Секция «Обеспечение финансовой безопасности России: финансовые расследования в цифровой экономике»

Мошенничество: особенности противодействия в рамках цифровой экономики и перспективы использования современных технологий при расследовании

Научный руководитель – Анищенко Евгений Владимирович

Стальмахов Александр Александрович
Выпускник (бакалавр)
Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра экономических и финансовых расследований, Москва, Россия
E-mail: sannicx@mail.ru

Несмотря на то, что понятие экономические преступления не закреплено официально, данный вид преступлений является одним из самых распространенных и обладает характерными признаками, позволяющие отличить от других видов. С развитием информационных технологий появляются новые способы их совершения. Особенно популярным становится совершение онлайн. Мошенничество не стало исключением, напротив, статистика показывает, что число совершенных противоправных деяний с каждым годом растет. Это, в свою очередь, становится и является серьезной проблемой для экономики страны в целом. Особенно это сказывается на цифровой экономике, поскольку в большое количество мошеннических действий происходят посредством сети Интернет или мобильных средств связи. В российском законодательстве, на сегодняшний день, в статьях 159.3 и 159.6 закреплены составы преступлений, которые относят к мошенничеству в сети Интернет. Из этого следует, что правоохранительные органы должны совершенствовать способы борьбы с данным видом мошенничества, также используя современные технологии.

При помощи современных технологий механизмы противодействия мошенничеству продолжают развиваться. В рамках цифровой экономики принято выделять несколько аспектов, которые активно используют для противодействия «онлайн-мошенников».

Стоит начать с использования искусственного интеллекта и аналитики данных. Данный аспект примечателен тем, что современные технологии способны помочь в выявлении аномалий и обнаружении подозрительной активности. Это способствует раннему распознаванию мошеннических схем. Хорошим примером можно привести официальный сайт и приложения мэра Москвы «Мос.Ру». Следующей особенностью считается технология блокчейн, которая может быть использована для создания прозрачных и безопасных систем хранения и передачи данных, что помогает бороться с фальсификацией информации. Далее выделяют биометрическую идентификацию. Системы биометрической идентификации могут значительно повысить уровень безопасности, предотвращая несанкционированный доступ к информации. Обучение машин – это техника, что позволяет создавать модели поведения, которые могут автоматически выявлять подозрительные действия и предотвращать мошенничество.

Далее следует перейти к вопросу перспектив использования современных технологий при расследовании мошенничества в цифровой экономике. Здесь также существуют определенные методы.

Первой можно выделить цифровую криминалистику, или как ее еще называют цифровая форензика. Специалисты по цифровой форензике могут использовать технологии для анализа цифровых следов и доказательств, предоставляемых в ходе расследования. Вторым обозначают распознавание образов и текста. Автоматизированные системы распознавания позволяют анализировать текстовую и графическую информацию для выявления

мошенничества. Следующим методом являются системы мониторинга и аналитики. Построение системы мониторинга активности пользователей и аналитических инструментов помогает выявлять аномалии и подозрительные тенденции. И последнее это киберсистемы безопасности. Развитие киберзащиты и систем мониторинга угроз позволяет оперативно реагировать на потенциальные атаки и предотвращать утечку данных.

Таким образом, эффективное противодействие мошенничеству в рамках цифровой экономики требует комплексного подхода, включающего в себя как использование современных технологий для предотвращения преступлений, так и их применение при расследовании данного вида преступлений и установления причастных лиц.

Источники и литература

1) Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ, ст. 159.6, ст. 159.3 // Собрание законодательства РФ, 1996, № 25.
2) Вестов Ф. А., Шамьенов Н. Р. Уголовная политика по использованию возможностей цифровых технологий в противодействии мошенничеству. // Основы экономики, управления и права. 2020.
3) Федотов Н.Н. Форензика – компьютерная криминалистика // Юридический мир 2007.
4) Шевченко Д. Н. Методы цифровой криминалистики и компьютерной форензики для расследования инцидентов информационной безопасности // Проблемы науки. 2020.
5) Официальный сайт Министерства Внутренних Дел Российской Федерации // мвд.рф.