МЕТОДЫ ФОРМИРОВАНИЯ ДОКАЗАТЕЛЬНОЙ БАЗЫ ДЛЯ ПРЕСТУПЛЕНИЙ В IOT-СИСТЕМАХ УМНЫХ ДОМОВ: ДОСТИЖЕНИЯ И ВЫЗОВЫ

Курмаева Маликахон Рустамовна

[**Введение]** Современные умные дома значительно упрощают повседневную жизнь, но одновременно становятся мишенью для злоумышленников. Преступления, совершаемые с использованием IoT-систем, требуют разработки эффективных методов сбора и анализа данных для формирования доказательной базы. Это исследование направлено на анализ существующих подходов, выявление актуальных вызовов и определение практических путей их преодоления.

[Актуальность исследования] Исследование актуально в условиях роста числа подключенных устройств по всему миру, что делает проблему киберпреступлений, связанных с утечкой данных, несанкционированным доступом и саботажем систем умных домов, глобальной и требующей координации усилий специалистов. Несмотря на значительный прогресс в области кибербезопасности, создание надежной доказательной базы для судебного рассмотрения остается сложной задачей.

[Цели и задачи работы] Основной целью данного исследования является изучение современных достижений и выявление ключевых вызовов в формировании доказательной базы для преступлений, совершаемых в умных домах. Для достижения этой цели поставлены следующие задачи:

1. Провести анализ существующих методов сбора данных в IoT-системах.
2. Изучить технологии анализа доказательств, так как выводы, сделанные из полученных данных IoT-систем, играют ключевую роль в расследовании преступлений.
3. Определить основные проблемы, с которыми сталкиваются эксперты, и предложить перспективные направления для дальнейших исследований.

[Методы исследования] Исследование базируется на анализе научной литературы в сфере цифровой криминалистики, посвященной формированию доказательственной базы преступлений в умных домах и использовании методов сравнительного анализа. Сравнительный анализ позволил выявить сильные и слабые стороны существующих методов, а также определить их применимость в реальных условиях.

[Результаты исследования] Выявлены основные достижения, такие как разработка методологии автоматизированного извлечения данных и создание фреймворка для сбора информации. Однако большинство представленных решений требуют дальнейшей валидации через реальные кейсы. Предложены перспективные направления, включая разработку искусственного интеллекта для определения возможных доказательств.

[Выводы] Развитие IoT-систем требует интеграции более надежных методов цифровой криминалистики. Ключевыми вызовами остаются сложность стандартизации и необходимость учета специфики IoT-устройств. Для преодоления этих проблем важно адаптировать технологии искусственного интеллекта к потребностям криминалистики и развивать международное сотрудничество в данной сфере.