ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 212.288.07 НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 09.10.2020 № 4

О присуждении Полетаеву Владиславу Сергеевичу, гражданину РФ, ученой степени кандидата технических наук.

Диссертация «Информационно-аналитическая система прогнозирования угроз и уязвимостей информационной безопасности на основе анализа данных тематических интернет-ресурсов» по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность принята к защите 23.03.2020 г., протокол № 2 диссертационным советом Д 212.288.07 на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский государственный авиационный технический университет» Министерства науки и высшего образования Российской Федерации, 450008, г. Уфа, ул. К. Маркса, 12, созданного приказом Министерства образования и науки Российской Федерации № 192/нк от 09.04.2013 г.

Соискатель Полетаев Владислав Сергеевич 1984 года рождения, проходит службу в войсковой части №26035 Министерства обороны Российской Федерации.

В 2006 году соискатель окончил Академию федеральной службы безопасности Российской Федерации по специальности «Компьютерная безопасность».

С 05.12.2014 г. по 30.11.2017 г. для подготовки диссертации был прикреплен к кафедре телекоммуникационных технологий и сетей ФГБОУ ВО «Ульяновский государственный университет».

Диссертация выполнена на кафедре телекоммуникационных технологий и сетей Ульяновского государственного университета Министерства науки и высшего образования РФ.

Научный руководитель – доктор технических наук, профессор Смагин Алексей Аркадьевич, профессор кафедры телекоммуникационных технологий и сетей ФБГОУ ВО «Ульяновский государственный университет».

Официальные оппоненты:

1. Доктор технических наук, профессор Захаров Александр Анатольевич, заведующий кафедрой безопасных ИТ умного города ФБГОУ ВО «Тюменский государственный университет»;

2. Кандидат технических наук, доцент Вульфин Алексей Михайлович, доцент кафедры вычислительной техники и защиты информации ФБГОУ ВО «Уфимский государственный авиационный технический университет».

дали положительные отзывы на диссертацию.

Ведущая организация ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева–КАИ», в своем положительном заключении, рассмотренном 20.04.2020 г. на заседании кафедры компьютерных систем и утвержденном проректором по научной и инновационной деятельности д.т.н., профессором Михайловым Сергеем Анатольевичем, указала, что диссертация Полетаева В.С. на соискание ученой степени кандидата технических наук является законченной научно-квалификационной работой, в которой содержится решение актуальной задачи по созданию методов, моделей и средств выявления, идентификации и классификации угроз нарушения информационной безопасности. Работа соответствует требованиям п.9 «Положения ВАК о присуждении ученых степеней», а её автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Соискатель имеет 9 опубликованных работ, в том числе по теме диссертации 9 работ, опубликованных в рецензируемых научных изданиях – 3.

Наиболее значимые научные работы по теме диссертации:

1. Смагин А.А., Полетаев В.С. Модель потока текстовых сообщений тематических интернет–форумов // Вестник НГИЭИ. № 10 (77), Княгинино – 2017, с. 16 – 24.

2. Смагин А.А., Полетаев В.С. Алгоритм прогнозирования угроз информационной безопасности // Инфокоммуникационные технологии. Том 16, №2, Самара – 2018, с. 192–198.

3. Полетаев В.С. Нечеткий логический вывод о возникновении угроз информационной безопасности на основе анализа данных хакерских форумов // Автоматизация процессов управления. Вып. №4 (54) – Ульяновск: ФНПЦ АО «НПО «Марс», 2018, с. 64–75.

На диссертацию и автореферат поступили отзывы:

- Ведущей организации ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева–КАИ». Отзыв рассмотрен 20.04.2020 г. на заседании кафедры компьютерных систем, утвержден проректором по научной и инновационной деятельности д.т.н., профессором Михайловым Сергеем Анатольевичем. В отзыве указаны следующие замечания: 1. В диссертационной работе желательно было бы представить подробный анализ наиболее известных на сегодняшний день тематических интернет-ресурсов и обоснование выбора конкретных из них для включения в информационно-аналитическую систему; 2. Остался за кадром механизм получения рейтинга А автора сообщения и то, в каких единицах он измеряется? Если на разных интернет-ресурсах используются различные механизмы получения рейтинга, то как это учитывается в формулировках правил и функциях принадлежности данного показателя; 3. Производились ли исследования эффективности прогнозирования при выборе различных параметров модели Мамдани; 4. В диссертации не сказано, охватывает ли построенная онтология все угрозы БД ФСТЭК; 5. В таблице 4.2. диссертации говорится о количестве записей об угрозах и уязвимостях в базе данных ФСТЭК России. В данном случае не совсем понятно,

что автор имеет ввиду – количество вновь появившихся записей в заданный период времени в БД ФСТЭК России или что-то иное.

- Официального оппонента **Захарова Александра Анатольевича**, доктора технических наук, профессора, заведующего кафедрой «Безопасные информационные технологии умного города» ФГАОУ ВО «Тюменский государственный университет». В отзыве указаны следующие замечания: 1. Задача исследования 5. Стр. 10. Оценка эффективности алгоритма прогнозирования угроз. В чем измеряется эффективность? Представленная технология (рис. 4.5-4.7 стр. 115-116) определяет возможную угрозу на 1-2 дня раньше, чем она появляется на сайте ФСТЭК. Может такая задержка публикации объясняется недостаточной оперативностью публикации, например, ФСТЭК проводит дополнительные проверки прежде чем публиковать информацию; 2. Рис. 1. стр. 24. Цели защиты информации (указано 10 штук). Но это не цели, а методы. Например, целью защиты информации не может быть «Создание комплексной системы защиты» или «Организация и проведение контроля состояния и эффективности системы защиты информации» и т.д.; 3. Стр.27. Перечислены следующие системы обнаружения атак (RealSecure, ISS, Cisco, Snort). Система обнаружения атак RealSecure™ разработана американской компанией Internet Security Systems, Inc. 2004 г. ISS – Российская компания разработчики видео менеджмента SecurOS, Cisco – мировой лидер в создании оборудования для Интернета, Snort – свободная сетевая система предотвращения вторжений (IPS). И всё это выдается как IDS со ссылкой на очень странный источник 73 – Трахтенгерц Э.А. Компьютерная поддержка принятия решений: Научно-практическое издание. Серия XXI века. – М.:СИНТЕГ, 2012. 396 с.; 4. Стр.28. «Атаки типа межсайтовый скриптинг или SQL-инъекций не имеют сигнатур». Элементы языка SQL запросов в пароле – разве не сигнатура; 5. Стр. 58. формулы 2.1 и 2.2 в которых фигурирует О – онтология предметной области не учитывают её изменения во времени (ранее, Рис 2.2 стр. 55. указывалось, что онтология актуализируется, т.е. зависит от времени). Не описан механизм актуализации и синхронизации по периодам времени.

- Официального оппонента **Вульфина Алексея Михайловича**, кандидата технических наук, доцента кафедры вычислительной техники и защиты информации ФГБОУ ВО «Уфимский государственный авиационный технический университет». В отзыве указаны следующие замечания: 1. Не отражены вопросы использования алгоритмов автоматического анализа и построения семантического пространства, а также построения модели языка (Fast2Text, Word2Vec, Doc2Vec); 2. Не достаточно подробно раскрыты вопросы фильтрации текстовых сообщений интернет-ресурсов: объем собранной базы, параметры отдельных сообщений, процесс построения стоп-словаря, фильтра; 3. Недостаточно подробно приведена классификация выявленных событий и не описан процесс построения базы правил на основе автоматизированного подходов с извлечением знаний – TextMining; 4. Слишком обширная классификация и анализ базовых понятий и определений информационной безопасности без достаточной привязки к предмету исследования – тематическим интернет-ресурсам; 5. Разработка алгоритма прогнозирования сводится к построению нечеткой модели, входные параметры которой не раскрыты детально; 6. Не раскрыт в полной мере механизм построения базы знаний на основе совокупности выделенных эвристических правил функционирований хакерских форумов; 7. Не описаны особенности используемых алгоритмов обучения нейронных сетей на этапе адаптивной сегментации; 8. Для пояснения работы всех элементов разработанной системы не хватает «сквозного» детального примера анализа; 9. Оформление таблиц, оформление блок-схем алгоритмов, нумерация формул, не все аббревиатуры на рисунках расшифрованы.

На автореферат поступило 6 положительных отзывов:

1. От Центра проектирования инноваций АУ «Технопарк-Мордовия», подписанный директором, д.т.н., профессором **Беловым Владимиром Федоровичем**. В отзыве указано следующее замечание: Автор счел правильным не указывать о каких формирующих угрозы форумах идет речь в диссертации, нет их характеристик, как источников семантической информации, что для корректного вывода угрозы является немаловажным обстоятельством.

2. От ФГБОУ ВО «Поволжский государственный университет сервиса», подписанный заведующим кафедрой «Информационный и электронный сервис», д.т.н., доцентом **Воловачем Владимиром Ивановичем**. В отзыве указано следующее замечание: В диссертации предложена и используется логическая модель базы данных тематических интернет-ресурсов. Хотелось бы увидеть её как структурно-логическую модель, информационного объекта, генерирующего по зашумленным каналам связи множество сообщений, что могло бы позволить для их анализа механизмы их семантической фильтрации.

3. От ФГАОУ ВО «Самарский национальный исследовательский университет имени академика С.П. Королева», подписанный заведующим кафедрой информационных систем и технологий д.т.н., профессором **Прохоровым Сергеем Анатольевичем**. В отзыве указаны следующие замечания: 1. Отсутствуют публикации, индексируемые в международных базах Scopus и WoS; 2. Представленное в формуле (6) обозначение максимума числовой последовательности не является общепринятым; 3. В автореферате отсутствует формальное представление функций принадлежности, отраженных на рисунке 5.

4. От ФГАОУ ВО «Поволжский государственный университет телекоммуникаций и информатики», подписанный заведующим кафедрой информационной безопасности д.т.н., профессором **Карташевским Вячеславом Григорьевичем**. В отзыве указано следующее замечание: не совсем понятен смысл предложения о «применении более точных правил нечетких продукций, увеличения количества входных переменных, характеризующих закономерности изменения потока сообщений тематических интернет-ресурсов».

5. От ФБГОУ ВО «Ульяновский государственный технический университет», подписанный директором департамента информационных технологий, заведующим кафедрой «Измерительно-вычислительные комплексы» д.т.н. доцентом **Киселевым Сергеем Константиновичем**. В отзыве указаны следующие замечания: 1. Не ясно, насколько рассмотренная в первой главе модель базы данных тематического интернет-ресурса и алгоритмы работы с потоками текстовых сообщений специализированы именно областью прогнозирования угроз и уязвимостей информационной безопасности; 2. В

алгоритме на рис. 3 присутствует блок «Дополнение онтологии новыми терминами», однако не ясно как производится проверка релевантности новых терминов и необходимости их занесения в онтологию, т.к. в рамках интернет-форума новые термины могут порождаться достаточно произвольно; 3. Не понятно почему в таблице оценки сходимости значений прогнозов информационно-аналитической системы о возникновении угроз и уязвимостей информационной безопасности и количестве выявленных угроз и уязвимостей по данным ФСТЭК России значения MAE (средняя абсолютная ошибка), RMSE (квадратный корень из средней квадратичной ошибки) указаны в процентах.

6. От ФБГОУ ВО «Казанский национальный исследовательский технологический университет», подписанный заведующим кафедрой информатики и прикладной математики, к.т.н., д.п.н. профессором **Нуриевым Наилем Кашаповичем**. В отзыве указано следующее замечание: в автореферате не совсем ясно, как оцениваются некоторые метрики, характеризующие надежность прогноза угроз и уязвимостей информационной безопасности.

Выбор официальных оппонентов и ведущей организации обосновывается их компетентностью и научными разработками в области информационной безопасности, значительным числом научных трудов, в том числе по рассматриваемым в диссертации проблемам.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

доказана перспективность использования анализа данных тематических интернет–ресурсов для прогнозирования возникновения угроз и уязвимостей информационной безопасности, а также своевременной выработки мер и средств защиты информации;

предложены: 1) модель базы данных тематического интернет–ресурса, являющаяся основным компонентом информационно-аналитической системы прогнозирования угроз и уязвимостей информационной безопасности, позволяющая работать с данными различных программных платформ, применяемых для создания дискуссионных тематических информационных ресурсов; 2) модель потока текстовых сообщений, относящихся к предметной

области, заданной онтологией, позволяющей прогнозировать угрозы и уязвимости, учитывая их контекстуальную принадлежность;

разработаны: 1) алгоритм анализа потока текстовых сообщений тематических интернет–ресурсов, основанный на статистическом и семантическом анализе, отличающийся от аналогов возможностью осуществлять семантическую фильтрацию сообщений, а также вычислять статистические параметры для нечеткого логического вывода о прогнозируемом событии; 2) алгоритм прогнозирования угроз и уязвимостей информационной безопасности, основанный на нечетком логическом выводе, статистическом и семантическом анализе, отличающийся от аналогов возможностью выявления угроз и уязвимостей до их непосредственной реализации;

реализованы компоненты информационно–аналитической системы прогнозирования угроз и уязвимостей информационной безопасности на основе моделей базы данных тематических интернет-ресурсов, потока текстовых сообщений и предложенных алгоритмов, позволяющие исследовать её возможности на практике;

Теоретическая значимость исследования обоснована тем, что:

доказана, путем проведения многочисленных экспериментальных исследований с функционирующими популярными тематическими интернет-ресурсами, эффективность и перспективность использования разработанных методов и алгоритмов, информационно-аналитической системы для анализа данных тематических интернет–ресурсов, прогнозирования возникновения угроз и уязвимостей информационной безопасности;

применительно к проблематике диссертации результативно использован комплекс методов системного анализа, логического вывода, объектно–ориентированного программирования, теории нечетких множеств, математической логики и статистики, онтологического и семантического анализа текста, функционального и информационного моделирования;

изложены результаты работы и модель потока текстовых сообщений, относящихся к предметной области, заданной онтологией, позволяющая осуществлять семантическую фильтрацию сообщений и проводить

статистический анализ;

раскрыты и выявлены основные недостатки работы современных систем обнаружения и прогнозированию компьютерных атак, которые могут быть устранены за счет использования результатов аналитической обработки сообщений тематических интернет–ресурсов;

изучены закономерности процесса наполнения тематических интернет–ресурсов новыми сообщениями, позволяющие применять для прогнозирования угроз и уязвимостей информационной безопасности алгоритмы, основанные на нечетком логическом выводе, статистическом и семантическом анализе;

проведена модернизация существующих в настоящее время методов и алгоритмов защиты информации на основе предложенных моделей и алгоритмов автоматизированного сбора и анализа данных тематических интернет–ресурсов, позволяющих прогнозировать угрозы и уязвимости информационной безопасности, а также принимать меры по противодействию им;

предложены: 1) модель базы данных тематического интернет–ресурса, предназначенная для прогнозирования угроз и уязвимостей информационной безопасности, позволяющая работать с разнородными данными различных программных платформ; 2) модель потока текстовых сообщений, относящихся к предметной области, заданной онтологией, отличающаяся возможностью семантического и статистического анализа данных для прогнозирования угрозы и уязвимости информационной безопасности;

разработаны: 1) алгоритм прогнозирования угроз и уязвимостей информационной безопасности, основанный на нечетком логическом выводе, статистическом и семантическом анализе, позволяющий повысить эффективность защиты информации; 2) алгоритм анализа потока текстовых сообщений тематических интернет–ресурсов, основанный на статистическом и семантическом анализе, отличающийся от аналогов возможностью осуществлять семантическую фильтрацию сообщений, а также вычислять статистические параметры для нечеткого логического вывода о прогнозируемом событии;

раскрыт процесс формирования информационно-аналитической системы и взаимодействия её программных модулей, а также представлена методика

автоматизированного анализа данных тематических интернет–ресурсов, реализующего предложенные выше алгоритмы и позволяющего прогнозировать угрозы и уязвимости, принимать меры по защите информации.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

разработанные модели и алгоритмы **внедрены** в ФНПЦ АО «НПО «Марс», где использовались при проектировании и разработке программного комплекса в ОКР «Разработка ПАК интеллектуального поиска, анализа и прогнозирования социальной активности в открытых источниках информации», а также в учебном процессе подготовки магистрантов, специалистов и бакалавров ФГБОУ ВО «Ульяновский государственный университет» при изучении дисциплин: «Защита информации в инфокоммуникационных системах», «Информационная безопасность и защита информации», «Обнаружение вторжений и защита информации»;

определены перспективы практического использования разработанных моделей, алгоритмов и информационно-аналитической системы для решения прикладных задач, актуальных в области защиты информации;

создана информационно–аналитическая система прогнозирования угроз и уязвимостей информационной безопасности на основе анализа данных тематических интернет–ресурсов с использованием следующих программных продуктов: в качестве хранилища данных – СУБД MySQL, системы нечеткого логического вывода – Fuzzy Logic Designer, редактора онтологии – Protégé, средства морфологического анализа текста сообщений – Mystem;

представлены предложения по практическому применению разработанной информационно-аналитической системы и повышению эффективности прогнозирования угроз и уязвимостей информационной безопасности.

Оценка достоверности результатов исследования выявила:

идея исследования базируется на обобщении передового опыта отечественных и зарубежных исследователей в области информационной безопасности и защиты информации, в том числе в области решения прикладных задач, согласуется с опубликованными данными по теме диссертации;

использованы современные методы системного анализа и логического вывода, теории нечетких множеств, математической логики и статистики, онтологического и семантического анализа текста, функционального и информационного моделирования, методики сбора и обработки исходной информации с применением современных информационных технологий;

использованы результаты свыше ста экспериментов по анализу сообщений тематических интернет–ресурсов с целью оценки предложенных методов и алгоритмов. Рассчитаны значения предложенного Четыркиным Е.М. показателя точности прогноза: для доверительного интервала 20% - 0,685, 15% - 0,556, 10 % - 0,519. Результаты прогнозирования в большинстве случаев подтверждаются данными базы угроз и уязвимостей ФСТЭК России с временными расхождениями в 1 – 2 дня между активизацией обсуждения вопросов информационной безопасности на тематических интернет–ресурсах и добавлением записей о выявленных угрозах и уязвимостях в базу данных ФСТЭК России;

установлено качественное совпадение авторских результатов в области прогнозирования угроз и уязвимостей информационной безопасности с аналогичными данными базы угроз и уязвимостей ФСТЭК России;

Личный вклад соискателя состоит в: выборе темы исследования, постановке цели и задач, формализации предложенных моделей, формировании и применении методик исследования, разработке алгоритмов и программных средств, с последующей их реализацией, научном анализе, обработке и интерпретации экспериментальных данных, обобщении и апробации результатов исследования, подготовке публикаций по теме научных исследований.

Диссертационный совет пришел к выводу о том, что в диссертации:

- соблюдены установленные Положением о присуждении ученых степеней критерии, которым должна отвечать диссертация на соискание ученой степени;

- отсутствуют недостоверные сведения об опубликованных соискателем ученых степеней работах, в которых изложены основные научные результаты диссертации;

- соискатель ссылается на авторов и источники заимствования;

- оригинальность диссертационной работы составляет 88,69 %.

Диссертационная работа Полетаева В.С. соответствует п. 9 Положения о присуждении ученых степеней (утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 года № 842, в редакции с изменениями, утв. Постановлением Правительства РФ от 21 апреля 2016 года № 335), предъявляемых к кандидатским диссертациям.

Диссертация Полетаева В.С. является законченной научно-квалификационной работой, в которой решена задача по созданию методов, моделей и средств выявления, идентификации и классификации угроз нарушения информационной безопасности.

На заседании 09.10.2020 г. диссертационный совет принял решение присудить Полетаеву В. С. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 17 человек, из них 5 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 23 человек, входящих в состав совета, проголосовали: за – 16, против – 1, недействительных бюллетеней – 0.

Председатель
диссертационного совета Султанов Альберт Ханович

Ученый секретарь
диссертационного совета Виноградова Ирина Леонидовна

9 октября 2020 года