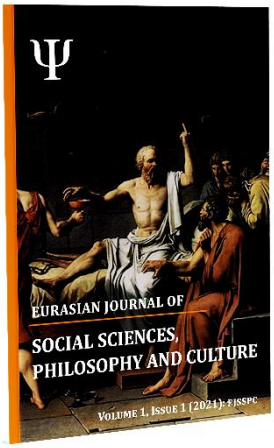
EURASIAN JOURNAL OF SOCIAL SCIENCES, PHILOSOPHY AND CULTURE
Innovative Academy Research Support Center
www.in-academy.uz



ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Нуриддинов Саидолим Саидкамолўғли

Начальник Главного экспертно-криминалистического центра МВД Республики Узбекистан

https://doi.org/10.5281/zenodo.5558850

ИСТОРИЯ СТАТЬИ

Принято: 01 октябрь 2021 г.
Утверждено: 05 октябрь 2021 г.
Опубликовано: 10 октябрь 2021 г.

КЛЮЧЕВЫЕ СЛОВА

киберпреступность, интернет, информационно-коммуникационные технологии.

АННОТАЦИЯ

В данной статье рассматриваются проблемы информационной безопасности, преступления, совершаемые с использованием современных компьютерных технологий. Также предлагаются изучение опыта борьбы с киберпреступностью и подготовки специалистов в вузах зарубежных стран.

Актуальность борьбы с преступностью в сфере информационной безопасности приобретает в современных условиях все более глобальное значение. Крупнейшими международными организациями приняты специальные акты, направленные на противодействие и предупреждение вопросам обеспечения информационной безопасности на региональном и международном уровнях.

Обеспечение информационной безопасности в настоящее время несёт очень актуальный характер, ведь на сегодняшний день информационные технологии все глубже проникают в повседневную жизнедеятельность большинства граждан.

В мире за последние годы наблюдается неуклонный рост числа пользователей сети Интернет, увеличивается и количество пользователей социальных сетей. В настоящее время ими охвачено 4,2 миллиарда человек, что составляет 53,6% населения планеты.

Активный рост числа пользователей Интернета наблюдается и в Узбекистане. Их количество сегодня свыше 22,1 миллиона человек. Социально-демографический портрет пользователей сети: 35,1% – женщины, 64,9% – мужчины; по возрасту: 36,3% – лица от 18 до 24 лет, 35,1% – лица от 25 до 34 лет, 12,7% – лица от 34 до 44 лет.

С широким распространением информационно-коммуникационных технологий меняется характер

преступности. Республика Узбекистан как и многие другие государства не исключение!

Преступления, совершаемые с использованием современных компьютерных технологий, имеют определенную специфику, при этом, развитие компьютерной преступности происходит по двум направлениям: с одной стороны, появляются новые неизвестные ранее преступления, с другой стороны, преступники используют компьютерные технологии при совершении преступлений, ответственность за которые уже определена.

За первое полугодие 2021 года на территории Республики Узбекистан было совершено свыше трёх ста тридцати преступлений, с использованием компьютерных технологий, среди которых такие преступления как хищение путем присвоения или растраты; кражи; клевета; оскорбление в сети интернет; незаконная деятельность по привлечению денежных средств и (или) иного имущества; изготовление, хранение, распространение или демонстрация материалов, содержащих угрозу общественной безопасности

и общественному порядку и т.п.

Мы полагаем, что подобный перечень преступлений аналогичен тому, с чем сталкиваются сегодня и другие государства.

Сложность обнаружения действий преступника, использующего компьютерные технологии и его возможности совершать преступления в том числе и в киберпространстве, не имеющем государственных границ, многократно увеличивают степень общественной опасности таких деяний.

Начиная с 2016 года в системе органов внутренних дел осуществляется полномасштабная работа по эффективному противодействию преступлениям, с использованием компьютерных технологий.

Основными направлениями противодействия являются:

- выявление материалов, пропагандирующих терроризм

и экстремизм в сети Интернет;

- выявление в сети Интернет информации, касающейся торговли людьми, распространения наркотических средств, незаконного оборота оружия и боеприпасов;

- выявление фактов взлома компьютерных систем, средств электронных платежей;

- разработка действенных планов мероприятий

по противодействию киберпреступности на основе анализа совершаемых правонарушений в киберпространстве.

При этом, взаимодействие с подразделениями

по противодействию преступлениям, с использованием компьютерных технологий других стран является одним

из приоритетных направлений.

Полагаем, необходимо затронуть некоторые проблемные вопросы

в сфере расследования киберпреступлений.

Прежде всего, хотелось бы отметить отсутствие

в настоящее время действенного механизма взаимодействия в сфере

обмена необходимой информацией. Например, в получении данных о транзакциях, владельцах

и абонентских номерах электронных кошельков различных платежных систем, которые используются преступниками для вывода средств с территории Республики Узбекистан.

Считаю, что успех расследования и раскрытия преступлений, совершаемых с использованием компьютерных технологий, напрямую зависит от уровня информационного взаимодействия стран!

На сегодняшний день Министерство внутренних дел Республики Узбекистан взаимодействует с другими странами ближнего и дальнего зарубежья на основе достигнутых Соглашений о сотрудничестве.

Хотелось бы отметить в качестве примера деятельность Совета министров внутренних дел государств-участников СНГ.В результате плодотворного сотрудничества в этом формате практически каждый год раскрываются сотни резонансных преступлений.

Наше сотрудничество, в последние годы динамично развивается, постепенно превращаясь в непреодолимый заслонна пути преступных элементов.

Говоря об информационном взаимодействии, хочется отметить, налаженный взаимный информационный обмен

по некоторым видам учётов, с информационными банками данных государств-участников СНГ, осуществляемый

по следующим направлениям:

- по осужденным лицам,

- по лицам, находящимся в межгосударственном розыске, без вести пропавшим лицам, лицам, неспособным

по состоянию здоровья или возрасту сообщить сведения

о себе;

- по неопознанным трупам;

- по сведениям о предметах преступного посягательства, утраченным, изъятым и бесхозным вещам, огнестрельном оружии, похищенным транспортным средствам и т.п.

Активная работа в данном направлении подтверждается количеством обращений в информационные банки данных государств-участников СНГ со стороны МВД Республики Узбекистан.

Таким образом:

- в 2020 году было осуществлено – свыше10 тыс. запросов о розыске или судимости проверяемых лиц;

- за первое полугодие текущего года посредством информационного обмена объявлено в меж.гос.розыск– более 500 (пятиста) лиц, в результате было задержано и экстрадировано – свыше 60 (шестидесяти) лиц.

Для повышения эффективности информационного обмена, Министерством внутренних дел Республики Узбекистан осуществляется поэтапная работа по запуску программно-аппаратных комплексов для обмена информацией посредством защищенной мульти сервисной сети передачи данных.

Также, для расширения списка учётов по обмену информации в электронном виде в нашем Министерстве модернизируются действующие информационные системы.

Немаловажным в противодействии преступникам, которые в своих деяниях используют компьютерные технологии, является процесс сбора и анализа цифровых доказательств. В связи с этим, в Министерстве внутренних дел Республики Узбекистан, начиная с 2018 года, проводятся криминалистические исследования компьютерной техники, мобильных устройств и любых цифровых носителей информации. В данном направлении ежегодно проводятсяпорядка200 исследований.

Для обеспечения безопасности населения и гостей (туристов) от преступных посягательств, в том числе террористических угроз, повышения защищенности мест массового скопления, а также предупреждения и пресечения административных правонарушений, в подразделениях органов внутренних дел созданы ситуационные центры, использующие современные информационно-коммуникационные технологии.

Основным информационно-аналитическим инструментом ситуационных центров является Автоматизированная информационная система Службы «102».

Данная система основана на электронно-карточной платформе, позволяющей минимизировать человеческий фактор в процессе учета и регистрации преступлений, а также оптимизировать управление силами и средствами ОВД.

Отдельно хотелось бы отметить, что для противодействия преступности в деятельности органов внутренних дел широко используются технологии биометрической идентификации, основанные

на искусственном интеллекте, а так же технологии работы

с большими объемами данных.

В частности, применение биометрической идентификации в процессе расследования и раскрытия преступлений оказывает существенное влияние

на результативность самих расследований.

В результате эффективного использования биометрической идентификации ежегодно раскрывается порядка 500 преступлений, устанавливаются личности неизвестных лиц, представляющих интерес для следствия, а также личности неопознанных трупов.

В ближайшем будущем возможности биометрической идентификации запланировано внедрить для установления личности при помощи «умных» камер уличного видеонаблюдения, в рамках решаемых задач проекта «Безопасный город».

Наряду с этим, в настоящее время Министерством внутренних дел прорабатываются вопросы применения беспилотных летальных аппаратов («Дронов») для решения повседневных задач органов внутренних дел.

Их применение в таких областях, как патрулирование

и наблюдение больших территорий, поиск и обнаружение людей с помощью тепловизора, контроль за соблюдением порядка на массовых мероприятиях, мониторинг дорожной ситуации, анализ мест ДТП, осмотры мест происшествий и координация действий сотрудников с воздуха–

во многом повысят оперативность и качество выполняемых задач сотрудниками органов внутренних дел.

В современном мире многие государства накопили большой опыт активного внедрения IT-технологий и принятия мер по противодействию преступлениям с их использованием.

В целях консолидации наших усилий и налаживанию сотрудничества в области информационно-коммуникационных технологий мы со своей стороны хотели бы предложить следующее:

- среди правоохранительных структур, стран участников СНГ, рассмотреть возможность создания базового научно-исследовательского подразделения, осуществляющего свою деятельность на постоянной основе, в функции которого будет входить проведение анализа совершаемых преступлений с использованиями информационных технологий, для дальнейшей выработки действенных решений по противодействию и их пресечению;

- наладить механизм обеспечения информацией, посредством издания периодических, аналитических материалов для служебного пользования, с целью широкого информирования о передовом опыте соответствующих специалистов правоохранительных органов и соискателей

в данной области;

- в целях формирования высоко профессионального кадрового ядра углубить взаимодействие по подготовке, переподготовке и повышению квалификации специалистов

в области противодействия преступлениям

с использованиями информационных технологий;

-изучить опыт борьбы с киберпреступностью и подготовки специалистов в вузах зарубежных стран в рассматриваемой области будет способствовать совершенствованию системы подготовки национальных кадров;

- на базе Академии МВД Республики Узбекистан открыть новое специализированное направление подготовки узкопрофильных специалистов в области противодействия преступлениям в сфере цифровых технологий, киберпреступности и информационной безопасности.

Принимая во внимание рост и масштабность преступлений связанных с использованием информационно-коммуникационных технологий, назрела необходимость кардинального пересмотра программ и методик подготовки и переподготовки специалистов, противостоящих ей. Наступил момент, когда общество, правоохранительные органы, национальные вузы должны консолидироваться и принять

решительные меры по эффективному реагированию на риски и угрозы, исходящие от данного вида преступности.

Полагаем, что реализация этих и других предложений, которые активно обсуждаются правоохранительными органами как Республики Узбекистан, так и всего мира, будут способствовать повышению защищенности граждан, обеспечению стабильности и правопорядка.

References:

1. https://www.gazeta.uz/ru/2020/12/11/network/
2. https://lex.uz/docs/3159825?ONDATE