



ХАРАКТЕРИСТИКА И СПЕЦИФИЧЕСКИЕ ОСОБЕННОСТИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ ЧЕРЕЗ СЕТЬ ИНТЕРНЕТ

У.У.Муродов

Независимый соискатель Академии МВД Республики Узбекистан
<https://doi.org/10.5281/zenodo.19640583>

В современном мире достижения науки и техники оказывают влияние на все явления общественной жизни. Не является исключением и преступность. Проникновение криминальных угроз в информационно-телекоммуникационную среду, включая сеть Интернет, является одним из наиболее опасных процессов нашего времени.¹ В настоящее время актуальность проблем понимания преступности в сети Интернет, её оценки и противодействия ей особо признаётся всеми учёными.²

Использование сети Интернет для хищения чужого имущества причиняет экономический ущерб не только предприятиям и организациям, но и приводит к нарушению нормального функционирования локальных сетей, что, в свою очередь, вызывает сбои в работе связанных с ними сетей. Это препятствует нормальной деятельности крупных предприятий и организаций и влечёт серьёзные негативные последствия и невозможные потери.

Действующие системы защиты во многих случаях оказываются неспособными эффективно обеспечить защиту коммерческого сектора и государственных учреждений от хищений, совершаемых с использованием сети Интернет. Это объясняется наличием уязвимых и незащищённых элементов в таких системах, а также их низкой эффективностью в противодействии подобным преступлениям.³

Криминологический анализ преступности включает статистический анализ, структурный анализ, изучение показателей преступности и другие аналитические критерии. В частности, статистический анализ преступности представляет собой исследование количественных и качественных характеристик преступности на определённой территории за определённый период времени на основе статистических данных.⁴

Результаты криминологического и социально-правового анализа преступлений, совершаемых с использованием сети Интернет, требуют

¹ Kerr, O.S., 2005. Search Warrants in an Era of Digital Evidence. Mississippi Law Journal, 75:85.

² Metchik E. A tipology of crime on the Internet // Security Journal. – 1997. – Vol. 9, №1-3. – P. 27.

³ Коняевский В.А., Лопаткин С.В. Компьютерная преступность: Том I. – М., Image LAB, 2006. – С. 18.

⁴ Абдурасулова Қ.Р. Криминология: Ўқув-услубий қўлланма. – Т.: ТДЮУ, 2013. – Б. 42.





разработки правоохранительными органами системы организационно-правовых и профилактических мер, а также проведения комплексных исследований преступности, в том числе насильственных преступлений против личности и обуславливающих их факторов.

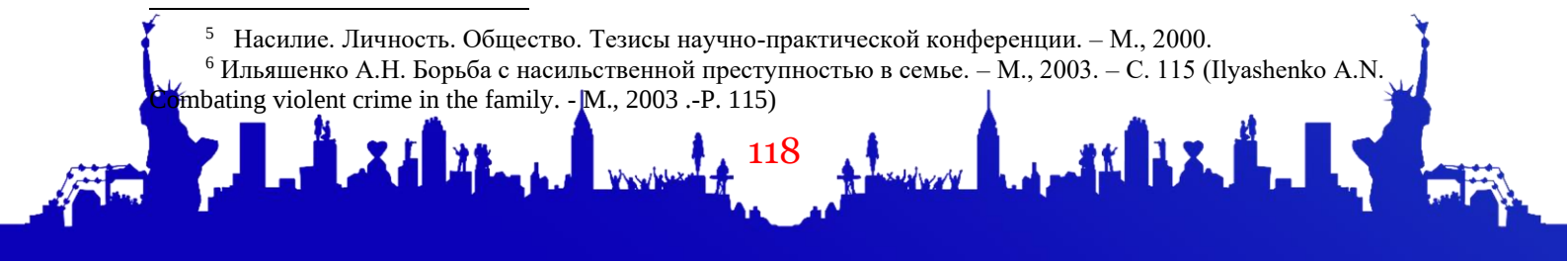
Как отмечалось выше, были рассмотрены лишь наиболее общественно опасные виды преступлений, совершаемых посредством сети Интернет. Наряду с общими закономерностями их совершения различаются мотивы, условия и совокупность факторов, лежащих в их основе. По данным криминологических исследований,⁵ на рост преступлений, совершаемых через Интернет, и уровень их общественной опасности влияет множество факторов. Одним из них является формирование мотивации человеческого поведения.

По мнению А. Н. Ильяшенко, эффективное изучение личности преступника и причин её формирования требует исследования мотивов преступного поведения, поскольку мотив тесно связан с личностью, её особенностями, склонностями и интересами.⁶ Чётко определить преступную мотивацию удаётся не всегда — нередко за преступлением стоит целый комплекс мотивов. Стремление к материальной выгоде может сочетаться с легкомыслием, политическими или иными мотивами. Многие преступления, даже внешне бытовые, в мотивационном плане оказываются значительно более сложными, поскольку обусловлены множеством объективных социальных и психологических факторов, ранее не имевших столь существенного значения в поведении индивида. Корыстная мотивация, лежащая в основе преступлений, совершаемых с использованием Интернета, формируется под воздействием негативных социально-экономических и индивидуально-психологических факторов, возникших за последние годы. По нашему мнению, среди наиболее значимых факторов, которые традиционно продолжают занимать ведущую позицию в системе мотивов преступлений, совершаемых с использованием сети Интернет, следует отметить психологическую зависимость и психологическую ограниченность — совершение преступления как следствие изоляции.

Некоторые ученые - криминологи указывают, что зависимость от виртуальной среды по степени общественной опасности сопоставима с состоянием алкогольного опьянения при совершении преступления.

⁵ Насилие. Личность. Общество. Тезисы научно-практической конференции. – М., 2000.

⁶ Ильяшенко А.Н. Борьба с насильственной преступностью в семье. – М., 2003. – С. 115 (Ilyashenko A.N. Combating violent crime in the family. -M., 2003.-P. 115)





Согласно исследованиям А. Абубакарова, лица, совершившие преступления в состоянии опьянения, составляют 23,1 %⁷ от общего числа преступников; по данным Э. Абовяна, среди лишённых свободы их доля составляет 44,6 %⁸; по результатам исследований А. Кадилова, 51,4 % осуждённых за убийство и причинение телесных повреждений различной степени тяжести находились в состоянии алкогольного опьянения в момент совершения преступления⁹.

Распространение в сети Интернет видеороликов и фотографий тяжких насильственных преступлений формирует у пользователей атмосферу массового страха и паники. Рост интернет-преступности во многом связан с тем, что виновные не всегда привлекаются к ответственности, а также с серьёзными проблемами мониторинга локальных и региональных сегментов сети при организации охраны общественного порядка. Насильственные и сексуальные преступления в сфере досуга и быта также могут совершаться под воздействием интернет-контента.

Современное развитие социальных связей, обусловленное широким применением информационно-коммуникационных технологий, носит глобальный характер. Создаются технологии, позволяющие людям вести бизнес, приобретать товары и услуги, осуществлять денежные переводы, обмениваться информацией и общаться.

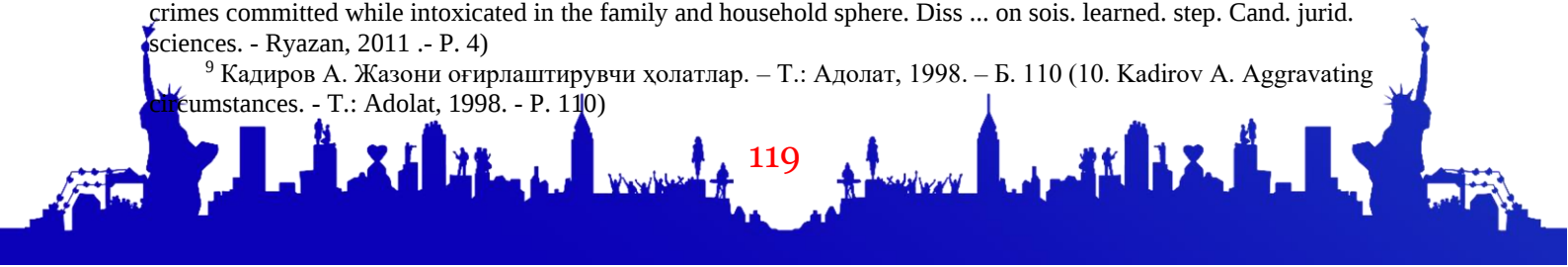
В нашей стране развитие и модернизация компьютерных и информационных технологий, телекоммуникаций, сетей передачи данных и интернет-услуг определены в числе приоритетных направлений. Реализация предусмотренных нормативными актами мер направлена на создание национальных информационных систем и ресурсов, внедрение компьютерной техники и информационных технологий в повседневную жизнь общества и экономику, а также на обеспечение конкурентоспособности экономики на мировом рынке.

Принятие соответствующих решений было обусловлено необходимостью оперативного информационного обмена, использования

⁷ Абубакаров А. Криминологический анализ и предупреждение пьянства и алкоголизма как негативного социального явления в современной России. Дисс... на соис. учен. степ. канд. юрид. наук. – М., 2002. – С. 3 (Abubakarov A. Criminological analysis and prevention of drunkenness and alcoholism as a negative social phenomenon. Diss ... on sois. learned. step. Candidate jurid. science. - M., 2002.-P. 3).

⁸ Абовян Э. Предупреждение преступлений, совершаемых в состоянии алкогольного опьянения в семейно-бытовой сфере. Дисс... на соис. учен. степ. канд. юрид. наук. – Рязань, 2011. – С. 4. (Abovyan E. Prevention of crimes committed while intoxicated in the family and household sphere. Diss ... on sois. learned. step. Cand. jurid. sciences. - Ryazan, 2011. - P. 4)

⁹ Кадилов А. Жазони огирлаштирувчи ҳолатлар. – Т.: Адолат, 1998. – Б. 110 (10. Kadirov A. Aggravating circumstances. - T.: Adolat, 1998. - P. 110)





мировых информационных ресурсов, компьютеризации образования и повседневной жизни, а также обеспечением безопасности информации и баз данных.

В условиях продолжающихся реформ экономика республики демонстрирует устойчивый рост, укрепляется доверие населения к государственным органам.

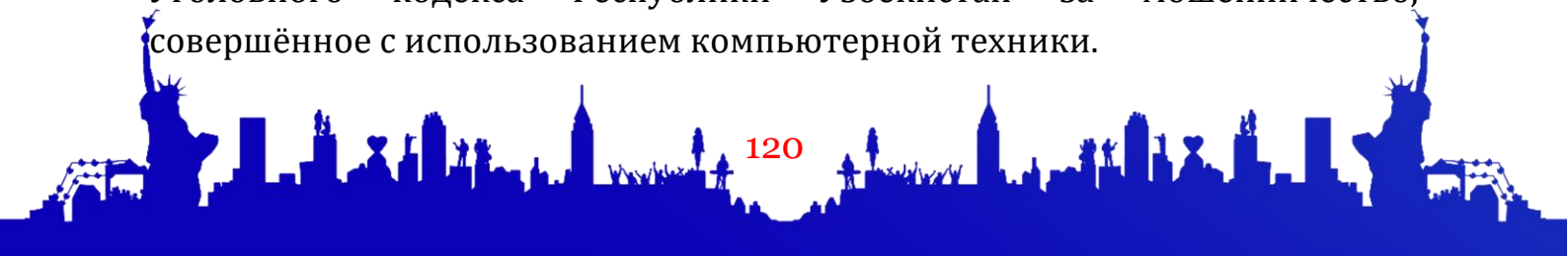
Однако значительный ущерб этим процессам наносят мошенничества, отличающиеся широким охватом. Большинство из них совершается с использованием информационных технологий и коммуникаций либо при создании условий для их совершения. Примером служат схемы мошенничества, связанные с биткоинами, а также распространённые в интернете рекламные предложения быстрого обогащения, являющиеся по сути обманом.

Вместе с тем в национальном законодательстве отсутствует чёткое определение понятия «компьютерная технология» и её механизма, предусмотрены лишь нормы, касающиеся электронно-вычислительных машин. При этом данное понятие является узким и фактически охватывается более широким понятием информационных технологий и коммуникаций.

Согласно действующему законодательству, информацией признаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от источников и формы их представления, а информационными технологиями — совокупность методов, устройств, способов и процессов, используемых для сбора, хранения, поиска, обработки и распространения информации.

Исходя из этого, под кибермошенничеством целесообразно понимать общественно опасное деяние (действие или бездействие), выражающееся в причинении ущерба путём обмана или злоупотребления доверием с использованием информационных технологий и коммуникаций с целью завладения чужим имуществом или правом на него, под угрозой применения наказания.

В настоящее время одним из современных видов мошенничества является кибермошенничество или интернет-мошенничество. Однако данное понятие прямо не закреплено в законодательстве; уголовная ответственность предусмотрена лишь пунктом «в» части второй статьи 168 Уголовного кодекса Республики Узбекистан за мошенничество, совершённое с использованием компьютерной техники.





Примечательно, что под мошенничеством с использованием компьютерной техники понимается хищение имущества (в том числе находящегося в финансовых и банковских учреждениях, фондах и т. п.) путём обмана с применением манипуляций средствами компьютерной техники. Такое мошенничество может совершаться как посредством изменения информации, обрабатываемой в компьютерной системе, хранящейся на соответствующих носителях или передаваемой по сетям передачи данных, так и путём введения ложной информации в компьютерную систему.

В то же время Пленум Верховного суда Республики Узбекистан разъяснил, что если лицо изготовило поддельный документ с использованием компьютерной техники и впоследствии использовало его для завладения имуществом, содеянное не подлежит квалификации по пункту «в» части второй статьи 168 УК. При этом в действующем законодательстве отсутствует чёткое определение того, какие именно средства следует относить к средствам компьютерной техники, что порождает практические проблемы правоприменения..

