МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Анализ надежности современных САРТСНА

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Яшина Максима Алексеевича

Научный руководитель
д. ф.-м. н., профессор _____ М. Б. Абросимов
19.01.2026 г.

Заведующий кафедрой
д. ф.-м. н., профессор _____ М. Б. Абросимов
19.01.2026 г.

Саратов 2026

ВВЕДЕНИЕ

В условиях стремительного развития цифровых сервисов растёт количество автоматизированных действий, направленных на злоупотребление функциональностью веб-ресурсов: массовые регистрации, несанкционированные запросы к API, автоматизированная рассылка и подбор учётных данных. Для защиты от подобных угроз широко применяются механизмы, основанные на различении человека и программы. Теоретической основой таких механизмов стал тест Тьюринга, предложенный для определения способности машины имитировать интеллектуальное поведение[1]. Его переосмысление привело к появлению обратного теста Тьюринга – CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart, далее «капча»), впервые подробно описанного в работе Л. фон Ана и соавторов[2].

Текстовые капчи долгое время являлись массовым и практически удобным средством защиты благодаря простоте генерации и низким требованиям к пользовательскому устройству. Однако развитие методов машинного обучения, появление эффективных алгоритмов распознавания изображений и сквозных моделей существенно снизили устойчивость таких схем. Современные исследования Ли Ч.[3], Ши Ч.[4] и Чжан Н.[5] демонстрируют способность нейросетевых атак корректно распознавать даже сложные искажённые капчи с высокой точностью.

---

[1] Turing, A. M. Computing Machinery and Intelligence / A. M. Turing // Mind. – 1950. – Vol. 59. – Pp. 433-460.

[2] von Ahn, L. *CAPTCHA: Using Hard AI Problems For Security / L. von Ahn, M. Blum, N. J. Hopper, J. Langford //* LNCS. – 2003. – Vol. 2656. – Pp. 294-311.

[3] Li, C. An End-to-End Attack on Text-based CAPTCHAs Based on Cycle-Consistent Generative Adversarial Network / C. Li, X. Chen, H. Wang, Y. Zhang, P. Wang // ArXiv. – 2020. – Vol. 1. – Pp. 1–14.

[4] Shi, C. Text Captcha Is Dead? A Large Scale Deployment and Empirical Study / C. Shi, Sh. Ji, Q. Liu, Ch. Liu, Y. Chen, Y. He, Zh. Liu, R. Beyah, T. Wang // Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS'21). – 2021. – DOI: 10.1145/3460120.3484558. – Pp. 1949–1963.

[5] Zhang, N. A Generative Adversarial Learning Framework for Breaking Text-Based CAPTCHA in the Dark Web / N. Zhang, M. Ebrahimi, W. Li, H. Chen // Proceedings of the 2020 IEEE International Conference on Intelligence and Security Informatics (ISI 2020). – 2020. – DOI: 10.1109/ISI49825.2020.9280537. – 6 p.

Актуальность исследования обусловлена тем, что, несмотря на наличие более современных решений, текстовые капчи до сих пор широко используются в государственных, образовательных и корпоративных системах. Их распространённость и технологическая простота делают анализ устойчивости таких схем крайне важным для оценки реальной эффективности применяемых механизмов защиты. Кроме того, именно текстовые капчи являются удобной экспериментальной площадкой для сравнения различных подходов автоматического распознавания – от методов сегментации до моделей прямого распознавания всей капчи и гибридных схем, сочетающих детекторы символов с нейронными классификаторами. Это позволяет объективно оценивать сильные и слабые стороны современных алгоритмов.

По мимо этого текстовые капчи продолжают выполнять важную роль в составе гибридных и поведенческих систем защиты. На многих современных платформах они используются как резервный механизм и предъявляются пользователю в случаях, когда поведенческая модель не может уверенно классифицировать взаимодействие как человеческое. Такая комбинированная архитектура подтверждает, что даже в условиях развития более сложных методов проверки текстовые капчи остаются значимым элементом многоуровневых систем кибербезопасности.

Цель данной работы заключается в разработке программного инструмента для анализа надёжности текстовой капчи и сравнении эффективности различных методов её автоматического распознавания.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Изучить теоретические основы обратного теста Тьюринга и провести детальный обзор современных капч.
2. Исследовать архитектуры сверточных нейронных сетей и методы компьютерного зрения, применяемые для задач распознавания текстовых капч.

3. Разработать, реализовать и протестировать детерминированный метод распознавания текстовой капчи, основанный на анализе структуры изображения и последовательности преобразования.
4. Спроектировать, обучить и экспериментально оценить модель распознавания капчи на основе сверточной нейронной сети.
5. Разработать, реализовать и испытать на практике комплексный метод распознавания капчи с использованием детектора объектов и посимвольной классификации с помощью сверточных нейронных сетей.
6. Провести сравнительный анализ трех разработанных методов по ключевым параметрам надежности текстовых капч.

Дипломная работа состоит из введения, 10 разделов, заключения, списка использованных источников и 6 приложений. Общий объем работы – 99 страниц, из них 72 страниц – основное содержание, включая 36 рисунков и 3 таблицы, список использованных источников из 34 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В разделе 1 «Теоретическая часть» рассматриваются основные понятия и современные подходы к построению CAPTCHA (далее «капча»), а также теоретические основы методов распознавания.

В подразделе 1.1 «Современные капчи» приведён обзор назначения капчи как обратного теста Тьюринга и рассмотрены основные типы современных капч: текстовые, графические и поведенческие. Показано, что развитие нейросетевых методов компьютерного зрения и автоматизации браузеров существенно снизило стойкость классических схем. Отмечено, что в реальных сервисах всё чаще используется многоуровневая защита: поведенческий анализ сочетается с предъявлением капчи только при подозрительной активности. При этом текстовые капчи, несмотря на устаревание как концепции, продолжают широко применяться в системах, где замена инфраструктуры затруднена, и поэтому остаются актуальным объектом анализа.

Ни один тип капчи не является окончательным решением: появление новых схем сопровождается быстрым развитием методов обхода. Текстовые капчи остаются практически значимыми, так как до сих пор распространены и служат резервным механизмом в гибридных системах защиты.

В подразделе 1.2 «Сверточные нейронные сети» рассмотрены сверточные нейронные сети (CNN) как базовый инструмент анализа изображений. Описаны ключевые элементы архитектуры сверточных нейронный сетей: сверточные слои (извлечение пространственных признаков), функции активации (в частности ReLU), слои объединения (уменьшение размерности и повышение устойчивости признаков), полносвязные слои (формирование итогового решения). Подчёркнута применимость сверточных нейронный сетей к задачам распознавания символов и текстовых последовательностей на изображениях, включая случаи с шумами, наложенными линиями и искажениями – то есть к условиям, характерным для текстовых капч.

Сверточные нейронные сети являются эффективной основой для распознавания капч, поскольку позволяют обучаемым образом извлекать устойчивые признаки и снижать зависимость от ручных эвристик обработки изображения.

В подразделе 1.3 «Обзор сервисов подключения капч и общих решений для защиты от DDoS-атак» рассмотрено место капчи в промышленной защите веб-ресурсов. Показано, что на практике капча редко используется как единственный барьер и обычно входит в состав многоуровневых систем защиты, где решение о предъявлении проверки принимается по контексту: характеристикам трафика, частоте запросов, поведению клиента и оценке риска. На примерах промышленных решений, в частности Cloudflare и Yandex SmartCaptcha, описаны типовые механизмы: ограничение частоты запросов, фильтрация трафика и включение капчи по условию подозрительной активности. Отдельно отмечено, что против объёмных сетевых DDoS-атак ключевую роль играет инфраструктурная фильтрация, а капча наиболее полезна против атак прикладного уровня.

Капча в современных платформах выступает как вспомогательный элемент риск-ориентированной защиты: её эффективность максимальна в сочетании с поведенческими механизмами и ограничением запросов, а не в виде единственного рубежа безопасности.

В разделе 2 «Практическая часть» выполнен экспериментальный анализ устойчивости конкретного типа текстовой капчи к автоматическому распознаванию. Для сопоставления реализованы и протестированы три различных подхода: детерминированный, нейросетевой и комплексный.

В подразделе 2.1 «Постановка задачи и общая схема практической части» сформулирована практическая задача: оценить, насколько исследуемая текстовая капча устойчива к современным методам распознавания, и сравнить эффективность различных подходов в одинаковых условиях. Описан формат исследуемых капч и подготовка базы данных для тестирования: использовались изображения фиксированного формата (400×153 пикселей) с ограниченным

алфавитом и длиной строки 4 или 5 символов; сформирована размеченная база из 3000 капч. Определены принципы эксперимента: единая база данных для всех методов и сравнение по ключевым метрикам качества распознавания.

Подготовленная база и единая схема тестирования обеспечивают корректное и сопоставимое сравнение методов, позволяя объективно оценить реальную устойчивость выбранной текстовой капчи.

В подразделе 2.2 «Детерминированный метод» описан классический алгоритм распознавания без машинного обучения, основанный на последовательной обработке изображения. Приведены основные этапы: бинаризация, очистка от шумов и линий, скелетизация, сегментация символов, построение признаков, а затем распознавание по эвристикам. Подчёркнуто, что качество такого подхода критически зависит от успешной сегментации и устойчивости к помехам.

Детерминированный метод показал низкую устойчивость к искажениям и помехам исследуемой капчи и обеспечил невысокую точность распознавания полной капчи (порядка 33%), что ограничивает его практическую применимость. Ниже представлена таблица 2 с информацией о количестве капч по числу распознанных символов в ней.

Таблица 2 – Информация о количестве распознанных капч

Количество символов в капче	Количество капч по числу распознанных символов					
	0	1	2	3	4	5
4 символа	2	24	75	87	120	–
5 символов	7	10	51	64	82	78

В подразделе 2.3 «Нейросетевой метод» реализован подход прямого распознавания капчи целиком на основе сверточной нейронной сети. Описана постановка как задачи классификации последовательности символов по изображению и переход от ручных эвристик к обучаемому извлечению признаков. Приведены этапы подготовки данных: преобразование изображения в оттенки серого, масштабирование до 180 на 60 пикселей, нормализация значений пикселей и формирование входа для сверточной нейронной сети.

Указано, что из-за различной длины строки (4 и 5 символов) были обучены две отдельные модели на соответствующих поднаборах.

Нейросетевой метод существенно превзошёл детерминированный по точности распознавания полной капчи (около 94,33%), однако требует отдельной модели для разных длин строки, что снижает универсальность решения.

В подразделе 2.4 «Комплексный метод YOLO и CNN» описан двухэтапный комплексный метод: сначала детектор объектов YOLO выполняет явную сегментацию символов (находит ограничивающие рамки), затем каждый вырезанный символ распознаётся CNN-классификатором. Приведён процесс подготовки данных для детектора: вручную размечен набор капч в labelImg, при этом используется единый класс «symbol», а различение конкретных знаков выполняется на следующем этапе классификатором. Описано обучение модели YOLOv8s и общий смысл метрик обучения. Подчёркнуты преимущества метода: контролируемая сегментация, модульность и независимость от длины строки (число символов определяется на этапе детекции).

Комплексный подход показал наилучшее качество распознавания (99,83% на уровне всей капчи) и высокую устойчивость к типичным искажениям капчи, и единственная ошибка, представленная на рисунке 36, обусловлена не систематическим дефектом модели, а неблагоприятным сочетанием шума и формы символа, так как ошибка возникла на этапе классификации: истинная строка – «шасж», предсказание программы – «шаеж». Благодаря явной сегментации и модульности данный метод более универсален и удобен для практического применения.

Рисунок 36 – Неверно распознанная капча и ее сегментация

В подразделе 2.5 «Сравнение трех методов распознавания капчи» выполнено итоговое сравнение методов по ключевым параметрам: необходимость сегментации, использование машинного обучения, зависимость от длины капчи, устойчивость к искажениям, точность полной капчи и практическая применяемость. Показано, что детерминированный метод обладает низкой устойчивостью и точностью (33%), нейросетевой метод даёт высокую точность (94,33%), а наиболее эффективным оказался комплексный метод YOLO-детектора и CNN-классификатора, обеспечивший точность порядка 99,83% и независимость от длины строки. Сравнение полученных результатов, представленных в таблице 3, позволяет не только оценить эффективность каждого метода, но и проследить эволюцию инструментов, необходимых для достижения высокой точности в условиях шумных искажённых капч.

Таблица 3 – Сравнение результатов по ключевым показателям

Характеристика	Детерминированный метод	Нейросетевой метод	Комплексный метод
Использование машинного обучения	Нет	Да	Да
Необходимость в сегментации	Ручная, чувствительная	Неявная, внутренняя	Явная, контролируемая
Зависимость от длины капчи	Нет	Да, две отдельные модели	Нет
Устойчивость к искажениям	Низкая	Средняя	Очень высокая
Точность полной капчи	33%	94.33%	99.83%
Реальная применяемость	Низкая	Средняя	Высокая

Результаты практики убедительно показывают, что применение классических алгоритмов обработки изображений недостаточно для взлома современных капч и переход к машинному обучению – необходимое условие для повышения точности.

С практической точки зрения можно утверждать, что данная текстовая капча не является устойчивой к современным средствам анализа, поскольку корректно обученная нейросетевую связка детектора и классификатора способна обходить её практически безошибочно.

ЗАКЛЮЧЕНИЕ

В ходе выполнения данной работы все поставленные задачи решены и цель достигнута. В работе проведён анализ современных схем капч, рассмотрены их уязвимости и методы атак, основанные на нейронных сетях, а также разработаны и реализованы три практических метода автоматического распознавания текстовых капчи.

В теоретической части были подробно изучены особенности современных капч, включая текстовые, графические и поведенческие схемы. Показано, что, несмотря на развитие фоново выполняемых и поведенческих методов верификации, текстовые капчи продолжают широко использоваться в государственных, образовательных и корпоративных системах. Их устойчивость к современным атакам напрямую зависит от степени сложности и разнообразия искажений, что делает задачу анализа методов распознавания актуальной и практически значимой.

В практической части был проведён экспериментальный анализ эффективности всех трех методов. Предложенные решения полностью соответствуют поставленным задачам и демонстрируют высокую эффективность. Все методы были реализованы, протестированы и объективно сравнены, и был обоснован выбор оптимального подхода для автоматического распознавания текстовых капч.

Результаты работы могут быть использованы при разработке модулей распознавания в автоматизированных системах тестирования капч, а также в исследовательских целях для анализа устойчивости существующих капч.

В целом выполненная работа обладает как теоретической, так и практической значимостью и демонстрирует, что применение сверточных нейронных сетей и современных детекторов объектов является эффективным подходом для автоматического распознавания текстовых капч.