На правах рукописи

ГОРОХОВА ВАЛЕРИЯ ФЕДОРОВНА

МАТЕМАТИЧЕСКИЕ МОДЕЛИ, ЧИСЛЕННО-АНАЛИТИЧЕСКИЕ МЕТОДЫ И ПРОГРАММЫ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ И ОПТИМИЗАЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ПОГЛОЩАЮЩИХ ЦЕПЕЙ МАРКОВА

Специальность: 05.13.18 – Математическое моделирование,
численные методы и комплексы программ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Омск-2022

Работа выполнена в Федеральном государственном автономном образовательном учреждении высшего образования «Омский государственный технический университет» (ОмГТУ) на кафедре «Комплексная защита информации».

Научный руководитель:	**Магазев Алексей Анатольевич** доктор физико-математических наук, профессор кафедры «Комплексная защита информации» Федерального государственного автономного образовательного учреждения высшего образования «Омский государственный технический университет»
Официальные оппоненты:	**Филимонов Вячеслав Аркадьевич** доктор технических наук, профессор, старший научный сотрудник лаборатории методов преобразования и представления информации Омского филиала Федерального государственного бюджетного учреждения науки «Институт математики им. С. Л. Соболева Сибирского отделения Российской академии наук», г. Омск **Ручай Алексей Николаевич** кандидат физико-математических наук, доцент, заведующий кафедрой компьютерной безопасности и прикладной алгебры Федерального государственного бюджетного образовательного учреждения высшего образования «Челябинский государственный университет», г. Челябинск
Ведущая организация:	Федеральное государственное бюджетное образовательное учреждение высшего образования «Новосибирский государственный технический университет», г. Новосибирск

Защита состоится «20» сентября 2022 г. в 10-30 на заседании диссертационного совета Д 212.178.15, созданного на базе Омского государственного технического университета по адресу: 644050, г. Омск, пр. Мира, д. 11, Главный корпус, ауд. П-202.

С диссертацией можно ознакомиться в библиотеке Омского государственного технического университета и на официальном сайте http://www.omgtu.ru.

Отзывы на автореферат в двух экземплярах, заверенные гербовой печатью учреждения, просим направить по адресу: 644050, г. Омск, пр. Мира, д.11, ОмГТУ, ученому секретарю диссертационного совета Д 212.178.15. Тел.: (3812) 65-24-79, E-mail: dissov_omgtu@omgtu.ru.

Автореферат разослан «____» _____ 2022 г.

Ученый секретарь
диссертационного совета Д 212.178.15,
доктор технических наук, доцент **Варепо Л.Г.**

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования и степень ее разработанности. Роль математического моделирования в различных вопросах исследования информационных систем и систем компьютерной безопасности переоценить сложно. Среди наиболее актуальных задач, на решение которых направлены усилия специалистов, следует отметить задачи теоретического обоснования механизмов и методов кибербезопасности, используемых при проектировании и эксплуатации реальных информационных систем и технологий.

Особое место среди применяемых методов исследования указанных проблем занимает *стохастическое моделирование*. Действительно, постоянное усложнение компьютерных систем и технологий, а также непрерывный рост числа взаимодействующих с ними пользователей позволяют описывать происходящие в них процессы как случайные. В качестве наиболее популярных математических моделей таких процессов выступают *марковские процессы*, применяемые также в различных областях науки, в частности, в биологии, химии, физике и т. д.

В связи с популярностью применения к моделированию информационных систем стохастических подходов, не удивительно, что эти методы стали также проникать и в область информационной безопасности. Наблюдается тенденция к использованию в этой области марковских моделей, как с непрерывным, так и дискретным временем. При этом спектр решаемых с помощью этих моделей задач оказывается неожиданно широким: обнаружение вторжений в компьютерные системы[1], моделирование процессов распространения компьютерных вирусов[2], управление рисками информационной безопасности[3], моделирование процессов возникновения киберугроз и эксплуатации уязвимостей в информационных и киберфизических системах[4], оптимизация и повышение надежности защищенных информационных систем[5].

Интенсивное применение специалистами по кибербезопасности методов и подходов стохастического моделирования привело к появлению большого числа соответствующих моделей, слабо исследованных с математической точки зрения.

---

[1] Anomaly-based network intrusion detection: Techniques, systems and challenges / P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, E. Vazquez. – https://doi.org/10.1016/j.cose.2008.08.003 // Computers and Security. – 2009. – Vol. 28, no. 1–2. – P. 18–28.

[2] Billings, L. A unified prediction of computer virus spread in connected networks / L. Billings, W. Spears, I. Schwartz. – https://doi.org/10.1016/S0375-9601 (02)00152-4 // Physics Letters A. – 2002. – Vol. 297, no. 3–4. – P. 261–266.

[3] Research on Cloud Computing Security Risk Assessment Based on Information Entropy and Markov Chain / M. Yang, R. Jiang, T. Gao [et al.]. – DOI: 10.6633/IJNS.201807 20(4).08 // International Journal of Network Security. – 2018. – Vol. 20, no. 4. – P. 664–673.

[4] Almasizadeh, J. A stochastic model of attack process for the evaluation of security metrics / J. Almasizadeh, M. A. Azgomi. – https://doi.org/10.1016/j.comnet.2013.03.011 // Computer Networks. – 2013. – Vol. 57, no. 10. – P. 2159–2180.

[5] Yunxiao, Z. Optimization-Time Analysis for Cybersecurity / Z. Yunxiao, P. Malacaria. – DOI:10.1109/TDSC.2021.3055981 // IEEE Transactions on Dependable and Secure Computing. – 2021. – February – URL: https://qmro.qmul.ac.uk/xmlui/handle/123456789/74641 (дата обращения: 05.12.2021).

Получаемые при этом результаты носят численный или даже качественный характер, что ограничивает возможности их использования. Точные же аналитические результаты в литературе появляются очень редко и относятся, как правило, к простейшим ситуациям, не представляющим интереса с практической точки зрения. Проблема также усугубляется и тем, что многие хорошо изученные модели систем массового обслуживания напрямую не могут быть применены к задачам информационной безопасности, в силу особой специфики последних. Поэтому актуальной на сегодняшний день задачей является проблема развития аналитических и/или приближенных методов исследования стохастических математических моделей, применяемых в информационной безопасности и смежных с нею областей.

А. П. Росенко в цикле своих работ[6] сформулировал ряд универсальных стохастических марковских моделей, призванных количественно описывать процессы типа «атака – отражение», происходящие в информационных системах, подвергающихся компьютерным атакам. Его модели формулировались в терминах поглощающих цепей Маркова, состояния которых ассоциировались с состояниями информационной системы, подвергающейся или не подвергающейся в настоящий момент какой-либо из атак. Параллельно с этим схожие концепции и построенные на их основе стохастические модели компьютерных атак были предложены и некоторыми западными авторами[7]. Указанные модели привлекли внимание специалистов в смысле их применения к задаче *оценки эффективности* систем защиты информации. Для предложенных марковских моделей эта проблема решается введением так называемых *метрик безопасности*, количественная оценка которых позволяет оценить эффективность применяемых контрмер.

Отметим также, что ряд марковских моделей, подобных предложенных А. П. Росенко для моделирования процессов типа «атака – отражение», также активно применяются и в других областях науки: в экономике[8], обработке

---

[6] Росенко, А. П. Марковские модели оценки безопасности конфиденциальной информации с учетом воздействия на автоматизированную информационную систему внутренних угроз / А. П. Росенко // Вестник Ставропольского государственного университета. – 2005. – № 43. – С. 34–40; Росенко, А. П. Математическое моделирование влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированной информационной системе / А. П. Росенко // Известия Южного федерального университета. Технические науки. – 2008. – № 85 (8). – С. 71–81;
Росенко, А. П. Внутренние угрозы безопасности конфиденциальной информации. Методология и теоретическое исследование : моногр. / А. П. Росенко ; Ставропольский гос. ун-т. – Москва : КРАСАНД, 2010. – 156 с. – ISBN 978-5-396-00121-3.

[7] Subil, A. Cyber security analytics: a stochastic model for security quantification using absorbing markov chains / A. Subil, S. Nair. – DOI: 10.12720/jcm.9.12.899-907 // Journal of Communications. – 2014. – Vol. 9, no. 12. – P. 899–907.

[8] Olivera, K. On the structure of the world economy: An absorbing Markov chain approach / K. Olivera, V. Stojkoski, L. Kocarev. – DOI: 10.3390/e22040482 // Entropy. – 2020. – Vol. 22 (4). – P. 482-1–482-24.

изображений[9], образовании[10]. С математической точки зрения все они относятся к классу так называемых *поглощающих марковских цепей*.

Помимо самой задачи получения количественных оценок различных метрик безопасности, призванных дать ответ об эффективности применяемых мер защиты от кибератак, огромное значение представляет также и проблема *оптимизации* этих мер относительно тех или иных критериев. Стандартные подходы здесь сводятся к *минимизации рисков*, хотя многие специалисты в области информационной безопасности отмечают однобокость такого подхода. Модели атак, основанные на применении поглощающих марковских цепей, позволяют принимать во внимание ряд и других важных количественных характеристик систем защиты, отражающих способность их длительного безотказного функционирования. Подобные оценки также могут быть использованы как оптимизационные критерии, либо как условия, ограничивающие область поиска оптимальных решений. На эту возможность, по-видимому, впервые указал автор настоящего диссертационного исследования вместе со своим научным руководителем[11]. Плодотворное использование, а также некоторые дальнейшие перспективы развития этого класса оптимизационных задач можно также найти в недавней статье Ю. Дженга и П. Малакарио [12].

Следует также отметить, что оптимизационные задачи, формулируемые с применением марковских моделей типа «атака – отражение», оказываются принадлежащими к классу задач нелинейного дискретного программирования. Это приводит к актуальной проблеме разработки эффективных методов и алгоритмов их решения, так как подобные задачи относятся к наиболее сложным в теории оптимизации.

Целью диссертационной работы является оценка эффективности и оптимизация систем защиты информации на основе математических моделей, численно-аналитических методов и программ, использующих поглощающие цепи Маркова.

Для достижения поставленной цели в диссертации сформулированы и решены следующие **задачи**:

1. Разработан ряд численно-аналитических методов оценки вероятностно-временных характеристик поглощающих марковских цепей с

---

[9] Salient object detection via two-stage absorbing Markov chain based on background and foreground / T. Wei, W. Zhijian, Z. Jiyou, Y. Zhangjing. – DOI: 10.1109/ICCV.2013.209 // Journal of Visual Communication and Image Representation. – 2020. – Vol. 71. – P. 102727.

[10] Shahab, B. Improving graduation rate estimates using regularly updating multi-level absorbing markov chains / B. Shahab, A. E. Vela. – DOI: 10.3390/educsci10120377 // Education Sciences. – 2020. – Vol. 10 (12). – P. 377-1–377-18.

[11] Магазев, А. А. Исследование одной марковской модели угроз безопасности компьютерных систем / А. А. Магазев, В. Ф. Цырульник. – DOI: 10.18255/1818-1015-2017-4-445-458 // Моделирование и анализ информационных систем. – 2017. – Т. 24, № 4. – С. 445–458.

[12] Yunxiao, Z. Optimization-Time Analysis for Cybersecurity / Z. Yunxiao, P. Malacaria. – DOI:10.1109/TDSC.2021.3055981 // IEEE Transactions on Dependable and Secure Computing. – 2021. – February – URL: https://qmro.qmul.ac.uk/xmlui/handle/123456789/74641 (дата обращения: 05.12.2021).

дискретным временем, ассоциированных с моделями отражения последовательных атак на компьютерные системы.

2. Предложен метод аналитической оценки вероятностно-временных характеристик поглощающих марковских моделей атак с непрерывным временем, основанный на вычислении собственных векторов и собственных чисел матрицы интенсивностей.

3. На основе исследованных марковских моделей атак с дискретным и непрерывным временем, сформулирован ряд однокритериальных оптимизационных задач о поиске оптимальной конфигурации средств защиты информации.

4. Разработан эффективный алгоритм решения задачи о выборе оптимальной конфигурации средств защиты в случае одной атаки, максимизирующей среднее время до отказа безопасности при имеющихся ограничениях на стоимость. Оценить вычислительную сложность этого алгоритма.

5. Разработаны библиотеки подпрограмм, реализующие алгоритмы для вычисления количественных показателей эффективности и оптимизации систем защиты информации на основе марковских моделей атак.

Научная новизна работы состоит в следующем.

1. Для базовой модели атак с дискретным временем, предложенной А. П. Росенко, впервые получены явные аналитические формулы для вероятностей состояний соответствующей марковской цепи.

2. На основе параметра, называемого *временем релаксации* системы, сформулировано понятие *допустимой области* параметров защиты и доказана теорема, в которой приводится явная математическая конструкция этой области.

3. Для дискретной модели последовательных атак впервые исследовано распределение случайной величины, называемой *временем до отказа безопасности*; получены явные аналитические формулы для вычисления начальных моментов этой величины.

4. Показано, что базовая марковская модель А. П. Росенко может быть *расширена* на случай совместных атак. Для данной расширенной модели впервые получены явные аналитические формулы для математического ожидания и дисперсии времени до отказа безопасности.

5. Для марковской модели с дискретным временем, в которой атаки представляются *зависимыми* случайными событиями, разработана *теория возмущений* первого порядка, позволяющая приближённо вычислять основные вероятностно-временные характеристики системы.

6. Разработан алгоритм оценки числовых характеристик времени до отказа безопасности для марковской модели атак с непрерывным временем, основанный на вычислении собственных векторов матрицы интенсивностей.

7. На основе исследованных моделей атак сформулированы две задачи о выборе оптимальной конфигурации средств защиты, принадлежащие классу задач нелинейного дискретного программирования. Предложен эффективный алгоритм

решения одной из этих задач в случае одной атаки. Проведена оценка вычислительной сложности данного алгоритма.

Теоретическая и практическая значимость работы. Результаты исследований вносят вклад в развитие методов и моделей теории марковских процессов, применяемых при разработке, проектировании и эксплуатации систем защиты информации. Базовая стохастическая марковская модель А. П. Росенко с дискретным временем обобщена на случай совместных и/или зависимых атак. Методы вычисления количественных характеристик моделей типа «атака – отражение», ассоциированных с поглощающими марковскими цепями, разработаны преимущественно в аналитической форме для произвольных значений входных параметров модели, определяющих размерность задачи. Важным теоретическим результатом являются *явные аналитические формулы* для среднего времени до отказа безопасности, которые позволяют осуществлять оценку этой величины без использования численных алгоритмов или методов имитационного моделирования. Разработанный метод нахождения оптимального набора средств защиты информации, основанный на максимизации среднего времени до отказа безопасности при ограничении на стоимость, позволяет находить требуемую оптимальную конфигурацию за полиномиальное время.

Результаты диссертационной работы могут быть использованы на практике в задачах проектирования систем защиты информации. Предложенные в диссертации методы и модели позволяют повысить эффективность функционирования таких систем при одновременном снижении затрат на их эксплуатацию. Разработанный программный комплекс помогает эффективно решать задачи исследования и оптимизации систем кибербезопасности, функционирующих в условиях постоянно возрастающего числа атак. Разработанные методы и алгоритмы могут применяться и для решения задач в других областях, в которых актуальны модели поглощающих марковских цепей с непрерывным или дискретным временем: в экономике, теории сетей, образовании, задачах анализа изображений.

Для решения поставленных задач были разработаны библиотеки подпрограмм, реализующие разработанные методы и алгоритмы. Эти библиотеки были внедрены в практическую деятельность следующих организаций:

- ООО «Инновационные ВЕБ-технологии» (для поиска оптимальной конфигурации средств защиты информации в составе информационной (автоматизированной) системы с целью повышения эффективности системы защиты информации), г. Омск;
- ФГАОУ ВО «ОмГТУ» при подготовке бакалавров по направлению 10.03.01 «Информационная безопасность», специалистов по направлению 10.05.05 «Безопасность информационных технологий в правоохранительной сфере» и при подготовке магистров по направлению 09.04.01 «Информатика и вычислительная техника» при чтении курсов: «Модели компьютерной безопасности», «Теория информационно безопасности и методология защиты информации», «Аудит информационной безопасности», «Экономика защиты информации».

Объектом исследования являются компьютерные системы, имеющие средства и механизмы защиты и подвергающиеся внешним атакам.

Предметом исследования являются математические модели, методы и алгоритмы, предназначенные для количественной оценки эффективности и оптимизации систем защиты информации.

Методология и методы исследования. Применяются стандартные математические методы исследования марковских процессов, включающие в себя метод производящей функции, метод рекуррентных последовательностей, метод Лапласа и метод собственных векторов и собственных чисел (для решения уравнений Колмогорова). Для решения задач оптимизации используется метод динамического программирования.

Положения, выносимые на защиту:

1. Точные и приближённые аналитические методы получения количественных оценок для основных вероятностно-временных характеристик марковских цепей с дискретным временем, ассоциированных с моделями отражения атак на компьютерные системы.
2. Точный метод аналитической оценки вероятностно-временных характеристик марковских цепей с непрерывным временем, основанный на вычислении собственных векторов и собственных чисел матрицы интенсивностей.
3. Эффективный алгоритм решения задачи о выборе оптимальной конфигурации средств защиты в случае одной атаки, максимизирующей среднее время до отказа безопасности при имеющихся ограничениях на стоимость.
4. Библиотеки подпрограмм, реализующие алгоритмы для вычисления количественных показателей эффективности и оптимизации систем защиты информации на основе марковских моделей атак.

Степень достоверности полученных результатов. Достоверность результатов подтверждается математически корректными выводами и доказательствами утверждений и теорем, представленных в работе, согласованностью полученных аналитических результатов с результатами имитационного моделирования для различных стохастических марковских моделей, описанных в диссертационной работе. Имитационное моделирование проводилось с использованием стандартных математических пакетов и программ, а также с применением разработанных в рамках диссертационной работы программными библиотеками и пакетами расширений.

Апробация результатов исследования. Основные положения и результаты диссертации докладывались и обсуждались на следующих научных конференциях: IV Международная конференция и молодая школа «Информационные технологии и нанотехнологии», Самара, 2018; IX Международная молодежная научно-практическая конференция с элементами научной школы «Прикладная математика и фундаментальная информатика», Омск, 2019; «Динамика систем, механизмов и машин», Омск, 2019; VI Международная конференция и молодая школа «Информационные технологии и нанотехнологии», Самара, 2020; IX

Международная научная конференция «Математическое и компьютерное моделирование», посвященная 85-летию профессора В. И. Потапова, Омск, 2021.

Соответствие паспорту научной специальности. Работа соответствует паспорту научной специальности 05.13.18 по следующим пунктам: п. 2 − Развитие качественных и приближенных аналитических методов исследования математических моделей; по п. 3 − Разработка, обоснование и тестирование эффективных вычислительных методов с применением современных компьютерных технологий; по п. 4 − Реализация эффективных численных методов и алгоритмов в виде комплексов проблемно-ориентированных программ для проведения вычислительного эксперимента.

Публикации. Основные результаты диссертационного исследования изложены в 16 работах, среди которых 3 статьи в журналах, включенных в «Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук», 5 статей, проиндексированных международными системами цитирования Web of Science/Scopus, 2 свидетельства о регистрации электронных ресурсов, 8 работ, опубликованных в сборниках материалов конференций.

Личный вклад автора. Представленные в диссертационном исследовании и выносимые на защиту аналитические методы получения количественных оценок для вероятностно-временных характеристик марковских моделей атак, эффективный алгоритм решения задачи о выборе оптимальной конфигурации средств защиты в случае одной атаки и библиотеки подпрограмм, которые реализуют эти методы и алгоритмы, принадлежат лично автору диссертации.

Связь работы с научными программами. В основу диссертационной работы положены результаты научных исследований, выполненных в Омской государственном техническом университете по теме «Оценка эффективности и оптимизация систем защиты информации с использованием стохастических марковских моделей» в рамках гранта РФФИ №19-37-90122.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, списка используемых источников и 4 приложений. Объем диссертации с приложениями составляет 170 страниц, без приложений – 152 страниц. Диссертация содержит 7 таблиц и 28 рисунка. Список литературы включает 82 наименования.

В приложениях приводятся листинги кодов библиотек подпрограмм, свидетельства о государственной регистрации программ для ЭВМ, акты внедрения результатов диссертации.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность диссертационного исследования, сформулированы цели и задачи диссертационной работы, приведена новизна

работы, представлены теоретическая и практическая значимость, представлены основные положения, выносимые на защиту, описана структура диссертации.

В первой главе приводится описание базовой марковской модели атак с дискретным временем, которая была предложена А. П. Росенко. Это описание представлено в **разделе 1.1**. Рассматривается компьютерная система (далее просто система), подверженная воздействию n различных *независимых* атак A_i с вероятностями q_i. Любые изменения в системе происходят в дискретные моменты времени. Согласно предположениям модели, в каждый момент t система может быть подвержена *только одной атаке*, то есть одновременное воздействие двух и более атак невозможно. Если в момент времени t система подверглась воздействию i-ой атаки A_i, в следующий момент $t+1$ эта атака может быть либо отражена, либо, наоборот, успешно реализована. В последнем случае моделирование завершается и соответствующее событие называется *отказом безопасности*. Для количественной оценки эффективности защитных механизмов системы вводится набор обобщенных показателей $r_1, r_2, \dots, r_n$, где r_i – вероятность успешного отражения i-ой атаки.

В соответствии с вышесказанным, в каждый момент времени t система может находиться в одном из следующих состояний: $s_0, s_1, \dots, s_n, s_{n+1}$. Состояние s_0, называемое *безопасным*, означает отсутствие атак. Состояние s_i, где $i = 1, 2, \dots, n$, означает возникновение i-ой атаки, то есть появление события A_i. В следующий момент времени может реализоваться одна из двух возможностей: либо система возвращается в безопасное состояние s_0 после успешного отражения i-ой атаки с вероятностью r_i, либо с вероятностью $\overline{r_i} = 1 - r_i$ система переходит в состояние s_{n+1}, что приведёт к событию «отказ безопасности».

Иллюстрация возможных переходов между состояниями системы приведена на графе, изображённом на рисунке 1.

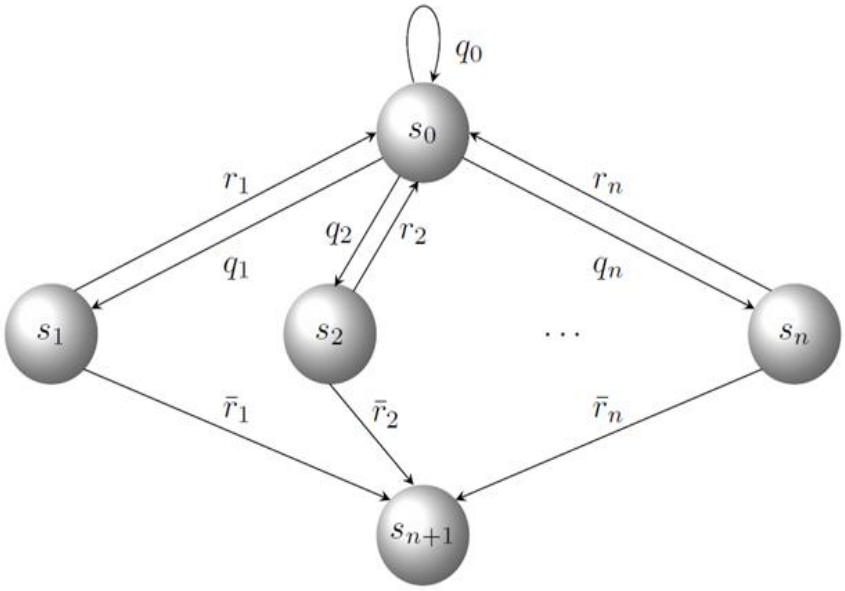

Рисунок 1 − Граф переходов между состояниями системы

В **разделе 1.2** проведено детальное аналитическое исследование данной модели. В предположении, что в начальный момент времени система находилась в безопасном состоянии s_0, были получены явные аналитические формулы для вероятностей состояний системы в произвольный момент времени $t > 0$:

$$p_0(t) = w^{-1}\left[\left(\frac{q_0 + w}{2}\right)^{t+1} - \left(\frac{q_0 - w}{2}\right)^{t+1}\right],$$
$$p_i(t) = p_0(t-1)q_i, \qquad i = 1,2,\dots,n,$$
$$p_{n+1}(t) = 1 - p_0(t) - p_0(t-1)\sum_{i=1}^{n} q_i,$$

где положительный параметр w определяется как $w^2 = q_0^2 + 4\sum_{i=1}^{n} r_i q_i$.

В **разделе 1.3** для количественной оценки длительности безотказного функционирования системы вводится понятие *времени релаксации* − времени τ, за которое вероятность состояния безопасности системы уменьшится в два раза, по отношению к моменту времени $t = 0$:

$$\tau = \log_{\frac{q_0+w}{2}}\left(\frac{w}{2}\right) - 1.$$

На основе этой величины сформулировано понятие *допустимой области* параметров защиты – области $R_{t_0}(q_1,\dots,q_n) \subset \mathbb{R}_+^n$ значений параметров $r_1, r_2, \dots, r_n$ (при фиксированных $q_1, q_2, \dots, q_n$), для которых выполняется условие $\tau \geq t_0$. В диссертации доказана теорема, в которой приводится явная математическая конструкция этой области.

ТЕОРЕМА 1. *Пусть $q_1, q_2, \dots, q_n$ – заданный набор вероятностей атак, такой, что $0 < q_0 = 1 - \sum_{i=1}^{n} q_i < 1$, и пусть $t_0 \geq 4$ – целое положительное число. Тогда допустимая область $R_{t_0}(q_1,\dots,q_n)$ параметров защиты системы имеет вид*

$$R_{t_0}(q_1,\dots,q_n) = \left\{(r_1, r_2, \dots, r_n) \in \mathbb{R}^n \ : \sum_{k=1}^{n} q_k r_k \geq \lambda(\lambda - q_0) \text{ и } 0 \leq r_i \leq 1\,,\ i = 1,2,\dots,n\right\},$$

где $\lambda = q_0$, если ${q_0}^{t_0} > 1/2$, и λ – единственный корень многочлена $f(x) = x^{t_0+1} - x + q_0/2$ из отрезка $[q_0, 1]$, если ${q_0}^{t_0} \leq 1/2$.

В качестве еще одного количественного показателя длительности безотказного функционирования системы в **разделе 1.4** рассмотрено понятие *времени до отказа безопасности T* – времени, за которое система, находясь в момент $t = 0$ в безопасном состоянии s_0, впервые перейдет в состояние отказа безопасности s_{n+1}. Определённая таким образом характеристика системы является

дискретной случайной величиной, которая принимает целые значения: $T = 2, 3, 4, \ldots$. В диссертации был получен явный вид вероятностного распределения этой случайной величины:

$$P(T) = w^{-1}\left[\left(\frac{q_0 + w}{2}\right)^{T-1} - \left(\frac{q_0 - w}{2}\right)^{T-1}\right]\sum_{i=1}^{n} q_i \bar{r}_i\,, \qquad T = 2, 3, 4, \ldots. \tag{1}$$

На рисунке 2 приведена иллюстрация распределения (1) для случая трех атак со значениями параметров $q_1 = 0.05,\ q_2 = 0.10,\ q_3 = 0.25,\ q_4 = 0.18,\ q_5 = 0.35$ и $r_1 = 0.87, r_2 = 0.90, r_3 = 0.88, r_4 = 0.83, r_5 = 0.95$.

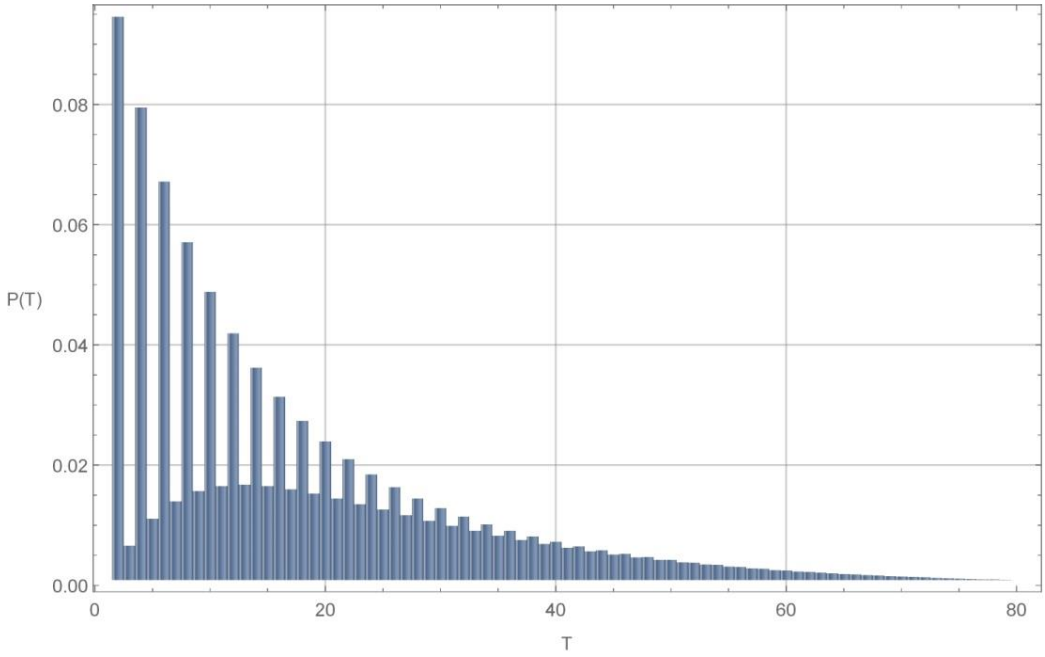

Рисунок 2 − Пример распределения $\boldsymbol{P(T)}$ для случая трех атак

С использованием распределения (1) были выведены формулы для определения *k-ых начальных моментов* $\mu_k[T]$ *времени до отказа безопасности* T:

$$\mu_k[T] = w^{-1}\left[\frac{2}{q_0 + w}\, S_k\left(\frac{q_0 + w}{2}\right) - \frac{2}{q_0 - w}\, S_k\left(\frac{q_0 - w}{2}\right)\right]\sum_{i=1}^{n} q_i \bar{r}_i,$$

где $S_k(x) \equiv \left(x\frac{d}{dx}\right)^k \frac{1}{1-x}$. В частности, математическое ожидание τ и дисперсия D этой случайной величины равны:

$$\tau = \frac{1 + \sum_{i=1}^{n} q_i}{\sum_{i=1}^{n} q_i(1 - r_i)},$$

$$D = \frac{1 - \sum_{i=1}^{n} q_i + \sum_{i=1}^{n} q_i r_i (3 + \sum_{j=1}^{n} q_j)}{[\sum_{i=1}^{n} q_i(1 - r_i)]^2}.$$

В **разделе 1.5** проведено обобщение базовой марковской модели А. П. Росенко на случай одновременного воздействия на систему сразу нескольких атак (выбранных из данного набора n возможных). Совместное появление таких атак описывается n-мерным булевым вектором $\mathbf{x} = (x_1, x_2, \dots, x_n)$. Считая, что атаки возникают независимо друг от друга, вероятность $Q_{\mathbf{x}}$ перехода системы из состояния s_0 в состояние $s_{\mathbf{x}}$ будет равна

$$Q_{\mathbf{x}} = \prod_{i=1}^{n} [x_i q_i + (1 - x_i)(1 - q_i)].$$

Если в момент t система находилась в состоянии $s_{\mathbf{x}} \neq s_0$, тогда, в момент времени $t + 1$ возможны два варианта исхода:

1) все атаки отражены и система возвращается в безопасное состояние s_0;

2) какая-либо из атак успешно реализовалась и система переходит в состояние отказа безопасности s_f. Вероятности двух таких переходов равны, соответственно:

$$R_{\mathbf{x}} = \prod_{i=1}^{n} [x_i(r_i - 1) + 1], \qquad \bar{R}_{\mathbf{x}} = 1 - R_{\boldsymbol{x}},$$

где параметр r_i, как и ранее, означает вероятность успешного отражения i-ой атаки, $i = 1,2, \dots, n$.

Переходная матрица соответствующей марковской цепи получается из переходной матрицы базовой модели А. П. Росенко формальной заменой:

$$n \to 2^n - 1, \quad q_i \to Q_i, \quad r_i \to R_i.$$

Таким образом, никаких качественных отличий базовой марковской модели от данной обобщённой модели нет; это позволяет без каких-либо усилий перенести все полученные выше результаты на настоящий случай. В частности, в рамках данного обобщения были получены явные аналитические формулы для среднего времени до отказа безопасности и её дисперсии в случае совместных атак:

$$\tau = \frac{1 + \sum_{\mathbf{x} \neq 0} Q_{\mathbf{x}}}{\sum_{\mathbf{x} \neq 0} Q_{\mathbf{x}}(1 - R_{\mathbf{x}})},$$

$$D = \frac{1 - \sum_{\mathbf{x} \neq 0} Q_{\mathbf{x}} + \sum_{\mathbf{x} \neq 0} Q_{\mathbf{x}} R_{\mathbf{x}} (3 + \sum_{\mathbf{x} \neq 0} Q_{\mathbf{x}'})}{[\sum_{\mathbf{x} \neq 0} Q_{\mathbf{x}}(1 - R_{\mathbf{x}})]^2}.$$

Была осуществлена проверка этих формул с помощью проведения имитационного моделирования.

Практика информационной безопасности показывает, что иногда возникновение одной атаки влечёт за собой возможность появления другой. В **разделе 1.6** исследована еще одна возможность обобщения описанных выше марковских моделей атак, в которых предполагаются возможными переходы между состояниями s_i, ассоциированными с кибератаками, $i = 1, 2, \dots, n$. В рамках

данного обобщения была разработана соответствующая теория возмущений (первого порядка). Предполагая, что переходы между состояниями s_i являются *редкими* случайными событиями, для вероятностей соответствующих переходов имеем:

$$\epsilon_{ij} \ll 1 \text{ для всех } i,j = 1,\dots,n.$$

С учетом данного требования были получены приближённые выражения для вероятностей состояний системы (в первом порядке по ϵ_{ij}):

$$p_0(t) \approx \frac{1}{w}\left(\frac{q_0+w}{2}\right)^{t+1} - \frac{1}{w}\left(\frac{q_0-w}{2}\right)^{t+1} + \\ + \left[\frac{t}{w^2}\left(\frac{q_0+w}{2}\right)^{t-1} + \frac{t}{w^2}\left(\frac{q_0-w}{2}\right)^{t-1} - \frac{2}{w^3}\left(\frac{q_0+w}{2}\right)^{t} + \right. \\ \left. + \frac{2}{w^3}\left(\frac{q_0-w}{2}\right)^{t}\right]\sum_{i=1}^{n}\sum_{j=1}^{n} q_i r_j \epsilon_{ij}\,.$$

$$p_i(t) \approx p_0(t-1)q_i + p_0(t-2)\sum_{j=1}^{n} q_j \epsilon_{ji}\,, \quad i = 1,\dots,n;$$

$$p_{n+1}(t) \approx 1 - \sum_{i=0}^{n} p_i(t).$$

Также было получено приближенное выражение для среднего времени до отказа безопасности в первом порядке теории возмущений. В конце раздела рассмотрено несколько примеров, иллюстрирующих применимость теории возмущений.

Во второй главе была рассмотрена марковская модель атак с непрерывным временем. В **разделе 2.1** приведено описание положений этой модели:

1. Последовательность моментов появления i-ой кибератаки представляет собой простейший пуассоновский поток событий с интенсивностью $\lambda_i > 0$.

2. После появления i-ой атаки последовательность моментов «активизации» ответных действий со стороны защитных механизмов системы также представляет собой простейший пуассоновский поток с интенсивностью $\mu_i > 0$. Вероятность успешного отражения i-ой атаки обозначим через r_i, а вероятность неуспешного – через $\bar{r}_i = 1 - r_i$.

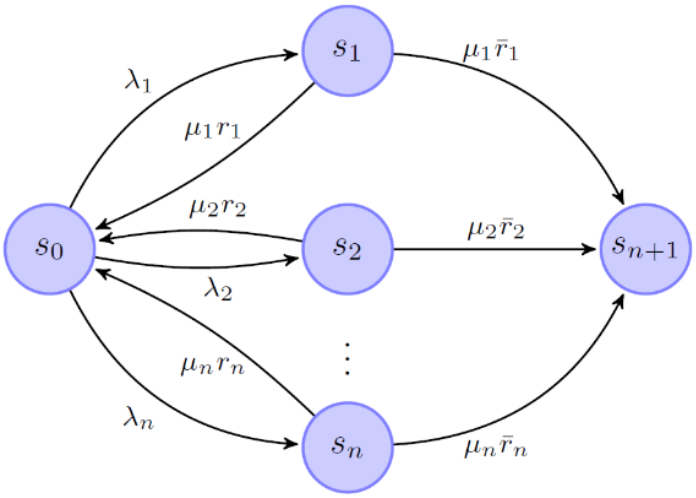

Рисунок 3 – Граф состояний системы

Состояния марковской модели с непрерывным временем имеют идентичную интерпретацию состояний марковской модели атак с дискретным врменем. Динамика переходов системы иллюстрируется в виде графа перехода вида, изображенного на рисунке 3.

В **разделе 2.1** также приведены уравнения Колмогорова, описывающие динамику данной модели. В матрично-векторной нотации эти уравнения имеют вид:

$$\frac{d\mathbf{p}(t)}{dt} = \mathbf{p}(t) \cdot \Pi, \tag{2}$$

где $\mathbf{p}(t) = (p_0(t), p_1(t), \dots, p_{n+1}(t))$ – вектор-строка вероятностей состояний системы в момент времени t, Π – квадратная матрица порядка $n+2$:

$$\Pi = \begin{pmatrix} -\lambda_0 & \lambda_1 & \lambda_2 & \dots & \lambda_n & 0 \\ \mu_1 r_1 & -\mu_1 & 0 & \dots & 0 & \mu_1\bar{r}_1 \\ \mu_2 r_2 & 0 & -\mu_2 & \dots & 0 & \mu_2\bar{r}_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \mu_n r_n & 0 & 0 & \dots & -\mu_n & \mu_n\bar{r}_n \\ 0 & 0 & 0 & \dots & \dots & 0 \end{pmatrix}. \tag{3}$$

В качестве начальных условий задачи выступают требования:

$$p_0(0) = 1, \qquad p_1(0) = p_2(0) = \dots = p_{n+1}(0) = 0.$$

В **разделе 2.2** рассмотрен метод решения системы дифференциальных уравнений Колмогорова (2) с помощью преобразования Лапласа. Для наших целей, однако, более удобным является метод, основанный на вычислении собственных векторов и собственных чисел матрицы (3). Этот метод описан в **разделе 2.3**. Предварительно доказана следующая теорема.

ТЕОРЕМА 2. *Все собственные числа матрицы* (3) *вещественны и принадлежат отрезку* $[-2\gamma, 0]$, *где* $\gamma = \max\{\lambda_0, \mu_1, \dots, \mu_n\}$.

Учитывая структуру спектра матрицы (3), решение системы уравнений Колмогорова имеет вид:

$$\mathbf{p}(t) = \sum_{\nu=0}^{n+1} \mathbf{c}_\nu e^{\sigma_\nu t} = \mathbf{c}_0 + \mathbf{c}_1 e^{\sigma_1 t} + \cdots + \mathbf{c}_{n+1} e^{\sigma_{n+1} t}.$$

где $\mathbf{c}_\nu$ – собственный вектор матрицы интенсивностей П, отвечающий собственному числу σ_ν. При этом собственные векторы нормированы условием $\sum_{\nu=0}^{n+1} \mathbf{c}_\nu = \mathbf{e}_0$.

В **разделе 2.4** по аналогии с марковской моделью атак с дискретным временем был введен и исследован показатель оценки эффективности систем защиты информации, называемый *временем до отказа безопасности*. Это – время $T \in [0, +\infty)$ прошедшее с момента $t = 0$, когда система находилась в безопасном состоянии s_0, до момента первого попадания системы в состояние отказа безопасности s_{n+1}. Оно является непрерывной случайной величиной, для которой нами была получена формула для вычисления соответствующей плотности распределения $f_T(t)$:

$$f_T(t) = \sum_{v=1}^{n+1} c_{v,n+1} \sigma_v e^{\sigma_v t}.$$

Кроме того, вычислены начальные моменты этой случайной величины в терминах собственных чисел и собственных векторов матрицы П:

$$\mu_k[T] = -k! \sum_{v=1}^{n+1} \frac{c_{v,n+1}}{|\sigma_v|^k},$$

где $c_{v,n+1}$ – $(n+1)$-ая компонента собственного вектора $\mathbf{c}_v$ матрицы (3), который соответствует собственному числу σ_v. В частности, математическое ожидание $\tau \equiv \mu_1[T]$ случайной величины T (среднее время до отказа безопасности) вычисляется по формуле:

$$\tau = -\sum_{v=1}^{n+1} \frac{c_{v,n+1}}{|\sigma_v|}.$$

В конце раздела приведен пошаговый алгоритм нахождения среднего времени до отказа безопасности.

В **разделе 2.5** приводятся результаты сравнения полученных аналитических результатов с результатами имитационного моделирования.

На современном IT-рынке имеется немалое количество решений для обеспечения кибербезопасности, что делает задачу их выбора довольно нетривиальной. Ситуация здесь осложняется ещё и тем, что для противодействия одной и той же атаке может использоваться несколько отличных друг от друга средств или механизмов защиты, выпускаемых различными производителями. Таким образом, на практике часто возникает задача выбора некоторого набора средств защиты, оптимального с той или иной точки зрения.

В **третьей главе** исследуются оптимизационные задачи, связанные с выбором оптимального набора средств защиты от атак. Эти задачи формулируются с привлечением марковских моделей атак, описанных нами выше.

В **разделе 3.1** выделены две основные характеристики систем защиты информации, играющие важную роль на практике: среднее время до отказа безопасности τ и стоимость используемых средств и механизмов защиты c. Используя эти характеристики мы сформулировали две оптимизационные задачи:

1. Минимизация затрат на кибербезопасность c при ограничении снизу на среднее время до отказа безопасности τ (*первая оптимизационная задача*):

$$c \to \min, \;\; \tau \geq t_0.$$

2. Максимизация среднего времени до отказа безопасности τ при ограничении сверху затрат на кибербезопасность c (*вторая оптимизационная задача*):

$$\tau \to \max, \;\; c \leq c_0.$$

Для описания возможных наборов средств защиты используется векторная булева нотация:

$$\mathbf{z} = (z_1, z_2, \dots, z_m) \in \{0,1\}^m.$$

Здесь $z_a = 0$, если a-ое средство не используется, и $z_a = 1$ − в обратном случае. Обозначим через $r_{i,a}$ вероятность, с которой a-ое средство защиты отражает i-ую атаку. Тогда вероятность отражения i-ой атаки *хотя бы одним* средством кибербезопасности определяется в соответствии с формулой вероятности для суммы совместных случайных событий:

$$r_i(\mathbf{z}) = 1 - \prod_{a=1}^{m} \left(1 - r_{i,a} z_a\right), \;\; i = 1,..n.$$

Таким образом, параметры защиты $r_i(\mathbf{z})$, используемые в марковских моделях атак, становятся функциями от $\mathbf{z}$. То же самое касается и среднего времени до отказа безопасности, так как оно зависит от параметров защиты. Важно отметить нелинейный характер функции $\tau(\mathbf{z})$, в результате чего сформулированные выше оптимизационные задачи будут относиться к классу задач *нелинейной булевой оптимизации*.

В **разделе 3.2** предложен алгоритм решения второй оптимизационной задачи в случае одной атаки:

$$\tau(\mathbf{z}) = \frac{1+q}{q} \cdot \frac{1}{\prod_{a=1}^{m}(1-r_a z_a)} \to \max, \quad \sum_{a=1}^{m} c_a z_a \le c_0.$$

В диссертации было показано, что эта задача сводится к эквивалентной *сепарабельной* задаче нелинейного булева программирования с тем же ограничением, но с новой целевой функцией:

$$f(\mathbf{z}) = \sum_{a=1}^{m} f_a(z_a) = -\sum_{a=1}^{m} \ln(1-r_a z_a) \to \max, \quad \sum_{a=1}^{m} c_a z_a \le c_0.$$

Для решения последней, нами был разработан эффективный алгоритм, основанный на применении концепции *динамического программирования*. Алгоритм сводится к последовательному рекуррентному решению вспомогательных оптимизационных задач:

$$\Lambda_a(\rho) = \max_{z_a \in \{0,1\}} [f_a(z_a) + \Lambda_{a-1}(\rho - c_a z_a)], \qquad a = 1,2,\dots,m.$$

Здесь ρ – параметр вспомогательных задач, принимающий целые значения от 0 до c_0. Нами также была оценена эффективность разработанного алгоритма. В случае, когда $c_a = 1$ для всех a, число требуемых операций равно:

$$N_{\text{дин}}(m, c_0) = c_0 \left[m + \frac{(m-1)(c_0+1)}{2} \right] + m.$$

Как видно, это число линейно по m и кадратично по c_0.

В **разделе 3.3** анализируется возможность применения разработанного нами алгоритма для случая одной атаки к решению общей задачи для произвольного числа атак. Хотя общая задача и не сводится к сепарабельной, изложенный выше алгоритм может быть полезен и в этой ситуации. В частности, в диссертации получена интервальная оценка для искомого значения целевой функции для произвольного числа атак:

$$\sum_{i=1}^{n} q_i g_i(\mathbf{z}_i^*) \le g(\mathbf{z}^*) \le \min_{1 \le i \le n} \{g(\mathbf{z}_i^*)\}.$$

То есть, решив n вспомогательных оптимизационных задач с одной атакой, мы можем оценить числовой интервал, которому будет принадлежать значение целевой функции в общем случае. Данная оценка, в свою очередь, может служить для дополнительных эвристических соображений, позволяющих привлечь иные эффективные методы и алгоритмы оптимизации.

В **четвертой главе** описаны разработанные в рамках диссертационного исследования две библиотеки подпрограмм, реализующие основные методы и алгоритмы исследования описанных выше марковских моделей атак.

В **разделе 4.1** подробно рассматривается разработанный нами пакет расширения MMInfoSec для системы символьных вычислений Wolfram Mathematica. В этом пакете реализовано 9 подпрограмм для исследования марковской модели атак с дискретным временем.

В **разделе 4.2** представлено описание статической библиотеки MarkovAttackModel, написанной на языке программирования C++. В этой библиотеке присутствует специальный класс для работы с дискретными марковскими моделями атак, а также содержится функция для решения второй оптимизационной задачи в случае одной атаки.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

В данной работе были получены следующие основные результаты:

− получены явные аналитические формулы для определения вероятностей соответствующей марковской цепи в произвольный момент времени t;

− на основе параметра, называемого временем релаксации системы, сформулировано понятие допустимой области параметров защиты и доказана теорема, в которой приводится явная математическая конструкция этой области;

− исследовано распределение случайной величины, называемой временем до отказа безопасности; получены явные аналитические формулы для вычисления начальных моментов этой величины;

− показано, что базовая марковская модель А. П. Росенко может быть расширена на случай совместных атак, для которой затем получены явные аналитические формулы для математического ожидания и дисперсии времени до отказа безопасности;

− для марковской модели с дискретным временем, в которой атаки представляются зависимыми случайными событиями, разработана теория возмущений первого порядка, позволяющая приближённо вычислять основные вероятностно-временные характеристики системы;

− предложен алгоритм оценки числовых характеристик времени до отказа безопасности с помощью метода собственных векторов и собственных чисел матрицы интенсивностей;

− вычислены k-ые начальные моменты времени до отказа безопасности; в частности, получена явная аналитическая формула для математического ожидания времени до отказа безопасности;

− проведена оценка адекватности полученных аналитических результатов с помощью сравнения с результатами численных экспериментов на основе имитационного моделирования;

− сформулированы две однокритериальные оптимизационные задачи о поиске оптимальной конфигурации средств защиты, одна из которых была сведена

к эквивалентной сепарабельной задаче и решена с помощью эффективного алгоритма, основанного на концепции динамического программирования;

− разработаны две библиотеки подпрограмм, реализующие алгоритмы для вычисления количественных показателей эффективности и оптимизации систем защиты информации на основе марковских моделей атак.

Предложенные в работе методы и алгоритмы позволяют решить ряд важных задач в области информационной безопасности, в частности, проблему количественной оценки длительности безотказного функционирования компьютерных систем, а также задачу оптимизации систем защиты информации. Необходимо также отметить, что разработанные в диссертационной работе численно-аналитические методы и алгоритмы исследования марковских цепей с поглощающими состояниями также могут быть применены и к задачам из других областей знаний, в которых применяются аналогичные марковские модели. Такие модели, например, широко используются в экономике, образовании, теории сетей и анализе изображений.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИОННОЙ РАБОТЫ

а) Научные публикации в изданиях из перечня, рекомендованного ВАК:

1. Магазев, А. А. Исследование одной марковской модели угроз безопасности компьютерных систем / А. А. Магазев, **В. Ф. Цырульник**. – DOI: 10.18255/1818-1015-2017-4-445-458 // Моделирование и анализ информационных систем. – 2017. – Т. 24, № 4. – С. 445–458;

(Переводная версия WoS) Magazev, A. A. Investigation of a Markov model for computer system security threats / A. A. Magazev, **V. F. Tsyrulnik**. − DOI:10.18255/1818-1015-2017-4-445-458 //Automatic Control and Computer Sciences. – 2018. – Vol. 52. – P. 615–624.

2. Касенов, А. А. Марковская модель совместных киберугроз и ее применение для выбора оптимального набора средств защиты информации / А. А. Касенов, А. А. Магазев, **В. Ф. Цырульник**. – DOI: 10.18255/1818-1015-2020-1-108-123 // Моделирование и анализ информационных систем. – 2020. – Т. 27, № 1. – С. 108–123.

(Переводная версия WoS) Kassenov, A. A. Markov Model of Nonmutually Exclusive Cyberthreats and Its Applications for Selecting an Optimal Set of Information Security Tools / A. A. Kassenov, A. A. Magazev, **V. F. Tsyrulnik**. − DOI: 10.18255/1818-1015-2020-1-108-123 //Automatic Control and Computer Sciences. – 2018. – Vol. 52. – P. 615–624.

3. Магазев, А. А. Оценка среднего времени до отказа безопасности на основе марковских цепей с непрерывным временем / А. А. Магазев, А. С. Мельникова, **В. Ф. Цырульник**. – DOI: 10.24147/2222-8772.2020.4.112-125 // Математические структуры и моделирование. – 2020. – № 4 (56). – С. 112–125.

б) Научные публикации, включенные в международную систему цитирования Scopus:

4. Magazev, A. A. Optimizing the selection of information security remedies in terms of a Markov security model / A. A. Magazev, **V. F. Tsyrulnik**. – DOI: 10.1088/1742-6596/1096/1/012160 // Journal of Physics Conference Series. – 2018. – Vol. 1096. – P. 012160-1–012160-8.

5. A Markov model for optimization of information security remedies / A. A. Kasenov, E. F. Kustov, A. A. Magazev, **V. F. Tsyrulnik**. – DOI: 10.1088/1742-6596/1441/1/012043 // Journal of Physics: Conference Series. – Vol. 1441. – P. 012043-1–012043-8).

6. Magazev, A. A. On small perturbations of Markov cyber threat models / A. A. Magazev, **V. F. Tsyrulnik**. – DOI: 10.1088/1742-6596/1745/1/012111 // Journal of Physics Conference Series. – 2021. – Vol. 1745. – P. 012111-1–012111-9.

в) Научные публикации в других изданиях:

7. Магазев, А. А. Об оценке времени релаксации одной марковской модели безопасности / А. А. Магазев, **В. Ф. Цырульник** // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации : сб. ст. победителей Междунар. науч.-практ. конф. (Пенза, 15 дек. 2016 г.). – Пенза : Наука и Просвещение 2016. – С. 26–30.

8. Магазев, А. А. Оценка влияния угроз на вероятность безопасного состояния в рамках простейшей марковской модели безопасности / А. А. Магазев, **В. Ф. Цырульник** // Инновационные технологии научного развития : сб. ст. Междунар. науч.-практ. конф. (Казань, 20 окт. 2016 г.) : в 3 ч. – Уфа : Аэтерна , 2016. – Ч. 3. – С. 9–3.

9. Магазев, А. А. Оптимизация выбора средств защиты информации в рамках одной марковской модели безопасности / А. А. Магазев, **В. Ф. Цырульник** // Информационные технологии и нанотехнологии : сб. тр. IV Междун. конф. и молодеж. шк. (Самара, 24–27 апр. 2018 г.). – Самара : Новая техника, 2018. – С. 2050–2058.

10. Магазев, А. А. Применение одной марковской модели безопасности для повышения надежности и выбора оптимальной конфигурации средств защиты информации / А. А. Магазев, **В. Ф. Цырульник**. – DOI: 10.25206/2311-4908-2019-6-1-25-32 // Прикладная информатика и фундаментальная информатика. – 2019. – Т. 6, № 1. – С. 25–32.

11. **Горохова, В. Ф.** Оптимизация выбора средств защиты от атак с использованием поглощающих марковских цепей / В. Ф. Горохова // Системы управления, информационные технологии и математическое моделирование : сб. тр. по материалам IV Всероссийской научно-практической конференции с международным участием : в 2 т. Т. 1. – Омск : Изд-во Ом. гос. ун-та, 2022. – С. 126–134.

12. Марковская модель оптимизации средств защиты информации / А. А. Касенов, Е. Ф. Кустов, А. А. Магазев, **В. Ф. Цырульник** // Динамика систем, механизмов и машин. – 2019. – Т. 7, № 4. – С. 77–84.

13. Магазев, А. А. О малых возмущениях марковских моделей киберугроз / А. А. Магазев, **В. Ф. Цырульник** // Информационные технологии и нанотехнологии : сб. тр. по материалам VI Междунар. конф. и молодеж. шк. (Самара, 26–29 мая 2020 г.) : в 4 т. Т. 3. Математическое моделирование физико-технических процессов и систем. – Самара : Изд-во Самар. ун-та, 2020. – С. 833–842.

14. **Горохова, В. Ф.** Оптимизация средств защиты информации на основе стохастической марковской модели с непрерывным временем / В. Ф. Горохова, А. А. Магазев // Математическое и компьютерное моделирование : сб. материалов IX Междунар. науч. конф., посвящ. 85-летию проф. В. И. Потапова (Омск, 19 нояб. 2021 г.) – Омск : Изд-во Ом. гос. ун-та, 2021. – С. 292–294.

г) Свидетельства о государственной регистрации программ для ЭВМ:

15. Свидетельство о регистрации электронного ресурса № 22872 от 23.07.2017. Пакет расширения системы символьных вычислений Mathematica для исследования марковских моделей безопасности от 23.06.2017 / А. А. Магазев, **В. Ф. Цырульник** ; Ом. гос. техн. ун-т. – Москва : ОФЭРНиО. – 1 с.

16. Свидетельство о государственной регистрации программы для ЭВМ № 2022617720 Российская Федерация. Статическая библиотека для исследования марковской модели кибератак : № 2022617008 : заявл. 21.04.2022 : опубл. 25.04.2022 / **В. Ф. Горохова**, А. А. Магазев ; правообладатель Ом. гос. техн. ун-т. – 1 с.

Подписано в печать 14.07.2022. Формат 60х84 1/16. Бумага офсетная.
Отпечатано на дубликаторе. Усл. печ. л. 1,5. Уч.-изд. л. 1,5.
Тираж 100 экз. Заказ 255.

Издательство ОмГТУ. 644050, г. Омск, пр. Мира, 11; т. 23-02-12.
Типография ОмГТУ.