Научная статья
УДК 004.65:343.3/.7
https://doi.org/10.35266/2949-3455-2025-2-13

Методологические основы создания базы данных для систематизации и анализа преступлений в цифровой среде

Никита Владимирович Савин
Сургутский государственный университет, Сургут, Россия
ООО «СПК САВИН», Тюмень, Россия

Аннотация. В статье рассматриваются методологические основы создания базы данных, предназначенной для систематизации и анализа преступлений, совершаемых в цифровой среде. Предметом исследования является разработка концептуальной структуры базы данных, направленной на поддержку расследования интернет-мошенничеств и дистанционных преступлений. Основная цель работы заключается в проектировании и реализации базы данных, которая позволит структурировать разнородные цифровые следы, повышая эффективность анализа и выявления закономерностей преступной деятельности.

В рамках исследования были поставлены задачи по определению ключевых сущностей базы данных, установлению взаимосвязей между ними. Методология исследования включает концептуальное проектирование, инфологическое и даталогическое моделирование.

Научная новизна исследования заключается в разработке динамической структуры базы данных, способной к автоматическому обновлению и анализу данных в реальном времени. В отличие от существующих решений предложенная модель ориентирована не только на документирование преступлений. Основные результаты работы включают формирование инфологической модели базы данных, описание ее ключевых структурных элементов. В заключение подчеркивается значимость интеграции аналитических инструментов в процессы расследования для повышения оперативности и точности выявления преступных схем в цифровом пространстве.

Ключевые слова: база данных, интернет-мошенничество, цифровые следы, анализ данных, расследование преступлений, искусственный интеллект, машинное обучение, выявление мошеннических схем, криминалистическая аналитика, предсказание преступлений, автоматизация расследования, инфологическое моделирование, киберпреступность, финансовые транзакции, методы социальной инженерии

Для цитирования: Савин Н. В. Методологические основы создания базы данных для систематизации и анализа преступлений в цифровой среде // Вестник Сургутского государственного университета. 2025. Т. 13, № 2. С. 135–144. https://doi.org/10.35266/2949-3455-2025-2-13.

Original article

Database creation and its methodological basis for digital environment crimes systematization and analysis

Nikita V. Savin
Surgut State University, Surgut, Russia
OOO "SPK SAVIN", Tyumen, Russia

Abstract. The article examines the methodological basis for the creation of a database designed to systematize and analyze crimes committed in the digital environment. A conceptual database structure is being developed to aid research into internet and remote crime. The main purpose of the research is to design and implement a database that enables the structuring of diverse digital traces, increasing the efficiency of analysis and identification of crime patterns.

In the research framework, the tasks are set to determine the key entities of the database, to establish the correlations between them. The research methodology includes conceptual design, infological, and datalogical modeling.

The scientific novelty of the study lies in the development of a dynamic database structure capable of automatic updating and data analysis in real time. In contrast to existing solutions, the proposed model prioritizes more than mere crime documentation. The major results of the research include the formation of the database infological model, description of its key structural elements. The conclusion emphasizes the importance of integrating analytical tools into the investigation process to improve the speed and accuracy of criminal schemes detection in the digital space.

Keywords: database, internet fraud, digital footprints, data analysis, crime investigation, artificial intelligence, machine learning, detection of fraudulent schemes, forensic analytics, crime prediction, investigation automation, infological modeling, cybercrime, financial transactions, social engineering methods

For citation: Savin N. V. Database creation and its methodological basis for digital environment crimes systematization and analysis. *Surgut State University Journal*. 2025;13(2):135–144. https://doi.org/10.35266/2949-3455-2025-2-13.

ВВЕДЕНИЕ

В эпоху стремительной цифровой трансформации общества количество преступлений, совершаемых в цифровой среде, растет в геометрической прогрессии, ущерб от киберпреступлений в России достигает 156 миллиардов рублей в год, что свидетельствует о необходимости внедрения современных методов борьбы с мошенничеством [1]. Интернет-мошенничество, киберпреступность и различные формы цифрового обмана представляют серьезную угрозу для частных лиц, бизнеса и государственных учреждений. Отсутствие структурированного подхода к систематизации и анализу данных о таких преступлениях значительно затрудняет их расследование и предотвращение. В условиях усложнения мошеннических схем и повсеместного использования технологий анонимизации традиционные методы расследования оказываются недостаточно эффективными. Поэтому разработка интеллектуальной системы базы данных, интегрирующей методы искусственного интеллекта и машинного обучения, становится необходимым шагом для эффективной борьбы с цифровыми преступлениями.

Предыдущие исследования в данной области в основном фокусировались на отдельных аспектах выявления киберпреступлений, таких как мониторинг транзакций, обнаружение аномалий и цифровая криминалистика. В частности, данные, представленные в работе О. В. Ждановой, Ю. В. Лабовской, И. Ф. Дедюхиной, подчеркивают важность эффективных механизмов предупреждения и выявления мошенничества в финансовых операциях [2]. Например, в исследовании Т. А. Осиповой, К. С. Зайцева и В. О. Биферта рассматривается применение алгоритмов машинного обучения для выявления мошенничества при использовании пластиковых карт, что имеет непосредственное отношение к анализу финансовых преступлений в цифровой среде [3]. Однако существующие модели не обеспечивают комплексного подхода к систематизации цифровых следов и установлению связей между разрозненными данными различных преступлений. Кроме того, остается нерешенной проблема обработки данных в реальном времени, что затрудняет прогнозирование и предотвращение новых угроз.

Важность разработки интегрированной системы хранения и анализа информации о цифровых преступлениях подтверждается на государственном уровне. В декабре 2024 г. в России было принято постановление Правительства РФ № 1805, в котором обозначены ключевые направления цифровизации правоохранительной деятельности [1]. В рамках данной программы предусматривается создание единой платформы обмена данными о мошеннических действиях, усиление сотрудничества между правоохранительными органами, банками и операторами связи, а также применение искусственного интеллекта для автоматизированного анализа преступных

схем. Кроме того, документ подчеркивает необходимость использования аналитических технологий для предсказания мошеннических схем и их предотвращения.

Настоящее исследование направлено на устранение этих недостатков путем разработки концептуальной структуры базы данных, ориентированной на систематический анализ преступлений в цифровой среде. Основные задачи исследования включают определение ключевых сущностей базы данных, установление взаимосвязей между ними и интеграцию аналитических инструментов на основе искусственного интеллекта для повышения эффективности расследований. Исследование также призвано решить нерешенные вопросы, такие как автоматизация выявления преступных паттернов и улучшение совместимости данных между правоохранительными органами.

А. В. Кокин и Ю. Д. Денисов в своей работе отмечают, что внедрение искусственного интеллекта в криминалистику и судебную экспертизу может существенно повысить эффективность расследований и аналитической работы. По их мнению, «машинное обучение считается одной из форм искусственного интеллекта и представляет собой использование математических моделей данных, обеспечивающих обучение компьютера посредством специализированных алгоритмов и тренировочных данных» [4, с. 30]. Это подтверждает актуальность интеграции технологий ИИ в криминалистические базы данных, что позволит повысить точность анализа мошеннических схем, автоматизировать выявление цифровых следов преступлений и минимизировать влияние человеческого фактора в процессах идентификации подозреваемых. В данном контексте исследование, посвященное разработке базы данных для систематизации и анализа преступлений в цифровой среде, дополняет современные подходы к внедрению технологий ИИ в правоохранительную деятельность.

МАТЕРИАЛЫ И МЕТОДЫ

Современный мир характеризуется огромным объемом создаваемой информации, которая часто оказывается неструктурированной и фрагментированной. Это особенно актуально для расследований интернет-мошенничеств, где данные поступают из различных источников: социальных сетей, мессенджеров, финансовых транзакций и цифровых следов. Отсутствие структурированности информации значительно осложняет ее анализ и использование. Для устранения данной сложности необходимо разработать специализированную базу данных, которая позволит систематизировать, обрабатывать и анализировать информацию, связанную с преступлениями, совершенными в цифровой среде.

Согласно определению, база данных представляет собой «набор взаимосвязанных сведений (фактов), относящихся к определенной предметной области, организованных по установленным правилам, предусматривающим их представление, хранение и манипулирование ими» [5].

Разработка подобной базы данных для расследований интернет-мошенничеств является важной задачей, направленной на систематизацию и структурированное хранение сведений о мошеннических действиях, цифровых следах и потерпевших. Одной из ключевых целей является эффективный анализ информации, который достигается путем интеграции алгоритмов искусственного интеллекта для выявления закономерностей и анализа паттернов поведения преступников. Кроме того, разработка такой базы данных позволит повысить доступность данных и значительно ускорить процесс расследования за счет создания единого информационного ресурса, и это позволит систематизировать данные и интегрировать в них инструменты искусственного интеллекта (ИИ) для анализа [6]. Это, в свою очередь, обеспечит улучшение координации между различными подразделениями, предоставляя удобный интерфейс для обмена информацией между ведомствами и правоохранительными структурами.

Кейтлин Гуруле в своей работе отмечает, что «применение автоматизированных методов анализа цифровых данных может не только ускорить расследование преступлений, но и выявлять новые преступные схемы до их

реализации» [7, с. 35]. В контексте исследования цифровых мошенничеств интеграция технологий искусственного интеллекта и методов анализа больших данных становится ключевым элементом проактивной защиты цифровой безопасности.

Современные технологии позволяют создавать два основных типа баз данных, которые могут использоваться в борьбе с интернет-мошенничествами:

Фактографические базы данных включают структурированную информацию и могут содержать информацию о случаях мошенничества, таких как:

- данные о мошенниках (IP-адреса, email, используемые сайты);
- цифровые следы (лог-файлы, метаданные сообщений);
- финансовые транзакции (переводы, криптовалютные кошельки).

Такие БД позволяют эффективно хранить и анализировать данные для быстрого извлечения необходимой информации.

Полнотекстовые базы данных ориентированы на хранение текстовых данных и могут содержать следующую информацию:

– переписка между мошенниками и потерпевшими;
– анализ текстов мошеннических писем (фишинговых);
– сохраненные архивы сообщений из мессенджеров.

Полнотекстовые БД позволяют выполнять поиск по текстам и проводить лингвистический анализ, что особенно важно для выявления мошеннических шаблонов.

Методологической основой создания базы данных для разработки системы выступает концепция проектирования реляционных баз данных. Это обеспечивает гибкость и масштабируемость системы, позволяя добавлять новые типы данных и связи между объектами.

Проектирование базы данных для расследования мошенничеств включает несколько ключевых этапов. На первом этапе проводится анализ предметной области, в ходе которого определяются основные объекты описания, такие как мошенники, их методы и цифровые следы, потерпевшие с характеристиками их личности и сумма ущерба, а также события, фиксирующие хронологию и обстоятельства преступлений. Выявляются взаимосвязи между этими объектами, например один мошенник может быть связан с несколькими преступлениями.

Далее формируется инфологическая модель, определяющая структуру данных. Основными элементами являются таблицы «Происшествия», содержащая сведения об IP-адресах, email и используемых устройствах; «Потерпевшие», включающая возраст, регион проживания и другую информацию о потерпевших; «Преступник», в которой фиксируются схемы мошенничества, даты происшествий и сумма нанесенного ущерба.

Следующим этапом является разработка даталогической модели, где детализируются атрибуты объектов и устанавливаются связи между ними. Для каждого происшествия фиксируются соответствующие цифровые следы, данные о мошенниках и потерпевших. Используются индексы для ускорения поиска и анализа информации.

Для реализации базы данных применяются современные системы управления базами данных (СУБД), такие как PostgreSQL и MySQL, обеспечивающие создание реляционных БД, а также MongoDB, которая позволяет хранить полуструктурированные данные, например переписку. Основой методологии послужил подход концептуального проектирования реляционных баз данных [8]. Интеграция с библиотеками Python способствует эффективному анализу данных и автоматизации обработки информации.

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

На первом этапе концептуального проектирования формулируется система задач, которые должна решать разрабатываемая база данных для расследования интернет-мошенничеств и дистанционных преступлений. Основная проблема, требующая решения, связана с систематизацией разнородных данных о мошенничествах, их методах, цифровых следах и потерпевших. В этом контексте

ключевые информационные задачи базы данных формулируются в виде вопросов, на которые должны быть получены ответы при помощи аналитических запросов:

1. Какие виды интернет-мошенничеств были зафиксированы в исследуемый период?
2. Какова динамика распространения различных схем мошенничеств по годам?
3. Какие платформы (социальные сети, мессенджеры, сайты) чаще всего использовались мошенниками?
4. Какова география преступлений? В каких регионах зарегистрировано наибольшее число случаев?
5. Какие цифровые следы оставляют мошенники (IP-адреса, доменные имена, устройства)?
6. Как связаны между собой разные случаи мошенничеств? Имеются ли повторяющиеся IP-адреса, email, номера карт?
7. Какие финансовые инструменты (банковские карты, криптовалютные кошельки) использовались для вывода средств?
8. Какова средняя сумма ущерба по различным видам мошенничеств?
9. Какие демографические группы наиболее подвержены интернет-мошенничествам (возраст, пол, профессия, регион)?
10. Как часто потерпевшие сообщают о мошенничестве в правоохранительные органы?
11. Какие методы социальной инженерии использовали мошенники (давление, манипуляция доверием, создание срочности и т. д.)?
12. Какой процент мошеннических схем включает фишинговые атаки?
13. Как часто мошенники меняют схемы работы и адаптируются к новым условиям?
14. Какова корреляция между видами мошенничества и каналами их распространения (email, телефон, сайты, соцсети)?
15. Какие группы мошенников действуют организованно, а какие – единичные случаи?
16. Как можно прогнозировать новые схемы мошенничества на основе накопленных данных?
17. Как связаны мошеннические группы между собой? Можно ли выявить связи через анализ сетевых данных?
18. Как часто мошенники используют поддельные документы, сайты, идентификаторы для сокрытия личности?
19. Какие действия чаще всего предпринимаются для минимизации последствий после мошенничества?
20. Какова средняя скорость расследования различных видов интернет-мошенничеств?

Определение данных вопросов служит основой для следующего этапа проектирования, включающего построение инфологической модели базы данных, разработку ее структуры и внедрение технологий искусственного интеллекта с целью автоматизированного анализа преступной деятельности.

На втором этапе концептуального проектирования проводится детальный анализ предметной области с последующим формированием ее инфологической модели в соответствии с поставленными задачами. В ходе этого процесса необходимо определить основные сущности базы данных, а также установить логические связи между ними, что позволит эффективно структурировать и организовать хранимую информацию.

В рамках данного исследования объектом рассмотрения выступает система расследования интернет-мошенничеств и дистанционных преступлений. Основными объектами описания являются:

– происшествия, зарегистрированные в исследуемый период;
– преступники, совершавшие мошеннические действия;
– потерпевшие и их характеристики.

Эти сущности формируют концептуальную структуру базы данных (рисунок). Ядром является таблица «Происшествия», которая объединяет вспомогательные объекты – таблицы, содержащие сведения о преступниках и потерпевших. Каждая сущность связана с записью о происшествии, что позволяет отслеживать всю цепочку событий, связанных с конкретным случаем мошенничества.

На третьем этапе проектирования разрабатывается даталогическая модель базы данных, определяющая структуру полей таблиц и их соответствие атрибутам объектов,

Рисунок. Инфологическая схема БД

Примечание: составлено автором на основании данных, полученных в исследовании.

представленных в системе. Каждая сущность базы данных характеризуется набором атрибутов, что обуславливает различия в структурах основной и вспомогательных таблиц. В соответствии с поставленными задачами, направленными на систематизацию и анализ интернет-мошенничеств, были разработаны даталогические схемы. Структура центральной таблицы «Происшествия» представлена в табл. 1.

Прокомментируем эту структуру:

1. Поле «Код происшествия» представляет собой уникальный числовой идентификатор, обеспечивающий однозначную идентификацию записей в базе данных, что позволяет системе корректно их обрабатывать и предотвращать дублирование.

2. Поле «Метод мошенничества» определяет, каким способом было совершено

Таблица 1

Структура таблицы «Происшествия»

Поле	Тип данных
Код происшествия	INTEGER
Метод мошенничества	VARCHAR
Канал коммуникации	VARCHAR
Дата и время	TIMESTAMP
Цифровые следы	TEXT
Финансовый ущерб	DECIMAL
Географическая привязка	VARCHAR
Связанные происшествия	TEXT
Статус расследования	VARCHAR

Примечание: составлено автором на основании данных, полученных в исследовании.

преступление (фишинг, взлом аккаунта, поддельные транзакции и т. д.).

3. Поле «Канал коммуникации» фиксирует платформу, через которую произошло взаимодействие между мошенником и потерпевшим (электронная почта, телефонный звонок, социальные сети и др.).

4. Поле «Дата и время» хранит временные параметры происшествия, что позволяет проводить анализ частоты преступлений.

5. Поле «Цифровые следы» содержит техническую информацию, включая IP-адреса, использованные устройства, почтовые адреса, номера телефонов и криптовалютные кошельки.

6. Поле «Финансовый ущерб» фиксирует сумму потерь, понесенных потерпевшим в результате мошенничества.

7. Поле «Географическая привязка» указывает регион, в котором произошло преступление, что важно для выявления территориальных закономерностей.

9. Поле «Связанные происшествия» позволяет устанавливать взаимосвязи между различными случаями мошенничеств на основе совпадения IP-адресов, финансовых операций и других факторов.

10. Поле «Статус расследования» отображает текущее состояние работы по делу (открыто, на рассмотрении, передано в суд и т. д.).

Даталогические схемы вспомогательных таблиц, содержащих информацию о преступниках (табл. 2) и потерпевших (табл. 3), имеют свою специфику.

Прокомментируем структуру таблицы «Преступник»:

1. Поле «Код преступника»: уникальный идентификатор записи.

2. Поле «Имя/псевдоним» отображает известное имя или никнейм преступника.

3. Поле «Связанные происшествия» связывает преступника с зарегистрированными случаями мошенничества.

4. Поле «Цифровые следы» фиксирует IP-адреса, email, устройства и другие технические идентификаторы.

5. Поле «Метод работы»: описание схем и инструментов, используемых преступником.

Таблица 2

Структура таблицы «Преступник»

Поле	Тип данных
Код преступника	INTEGER
Имя/псевдоним	VARCHAR
Связанные происшествия	TEXT
Цифровые следы	TEXT
Метод работы	TEXT
Статус	VARCHAR

Примечание: составлено автором на основании данных, полученных в исследовании.

Таблица 3

Структура таблицы «Потерпевший»

Поле	Тип данных
Код потерпевшего	INTEGER
Возраст	INTEGER
Регион проживания	VARCHAR
Способ взаимодействия	VARCHAR
Финансовые потери	DECIMAL
Обращение в полицию	BOOLEAN
Связанные происшествия	TEXT

Примечание: составлено автором на основании данных, полученных в исследовании.

6. Поле «Статус» указывает на текущий статус (идентифицирован, в розыске, задержан и т. д.).

Структура таблицы «Потерпевший»:

1. Поле «Код потерпевшего»: уникальный идентификатор записи.

2. Поле «Возраст»: возраст потерпевшего для выявления уязвимых групп.

3. Поле «Регион проживания» помогает анализировать географическое распространение мошенничеств.

4. Поле «Способ взаимодействия» фиксирует, каким образом мошенник вышел на контакт.

5. Поле «Финансовые потери» отражает сумму ущерба.

6. Поле «Обращение в полицию» указывает, было ли подано официальное заявление.

7. Поле «Связанные происшествия» связывает потерпевшего с зарегистрированными случаями мошенничества.

Представляется обоснованным предположить, что предложенная структура базы данных подлежит дальнейшей оптимизации в процессе разработки программного обеспечения, что обеспечит ее адаптивность, возможность расширения функционала и интеграцию с автоматизированными инструментами анализа данных.

В соответствии с обозначенной структурой целесообразно продемонстрировать решение ряда задач путем моделирования конкретных сценариев обработки информации в рамках расследования интернет-мошенничеств.

Задача 1: Сколько случаев интернет-мошенничества зарегистрировано за определенный период? → Задание: определить количество записей в таблице «Происшествия» → Запрос на подсчет всех записей в данной таблице.

Задача 2: Какие типы мошенничеств были наиболее распространены? → Задание: определить частоту вхождения значений в поле «Тип мошенничества» → Запрос на поиск повторяющихся значений в этом поле и их подсчет.

Задача 3: Какие схемы мошенничества наиболее часто использовались? → Задание: анализ частоты определенных методов обмана (фишинг, социальная инженерия, поддельные инвестиции) → Запрос на группировку данных по схеме мошенничества.

Задача 4: Какова связь между различными случаями мошенничества? → Задание: выявить случаи, имеющие общие цифровые следы (IP-адреса, криптовалютные кошельки, телефонные номера) → Запрос на поиск пересечений значений между различными происшествиями.

Несомненно, предложенные выше подходы являются демонстрационными и могут быть дополнены новыми методами и сценариями в рамках дальнейших исследований. На данном этапе проектирования уже прослеживается потенциал создаваемой информационной системы в части решения сформулированных исследовательских вопросов. Ее применение обеспечит возможность комплексного количественного анализа преступлений, что, в свою очередь, позволит выявлять закономерности в деятельности мошеннических группировок и разрабатывать эффективные стратегии противодействия цифровым преступлениям.

При разработке содержания системы предполагается провести масштабный мониторинг и сбор информации из различных источников:

1) баз данных правоохранительных органов, содержащих сведения о зарегистрированных преступлениях;

2) аналитических отчетов финансовых учреждений о подозрительных транзакциях;

3) интернет-ресурсов, включая форумы, черные рынки и платформы, где мошенники координируют свои действия.

Критерием формирования выборки станет период совершения преступлений, а также типология мошеннических схем. Объем выборки не ограничен, так как база данных должна быть динамической и регулярно пополняться новыми случаями.

Собранный материал послужит основой для дальнейшей работы по созданию концепции аналитической платформы, интегрирующей методы искусственного интеллекта для выработки тактики их расследования.

ЗАКЛЮЧЕНИЕ

Проведенное исследование позволило реализовать ключевые цели, поставленные в начале работы, а именно: разработать концептуальные и методологические основы создания базы данных для расследования интернет-мошенничеств. В ходе анализа были определены основные объекты предметной области, структурированы взаимосвязи между ними и предложена модель базы данных, обеспечивающая эффективное хранение, обработку и анализ информации о преступлениях, совершенных в цифровой среде.

Разработка базы данных, интегрированной с методами искусственного интеллекта, позволяет значительно повысить эффективность расследований, минимизировать временные затраты на анализ информации и автоматизировать процесс выявления закономерностей в деятельности мошенников. Применение методов машинного обучения в задачах классификации мошеннических схем, предсказания потенциальных угроз и детектирования аномалий в цифровых данных представляет собой одно из наиболее перспективных направлений современных исследований в области кибербезопасности и криминалистического анализа. Дальнейшая разработка таких алгоритмов может способствовать значительному повышению эффективности автоматизированного выявления преступных паттернов и адаптации системы к динамически изменяющимся схемам мошенничества.

Вклад проведенного исследования в научный контекст заключается в предложении комплексного подхода к созданию базы данных, сочетающего концептуальное проектирование, инфологическую и даталогическую модели, а также применение аналитических инструментов для выявления преступных паттернов. В отличие от существующих решений предложенная модель ориентирована не только на документирование преступлений, но и на их динамический анализ с возможностью предсказания новых схем мошенничества.

Дальнейшие исследования могут быть сосредоточены на разработке автоматизированных инструментов взаимодействия базы данных с правоохранительными органами, создании моделей глубокого обучения для повышения точности классификации мошеннических действий, а также интеграции с международными базами данных для борьбы с трансграничной киберпреступностью. Кроме того, особого внимания заслуживает правовой аспект использования баз данных в уголовном процессе, включая вопросы защиты персональных данных и соблюдения требований законодательства при автоматизированном анализе преступной деятельности.

Таким образом, представленная работа формирует научную и практическую основу для дальнейшего совершенствования цифровых инструментов расследования интернет-мошенничеств, способствуя повышению эффективности работы правоохранительных органов в условиях стремительного роста киберпреступности.

Список источников

1. О внесении изменений в некоторые акты Правительства Российской Федерации : постановление Правительства Российской Федерации от 17.12.2024 № 1805 // СЗ РФ. 2024. № 52. Ст. 8344. Доступ из СПС «Гарант».
2. Жданова О. В., Лабовская Ю. В., Дедюхина И. Ф. Финансовое мошенничество в современном мире // Государственная служба и кадры. 2020. № 4. С. 95–97.
3. Осипова Т. А., Зайцев К. С., Биферт В. О. Применение алгоритмов машинного обучения к задаче выявления мошенничества при использовании пластиковых карт // International Journal of Open Information Technologies. 2021. Т. 9, № 8. С. 23–29.

References

1. On Amendments to Certain Acts of the Government of the Russian Federation: Resolution of the Government of the Russian Federation of December 17, 2024, No. 1805. Collection of Legislation of the Russian Federation. 2024. No. 52. Art. 8344. Accessed through Law assistance system “Garant”. (In Russ.).
2. Zhdanova O. V., Labovskaya Yu. V., Dedyukhina I. F. Financial fraud in the modern world. *Gosudarstvennaya sluzhba i kadry*. 2020;(4):95–97. (In Russ.).
3. Osipova T. A., Zaytsev K. S., Bifert V. O. The Use of ML algorithms in the task of detecting fraud when using plastic cards. *International Journal of Open Information Technologies*. 2021;9(8):23–29. (In Russ.).

4. Кокин А. В., Денисов Ю. Д. Искусственный интеллект в криминалистике и судебной экспертизе: вопросы правосубъектности и алгоритмической предвзятости // Теория и практика судебной экспертизы. 2023. Т. 18, № 2. С. 30–37. https://doi.org/10.30764/1819-2785-2023-2-30-37.
5. ГОСТ Р 43.0.11-2014. Информационное обеспечение техники и операторской деятельности. Базы данных в технической деятельности. М. : Стандартинформ, 2018.
6. Харина Е. А. Особенности методики расследования мошенничества в сфере компьютерной информации : дис. … канд. юрид. наук. Красноярск : Красноярский государственный аграрный университет, 2024. 248 с.
7. Gurule K. An analysis of digital forensic units. Master of Sci. Thesis. Purdue University, 2016. 78 p.
8. Попова-Коварцева Д. А., Сопченко Е. В. Основы проектирования баз данных. Самара : Изд-во Самарского университета, 2019. 112 с.

4. Kokin A. V., Denisov Yu. D. Artificial Intelligence in Criminalistics and Forensic Examination: Issues of Legal Personality and Algorithmic Bias. *Theory and Practice of Forensic Science*. 2023;18(2):30–37. https://doi.org/10.30764/1819-2785-2023-2-30-37. (In Russ.).
5. GOST (State Standard) R 43.0.11-2014. Information support for technology and operator activities. Databases in technical activities. Moscow: Standartinform; 2018. (In Russ.).
6. Kharina E. A. Osobennosti metodiki rassledovaniya moshennichestva v sfere kom-pyuternoy informatsii. Cand. Sci. (Law) Thesis. Krasnoyarsk: Krasnoyarsk State Agrarian University; 2024. 248 p. (In Russ.).
7. Gurule K. An analysis of digital forensic units. Master of Sci. Thesis. Purdue University; 2016. 78 p.
8. Popova-Kovartseva D. A., Sopchenko E. V. Osnovy proektirovaniya baz dannykh. Samara: Izd-vo Samara State University; 2019. 112 p. (In Russ.).

Информация об авторе

Н. В. Савин – аспирант, генеральный директор; https://orcid.org/0009-0004-0336-726X, savin_nv@edu.surgu.ru

About the author

N. V. Savin – Postgraduate, Chief Executive Officer; https://orcid.org/0009-0004-0336-726X, savin_nv@edu.surgu.ru