лекин унга озодликдан маҳрум қилиш билан боғлиқ бўлмаган жазо тайинланган ва ҳ.қ [3.].

Ўзбекистон Республикаси Президенти Ш. М. Мирзиёев суд идораларининг фаолияти, ундаги муаммолари ва камчиликларига тўхталар эканлар, куюниб «Адолат ва маънавият ўзаро чамбарчас боғлиқ тушунчалар, маънавият бўлмаган жойда ҳеч қачон адолат бўлмайди, шунинг учун ҳам судьялар, юрист кадрларни тайёрлаш ва судьялик лавозимига тайинлашда бу масалага алоҳида эътибор қаратиш лозим, айнан маънавий фазилатларнинг етишмаслиги туфайли айрим судьялар ўртасида қонунга зид ҳаракатлар содир этиш, нопоклик, таъмагирлик, одамларнинг дарду ташвишиларига лоқайд қараш, адолат мезонларига хилоф равишда қарорлар қабул қилиш ҳолатлари учрайди» деб таъкидладилар.

Шу боис Ўзбекистон Республикаси Президенти Ш. М. Мирзиёев таъбири билан айтганда судьялар томонидан чиқариладиган процессуал қарорлар қонуний, асосли ва адолатли бўлиши учун энг аввало адолатли ва кучли судьялар корпусини яратиш, судьяларнинг онгида фақат адолат, дилида поклик, тилида ҳақиқат устувор бўлиши керак, судья – бу адолат посбони бўлмоғи керак. Шундагина халқ суд идораларидан рози бўлади ва инсон манфаатлари таъминланади.

Адабиётлар рўйхати:

1. Ўзбекистон Республикаси «Судлар тўғрисида» ги қонун. 2000 йил 14 декабрь.

2. Ўзбекистон Республикаси Президентининг 2017 йил 21 февралдаги «Ўзбекистон Республикаси суд тизими тузилмасини тубдан такомиллаштириш ва фаолияти самарадорлигини ошириш чора-тадбирлари тўғрисида»ги фармони.

3. Ўзбекистон Республикаси Президенти Ш.М. Мирзиёевнинг2017 йил 13 июнь куни А.Навойи номли Симпозимлар саройи маърифат марказида «Суд органлари тизимида одил судловни таъминлаш борасидаги ишларнинг аҳволи, муаммолари ва истиқболдаги вазифалар»га бағишланган видеоселектор йиғилишида сўзлаган нутқи.

4. Жиззах шаҳар жиноят ишлари бўйича судида суд мажлиси жараёнида кўрилган жиноят ишларининг муҳокамаси. 2017 йил 24 апрель. Жиззах шаҳри.

А.К.Расулев,
и.о. доцента кафедры «Профилактика правонарушений» Академии МВД Республики Узбекистан, д.ю.н.

ВЛИЯНИЕ СЕТИ ИНТЕРНЕТ НА ФОРМИРОВАНИЕ ЛИЧНОСТИ МОЛОДЫХ ХАКЕРОВ

Аннотация: Мақолада статистик маълумотлар асосида Интернет тармоғининг хакер шахсини шаклланишига таъсири таҳлил қилинган, тегишли хулосалар қилинган ва таклифлар ишлаб чиқилган.

Калит сўзлар: хакер, Интернет, жиноятчи шахси, болалар, ёш.

Аннотация: В статье были на основании статистических данных было проанализировано влияние сети Интернет на формирование личности хакера, были сделаны соответствующие выводы и разработаны предложения.

Ключевые слова: хакер, Интернет, личность преступника, дети, возраст.

Annotation: Article analysed influence of the Internet on formation of the identity of the hacker on the basis of statistical data, drawn the corresponding conclusions and developed offers.

Key words: hacker, Internet, identity of the criminal, children, age.

В юридической литературе вопрос личности преступника, совершившего преступления в сфере информационных технологий и безопасности, иначе говоря, киберпреступника, рассматривается, в основном, через призму обособленной группы лиц, именуемых «хакерами». Традиционно хакеры рассматриваются как группа профессионалов высокого класса, которые используют свои интеллектуальные способности для разработки способов и методов осуществления противоправных посягательств на информационно-коммуникационные ресурсы и сети. Преимущественно эти взломы наносят ущерб системе защиты и безопасности информационных технологий. Поэтому часто хакеров называют компьютерными хулиганами. Тенденция развития компьютерной преступности показывает, что сеть Интернет является потенциальной средой для формирования личности юных хакеров.

По статистике в 2018 году больше чем у 3,580 миллиардов человек во всем мире есть доступ к Интернету, то есть средний глобальный уровень проникновения составляет 47,1 процентов. По состоянию на ноябрь месяц 2018 года количество пользователей социальных сетей составил 2,46 миллиардов человек, то есть 68,71 % от всех пользователей сети Интернет в мире [12].

Большинство пользователей приходится на развивающиеся страны – в них насчитывается 2,5 миллиарда пользователей, а в развитых странах – 1 миллиард. В процентном отношении наибольшее проникновение интернета остается в развитых странах – 81%, по сравнению с 40% в развивающихся странах и 15% в наименее развитых странах. В Европе 76% населения имеют возможность выходить в онлайн. На втором месте находятся страны СНГ – 67,7%, на третьем - государства Северной и Южной Америки с показателем в 65,9%. Самый низкий показатель в Африке – всего 21,8% [5].

К 2018 года количество интернет-пользователей в Узбекистане превысило 15 миллионов человек, число абонентов мобильной связи в стране составляет более 26 миллионов, количество домашних хозяйств, имеющих компьютер, в настоящее время составляет 38,4%, доступ в интернет – 60,5% [9].

Согласно аналитическим данным 26,5% пользователей сети Интернет в мире составляют лица в возрасте от 10 до 24 лет, 26,7% пользователей – от 25 до 34 лет, 20,4% – от 35 до 44 лет [12]. Как мы видим, большое количество пользователей сети Интернет составляет молодежь. Определение возрастной характеристики пользователей сети Интернет позволяет также определить потенциальных субъектов преступлений в сфере информационных технологий и безопасности.

Учитывая, что основной частью пользователей сети Интернет является молодежь, актуальным становится вопрос уголовной ответственности за преступления в сфере информационных технологий и безопасности. В Республике Узбекистан возраст субъекта уголовной ответственности колеблется от 13 до 18 лет, при этом общий возраст составляет 16 лет. В Англии к уголовной ответственности можно привлечь с 8 лет, в Греции – с 13 лет, в Швеции – с 15 лет, в Финляндии – с 16 лет, в Египте, Ливане и Ираке, США – с 7 лет, в Израиле – с 9 лет, в Иране, Турции – с 11 лет [3; 29-с.].

Следует отметить, что в мировой практике наблюдается тенденция снижения возраста субъекта преступлений в сфере информационных технологий и безопасности. Этому способствуют, на наш взгляд, две причины:

1) Интернет стал важным и значимым ресурсом в жизни молодежи, практически незаменимой средой коммуникации;

2) в последнее время стали распространяться атаки со стороны юных хакеров – школьников и подростков.

К примеру, в Беларуси снижен до 14 лет возраст привлечения к уголовной ответственности за хищение путем использования компьютерной техники и уклонение от отбывания наказания в виде ограничения свободы. По данным Национального центра правовой информации это обусловлено ростом числа таких преступлений, совершенных несовершеннолетними [7].

По некоторым данным, в США группа юных хакеров (школьников), которая называет себя CWA, в 2015 году взломала личную электронную почту директора ЦРУ Джона Бреннана и министра национальной безопасности Джея Джонсона [10].

Специалисты одного из крупнейших российских медиа об IT и IT-безопасности «ХАКЕР» утверждают, что большинство хакеров – просто скучающие дети, у которых слишком много свободного времени. Только 10% хакеров отдают отчет в своих действиях. 90% актов вандализма в Интернете осуществляют 13-тилетние подростки, которым просто нужно «хорошо провести время» [14].

Рассматривая вопрос о личности преступника и его признаках, невозможно оставить без внимания мнение известного американского специалиста по борьбе с фишингом (разновидностью компьютерного мошенничества) Лэнса Джеймса, считающего, что в XXI веке наибольшее распространение среди компьютерных преступников получили скриптkидди (script kiddies) [4]. К их главным особенностям он относит их юный возраст, непрофессиональные хакерские способности, наличие свободного времени, упорство в достижении поставленной цели, использование уже готовых кодов, разработанных специалистами [4].

С учетом широкой вовлеченности молодежи в информационно-коммуникационное пространство, совершения различных правонарушений и преступлений подростками и молодежью необходимо **снизить возраст уголовной ответственности за преступления в сфере информационных технологий и безопасности до 14 лет.**

Было бы ошибочным полагать, что юный возраст пользователей позволяет судить о трансформации пользователей в хакеров. Специальное исследование, проведенное аналитическим агентством B2B International специально для «Лаборатории Касперского» среди пользователей среды Интернет в возрасте до 16 лет, охватившее 11.135 респондентов из стран Америки, Ближнего Востока, Африки и России, показало, что действие Интернет в отношении несовершеннолетних имеет двоякий характер:

Во-первых, Интернет является потенциальной средой, оказывающей негативное влияние на психику и здоровье детей, при этом немаловажную роль играет позиция родителей. Согласно статистическим данным, в 58 % случаев взрослые были вынуждены вмешаться, чтобы помочь ребенку, 13 % виртуальных конфликтов переросли в реальные, 7 % пострадавших получили настолько тяжелую психологическую травму, что длительное время переживали случившееся, 26 % родителей узнали об инцидентах намного позже того, как они случились [11]. По данным проведенного в Польше исследования, из 9 тысяч детей и подростков в возрасте 12-17 лет вовлекались в разговоры сексуального характера в сети Интернет в течение 2015-2016 годов 56 %, а 75,3 % получили предложение встретиться вне сети. Международная организация ECPAT (End Child Prostitution, Child Pornography and the Trafficking of Children for Sexual Purposes) также проводила свой опрос, который показал, что 92 % детей, общающихся в чатах, вовлекались в разговоры о сексе, при этом четверть респондентов понятия не имеет, как избавиться от настойчивых ухаживаний со стороны виртуальных насильников. Более того, многие юные жертвы «киберохотников» не сообщают о преследовании, в первую очередь, из-за того, что не верят в понимание и помощь со стороны взрослых, боятся реакции родителей, стесняются огласки. Многие опасаются, что им вообще запретят пользоваться Интернетом [6].

Вышеприведенные данные ярко демонстрируют потенциальную опасность и угрозу сети Интернет для молодежи. С учетом опасности распространения среди детей негативной информации, наносящей вред их здоровью, 8 сентября 2017 года в Республике Узбекистан был принят Закон Республики Узбекистан «О защите детей от информации, наносящей вред их здоровью» №ЗРУ–444 (вступил в силу 9 марта 2018 года), который предусматривает защиту детей от информационной продукции, распространение которой влияет на состояние физического, психического и социального благополучия детей [2].

В частности, в КоАО Республики Узбекистан следует внести административную ответственность за нарушение законодательства о защите детей от информации, наносящей вред их здоровью:

«**Статья 47[4]. Нарушение законодательства о защите детей от информации, наносящей вред их здоровью**

Умышленное распространение среди детей продукции, наносящей вред их здоровью, –

влечет наложение штрафа от десяти до пятидесяти минимальных размеров заработной платы».

В свою очередь, УК Республики Узбекистан должен быть дополнен статьей 130[2] следующего содержания:

«**Статья 130[2]. Нарушение законодательства о защите детей от информации, наносящей вред их здоровью**

Умышленное распространение среди детей продукции, наносящей вред их здоровью, совершенные после применения административного взыскания за такие же действия, –

наказывается штрафом от четырехсот до шестисот минимальных размеров заработной платы или обязательными общественными работами до трехсот шестидесяти часов либо исправительными работами до трех лет.

Те же действия, совершенные:

а) повторно или опасным рецидивистом;

б) по предварительному сговору группой лиц;

в) с использованием средств массовой информации либо сетей телекоммуникаций, а также всемирной информационной сети Интернет, -

наказываются обязательными общественными работами от трехсот шестидесяти до четырехсот восьмидесяти часов или ограничением свободы от одного года до трех лет либо лишением свободы до трех лет.

Осуществление противоправного информационно-психологического воздействия на сознание детей, манипулирования ими, распространения информационной продукции, провоцирующей детей на антисоциальные действия, -

наказывается ограничением свободы от трех до пяти лет либо лишением свободы от трех до пяти лет.

Действие, предусмотренное частью третьей настоящей статьи:

а) членом организованной группы или в ее интересах

б) повлекшее наступление тяжких последствий», -

наказывается лишением свободы от пяти до десяти лет.

Во-вторых, Интернет является очень комфортной средой для формирования личности хакера. В глобальной сети существует ряд ресурсов, предназначенных для обучения хакерским навыкам, в частности, сайты http://dfiles.ru, https://ru.wikihow.com, https://kakbog.ru, а также медиа-файлы в канале You Tube. В XXI веке быстро растет процесс институализации хакеров, хотя они по-прежнему строго соблюдают принцип анонимности (вместо собственного имени используются псевдонимы типа «Ludichrist». «Sicko», «Packet Rat» и др.). Создаются регулярно действующие сообщества хакеров, они имеют свои сайты, журналы – «Access All Areas» («Вседоступность»), «Crypt NewsLetter's Home Page» («Популярные криптографические новости»), «Old and New Hackers» («Старые и новые хакеры»), «Chaos Computer Club» («Клуб компьютерного хаоса») [8].

Однако следует указать, что кроме негативных связей хакеров с преступными группировками, в последнее время отчетливо прослеживается тенденция взаимодействия хакерского движения с государственными и коммерческими структурами. В них принимают участие представители государственных органов безопасности, администраторы крупнейших фирм. Более того, некоторые из известных хакеров активно участвуют в государственных и международных организациях по информационной безопасности. Так, например, президент и основатель «Chaos Computer Club» (Клуб компьютерного хаоса) Энди Мюллер-Мэган входит в состав всемирной организации «ICANN» (Internet Corporation for Assigned Names and Numbers). Организованы хакерские школы всех уровней для детей (Гражданская школа хакеров), студентов (Foundstone-s hacking school) и сотрудников безопасности (Black Hat Briefings, Ethical Hacking).

На наш взгляд, данный опыт был бы полезным для Республики Узбекистан. Взаимодействие и тесное сотрудничество хакеров с государственными и правоохранительными органами, организациями и учреждениями позволит не только обеспечить эффективное раскрытие и предупреждение киберпреступлений, но и может способствовать исправлению нарушителей, перехода их из категории «правонарушителей» в категорию «исправленных» лиц. В свою очередь, практика показывает, что многие профессиональные хакеры являются отличными специалистами и мастерами своего дела, зачастую совершают преступления из корысти, редко преследуя политические и иные цели, а некоторые из них совершают правонарушения из чувства забавы или интереса. По данным исследований киберпреступности в 2014-2017 годах, проведенных компанией Group IB, практически все киберпреступления нацелены на получение финансовой выгоды максимально простым путем, а именно 98 % информационных преступлений совершаются из корыстных побуждений (кража, шантаж, вымогательство, мошенничество), по 1 % – с целью завладения информацией и кибертерроризма соответственно [13].

Такая практика, на наш взгляд, вполне соответствует государственной молодежной политике в Республике Узбекистан. Как отмечал Президент Республики Узбекистан Ш.Мирзиёев, «Вместе с тем все мы как родители, наставники и учителя хорошо понимаем, что в нынешнее сложное и непростое время вопрос воспитания молодежи остается для нас важнейшей и актуальной задачей. Поэтому мы не имеем никакого права допускать ошибки в вопросах обеспечения законных прав и интересов нашей молодежи, ее образования и воспитания. Ошибки в этом вопросе означают измену нашим детям, Родине» [1]. Следовательно, активное вовлечение молодых хакеров в деятельность государственных и, особенно, правоохранительных органов способно оказать положительное влияние на криминогенное состояние в республике.

Список литературы:

1. Мирзиёев Ш.М. Выступление Президента Республики Узбекистан на сессии Самаркандского областного Кенгаша народных депутатов от 10 ноября 2017 года.

2. Закон Республики Узбекистан «О защите детей от информации, наносящей вред их здоровью» от 7 сентября 2017 года № ЗРУ–444.

3. Абдурасулова К.Р. Жиноятнинг махсус субъекти. Ўқув қўлланма. – Т.: ТДЮИ, 2005. – 180 б.

4. Джеймс Л. Фишинг. Техника компьютерных преступлений / пер. с англ. Р. В. Гадицкого. –М.: НТ Пресс, 2008. –С.86.

5. http://www.bizhit.ru/

6. http://www.ecpat.org/
7. http://www.interfax.by/
8. http://www.psyfactor.org/
9. http://www.ru.sputniknews-uz.com/
10. http://www.russian.rt.com/
11. http://www.sch2.sharkovschina.edu.by/
12. http://www.statista.com/
13. http://www.vestifinance.ru/
14. http://www.xakep.ru/

И.Ф.Мирзамухамедова,
докторант Каспийского Университета,
Республика Казахстан, город Алматы

ПРИРОДА БАНКРОТСТВА БАНКОВ КАК БЛАГОДАТНАЯ ПОЧВА ДЛЯ КРИМИНАЛЬНОГО БАНКРОТСТВА, А ТАКЖЕ КАК ВЕСОМОЕ ПРЕПЯТСТВИЕ РАЗВИТИЮ ВСЕЙ ЭКОНОМИКИ РЕСПУБЛИКИ КАЗАХСТАН. ОПЫТ ЗАРУБЕЖНЫХ СТРАН В ПРОТИВОДЕЙСТВИИ БАНКРОТСТВУ БАНКОВ

Аннотация: в данной статье рассматривается непосредственное банкротство банков как одно из явных детерминантов криминального банкротства, а также как препятствие для нормального развития всей экономической системы Республики Казахстан. Включительно анализируется зарубежный опыт банкротства банков, а так же меры противодействия данному банкротству для более полного представления о возможном внедрении данного опыта к нашим экономическим реалиям.

Ключевые слова: банковская система, банкротство, криминальное банкротство, экономика, экономическая устойчивость, финансовое положение, риск банкротства, диагностика, мониторинг, собственность.

Annotation: this article considers the immediate bankruptcy of banks as one of the obvious determinants of criminal bankruptcy, and also as an obstacle to the normal development of the entire economic system of the Republic of Kazakhstan. Inclusively, foreign experience of bank bankruptcy is analyzed, as well as countermeasures to this bankruptcy for a more complete picture of the possible implementation of this experience to our economic realities.

Keywords: banking system, bankruptcy, criminal bankruptcy, economy, economic stability, financial situation, bankruptcy risk, diagnostics, monitoring, property.

Мировой экономический кризис, а также его возможные будущие последствия установились в рамках прочных предпосылок для так называемой эпохи «экономический неопределенности» в Республике Казахстан. В глобальном масштабе опыт зарубежных стран ясно дал понять нашей республике, что даже лучшие международные компании должны непрерывно и качественно мониторить свое финансовое положение и экономическую устойчивость сотрудничающих с ними компаний. Однако, ни одна компания в мире, в какой бы развитой стране она не находила, не может гарантировать четкую определенность в построении этой самой финансовой устойчивости.

Глобализационные процессы в мировой экономике лишь добавляют этой неопределенности новые, запутанные схемы связей между сторонами договора и их финансовой независимостью.

Необходимо в обязательном порядке разграничивать банкротство фирмы и банкротство непосредственно банка. Финансовый крах одной из фирм создаст проблемы лишь только для ее клиентской базы, равно как и партнерским отношениям с другими фирмами и кредиторами. Банкротство такого типа не может нанести весомого ущерба государству, равно как и не может оказаться хоть сколь-нибудь значимым детерминантом в развитии криминального банкротства как явления в Республике Казахстан. Совсем другое