ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В КРИМИНАЛИСТИКЕ

Алчакова Алина Шамильевна

студент, Юридический институт, Северо-Кавказский Федеральный Университет, РФ, г. Ставрополь

Щербалев Андрей Андреевич

научный руководитель, ассистент кафедры уголовного права и процесса юридического института Северо-Кавказского Федеральный Университет, РФ, г.Ставрополь

ARTIFICIAL INTELLIGENCE IN FORENSIC SCIENCE

Alina Alchakova

Student, Law Instituter, North-Caucasus Federal University, Russia, Stavropol

Andrey Shcherbalev

Assistant of the department of criminal law and procedure law institute, North-Caucasus Federal University, Russia, Stavropol

В эпоху передовых технологий и их активного внедрения в жизни людей увеличилось и количество киберпреступлений. К сожалению, традиционные методы расследования данной категории преступлений менее эффективны, поэтому искусственного интеллекта в работе криминалистов в сфере кибербезопасности поможет их результативности.

Применение технологии искусственного интеллекта в сфере цифровой криминалистики предоставляет новые перспективы для расследования. Особенно насущно в сфере киберпреступлений, так как для их раскрытия необходимо проанализировать огромный объем данных.

Для выполнения рутинных операций, таких как сбор и систематизация информатизация, можно использовать алгоритмы машинного оборудования, что поможет снять нагрузку со специалистом. Благодаря этому они смогут обратить своё внимание на те задачи, которые требуют их вмешательства, например, для разработки более эффективных стратегий противодействия преступной деятельности.

Ярким примером успешного применения подобных технологий служит система PredPol которая предназначена для выявления потенциальных преступлений. Эта система анализирует архивные данные о преступлениях и правонарушениях, помимо этого она способна прогнозировать место и время инцидентов, которые могут произойти в будущем, следовательно повышая результативность деятельности правоохранительных органов и позволяя оптимально распределить силы для проведения профилактического характера.

Ключевой особенностью ИИ является его способность адаптироваться к меняющейся криминальной обстановке. Из-за того, что мошенники постоянно совершенствуют свои

методы, то алгоритмы машинного обучения демонстрируют способность своевременно выявлять новые типы угроз и уязвимостей, которые могут остаться незамеченными при применении традиционных аналитических подходов, тем самым предоставляя сотрудникам правоохранительных органов возможности для предотвращения киберпреступлений ещё до их совершения.

Внедрения ИИ в сфере цифровой криминалистикой экспертизы связанно с рядом существенных проблем. Основными таким проблемами являются сложности в толковании работы алгоритмов и потенциальная возможность их использования преступниками для совершения киберпреступлений.

Очень важно для преодоления данных препятствий организовать качественную подготовку сотрудников в сфере цифровой криминалистики. В связи с этим образовательный процесс должен сочетать в себе не только технические аспекты взаимодействия с ИИ-системами, но и вопросы по обеспечению прозрачности работы алгоритмов. Что в свою очередь позволит сформировать доверие к результатам, которые будут получать при помощи системы, также сбалансировать взаимодействие всех участников мероприятий по раскрытию и предупреждению преступлений.

Создание комплексных рабочих групп является наиболее перспективным направлением по внедрению искусственного интеллекта в работу правоохранительных органов. Состав таких междисциплинарных экспертных групп должен включать в себя специалистов по кибербезопасности, разработчики систем ИИ и представителей правоохранительных структур. Следует упомянуть о том, что такое сочетание компетенций, поспособствует эффекту взаимодополнения, потому что обмен знаниями и практическим опытом, который есть у специалистов ускорит процесс принятия решений. Поэтому необходимо создать информационную среду, доступ которой будет предоставляться только специалистам, а так же защищаться от мошенников. Все это поможет наиболее результативно применить экспертизы коллег, а также продумать более надежную стратегию для раскрытия быстро совершающихся киберпреступлений.

Так же не следует забывать про этические принципы. В связи с эти нужно разработать нормы и регламенты их применения. Для того чтобы не возникало каких-либо проблем в применении данных норм, нужно как можно детальнее описать процедуры, гарантирующие соблюдение прав и свобод граждан, а также их законных интересов. То есть необходимо регламентации подлежат все стадии применения ИИ, начиная с первой – сбор информации, и заканчивая последней – финальная обработка данных. Тем самим мы сможем минимизировать все те риски, которые могут появиться, но помимо этого все это поспособствует укреплению общественного доверия к применению искусственного интеллекта.

Для постоянного совершенствования необходимо наладить взаимоотношения и с научными лабораториями, что будет способствовать разработке новых методов расследования данной категории преступлений. Тем самым предоставляя возможность сотрудникам правоохранительных органов расширить свой возможности по противодействию преступлениям, которые всегда совершенствуются. Симбиоз, интеллектуальных ресурсов искусственного интеллекта и криминалистов в сфере цифровой криминалистики, поможет разрабатывать новые стратегии для того, чтобы раскрыть киберпреступления, также разработать методы для предупреждения и предотвращения преступной деятельности кибермошенников.

Список литературы:

1. Мамекин Д.Н., Цехновецкая В.М. К вопросу применения цифровых технологий в криминалистике // Вестник Фак. бизнеса и права. – 2023. – № 1. – С. 432–438.

2. Скобелин С.Ю. Цифровая криминалистика: объект и направления развития // Российский следователь. – 2020. – № 4. – С . 27 – 29.