» халықаралық Сәтбаев оқуларының еңбектері, IV том, 2015 ж., с- 719-724
19. Мукапил., Бекетова Г. С., Төлімесова В., Жумангалиева Н.К . Ақпаратты қорғаудың биометриялық әдістері// Хабарщысы КазҰТУ. №2, 2015 г. с.250-261.
20. Мукапил., Бекетова Г. С., Төлімесова В., Жумангалиева Н.К ., Култан Я.. Biometric methods of nformational protection// Informational Technology Application, Словакия, №1, 2016 126-136
21. Ахметов Б.., Алимсеитова Ж., Коренко А., Жумангалиева Н.К . Система выявления аномального состояния в информационных системах// Қазақстан Республикасы Ұлттық ғылым академиясының баяндамалары Физика -математика 2017. – №5 (308). – С. 28-37
22. Ахметов Б.., Коренко А., Жумангалиева Н.К., Култан Я.. Model decision rules to detect anomalies in Information Systems// Informational Technology Application, Словакия, №1, 2016 126-136
23. Гнатюк С.О., Шаховал О.А., Бекетова Г., Жумангалиева Н.К.. Информационно-психологический аспект киберзащиты// «Состояние и совершенствование безопасности информационно-телекоммуникационных систем» (SITS-2016). //– Николаев-Коблево: Международный технологический университет, 9-12 июнь 2016 г. 32-34