НЕКОТОРЫЕ ВОПРОСЫ ПРОФИЛАКТИКИ И ПРЕДУПРЕЖДЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ (КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ)

Атакулов Бекзод Абдухалил угли
студент магистратуры Ташкентского государственного юридического университета
bekatakuloff@gmail.com

Аннотация: *Настоящая научная статья посвящена некоторым вопросам профилактики и предупреждения киберпреступлений (компьютерной преступности). Актуальность настоящей научной статьи состоит в том, что автором исследуются некоторые вопросы профилактики и предупрежд ения киберпреступлений (компьютерной преступности) с точки зрения не только исследования научно-правовой базы, но и с точки зрения критики существующего положения исследований. Учитывая глобальность информационных технологий, интенсивность и скорость их развития, исследования в сфере компьютерных преступлений не теряют своей востребованности, т.к. в каждом из них излагается новое мнение, дополненное результатами научных разработок. Методология научной статьи состоит в применении различных методов, в частности таких, как анализ, синтез, индукция, дедукция, метод криминологического анализа, обобщения и формулировки выводов. Результаты исследования в научной статье выражены в подготовленных предложениях, разработанных автором статьи. Общий вывод в научной статье будет состоять в том, что компьютерные преступления – социальный феномен, который необходимо прогнозировать. Для этого целесообразно создавать специализированные научные центры при государственных органах, ответственных за профилактику и предупреждение киберпреступлений в стране. Данная практика востребована особенно в деятельности прокуратуры Республики Узбекистан.*

Ключевые слова: *Профилактика, предупреждение, киберпреступления, компьютерные преступления, правовая культура, латентность, преступность.*

SOME ISSUES OF PREVENTION AND PREVENTION OF CYBERCRIME (COMPUTER CRIME)

Atakulov Bekzod Abduhalil ogli
Master's student at Tashkent State Law University
bekatakuloff@gmail.com

Abstract: *This scientific article is devoted to some issues of prevention and prevention of cybercrime (computer crime). The relevance of this scientific article consists in the fact that the author explores some issues of prevention and prevention of cybercrime (computer crime) from the point of view not only of the research of the scientific and legal framework, but also from the point of view of criticism of the existing state of research. Taking into account the globality of information technologies, the intensity and speed of their development, research in the field of computer crimes does not lose its relevance, because each of them presents a new opinion supplemented by the results of scientific developments. The methodology of the scientific article consists in the application of various methods, in particular, such as analysis, synthesis, induction, deduction, the method of criminological analysis, generalization and formulation of conclusions. The results of the research in the scientific article are expressed in prepared proposals developed by the author of the article. The general conclusion in the scientific article will be that computer crimes are a social phenomenon that needs to be predicted. To do this, it is advisable to create specialized research centers under state bodies responsible for the prevention and prevention of cybercrime in the country. This practice is in demand especially in the activities of the Prosecutor's Office of the Republic of Uzbekistan.*

Keywords: *Prevention, prevention, cybercrime, computer crimes, legal culture, latency, crime.*

КИБЕРЖИНОЯТЧИЛИК (КОМПЮТЕР ЖИНОЯТИ)НИНГ ОЛДИНИ ОЛИШ ВА ОЛДИНИ ОЛИШНИНГ АЙРИМ МАСАЛАЛАРИ

Атакулов Бекзод Абдуҳалил ўғли
Тошкент давлат юридик университети магистратура талабаси
bekatakuloff@gmail.com

Аннотация: *ушбу илмий мақола кибержиноятчилик (компютер жинояти) нинг олдини олиш ва олдини олишнинг айрим масалаларига бағишланган. Ушбу илмий мақоланинг долзарблиги шундан иборатки, муаллиф кибержиноятчиликнинг (компютер жиноятчилигининг) олдини олиш ва олдини олишнинг айрим масалаларини нафақат илмий-ҳуқуқий базани ўрганиш, балки мавжуд тадқиқот ҳолатини танқид қилиш нуқтаи назаридан ҳам ўрганади. Ахборот технологияларининг глобаллигини, уларнинг ривожланиш интенсивлиги ва тезлигини ҳисобга олган ҳолда, компютер жиноятлари соҳасидаги тадқиқотлар ўз аҳамиятини йўқотмайди, чунки уларнинг ҳар бири илмий ишланмалар натижалари билан тўлдирилган янги фикрни тақдим етади. Илмий мақола методологияси турли хил усулларни, хусусан, таҳлил, синтез, индукция, дедукция, криминологик таҳлил усули, умумлаштириш ва хулосаларни шакллантириш каби усулларни қўллашдан иборат. Илмий мақоладаги тадқиқот натижалари мақола муаллифи томонидан ишлаб чиқилган тайёрланган таклифларда ифодаланади. Илмий мақоладаги умумий хулоса шундан иборатки, компютер жиноятлари башорат қилиниши керак бўлган ижтимоий ҳодисадир. Бунинг учун мамлакатда кибержиноятчиликнинг олдини олиш ва олдини олишга масъул давлат органлари қошида ихтисослаштирилган илмий-тадқиқот марказларини ташкил етиш мақсадга мувофиқдир. Ушбу амалиёт, айниқса, Ўзбекистон Республикаси прокуратураси фаолиятида талабга ега*.

Калит сўзлар: *олдини олиш, олдини олиш, кибержиноятчилик, компютер жиноятлари, ҳуқуқий маданият, кечикиш, жиноятчилик*.

Введение

Актуальность исследования в научной статье обусловлена тем, что особым предметом исследования стали некоторые вопросы профилактики и предупреждения киберпреступлений (компьютерной преступности) с точки зрения не только исследования научно-правовой базы, но и с точки зрения критики существующего положения исследований. Учитывая глобальность информационных технологий, интенсивность и скорость их развития, исследования в сфере компьютерных преступлений не теряют своей востребованности, т.к. в каждом из них излагается новое мнение, дополненное результатами научных разработок.

Цель настоящей научной статьи состоит в необходимости раскрыть и дополнить особенности профилактики и предупреждения киберпреступлений, учитывая анализ актуальных проблем борьбы с ними.

Необходимость и практическая значимость научной статьи обусловлена тем, что на данный момент есть нужда в создании специализированных научных центров, при государственных органах,

ответственных за профилактику и предупреждение киберпреступлений в стране. Данная практика востребована особенно в деятельности прокуратуры Республики Узбекистан. Данная идея отстаивается как приоритетная в настоящей научной статье.

Анализ научной литературы по выбранной теме исследования показывает наличие довольно солидной научной базы по киберпреступлениям. В частности, теоретической основой для научной статьи послужило изучение научных трудов таких авторов, как Расулев А.К. [4], Симкин Л.С. [7], Айков Д., Сейгер К., Фонсторх У. [12], Лунеев В.В [14], Хусаинова А.М. [16], М.Х. Рустамбаев, и многих других.

Материалы и методы исследования

Понятие компьютерная преступность (или «преступность в сфере высоких технологий») наряду с такими понятиями как экономическая преступность, организованная преступность, коррупция, легализация криминальных доходов прочно вошло в понятийный аппарат криминологов и практических работников правоохранительных органов и судов. В криминологической науке Республики Узбекистан со стороны исследователей до сих пор не оказывается должного внимания фактам «наличия и увеличения компьютерной преступности, не достаточно проводятся с учетом современных вызовов и угроз научно-исследовательские работы по криминологической характеристике исследуемых преступлений. В целом, до недавнего времени компьютерной преступности, как явлению, не придавали особого значения и в других государствах СНГ, и преступления, совершаемые в сфере компьютерной информации, рассматривались в совокупности с отдельными видами экономической преступности» [1. С. 489].

Однако, как верно отмечают ученые, компьютерная преступность – это «бомба замедленного действия колоссальной разрушительной силы». Как отмечает Р. Гасанов: «компьютерные махинации, как правило, остаются незамеченными на фоне кровавой уличной преступности. Даже по неполным оценкам экспертов, эти преступления обходятся человечеству минимум в 200 млрд. долл. США ежегодно. Банковский грабитель рискует жизнью за 10 тыс. долл., а электронный, манипулируя компьютером и ничем, по сути, не рискуя, может получить миллионы долларов» [2. С. 155]. Здесь же нужно согласиться с позицией Б.Х. Толеубековой о том, что «компьютерная преступность охватывает собой только сферу быта, торговли, транспорта и т.д., то есть все то, что в целом составляет экономическую часть деятельности государства. Спектр преступного использования компьютерных технологий практически равен спектру его применения по прямому назначению. Это означает, что преступное вторжение через ЭВМ может быть и в сферу оборонной, космической

индустрии, политики и международных отношений» [3. С. 28]. Следовательно, можно сделать вывод, что компьютерная преступность перерастает рамки «новшества», превращаясь в наиболее распространенный вид преступности.

В этой связи, ученые считают, что «компьютерные преступления в криминологическом аспекте следует рассматривать, разделив их по крупным блокам, характеризующим собой отдельные сферы общественной жизни. В частности, речь идет о преступных посягательствах на информационную безопасность в сфере экономики, политики, социально-духовной сфере». Следует согласиться с мнением Расулева А.К., который считает целесообразным «характеризовать компьютерные преступления как социальное явление, установить закономерность его развития, а также социально опасные последствия, к которым может привести отсутствие мер предупредительного и противодействующего характера» [4].

В сфере экономики, в банковской и кредитно-финансовой системе особое распространение получили такие виды компьютерных преступлений как «мошенничество, кражи денежных средств, несанкционированный доступ в информационную систему, коммерческий шпионаж. Однако, с развитием финансово-банковской системы особую опасность для Узбекистана представляют такой вид компьютерного преступления как кардинг» [5. С. 28] («компьютерное мошенничество с электронными пластиковыми карточками»). В Республике Узбекистан, которая входит в мировую электронную торговлю, финансы, интеграционные процессы обеспечивает реализацию задачи обеспечения информационной безопасности в общественных отношениях. Это необходимо, особенно если учитывать слабость систем защиты во многих государственных органах республики, особенно на территории областей республики [6].

Информационная безопасность всегда подвергалась серьезным испытаниям, особенно в связи с распространившимися в Интернете нападениями и информационными атаками.

Особую тревогу вызывают факт, что в компьютерных сетях получило распространение компьютерное пиратство. По данным Ассоциации производители компьютерного обеспечения, уровень компьютерного пиратства в России составляет 90-94 %, в Германии – 50 %, В США – 35 %, в Швейцарии – 28 %, в Лихтенштейне – 18 %, в Китае – 98 %.

Таким образом, компьютерная преступность – это «сложная совокупность нескольких десятков составов преступлений, предусмотренных различными разделами уголовного закона» [7. С. 9] (хищения, несанкционированные доступы, случаи компьютерной фальсификации и мошенничества, компьютерного пиратства,

компьютерного шпионажа, компьютерного терроризма и т. д.), а также не полностью раскрытых пока в Уголовном кодексе, в большинстве своем, связанных с неправильным использованием информационных ресурсов Интернета.

Результаты исследования

Многие компьютерные преступления обладают очень большим процентом латентности. Незначительность судебно-следственной практики и руководящих указаний Верховного суда Республики Узбекистан по применению норм уголовного законодательства в этой сфере, зачастую приводят к тому, что даже в случаях явного ущерба общественным отношениям, интересам личности, общества и государства, принятие юридического решения весьма затруднительно.

Трансграничный характер компьютерных преступлений представляет серьезную проблему для правоохранительных органов. Эта особенность многих компьютерных преступлений обуславливает отмечаемое специалистами «постоянное усложнение в международном масштабе правовых и технических проблем, связанных с обнаружением и идентификацией преступников, проведением расследований и судебных преследований по фактам трансграничных компьютерных преступлений» [8. С. 245]. Серьезные проблемы возникают относительно того, что «в соответствии с законом какого государства должно нести ответственность лицо, совершившее преступление, находясь в одном государстве, в то время как объект преступного посягательства располагается в другом. Реальные пространства сжимаются в виртуальной реальности, и совершенно бессмысленно выстраивать в ней государственные границы» [9. С. 14]. Соответственно, применение к возникающим в глобальной сети правоотношениям локальных правовых норм внутреннего законодательства не может быть эффективно без учета и связи с законодательством других стран, международным правом.

Анализ полученных научно-практических результатов, их эффективность и обоснованность

Компьютерная преступность, в значительно большей степени, чем общеуголовная, «способна составлять образ жизни значительной части населения и формировать полукриминальный менталитет. Количество преступлений в сфере компьютерной информации стремительно растет по мере развития телекоммуникационных сетей и увеличения числа персональных компьютеров». По данным ЮНЕСКО сохраняется позитивная динамика развития телекоммуникационных систем. В частности, с 1995 по 2000 гг. число телекоммуникационных линий увеличилось в США с 165 тыс. до 199 тыс., в ФРГ – с 41 тыс. до 51 тыс., в Китае – с 41 тыс. до 141 тыс., В России – с 25 тыс. до 35 тыс. За это же время было инвестировано в

развитие этой сферы в США – 51 млрд. долл., в ФРГ – 16 млрд. долл., в Китае – 302 млрд. долл., в России – 8 млрд. долл. [10. С. 12]. Вполне обоснованно утверждение о том, что «распространенность компьютерных преступлений обусловлена расширением сферы применения средств ЭВМ, ростом доверия к автоматизированным системам обработки данных. В этих процессах участвует большое количество людей, удобность несанкционированного доступа к информационным системам в силу своей относительной простоты, скоротечности, анонимности, отсутствия непосредственного контакта с объектом преступления, подвигает людей к совершению такого рода преступлений. Например, четыре из пяти преступлений, расследованных ФБР США, имели отношение к неправомерному доступу» [11. С. 38].

Важно учитывать социально-психологические условия, в которых ведется расследования. Настроения общества относительно информационных преступлений, под воздействием СМИ постоянно меняется. Их отношения могут быть совершенно полярны. Например, «от полного неприятия преступных действий, повлиявших на интересы некоторых слоев общества в конкретной стране, до возвеличивания отдельных преступников. В судах и СМИ к компьютерным преступникам редко подходят с той же строгостью, как и к лицам, совершившим обычные преступления, в действительности их часто превращают в героев» [12. С. 19].

Вышеизложенный анализ показал, что на данный момент в обществе очевидна низкая правовая культура, слабая осведомленность о криминальности подобных деяний, о существовании в целом компьютерных правонарушений и понимании того, какие последствия это влечет, резко снижает эффективность противодействия компьютерным преступлениям. Компьютерная преступность, которая носит «по своей природе индивидуальный, сущностный признак, тем не менее, в последнее время приобретает более организованный и опасный характер» [13. С. 131]. Организованность проявляется «как в координации действий технического характера, так и в распределении ролей в группах. В компьютерных преступлениях экономической направленности высока вероятность сговора с персоналом информационных систем банков, финансовых учреждений и структур, что позволяет эффективно скрыть следы преступной деятельности». Важную роль в усложнении борьбы с компьютерной преступностью играет «интеллектуализация и профессионализация криминалитета. В результате расслоения общества, сохранения относительно высокой безработицы, сокращения государственных предприятий и учреждений в криминальную сферу вытесняется значительное число высококвалифицированных специалистов в области ИТ» [14. С. 465].

В Республике Узбекистане проводятся мероприятия по широкомасштабной работе в сфере совершенствования общественно-политической, социально-экономической и судебно-правовой сферах, а также «дальнейшей модернизации государственных программ, в том числе по противодействию компьютерной преступности», что включает в себя весь комплекс правовых и организационно-технических, социальных вопросов, борьба с компьютерной преступностью может быть более эффективной.

Выводы

Специалисты считают необходимой разработку «соответствующей методики по организации раскрытия и расследования преступлений в сфере компьютерных и информационно-телекоммуникационных технологий. Вопросы противодействия киберпреступности не просто не перестают быть актуальными, а остаются крайне острыми, требующими особого внимания со стороны правоохранительных органов и государства» [15]. Также для решения рассмотренных проблем предлагается увеличить количество экспертов, обладающих специальными знаниями и привлекать их для расследования киберпреступлений [16].

Учитывая глобальность информационных технологий, интенсивность и скорость их развития, исследования в сфере компьютерных преступлений не теряют своей востребованности, т.к. в каждом из них излагается новое мнение, дополненное результатами научных разработок. На данный момент есть нужда в создании специализированных научных центров, при государственных органах, ответственных за профилактику и предупреждение киберпреступлений в стране. Данная практика востребована особенно в деятельности прокуратуры Республики Узбекистан.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:

1. Криминология: Учебник для юрид. вузов / под общей ред. Долговой А.И. – М.: Инфра-М, 2007. – С. 612. – С. 489.

2. Гасанов Р.М. Шпионаж особого рода – М.: Юридическая литература, 2009. – С. 288. – С. 155.

3. Толеубекова Б.Х. Социология компьютерной преступности – Караганда, 2012. – С. 122. – С. 28.

4. Расулев А.К. Рахмонова С. Преступления в сфере информационных технологий и безопасности: детерминанты и предупреждение. Журнал «Общество и инновации». 2020 г. ВАК // Источник: https://cyberleninka.ru/article/n/prestupleniya-v-sfere-informatsionnyh-tehnologiy-i-bezopasnosti-determinanty-i-preduprezhdenie.

5. Осташева Н.А. Carding: реальное мошенничество в виртуальном мире // Ж. ЮРИСТ – 2009. – № 4 – С. 25–28.

6. Расулев А.К. Криминологическая характеристика преступлений в сфере информационных (компьютерных) преступлений. Журнал «Вопросы современной юриспруденции». 2016 г. // Источник: https://cyberleninka.ru/article/n/kriminologicheskaya-harakteristika-prestupleniy-v-sfere-informatsionnyh-kompyuternyh-prestupleniy.

7. Симкин Л.С. Программы для ЭВМ: правовая охрана (правовые средства против компьютерного пиратства) – М.: Городец, 2008. – 92 с. – С.9.

8. Горяинов К.К., Исеченко А.П., Кондратюк Л.В. Транснациональная преступность: проблемы и пути решения – М.: ИНФРА-М, 2007. – С. 386. – С. 245.

9. Волчинская Е.К. Есть ли в России компьютерное право? // – Ж. Юридический консультант. – 2007. – № 2. – С. 14–16.

10. Информационные вызовы национальной и международной безопасности / И.Ю. Алексеева и др. Под общ. ред. А.В. Федорова, В.Н. Цигичко. – М.: ПИР- Центр, 2011. – С. 160. – С.12.

11. Анин В. Наиболее серьезные нарушения в области информационной безопасности в 1996 году // Журнал «Конфидент». 2007. – № 6. – С. 48–52.

12. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. – М.: МИР, 2009. – С. 90. – С. 19.

13. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях. – М.: Норма, 2014. – С. 188. – С. 131.

14. Лунеев В.В. Преступность XX века: мировые, региональные и российские тенденции. – М.: МОСКВА, 2012 – С. 576. – С. 465.

15. Дерюгин Р.А. Киберпреступность в России: современное состояние и Актуальные проблемы. Вестник Уральского юридического института МВД России. 2019 г. // Источник: https://cyberleninka.ru/article/n/kiberprestupnost-v-rossii-sovremennoe-sostoyanie-i-aktualnye-problemy

16. Хусаинова А.М. Актуальные проблемы расследования киберпреступлений. Журнал «Достижения науки и образования». 2018 г. // Источник: https://cyberleninka.ru/article/n/aktualnye-problemy-rassledovaniya-kiberprestupleniy.

17. Топилдиева Д. Кибержиноятларни тергов қилиш муаммолари // Общество и инновации. – 2021. – Т. 2. – №. 11/S. – С. 292-296.

18. Каримов Бобуржон. Научно-теоретические вопросы категории цифровых доказательств // Review of law sciences. 2020. №Спецвыпуск. URL: https://cyberleninka.ru/article/n/nauchno-teoreticheskie-voprosy-kategorii-tsifrovyh-dokazatelstv (дата обращения: 14.03.2022).

19. Khamidov Bakhtiyor Khamidovich et al. “General Theoretical Issues of Improving Private Forensic Methods in the Field Of Combat against Cybercrime”. Psychology and education (2021) 58(1): 2705-2712 DOI: https://doi.org/10.17762/pae.v58i1.1153.