УДК 004.891.2

Разработка обучаемой интеллектуальной системы для автоматизированного принятия экспертных решений на основе анализа реальных данных в судебной деятельности

Гриценко Юнона Артемовна Yunagritsenko@yandex.ru
Молчанова Наталья Олеговна molchanovannoo@mail.ru
Князева Светлана Вадимовна knyazevasv@bmstu.ru

МГТУ им. Н.Э. Баумана, Москва, Россия

В работе представлена концепция и реализация обучаемой интеллектуальной системы, предназначенной для автоматизации процесса принятия экспертных решений в судебной деятельности. Система объединяет технические данные из MITRE ATT&CK и судебную практику по статьям УК РФ, связанным с киберпреступлениями. Разработан модуль анализа на C++, использующий алгоритм взвешивания техник по релевантности для судебных дел.

***Ключевые слова**: интеллектуальная система, киберпреступления, MITRE ATT&CK, судебная практика, экспертная система, машинное обучение, автоматизация*

Введение. Современный этап развития информационного общества сопровождается стремительным ростом количества и сложности кибератак. Киберпреступность сегодня является одной из наиболее значимых угроз для государства, бизнеса и частных пользователей. Злоумышленники применяют все более изощренные методы: от социальной инженерии и фишинга до целевых атак на критическую инфраструктуру. В результате резко возрастает нагрузка на судебную систему и экспертные подразделения, занимающиеся расследованием цифровых преступлений.

Традиционные методы судебной экспертизы и анализа киберинцидентов требуют больших затрат времени и человеческих ресурсов. При этом объем цифровых доказательств постоянно увеличивается, что делает невозможным их оперативную обработку без применения интеллектуальных технологий. Вследствие этого особую актуальность приобретает разработка обучаемых систем, способных автоматически анализировать судебную практику, выявлять закономерности и помогать экспертам принимать решения на основе реальных данных.

Актуальность исследования заключается в необходимости создания интеллектуальной платформы, которая объединяет методы искусственного интеллекта, анализ больших данных и правовую экспертизу для автоматизации экспертной деятельности. Такая система позволит повысить эффективность расследования цифровых преступлений, обеспечить единообразие судебных решений и сократить временные затраты на анализ прецедентов.

Объект исследования — процесс автоматизированного анализа судебных данных и экспертных решений, связанных с киберпреступлениями. Предмет

исследования — методы и программные средства построения обучаемых интеллектуальных систем, обеспечивающих принятие экспертных решений на основе анализа данных о кибератаках и судебной практике.

Целью работы является разработка концепции и прототипа интеллектуальной системы, интегрирующей данные о кибератаках и судебную практику для поддержки экспертов при анализе цифровых преступлений.

Поставленные задачи:

– изучение актуальных подходов к выявлению и классификации кибератак;

– формирование базы данных судебных решений по статьям УК РФ, связанным с компьютерными преступлениями;

– импорт и обработка информации из международной базы MITRE ATT&CK на C++ для взаимодействия с базой данных и анализа полученных данных [1];

– разработка алгоритма взвешивания кибертехник на основе судебной практики.

Создание такой системы открывает возможность интеграции технических аспектов цифровых инцидентов с юридическими нормами. Это формирует новый подход к судебной аналитике и экспертной оценке цифровых доказательств. Разработка прототипа интеллектуальной обучаемой системы для поддержки решений в судебной деятельности становится важным шагом к цифровой трансформации правосудия и внедрению элементов искусственного интеллекта в процессуальную практику.

Концепция и архитектура системы. В ходе практической работы была спроектирована модульная архитектура, ориентированная на удобство масштабирования и простоту сопровождения. Архитектура строится вокруг главной идеи, которая заключается в разделении ответственности между источниками данных, хранилищем и аналитическим ядром. Это позволяет гибко менять любой из компонентов без переработки всей системы, например, заменить парсер источника судебных решений или добавить альтернативный источник техник MITRE без серьезных изменений в аналитической логике.

Разрабатываемая система строится на взаимодействии трех ключевых компонентов: загрузчика данных MITRE, парсера судебных решений и аналитического модуля на C++ [2, 3]. Все элементы объединяются общей базой данных ODBC, что обеспечивает структурированное хранение информации.

Представленные модули формируют единый контур анализа данных, где юридическая и техническая информация объединяются для последующей интеллектуальной обработки (табл. 1).

Разработана архитектура, соответствующая задачам по сбору и анализу данных и подготовленная к масштабированию: интеграции новых источников данных, переходу на распределенную систему хранения при увеличении объемов информации и взаимодействию с нейронными сетями для обучения на основе рассчитанных весов [4].

Таблица 1

Основные компоненты интеллектуальной системы и их функции

Компонент системы	Назначение	Технологии и инструменты
Модуль MITRE (данные атак)	Импорт данных о кибератаках из MITRE ATT&CK	Python, REST API, JSON
Модуль судебной практики	Парсинг судебных решений по ключевым словам	Python, ODBC
База данных ODBC	Хранение и связи данных	ODBC, SQL, ODBC
C++ аналитический модуль	Расчет весов и анализ связей	C++17, ODBC API
Консольное меню	Интерфейс взаимодействия	C++ CLI

Описание алгоритма анализа и расчета весов. В основе интеллектуальной части системы лежит алгоритм анализа, предназначенный для оценки значимости техник MITRE ATT&CK на основе судебной практики (табл. 2). Его цель — связать статистические данные с реально выявленными судебными прецедентами, чтобы выявить, какие методы кибератак чаще встречаются в делах. А также оценить, насколько они релевантные экспертным заключениям. Алгоритм стал связующим элементом между технической и юридической частями системы. Он объединяет логику машинного анализа с элементами экспертного подхода. Наибольший удельный вес наблюдается у техник T1566.001 и T1055, что указывает на их частое использование в процессе расследования киберпреступлений.

Таблица 2

Распределение весов техник MITRE по судебным делам

Техника (ID)	Название техники	Количество дел	Средняя релевантность	Итоговый вес
T1566.001	Spearphishing Attachment	12	0,85	0,845
T1055	Process Injection	8	0,72	0,732
T1003	OS Credential Dumping	6	0,69	0,701
T1059.001	PowerShell Execution	5	0,65	0,674
T1543.003	Windows Service Creation	3	0,58	0,621
T1078	Valid Accounts	2	0,53	0,566
T1027	Obfuscated Files or Information	2	0,49	0,540
T1047	Windows Management Instrumentation	1	0,45	0,493

Этап 1. **Подготовка данных.** Перед началом анализа выполняется автоматическая проверка структуры базы. Система убеждается в наличии необходимых таблиц: techniques, tactics, court_decisions, recommendations и technique_court_decision. При отсутствии хотя бы одной из них программа уведомляет пользователя и завершает работу, предотвращая ошибки вычислений.

Далее из таблиц извлекаются ключевые поля: идентификатор техники (например, T1055), количество судебных дел, в которых она упоминается, оценка релевантности, основанная на экспертной шкале (от 0 до 1). Представленные данные формируют исходный массив для последующего анализа. Управление процессом осуществляется посредством программного кода, написанного на языке программирования C++, с применением структурированных запросов SQL через интерфейс ODBC. Данная архитектура обеспечивает высокую производительность и стабильность системы за счет непосредственной обработки данных на уровне сервера базы данных, что исключает необходимость создания избыточных копий в оперативной памяти.

Этап 2. **Расчет весов.** Основная концепция алгоритма заключается в интеграции двух ключевых метрик: релевантности (relevance_score), которая представляет собой экспертную оценку значимости технического средства в контексте конкретного вида преступления, и частоты (case_count), отражающей количество судебных решений, в которых данное техническое средство упоминается напрямую или косвенно.

Этап 3. **Нормализация и фильтрация данных.** После первичного расчета система нормализует все значения в диапазоне от 0 до 1. Это обеспечивает сравнение между техниками разных классов. Если техника имеет слишком низкий вес (например, менее 0,2), она исключается из итогового списка, чтобы не перегружать вывод малозначимыми элементами. Также алгоритм осуществляет фильтрацию записей, в которых количество дел равно нулю. Автоматически он проводит валидацию корректности заполнения полей. В случае отсутствия релевантных данных используется усредненное значение, соответствующее категории техники. Данная система фильтрации предотвращает искажения в итоговом анализе.

Этап 4. Формирование результатов. После окончания расчета отображается результат в виде таблицы с колонками: technique, name, weight, cases, relevance. Каждая строка сопровождается краткой статистикой, а сами данные сохраняются в базе, чтобы использовать их при дальнейшем обучении нейросетей. Результат сортируется по убыванию веса, что позволяет быстро определить наиболее значимые техники (рис. 1).

Эти значения показывают, что атаки с использованием фишинговых вложений и внедрения процессов наиболее часто встречаются в делах, связанных с несанкционированным доступом и мошенничеством в сети.

Этап 5. Визуализация и экспорт. Полученные результаты могут быть использованы не только в консольном режиме, но и экспортированы для построения диаграмм и гистограмм. Каждая техника представляется в виде точ-

ки на шкале, что облегчает экспертную интерпретацию рассчитанных данных (рис. 2).

```
=== WEIGHTED MITRE ATT&CK TECHNIQUES ===

Technique      Name                          Weight    Cases    Relevance

T1566.001      Spearphishing Attachment      0.845     12       0.85

T1055          Process Injection             0.732     8        0.72

T1003          OS Credential Dumping         0.701     6        0.69
```

Рис. 1. Пример результатов выполнения расчета

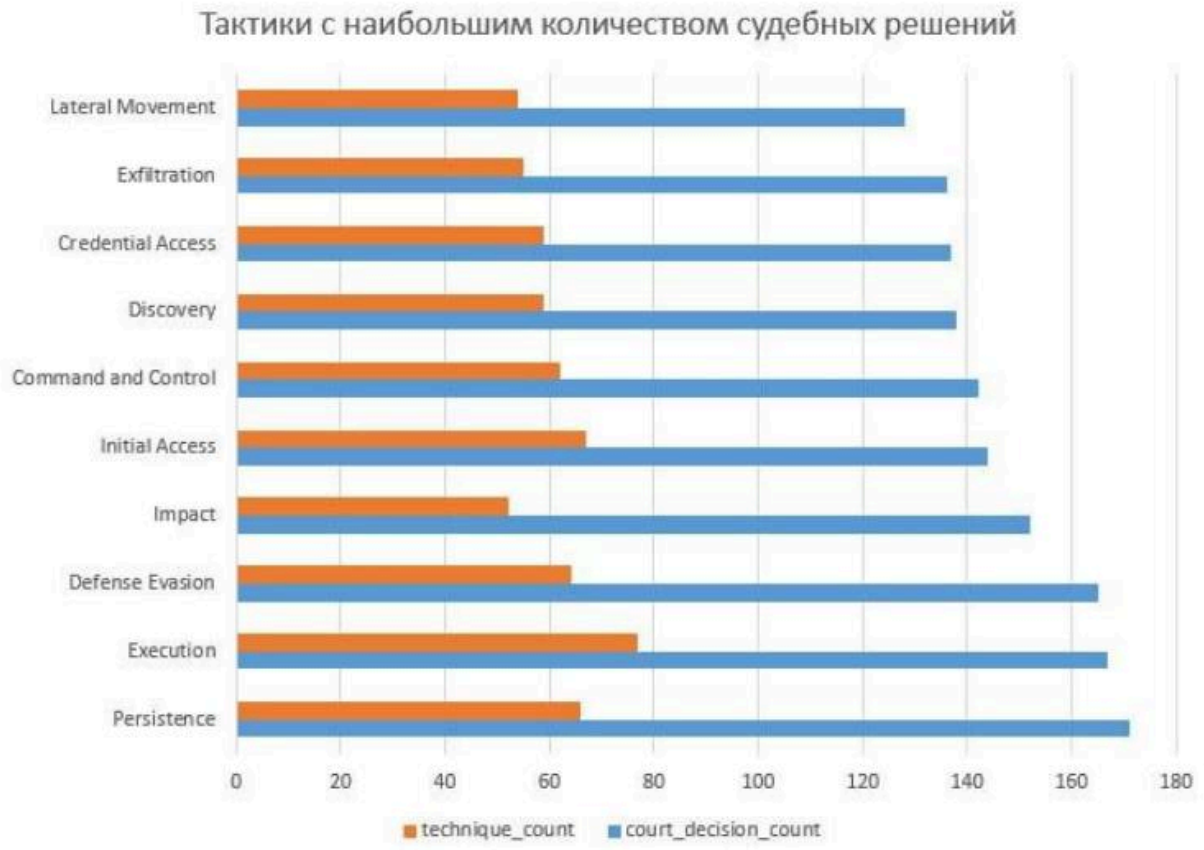

Рис. 2. Гистограмма тактик с наибольшим количеством судебных решений

Этап 6. Самообучение и обновление данных. Система рассчитана на постепенное дообучение. После каждого нового импорта судебных решений значения весов пересчитываются, а старые результаты обновляются с учетом накопленных данных. Это создает эффект адаптивности. Чем больше поступает судебных решений, тем точнее становятся выводы системы. Фактически формируется экспертная среда, где искусственный интеллект и юридическая практика дополняют друг друга.

Результат программной реализации алгоритма расчета весов. Алгоритм расчета весов стал центральным элементом всей архитектуры. Он не

только выполняет обработку, но и задает интеллектуальное поведение системы. Благодаря сочетанию аналитических и экспертных методов удалось получить объективную оценку влияния каждой техники MITRE на судебную практику. Результаты могут использоваться для обучения нейросетевых моделей, построения прогнозов или генерации рекомендаций для следователей и аналитиков при работе с цифровыми доказательствами.

Интерфейс системы и постпроцессорная обработка данных. При запуске программы пользователю отображается консольное меню, в верхней части которого выводятся диагностические строки, информирующие о подключении к базе данных. После установления соединения система сообщает о найденных таблицах и состоянии соединения. Эта информация носит служебный характер и не требует вмешательства со стороны пользователя.

Основная часть интерфейса представляет собой меню, где пользователь может выбрать одну из следующих функций: просмотр тактик MITRE, просмотр техник, расчет весов на основе судебной практики, анализ дел или вывод ранее полученной информации.

При выборе пункта «1» система выводит список тактик MITRE ATT&CK. Количество записей ограничено — в базе содержится 14 тактик, каждая из которых описывает этап атаки: от первичного доступа до командного управления и разведки.

При выборе пункта «2» программа отображает перечень техник MITRE. Всего в базе зарегистрировано 823 техники, охватывающие широкий спектр методов воздействия, включая компрометацию учетных данных, использование PowerShell, внедрение процессов и другие действия злоумышленников.

Консольное меню реализовано в минималистичном текстовом формате, что обеспечивает высокую скорость работы и совместимость с различными операционными системами. Вывод данных производится постранично, что облегчает анализ больших объемов информации.

Результаты парсинга судебных решений. Отдельный модуль отвечает за сбор данных из открытых источников сети Интернет. Парсер реализован на Python и использует библиотеку requests и ODBC. Он получает решения, связанные с компьютерными преступлениями по статьям 272, 273, 274, 159.6 и 183 УК РФ [5, 6].

Каждое дело анализируется построчно. Извлекаются данные о дате, суде, номере и кратком описании. Затем записи добавляются в таблицу court_decisions. Система автоматически связывает каждое решение с техникой MITRE по ключевым словам.

По результатам парсинга судебных решений выявлено, что большинство дел связаны с фишингом, внедрением вредоносного ПО и несанкционированным доступом. Результаты показали, что судебная практика тесно коррелирует с наиболее распространенными техниками MITRE ATT&CK (табл. 3).

Заключение. Разработанный алгоритм взвешивания техник MITRE ATT&CK на основе судебной практики показал свою эффективность в выявлении наиболее значимых и распространенных методов кибератак, использу-

емых в реальных преступлениях. Архитектура системы, построенная по модульному принципу, обеспечила гибкость и масштабируемость решения. Практическая значимость работы заключается в создании инструмента, способного существенно повысить эффективность расследования киберпреступлений за счет автоматизации анализа цифровых доказательств и выявления закономерностей в судебной практике. Система позволяет сократить временные затраты на экспертизу, обеспечить единообразие судебных решений и создать основу для прогнозирования тенденций роста киберпреступности.

Таблица 3

Фрагмент таблицы базы данных судебных решений

№	Номер дела	Дата решения	Суд	Категория	Описание
1	А40-123456/2023	2023-12-15	Арбитражный суд города Москвы	Компьютерные преступления	Несанкционированный доступ к информации
2	А41-789012/2023	2023-11-20	Арбитражный суд Московской области	Вредоносное ПО	Распространение вредоносного программного обеспечения
3	1-234/2023	2023-09-10	Московский городской суд	Компьютерное мошенничество	Дело по ст. 159 УК РФ
4	2-567/2023	2023-09-05	Санкт-Петербургский городской суд	Фишинг и социальная инженерия	Кража персональных данных
5	А43-345678/2024	2024-02-24	Арбитражный суд Нижегородской области	Конфиденциальные данные	Нарушение защиты персональных данных

Перспективы дальнейшего развития системы связаны с интеграцией нейросетевых моделей для более точного прогнозирования, расширением базы судебных решений и созданием интерактивных аналитических панелей для визуализации результатов. Окончательная версия системы будет представлять собой значительный шаг в цифровой трансформации правосудия

и создаст основу для широкого внедрения технологий искусственного интеллекта в юридическую практику. Это откроет новые возможности для повышения эффективности борьбы с киберпреступностью.

Литература

[1] *MITRE ATT&CK Framework Official Documentation*. URL: https://attack.mitre.org/ (accessed 15.09.2025).
[2] Sedgewick R. *Algorithms in C++. Part 5: Graph Algorithms*. Addison-Wesley Professional, 2002, 528 p.
[3] Stroustrup B. *The C++ Programming Language.* Addison-Wesley Professional, 2013, 1366 p.
[4] Осипов Д.Л. *Технологии проектирования баз данных*. Москва, ДМК Пресс, 2019, 498 с.
[5] *Уголовный кодекс РФ*. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 15.09.2025).
[6] *Постановление Пленума Верховного Суда РФ*. URL: https://www.vsrf.ru/documents/own/31913/ (дата обращения 15.09.2025).

Development of a trainable intelligent system for automated expert decision-making based on real data analysis in judicial practice

Gritsenko Yunona Artemovna Yunagritsenko@yandex.ru
Molchanova Natalia Olegovna molchanovannoo@mail.ru
Knyazeva Svetlana Vadimovna knyazevasv@bmstu.ru

BMSTU, Moscow, Russia

This paper presents the concept and implementation of a trainable intelligent system designed to automate expert decision-making in judicial practice. The system integrates technical data from MITRE ATT&CK and judicial precedents related to cybercrime articles of the Russian Criminal Code. An analysis module developed in C++ employs a weighting algorithm to evaluate technique relevance for court cases. The system aims to enhance the efficiency and accuracy of digital forensics and legal analysis by combining artificial intelligence with judicial expertise.

Keywords: *intelligent system, cybercrimes, MITRE ATT&CK, judicial practice, expert system, machine learning, automation*