НАУЧНЫЙ ОБЗОР

УДК 004.62
DOI 10.17513/snt.40280

ОБЗОР СОВРЕМЕННЫХ ПОДХОДОВ К МАТЕМАТИЧЕСКОМУ МОДЕЛИРОВАНИЮ КРИПТОГРАФИЧЕСКИХ АТАК НА СТРУКТУРЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Бережной И.В., Гурский С.М., Пятин В.С.

ФГБВОУ ВО «Военно-космическая академия имени А.Ф. Можайского» Министерства обороны Российской Федерации, Санкт-Петербург, e-mail: vka@mil.ru

Цель исследования – обзор современных подходов к анализу математических моделей криптографических атак на структуры информационных технологий. Обзор источников проведён с использованием баз данных научного цитирования eLIBRARY.RU, РИНЦ, Scopus. В указанных базах найдено 588 источников, в том числе 50 источников, включённых в данное исследование. Критериями включения в этот обзор были публикации, посвящённые: разработке математического моделирования криптографических угроз и атак; влиянию вредоносного программного обеспечения; моделям теории массового обслуживания, эпидемиологическим моделям, безопасности информации; публикации на английском и русском языках. Критериями исключения были: отсутствие доступа к полным текстам статьи; дублирующие исследования, репринты, исследования на иных языках, кроме заявленных (английский и русский), письма и краткие сообщения. В статье исследуются модели теории массового обслуживания, эпидемиологические модели, поведенческие модели, а также их комбинированное применение для более точного понимания криптографических угроз. Исследование сосредоточено на наиболее часто используемых моделях для исследования атак на структуры информационных технологий и моделях, применяемых для оценки распространения вредоносного программного обеспечения. Приводится пример расчёта эффективности предложенного комплексного подхода к анализу математических моделей криптографических атак на структуры информационных технологий, его преимущества и недостатки известных подходов. Только совместное использование нескольких видов моделей позволяет компенсировать недостатки, проявляющиеся при использовании каждой из однослойных моделей по отдельности. Тем самым обеспечивается наилучшее качество исследования криптографических атак, что обеспечивает более широкий охват потенциальных криптографических угроз в сравнении с известными однослойными моделями, учитывающими только одну из известных математических моделей. Проведенный обзор 50 источников, а также предложенный комплексный подход к анализу математических моделей криптографических атак на структуры информационных технологий могут позволить сформировать наилучшее качество рекомендаций по предотвращению исследуемых угроз и атак.

Ключевые слова: математическое моделирование, криптографические атаки, криптографические угрозы, вредоносное программное обеспечение, эпидемиологические модели, модели теории массового обслуживания, безопасность информации

REVIEW OF MODERN APPROACHES TO MATHEMATICAL MODELING OF CRYPTOGRAPHIC ATTACKS ON INFORMATION TECHNOLOGY STRUCTURES

Berezhnoy I.V., Gurskiy S.M., Pyatin V.S.

Mozhaisky Military Aerospace Academy of the Ministry of Defense of the Russian Federation, St. Petersburg, e-mail: vka@mil.ru

The purpose of the study is to review modern approaches to the analysis of mathematical models of cryptographic attacks on information technology structures. The review of the sources was carried out using scientific citation databases “eLIBRARY.RU “, RSCI, Scopus. 588 sources were found in these databases, including 50 sources included in this study. The criteria for inclusion in this review were publications devoted to: the development of mathematical modeling of cryptographic threats and attacks; the impact of malicious software; models of queuing theory, epidemiological models, information security; publications in English and Russian. The exclusion criteria were: lack of access to the full texts of the article; duplicate research, reprints, research in languages other than the declared ones (English and Russian), letters and short messages. The article examines queuing theory models, epidemiological models, behavioral models, as well as their combined application for a more accurate understanding of cryptographic threats. The research focuses on the most commonly used models for investigating attacks on information technology structures and models used to assess the spread of malicious software. An example of calculating the effectiveness of the proposed integrated approach to the analysis of mathematical models of cryptographic attacks on information technology structures, its advantages and disadvantages of known approaches are given. Only the combined use of several types of models makes it possible to compensate for the disadvantages that appear when using each of the single-layer models separately. This ensures the best quality of cryptographic attack research, which provides a broader coverage of potential cryptographic threats in comparison with known single-layer models that take into account only one of the known mathematical models. The conducted review of 50 sources, as well as the proposed comprehensive approach to the analysis of mathematical models of cryptographic attacks on information technology structures, can make it possible to form the best quality recommendations for preventing the threats and attacks under study.

Keywords: mathematical modeling, cryptographic attacks, cryptographic threats, malicious software, queuing theory models, epidemiological models, information security

Введение

Современные структуры информационных технологий подвергаются разнообразным криптографическим угрозам и атакам [1-3]. Эти угрозы требуют разработки эффективных методов обнаружения и противодействия [4-6].

Математическое моделирование позволяет формализовать и исследовать эти угрозы [7-9]. А прогнозирование их развития и оценка рисков позволяет с высокой эффективностью решать задачи защиты структуры информационных технологий.

При этом основными задачами математического моделирования в области кибербезопасности следует полагать [10; 11]: идентификацию и классификацию криптографических угроз; моделирование распространения и воздействия криптографических атак; оценку эффективности защитных мер.

В данной статье приведены результаты анализа подходов к обеспечению устойчивой работы систем сбора, хранения и обработки информации. Представлены количественные оценки, подтверждающие правильность предложенных подходов.

Цель исследования – обзор современных подходов к анализу математических моделей криптографических атак на структуры информационных технологий**.**

Материалы и методы исследования

Выполнен систематический обзор и метаанализ по применению современных подходов к анализу математических моделей криптографических угроз и атак на структуры информационных технологий по протоколу PRISMA. Научная область обзора «Криптография», с подразделами «Криптографические угрозы», «Криптографические атаки». Критериями включения в этот обзор были публикации, посвящённые: разработке математического моделирования криптографических угроз и атак; влиянию вредоносного программного обеспечения; моделям теории массового обслуживания, эпидемиологическим моделям, безопасности информации; публикации на английском и русском языках. Критериями исключения были: отсутствие доступа к полным текстам статьи; дублирующие исследования, репринты, исследования на иных языках, кроме заявленных (английский и русский), письма и краткие сообщения. В базах данных eLIBRARY.RU, РИНЦ, Scopus выполнен поиск исследований, посвящённых применению современных подходов к анализу математических моделей криптографических угроз и атак на структуры информационных технологий, и обзоров, посвящённых данной проблеме в период с 1 января 2005 г. по 10 декабря 2024 г. При поиске в базах данных eLIBRARY.RU, РИНЦ использовались следующие ключевые слова: «криптографические угрозы и атаки». Найдено 577 публикаций. Аналогичный алгоритм применён для других научных баз. Всего 588 исследований включены в этот систематический обзор: посвящены обзору проблемы – 124, разработке моделей криптографических угроз – 146, 156 – моделей криптографических атак, вредоносное программное обеспечение – 122, модели теории массового обслуживания – 10, эпидемиологические модели – 10, безопасность информации – 20. Представляющими интерес результатами были 50 публикаций: (1) обзоры применения математического моделирования криптографических угроз и атак, (2) случаи применения вредоносного программного обеспечения, (3) обзоры применения моделей теории массового обслуживания, эпидемиологических моделей, (4) обзоры безопасности информации. Полученные в результате систематического обзора и метаанализа научные данные могут быть применены при формулировании рекомендаций по применению современных подходов к анализу математических моделей криптографических угроз и атак на структуры информационных технологий [12].

Результаты исследования и их обсуждение

Для проведения исследования были выбраны следующие модели: теории массового обслуживания; эпидемиологические; поведенческие; комбинированные [13, с. 299; 14, с. 73; 15, с. 42].

Исследование сосредоточено на наиболее часто используемых моделях для исследования атак на структуры информационных технологий и моделях, применяемых для оценки распространения вредоносного программного обеспечения (ВПО) [16, с. 320; 17; 18].

Применение предложенных математических моделей включает исследование динамики последствий криптографических атак и их воздействие на структуры информационных технологий, а также оценку эффективности различных защитных мер [19-21].

Вредоносное программное обеспечение включает вирусы, черви, троянские программы и другие типы ВПО, предназначенные для выполнения нежелательных действий на целевой структуре информационных технологий [22-24]. Для моделирования распространения ВПО применяются эпидемиологические модели [25-27].

Фишинг (мошенничество с использованием социальной инженерии для получе-

ния конфиденциальной информации) представляет собой попытки получения конфиденциальной информации путем обмана пользователей через поддельные веб-сайты или электронные письма [28-30]. Для исследования таких криптографических атак используются модели теории игр и поведенческие модели [31-33].

Язык структурированных запросов Structured Query Language (SQL) используется для взаимодействия с реляционными базами данных [34-36].

При криптографической атаке путем SQL-инъекции (Structured Query Language Injection) злоумышленник внедряет вредоносный SQL-код в запросы к базе данных через пользовательский ввод. SQL-инъекции позволяют злоумышленникам выполнять произвольные SQL-запросы в базах данных через уязвимости в веб-приложениях [37-39]. Для исследования и предотвращения таких криптографических атак применяются модели теории конечных автоматов [15, с. 42; 40; 41].

Модели теории массового обслуживания M/M/1 и M/M/m относятся к стохастическим моделям, используемым для анализа систем массового обслуживания [42-44]. Эти модели помогают описать, как заявки (запросы) поступают в систему, как они обрабатываются и как долго они остаются в очереди. Модель описывается тремя частями (буквами), которые определяют свойства системы: первая M (Markovian arrivals) – поступление заявок (запросов); вторая M (Markovian service) – время обслуживания; 1 или m – количество обслуживающих каналов (серверов) в системе [45-47].

Модель M/M/1 для DoS-атак описывает систему массового обслуживания с одним сервером, где заявки поступают согласно распределению Пуассона с интенсивностью λ, а время обслуживания имеет экспоненциальное распределение. Вероятность отказа в обслуживании (перегрузка системы) может быть рассчитана с использованием формулы Эрланга [28; 29; 48]:

$$P_{отказа} = \frac{(\lambda / \mu)^n}{n!} \times \frac{1}{\sum_{k=0}^{n} \frac{(\lambda / \mu)^k}{k!}}, \qquad (1)$$

где $P_{отказа}$ – вероятность отказа в обслуживании, которая означает вероятность того, что ИТ-инфраструктура не сможет обработать запрос из-за перегрузки; λ – интенсивность поступления запросов в структуры информационных технологий (число запросов в единицу времени); μ – интенсивность обслуживания (число запросов, которые структура информационных технологий способна обслужить в единицу времени); n – число серверов (обслуживающих устройств) в структуре информационных технологий; k – количество возможных состояний структуры информационных технологий.

Результаты расчёта вероятности отказа структур информационных технологий в зависимости от числа серверов (рис. 1) показывают, как увеличение числа серверов в структуре информационных технологий влияет на вероятность отказа в обслуживании (отказа в доступе к ресурсу) при DoS-атаке.

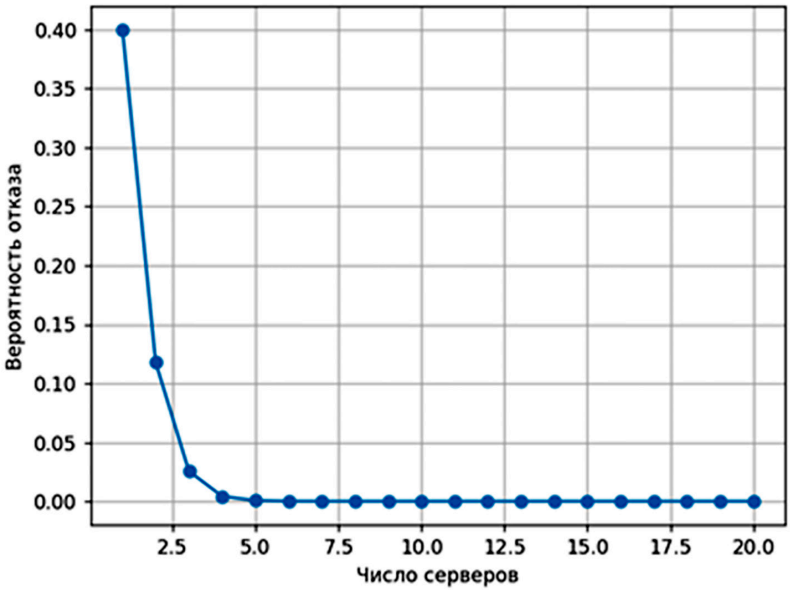

Рис. 1. Результаты расчёта вероятности отказа структуры информационных технологий в зависимости от числа серверов
Источник: разработано авторами

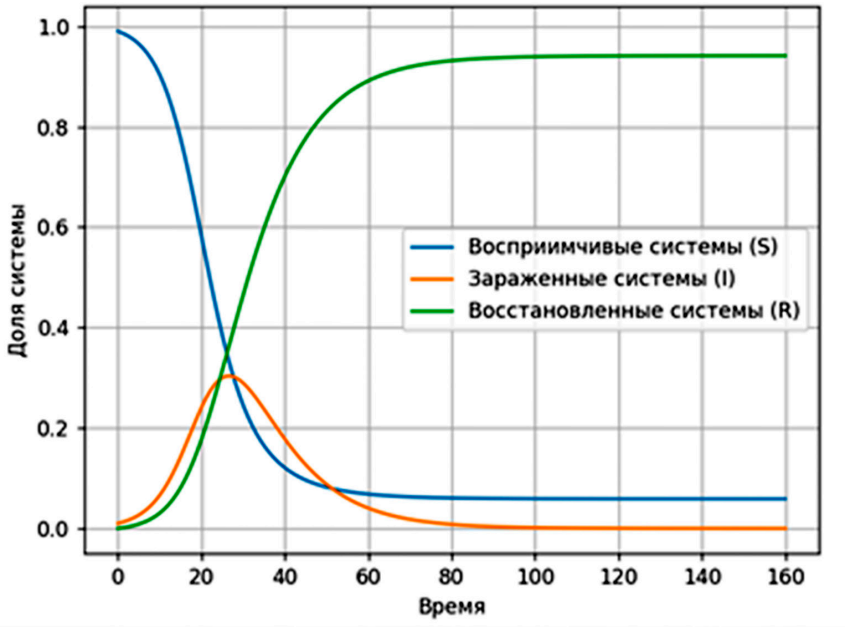

Рис. 2. Результаты расчёта доли отказавшей структуры информационных технологий в зависимости от времени криптографической атаки
Источник: разработано авторами

Анализ результатов позволяет сделать следующие выводы: с увеличением числа серверов вероятность отказа снижается; масштабирование структуры информационных технологий может служить защитной мерой против DoS-атак.

Результаты расчёта доли отказавшей структуры информационных технологий в зависимости от времени криптографической атаки (рис. 2) иллюстрируют поведение структуры информационных технологий, подверженной криптографической атаке ВПО, в зависимости от скорости восстановления зараженных элементов структуры информационных технологий.

Анализ результатов моделирования позволяет сделать следующие выводы: при высокой скорости восстановления локальных серверов общее число «зараженных» информационных систем быстро снижается; эффективное управление восстановлением может ограничить распространение ВПО.

При этом основными проблемами, связанными с криптографическими угрозами, являются: постоянно меняющиеся угрозы (злоумышленники разрабатывают новые методы криптографических атак, что требует обновления защитных мер); сложность обнаружения (многие криптографические атаки остаются незамеченными до тех пор, пока не причинят значительный ущерб); большие объемы данных (обработка и исследование больших объемов данных, связанных с криптографическими угрозами, требует мощных вычислительных ресурсов и эффективных алгоритмов). Преимущества комплексного подхода к конфигурациям атакуемых структур информационных технологий представлены в таблице 1, а результаты расчёта эффективности математических моделей криптографических атак на структуры информационных технологий представлены на рисунке 3. Модель теории массового обслуживания охватывает сетевые узлы, серверы и их пропускную способность, что делает её полезной для анализа и прогнозирования нагрузки на корпоративные системы, но ограничивает её применимость к поведенческим и криптографическим угрозам; эпидемиологические модели применяются к сетям и системам с высоким риском распространения угроз, таким как вирусы и черви, что полезно для корпоративных сетей. Однако они не охватывают поведенческие аспекты атак и не учитывают взаимодействие угроз. Теория игр и поведенческие модели эффективны для анализа стратегий атакующих и защитников, полезны для корпоративных сетей и серверов, где атакующие могут использовать сложные стратегии. Тем не менее они не учитывают конкретные системные уязвимости. Модели теории конечных автоматов и регулярных выражений ограничены системами с предсказуемым поведением, такими как процессы и системы с фиксированной последовательностью действий. Их полез-

ность ограничивается, когда поведение атакующих меняется или атака распространяется. Статистический анализ и визуализация применимы для анализа локальных и глобальных сетей, позволяют выявлять аномалии в поведении, но недостаточны для прогнозирования атак со сложным синергетическим эффектом. Комплексный подход поддерживает анализ всех компонентов корпоративной структуры информационных технологий, включая серверы, сети, базы данных, а также учет поведенческих факторов, что дает максимальное преимущество для моделирования сложных криптографических атак на всю структуру информационных технологий, включая взаимодействие угроз.

Для оценки эффективности F предложенного комплексного подхода к анализу математических моделей криптографических атак на структуры информационных технологий использован метод определения качества классификационных моделей из области информационного поиска и машинного обучения [49]. Предлагаемое соотношение (2) для оценки эффективности также известно как мера, объединяющая точность (precision) и полноту (recall) в единую метрику. Она особенно полезна в ситуациях, когда важно учитывать как точность (чтобы было как можно меньше ложных срабатываний), так и полноту (чтобы было обнаружено как можно больше реальных атак).

Эффективность предложенного комплексного подхода к анализу математических моделей криптографических атак на структуры информационных технологий (2) рассчитывается как гармоническое среднее точности и полноты. Используется именно гармоническое, а не обычное среднее, поскольку оно более строго учитывает малые величины. Впервые эта метрика была предложена в исследованиях по классификации текстов, но быстро нашла широкое применение, в том числе и в кибербезопасности для оценки эффективности моделей обнаружения угроз [50, с. 151].

$$F = 2 \times \frac{P \times R}{P + R} \times 100\%,$$

где $R = \frac{TP}{TP + FN} - recall$ *(полнота);*

$$P = \frac{TP}{TP + FP} - precision \quad \textit{(точность);}$$

TP (*True Positives*) – верно обнаруженные атаки;

FP (*False Positives*) – ложные срабатывания, когда модель сигнализирует об атаке, которой нет;

FN (*False Negatives*) – пропущенные атаки, когда угроза не была обнаружена.

Рассмотрим пример расчета эффективности. Пусть имеются следующие значения для параметра системы управления базами данных (СУБД): (TP = 80, FP = 20, FN = 30) при использовании только однослойной модели статистического анализа и (TP = 95, FP = 10, FN = 15) – для предложенного многослойного комплексного подхода. Представленные в примере результаты расчётов количественных значений параметров моделей (табл. 2) указывают на преимущество в эффективности предложенного многослойного комплексного подхода на 11,9%. Результаты расчёта эффективности (2) предложенных многослойных математических моделей криптографических атак на атакуемые структуры информационных технологий, реализующих предложенный комплексный подход, в сравнении с известными (однослойными вариантами моделей, учитывающими при расчёте эффективности только одну из моделей) приведены на рисунке 3, а преимущества комплексного подхода к конфигурациям атакуемых структур информационных технологий сведены в таблице 1.

Такой комплексный подход, учитывающий применение предложенных математических моделей криптографических атак на структуры информационных технологий, позволяет учитывать взаимодействие атак разного типа и анализировать синергетический эффект (рис. 3, табл. 1), что может привести к повышению точности оценки рисков на 20-40%, увеличению способности обнаружения уязвимостей на 30-50% и улучшению возможностей по предотвращению атак на 25-50% по сравнению с использованием известных однослойных моделей (учитывающих либо только модель из теории массового обслуживания, либо только эпидемиологические модели, либо только модели, основанные на теории игр, либо только модели теории конечных автоматов, либо только модели, основанные на статистическом анализе).

Поддержка анализа всех уровней системы и адаптация под реальные многослойные сценарии атак может позволить сделать предложенные математические модели криптографических атак на структуры информационных технологий более эффективными и точными по сравнению с известными однослойными моделями для защиты корпоративной структуры информационных технологий от современных сложных угроз (рис. 3).

Таблица 1

Преимущества комплексного подхода к конфигурациям атакуемых структур информационных технологий

Параметр анализа	Модель массового обслуживания (DDoS-атаки)	Эпидемиологические модели (черви, вирусы)	Теория игр и поведенческие модели (фишинг)	Модели конечных автоматов	Статистический анализ и визуализация	Комплексный подход к моделированию атак	Преимущество комплексного подхода
Точность оценки риска	55% (очереди и нагрузки)	60% (анализ распространения угроз)	65% (учёт стратегии атакующих)	50% (анализ поведения системных процессов)	70% (выявление аномалий)	90% (учёт всех факторов и синергетического эффекта)	+20-40%
Прогнозируемый уровень компрометации данных	25%	30%	35%	20%	40%	До 60% (влияние синергетического эффекта)	+20-40%
Обнаружение уязвимостей	50% (сетевые уязвимости)	55% (анализ уязвимостей в системах)	65% (учёт уязвимых стратегий)	45% (аналитика выполнения)	60% (выявление паттернов атак)	95% (выявление сложных и комбинированных уязвимостей)	+30-50%
Адаптация под реальные сценарии	45%	60%	65%	50%	55%	95% (учёт сложных многослойных атак)	+35-50%
Возможность предотвращения атак	40% (локальное предотвращение)	50% (снижение распространения)	55% (предотвращение на основе поведения)	35% (проверка ограниченного количества случаев)	60% (предсказание на основе статистики)	85% (распознавание и блокировка комбинированных атак)	+25-50%
Комплексность анализа воздействия	50% (сетевой уровень)	55% (уровень заражения)	60%	45% (уровень процессов)	65% (поведенческий уровень)	90% (анализ на всех уровнях системы)	+25-45%
Применимость к IT-инфраструктуре	Сетевые компоненты (серверы, узлы)	Корпоративные сети и системы	Корпоративные сети, серверы и пользователи	Ограниченные системы с предсказуемым поведением	Локальные и глобальные сети	Полная система: сети, серверы, базы данных, пользователи	Максимальная: поддержка комплексной инфраструктуры

Примечание: разработано авторами.

Таблица 2

Результаты расчета количественных значений параметров моделей: точности, полноты и эффективности

Однослойная модель статистического анализа	Предложенный многослойный комплексный подход
$P_{stat} = \frac{80}{80+20} = 0,8;$ $R_{stat} = \frac{80}{80+30} = 0,727;$	$P = \frac{95}{95+10} = 0,905;$ $R = \frac{95}{95+15} = 0,86;$
$F_{stat} = 2 \times \frac{0,8 \times 0,727}{0,8+0,727} \times 100\% = 76,2\%$	$F = 2 \times \frac{0,905 \times 0,86}{0,905+0,86} \times 100\% = 88,1\%$

Примечание: разработано авторами.

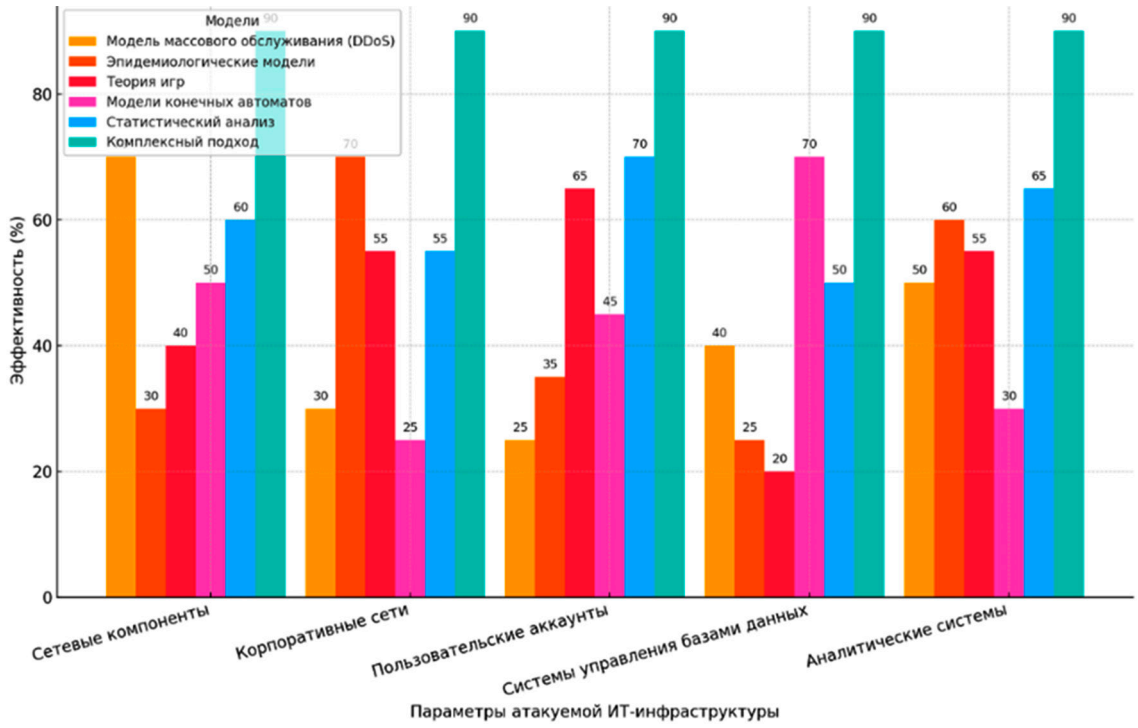

Рис. 3. Результаты расчёта эффективности математических моделей криптографических атак на структуры информационных технологий
Источник: разработано авторами

Заключение

Новизна полученных в статье результатов заключается в проведенном систематическом обзоре и метаанализе по протоколу PRISMA исследований 50 источников, опубликованных в индексированных базах данных российского индекса научного цитирования, а также в предложенном комплексном подходе к анализу математических моделей криптографических атак на структуры информационных технологий, которые могут позволить не только оценивать текущие риски, но и разрабатывать эффективные стратегии защиты от криптографических атак.

В отличие от большинства исследований, которые фокусируются на отдельных

аспектах криптографических угроз и атак, предложенные в статье систематический обзор 50 источников и комплексный подход могут позволить объединить модели теории массового обслуживания, эпидемиологические модели и поведенческие модели для создания более полного в сравнении с известными однослойными моделями представления о криптографических угрозах и атаках. Проведенный обзор и такой комплексный подход могут позволить уточнить процесс анализа и прогноза различных типов криптографических угроз и атак в сравнении с известными однослойными моделями, а также разрабатывать комплексные стратегии защиты от них, выраженные итоговыми результатами расчётов (рис. 1–3 с указанием «атакуемой» структуры информационных технологий и количественных значений эффективности предложенных моделей в сравнении с известными; табл. 1) применительно к достижению цели исследования.

Результаты указанного обзора и такой подход могут дать преимущество в масштабировании и повышении устойчивости к криптографическим атакам. Они могут обеспечить: увеличение пропускной способности структур информационных технологий на 50–80%; снижение вероятности отказов при DDoS-атаках на 60–70%; сокращение времени ожидания и улучшение защиты от перегрузок; оптимизацию скорости восстановления зараженных структур информационных технологий и снижение числа зараженных структур информационных технологий на 30–50%.

Список литературы

1. Бирюков Д.Н., Захаров О.О., Сабиров Т.Р. Подход к построению системы знаний для решения задач оценивания защищенности информационно-технических систем // Труды Военно-космической академии имени А.Ф.Можайского. 2024. № 691. С. 102-111.

2. Гурский С.М., Полубенцев В.А. Информационная безопасность в информационно-телекоммуникационной сети «Интернет» // Современные наукоемкие технологии. 2022. № 1. С.25-31. DOI: 10.17513/snt.39005.

3. Горецкий И.А., Лаврова Д.С. Интеллектуальная рекомендательная система для противодействия сетевым атакам // Проблемы информационной безопасности. Компьютерные системы. 2024. № S2 (60). С. 24–30. DOI: 10.48612/jisp/gxt5-d3m3-5ku4.

4. Smirnov S.I., Eremeev M.A., Magomedov Sh.G., Izergin D.A. Criteria and indicators for assessing the quality of the investigation of an information security incident as part of a targeted cyberattack // Russian Technological Journal. 2024. № 12(3). С. 25-36. DOI: 10.32362/2500-316X-2024-12-3-25-36.

5. Смарт Н. Криптография / Перевод с английского С.А. Кулешова; под редакцией С.К. Ландо. М.: Техносфера, 2005. 528 с.

6. Пилькевич С.В. Исследование атак, нацеленных на кражу модели искусственного интеллекта // Труды Военно-космической академии имени А.Ф.Можайского. 2023. № 689. С. 103-120.

7. Бирюков Д.Н., Лебедев С.Л., Руссу В.Ю. Подход к автоматизации поиска уязвимостей в прошивках телекоммуникационных устройств // Труды Военно-космической академии имени А.Ф. Можайского. 2023. № 688. С. 54-59.

8. Бирюков Д.Н., Дудкин А.С., Родионов Е.С. Подход к созданию криптозащищенной Mesh-сети // Труды Военно-космической академии имени А.Ф. Можайского. 2024. № 691. С. 94-101.

9. Гололобов Н.В. Систематизация вредоносного программного обеспечения для определения типов проявляемой ими активности // Проблемы информационной безопасности. Компьютерные системы. 2024. № 3 (61). С. 142-154. DOI: 10.48612/jisp/npp7-45tr-em48.

10. Бережной И.В., Фомин А.И., Гурский С.М. Применение новых информационных технологий при обработке специальной информации методом рандомизации // Естественные и технические науки. 2016. № 6 (96). С. 128-129.

11. Коржик В.И., Яковлев В.А., Изотов Б.В., Старостин В.С., Буйневич М.В. Прогресс в теории прикладной криптографии: обзор и некоторые новые результаты. Часть 1. Ключевая криптография // Труды учебных заведений связи. 2024. Т. 10, № 4. С. 126-141. DOI: 10.31854/1813-324X-2024-10-4-126-141.

12. Белобородов В.А., Воробьёв В.А., Семинский И.Ж., Калягин А.Н. Порядок выполнения систематического обзора и мета-анализа по протоколу PRISMA // Система менеджмента качества: опыт и перспективы. 2023. № 12. С. 5-9.

13. Сердюк В.А. Новое в защите от взлома корпоративных систем. М.: Техносфера, 2007. 360 с.

14. Басараб М.А., Коннова Н.С. Теория игр в информационной безопасности. М.: МГТУ им. Н.Э. Баумана (национальный исследовательский университет), 2024. 84 с.

15. Бушуев А.Ю., Кутыркин В.А. Введение в прикладную теорию автоматов. М.: МГТУ им. Н.Э. Баумана (национальный исследовательский университет), 2024. 53 с.

16. Мастицкий С.Э., Шитиков В.К. Статистический анализ и визуализация данных с помощью R. М.: ДМК Пресс, 2017. 498 с. URL: http://r-analytics.blogspot.com (дата обращения: 02.11.2024).

17. Eremeev M.A., Zakharchuk I.I. Risk assessment of using open source projects: analysis of the existing approaches // Automatic Control and Computer Sciences. 2023. Т. 57, № 8. С. 938-946. DOI: 10.3103/s0146411623080059.

18. Дун Х. Классификация изображений вредоносных программ без использования сверток с использованием механизмов внутреннего внимания // Информатика и автоматизация. 2024. Т. 23, № 6. С. 1869-1898. DOI: 10.15622/ia.23.6.11.

19. Дженифер Р., Пракаш В.Д. Алгоритм Rivest-Shamir-Adleman, оптимизированный для защиты устройств Интернета вещей от конкретных атак // Информатика и автоматизация. 2024. Т. 23, № 5. С. 1423-1453. DOI: 10.15622/ia.23.5.6.

20. Молдовян А.А., Молдовян Д.Н., Молдовян Н.А. Постквантовые двухключевые криптосхемы на конечных алгебрах // Информатика и автоматизация. 2024. Т. 23, № 4. С. 1246-1276. DOI: 10.15622/ia. 23.4.1 2.

21. Молдовян А.А., Молдовян Д.Н., Молдовян Н.А. Новый подход к разработке алгоритмов многомерной криптографии // Вопросы кибербезопасности. 2023. № 2 (54). С. 52-64. DOI: 10.21681/2311-3456-2023-2-52-64.

22. Синицин А.М. Методы защиты и криптографические протоколы для встроенных электронных систем // Экономика и управление: проблемы, решения. 2024. Т. 6, № 9 (150). С. 12-23. DOI: 10.36871/ek.up.p.r.2024.09.06.002.

23. Акбарова А.Н., Ахунжанов И.Б. Обзор угроз безопасности, уязвимостей и мер противодействия интернета медицинских вещей в сетях с поддержкой 5G // Оригинальные исследования. 2023. Т. 13, № 1. С. 312-320.

24. Брониковский Е.А., Никонов В.И. Актуальные вопросы обеспечения безопасности в manet-сетях // Динамика

систем, механизмов и машин. 2020. Т. 8, № 4. С. 113-119. DOI: 10.25206/2310-9793-8-4-113-119.

25. Новиков В.И., Каленик К.Г. Повышение безопасности криптографических стандартов // Проблемы инфокоммуникаций. 2015. № 2 (2). С. 18-22.

26. Кузьмин А.Р., Савельев М.Ф. Актуальные проблемы информационной безопасности программного обеспечения и каналов связи коммерческих беспилотных авиационных систем // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2023. № 3. С. 157-169. DOI: 10.18137/RNU.V9187.23.03.P.157.

27. Бельский В.С., Грибоедова Е.С., Царегородцев К.Д., Чичаева А.А. Безопасность RFID-систем // International Journal of Open Information Technologies. 2021. Т. 9, № 9. С. 1-20.

28. Гончаренко В.А., Хомоненко А.Д., Абу Хасан Р. Композиционный подход к имитационному моделированию систем массового обслуживания со случайными параметрами //Информатика и автоматизация. 2024. Т. 23, № 6. С. 1577-1608. DOI: 10.15622/ia. 23.6.1.

29. Куракин С.З., Онуфрей А.Ю., Разумов А.В. Исследование вариантов построения информационно-управляющих систем на основе сетевых моделей систем массового обслуживания // Информатика и автоматизация. 2024. Т. 23, № 6. С. 1609-1642. DOI: 10.15622/ia.23.6.2.

30. Нараянарао Ч., Мандапати В., Бодду Б. Синергетические подходы к улучшению обнаружения вторжений в Интернет вещей (IoT): балансировка характеристик с помощью комбинированного обучения // Информатика и автоматизация. 2024. Т. 23, № 6. С. 1845-1868. DOI: 10.15622/ia.

31. Северин Д.В., Пахоменкова М.И., Дроздов Д.В. Обзор стратегий обеспечения информационной безопасности в информационных системах // Наука и бизнес: пути развития. 2019. № 10 (100). С. 137-140.

32. Тетерин М.И. Влияние киберугроз на устойчивость телекоммуникационных сетей и методы их нейтрализации // Научный аспект. 2024. Т. 48, № 6. С. 6172-6178.

33. Кандаков А.Е. Современные методы киберзащиты в нефтегазовой промышленности: обзор актуальных технологий и стратегий для защиты автоматизированных систем от кибератак // Вестник науки. 2024. Т. 4, № 5 (74). С. 1411-1417.

34. Статистика уязвимостей в 2011 году // Защита информации. Инсайд. 2012. № 3 (45). С. 70-72.

35. Задирака В.К., Кудин А.М. Особенности реализации криптографических и стеганографических систем по принципу облачных вычислительных технологий // Искусственный интеллект. 2012. № 3. С. 438-444.

36. Gavrishev A.A., Zhuk A.P., Osipov D.L. An analysis of technologies to protect a radio channel of fire alarm systems against unauthorized access // SPIIRAS Proceedings. 2016. № 4 (47). С. 28-45. DOI: 10.15622/sp.47.2.

37. Бедило М.В., Олейников В.Т., Петренко А.Н., Страхолис А.А. Угрозы безопасности полевой мультисервисной сети передачи данных // Технологии гражданской безопасности. 2024. Т. 21, № 2 (80). С. 25-31.

38. Бобков Е.О., Балашова Е.А., Крыжановский А.В. Методы и средства обеспечения сетевой безопасности в локальных вычислительных сетях // Научный альманах Центрального Черноземья. 2022. № 1-7. С. 27-41.

39. Милосердов А.О. Классификация угроз и уязвимостей в беспроводных сетях // Ученые записки УлГУ. Серия: Математика и информационные технологии. 2023. № 2. С. 72-85.

40. Зорин Е.Л., Чичварин Н.В. Информационная безопасность САПР/PLM, применяющих облачные технологии // Вопросы кибербезопасности. 2014. № 4 (7). С. 23-29.

41. Алексеев Е.К., Ошкин И.Б., Попов В.О., Смышляев С.В. О криптографических свойствах алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 // Математические вопросы криптографии. 2016. Т. 7, № 1. С. 5-38.

42. Каменских А.Н., Наборщиков В.Г. Анализ структурно-функциональных моделей криптографических процессоров для систем «Интернета вещей» // Инновационные технологии: теория, инструменты, практика. 2020. Т. 1. С. 468-473.

43. Панин Д.Н., Козлов З.С. Информационная безопасность в сфере корпоративных сетей // Дневник науки. 2020. № 12 (48). С. 23.

44. Золотарёва С.А., Суковатицина Н.А. Информационная безопасность в условиях цифровизации экономики // Вестник науки. 2024. Т. 3, № 6 (75). С. 190-195.

45. Яковишин А.Д. Борьба с перехватом трафика RFID и дистанционного управления: методы защиты и повышение безопасности // Современные научные исследования и инновации. 2024. № 1 [Электронный ресурс]. URL: https://web.snauka.ru/issues/2024/01/101405 (дата обращения: 10.11.2024).

46. Брюхомицкий Ю.А., Макаревич О.Б. Обзор исследований и разработок по информационной безопасности // Известия ЮФУ. Технические науки. 2010. № 11 (112). С. 6-22.

47. Верещагин К.В. Защита корпоративных сетей от DDOS-атак: современные методы и тенденции // Научный Лидер. 2023. № 47 (145). С. 12-15.

48. Матвеев А.С., Поротников П.А. Программно-аппаратные средства защиты информации в системе МВД // Современные научные исследования и разработки. 2018. Т. 2, № 5 (22). С. 371-373.

49. Тали Д.И. Модель угроз безопасности метаданным в системе электронного документооборота военного назначения // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2020. № 1-2 (139-140). С. 95-101.

50. Маннинг Кристофер Д., Рагхаван Прабхакар, Шютце Хайнрих. Введение в информационный поиск. М.: Вильямс, 2020. 528 с.