

UDC: 343.97 (575.1)

Расулев Абдулазиз
доктор юридических наук, профессор кафедры
«Профилактика правонарушений»
Академии МВД Республики Узбекистан
E-mail: rasuleff@mail.ru

КИБЕРПРЕСТУПНОСТЬ: ПРИЧИНЫ И УСЛОВИЯ, ЛИЧНОСТЬ ПРЕСТУПНИКА

***Аннотация.** В данной статье автором были проанализированы детерминанты киберпреступлений, в частности исследованы причины и условия, способствующие совершению преступлений в сфере информационных технологий и безопасности, изучена личность преступника. В статье основными аспектами криминологической характеристики преступлений в сфере информационных технологий и безопасности указаны высокая общественная опасность и транснациональный характер информационных угроз, уязвимость информационно-технологической системы как важнейшего элемента стратегической инфраструктуры, недостаточная эффективность законодательства и несовершенство политических институтов, отсутствие профессионализма и «человеческий» фактор. Автор отмечает, что преступления в сфере информационных технологий и безопасности характеризуются высоким уровнем латентности. Поэтому официальная статистика не дает возможности получить соответствующие данные по криминологической особенности лиц, которые совершают преступления при помощи информационных технологий. Это происходит из-за отсутствия надлежащей статистики и высокой латентности таких преступлений. Отмечено, что при криминологической характеристике преступников в сфере информационных технологий и безопасности следует исходить из таких четырех факторов, как черты личности, техническое ноу-хау, социальные особенности, мотивирующие факторы, которые оказывают влияние на формирование правонарушителя в информационно-коммуникационном пространстве. На основе проведенного анализа были сделаны соответствующие выводы и разработаны предложения.*

***Ключевые слова:** киберпреступления, информационная безопасность, детерминанты преступности, личность преступника, уголовный закон.*

Расулев Абдулазиз
юримдик фанлар доктори, Ўзбекистон Республикаси ИИВ Академияси
«Ҳуқуқбузарликлар профилактикаси» кафедрасининг профессори

КИБЕРЖИНОЯТЧИЛИК: САБАБ, ШАРТ-ШАРОИТЛАР, ЖИНОЯТЧИ ШАХСИ

***Аннотация.** Мазкур мақолада кибержиноятларнинг детерминантлари таҳлил қилинган. Жумладан, ахборот технологиялари ва хавфсизлиги соҳасидаги жиноятларнинг сабаблари ҳамда уларнинг содир этилишига имкон яратувчи шарт-шароитлар тадқиқ этилиб, жиноятчи шахси ўрганилган. Мақолада ахборот технологиялари ва хавфсизлиги соҳасидаги жиноятлар криминологик тавсифининг асосий жиҳатлари сифатида ахборот хавфларининг юқори ижтимоий хавфлиги ва трансчегаравий тусда эканлиги, стратегик инфратузилманинг муҳим элементи сифатида ахборот-технологик тизимнинг заифлиги, қонунчиликнинг етарли даражада самарали эмаслиги ва сиёсий институтларнинг номукамаллиги, профессионалликнинг йўқлиги ва “инсоний” омил кўрсатиб ўтилган. Муаллиф-*

нинг фикрича, ахборот технологиялари ва хавфсизлиги соҳасидаги жиноятлар юқори даражадаги латентлик билан ажралиб туради. Шунинг учун расмий статистика ахборот технологиялари ёрдамида жиноят содир этаётган шахсларнинг криминалогик тавсифи бўйича тегишли маълумотлар олиш имконини бермайди. Бу эса лозим даражада статистика юритилмаслиги ва мазкур жиноятлар латентлиги оқибатида юзага келмоқда. Ахборот технологиялари ва хавфсизлиги соҳасидаги жиноятчиларнинг криминалогик тавсифида ахборот-коммуникация маконида ҳуқуқбузарнинг шаклланишига таъсир кўрсатувчи шахсий жиҳатлар, техник ноу-хау, ижтимоий хусусиятлар, рағбатлантирувчи омиллар каби тўртта омилни инобатга олиш кераклиги таъкидланган. Амалга оширилган таҳлил асо-сида тегишли хулосалар қилинган ва таклифлар ишлаб чиқилган.

Калим сўзлар: кибержиноятлар, ахборот хавфсизлиги, жиноятчилик детерминантлари, жиноятчи шахси, жиноят қонуни.

Rasulev Abdulaziz

Professor of the Offence Prevention Department,
MIA Academy of the Republic of Uzbekistan, Doctor of Sciences in Law

CYBERCRIME: CAUSES AND CONDITIONS, IDENTITY OF THE PERPETRATOR

Abstract. *In this article the author analyzes the determinants of cybercrime, in particular, the causes and conditions that contribute to the commission of crimes in the field of information technology and security, and studies the identity of the criminal (perpetrator). In the article, the main aspects of criminological characteristics of crimes in the sphere of information technology and security indicate serious public danger and the transnational nature of cyber threats, the vulnerability of information technology systems as an important element of strategic infrastructure, the lack of efficiency of legislation and the imperfection of political institutions, lack of professionalism and the «human» factor. The author notes that crimes in the field of information technology and security are characterized by a high level of latency. Therefore, official statistics do not make it possible to obtain relevant data on the criminological characteristics of persons who commit crimes with the help of information technologies. This is due to the lack of proper statistics and the high latency of such crimes. It is noted that the criminological characterization of criminals in the field of information technology and security should be based on such four factors as personality traits, technical know-how, social characteristics, motivating factors that influence the formation of the offender in the information and communication space. Based on the analysis, relevant conclusions are drawn and proposals are developed.*

Keywords: *cybercrime, information security, determinants of crime, criminal identity, criminal law.*

Сегодня трудно представить нашу жизнь без развития информационно-коммуникационных технологий. Отношения в современном мире все больше становятся виртуальными, включая отношения с государством, онлайн-обучение, онлайн-банкинг и т. д. Все больше наша жизнь зависит от информационно-коммуникационных технологий.

Преступность, как и любая другая сфера, не останавливается и продолжает модернизироваться наряду с другими отраслями жизнедеятельно-

сти человека. Преступники современности пытаются покорить виртуальные пространства, в связи с чем возникла новая эра преступности – эра киберпреступности. Борьба с киберпреступностью, то есть преступлениями в сфере информационных технологий и безопасности, приобретает все более глобальное значение. В частности, всеми государствами и международным сообществом принимаются меры для обеспечения информационной безопасности, предупреждению преступных посягательств с использованием информа-

ционно-коммуникационных технологий. Статистические данные указывают, что по состоянию на первое полугодие 2020 г. мобильными и/или телекоммуникационными сетями было охвачено около 7 млрд человек (94 % мирового населения) [1], размер ущерба от киберпреступности составляет 1,3 % мирового ВВП в год [2].

В Республике Узбекистан развитие информационных технологий происходит быстрыми темпами. Следует особо отметить плоды принимаемых мер по развитию информационно-коммуникационной сферы. Согласно данным Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан, количество интернет-пользователей в Узбекистане превысило 22 млн (из них 19 млн – пользователи мобильного интернета), для развития сетей мобильной связи в 2019 г. было установлено 2017 базовых станций, вследствие чего в республике их число составляет более 26000. При этом 96 % жителей Узбекистана охвачены мобильной связью, 70 % имеют доступ к широкополосной сети мобильного интернета [3].

В Стратегии действий по пяти приоритетным направлениям развития Республики Узбекистан в 2017-2021 годах предусмотрены вопросы «совершенствования уголовного законодательства, совершенствования системы обеспечения информационной безопасности и защиты информации, своевременное и адекватное противодействие угрозам в информационной сфере» [4]. В этой связи борьба с преступностью, представляющей угрозу правам и свободам личности, интересам общества и государства, охрана информационной безопасности в качестве объекта уголовно-правовой охраны, разработка комплекса мер по противодействию киберпреступлениям являются актуальными задачами. Пересмотр норм, касающихся ответственности в сфере информационных технологий с учетом технологического прогресса, в том числе расширения категорий преступлений, связанных с киберпреступностью, также предусмотрен Концепцией совершенствования уголовного и уголовно-процессуального законодательства Республики Узбекистан, утвержденной Постановлением Президента Республики Узбекистан от 14 мая 2018 года № ПП-3723 [5].

Если рассматривать данные в мировом масштабе, то в настоящее время, по данным веб-сай-

та Internet world stats, в мире по состоянию на первое полугодие 2020 г. насчитывается 4833521806 пользователей интернета, что составляет 62 % населения Земли (население Земли – 7796949710 человек), из них больше половины проживает в развивающихся странах. Первенство в мире по численности интернет-аудитории уже пять лет занимает Китай. По состоянию на июль 2020 г. количество интернет-пользователей в Китае составило 854 млн человек. В топ-10 стран по числу пользователей интернета, кроме Китая, вошли Индия – 560 млн, США – 313 млн, Индонезия – 171 млн, Бразилия – 149 млн, Нигерия – 126 млн, Япония – 118 млн, Россия – 116 млн, Бангладеш – 94 млн, Мексика – 88 млн человек [6].

Такой массовый характер использования информационного пространства, виртуализация отношений между людьми приводит к параллельному росту киберпреступности и в Республике Узбекистан, и во всем мире.

В настоящей статье будут обобщенно проанализированы детерминанты (причины и условия, личность преступника) и меры предупреждения преступлений в сфере информационных технологий и безопасности.

Проблема причин преступности является одной из центральных в науке криминологии и предупреждении правонарушений. Причинный комплекс преступности включает ее причины и условия, которые в совокупности составляют факторы преступности. Причины – это социально-психологические детерминанты, которые непосредственно порождают, воспроизводят преступность и преступления как свое закономерное следствие; условия – это такие социальные явления, которые сами не порождают преступность и преступления, а способствуют, облегчают, интенсифицируют формирование и действие причины [7, с. 167-168].

Анализ криминологической науки в Узбекистане, в частности научных трудов таких отечественных ученых, как К. Абдурасулова [8, с. 179-181], М. Рустамбаев [9, с. 98-100], Р. Кабулов [10, с. 23-27], свидетельствует о выделении причин, способствующих совершению рассматриваемых видов преступлений: недостаточная защита средств электронной почты; небрежность в работе пользователей инфомационно-коммуникационных технологий (ИКТ); недостаточная защита

при использовании ИКТ в конкретных технологических процессах и операциях и т. д. Кроме субъективных причин, по нашему мнению, наиболее типичными причинами и условиями совершения преступлений в сфере информационных технологий и безопасности на современном этапе являются:

- рост числа ИКТ и, как следствие, увеличение объемов информации, обрабатываемой и хранимой в ИКТ;
- недостаточность мер по защите ИКТ, систем ИКТ и их сетей;
- недостаточность защиты программного обеспечения;
- рост информационного обмена через мировые информационные сети, в первую очередь, посредством социальных сетей;
- отсутствие, несовершенство или отступление от правил эксплуатации программ для ИКТ, баз данных и аппаратных средств обеспечения сетевых технологий;
- отсутствие или несоответствие средств защиты информации современным информационным вызовам и угрозам;
- нарушение правил работы с охраняемой законом компьютерной информацией;
- низкий уровень специальной подготовки сотрудников правоохранительных органов, которые должны предупреждать, раскрывать и расследовать преступления в сфере информационных технологий и безопасности;
- отсутствие скоординированной и комплексной государственной политики в сфере обеспечения информационной безопасности.

В настоящей работе мы остановимся на двух основных причинах киберпреступлений. Одна из них, как уже говорилось выше, это рост числа пользователей. В социологии имеется «правило 15 %», согласно ему, если население Земли вырастет на 15 %, то число совершаемых преступлений вырастет на 15 %. Данное правило также применимо и для киберпреступлений. Так, по данным «Лаборатории Касперского», в мире число хакерских DDoS-атак в 2019 г. выросло на 25 % по сравнению с 2017 г. и на 18 % – с 2018 г. [11].

По оценкам мировых экспертно-аналитических центров, каждую секунду 24 пользователя старше 18 лет становятся жертвами киберпреступности, таким образом, ежедневно от действий

киберпреступников страдают более 2,4 млн человек. Количество жертв за 2019 г. составляет более 700 млн человек, каждый из которых в среднем теряет больше 376 долл. [12].

Особую актуальность вопросы противодействия преступлениям в сфере информационных технологий и безопасности приобретают в условиях мировой пандемии коронавируса. В этих условиях киберпреступники «переместили» свое внимание с простых людей и небольших организаций на государственные органы, учреждения здравоохранения и крупные корпорации, чтобы максимизировать свою прибыль и разрушения, вызванные коронавирусом. Из-за внезапного глобального перехода к удаленной рабочей среде во время пандемии коронавируса организациям пришлось быстро разворачивать удаленные системы, сети и приложения. В результате возник риск уязвимости в обеспечении безопасности при организации удаленной работы.

Например, с января по апрель 2020 г. поступило примерно 907 тыс. спам-сообщений, обнаружены 737 инцидентов, связанных с вредоносными программами, созданы 48 тыс. вредоносных URL-адресов, об этом говорится в докладе Интерпола [13].

В глобальной сети преступники обновили свои онлайн-мошеннические и фишинговые схемы, часто выдавая себя за правительственные и медицинские органы, чтобы обманом заставить жертв предоставлять личные данные и загружать вредоносный контент. Так, в течение первых двух недель апреля 2020 г. произошел всплеск атак вымогателей в сети Интернет, которые не наблюдались в 2019 г. и первые три месяца 2020 г. Расследования правоохранительных органов свидетельствуют о том, что большинство злоумышленников довольно точно оценили максимальную сумму выкупа, которую они могли потребовать от потерпевших лиц и организаций [14].

Киберпреступники также пользуются растущим спросом на медицинские принадлежности, а также своевременной информацией о COVID-19, причем мошенники все чаще регистрируют доменные имена, содержащие соответствующие ключевые слова, такие как «coronavirus» или «COVID». Коронавирус можно назвать идеальной средой для совершения преступлений. Стресс и неопределенность, вызванные кризисом COVID-19, создают

идеальную среду для киберпреступников, стремящихся обогатиться или создать хаос. Преступники не уклоняются от попыток воспользоваться этими возможностями, о чем свидетельствует их спешка с «обновлением» маршрута атак и использованием «фальшивых» новостей. Поскольку пандемия продолжается, «страх формирует неуверенность, а неуверенность и неопределенность приводят к плохой киберзащите», говорит адвокат Джейсон Вайс, эксперт по киберкриминалистике в юридической фирме Faegre Drinker, Biddle and Reath [15]. По мере того, как пандемия коронавируса и карантинные меры затягиваются, и случаи заболевания продолжают расти, можно предположить, что масштабы киберпреступлений будут огромными, особенно по причине того, что экономика «слабеет» и люди будут страдать от финансовых последствий коронавируса. В связи с этим возникает необходимость минимизации и ограничения потенциальных угроз кибератак, а также улучшить систему кибербезопасности.

Как отмечается в докладе Управления ООН по наркотикам и преступности, посвященном вопросам киберпреступности и коронавируса COVID-19, «пандемия COVID-19 представляет собой беспрецедентный вызов для всего мирового сообщества. Многие перешли от традиционных способов совершения операций в режим онлайн, также поступили и преступники. В то время, как масштабы и изощренность киберпреступлений растут, и увеличивается количество жертв, в некоторых странах представители правоохранительных органов вынуждены исполнять другие обязанности. Усугубляет ситуацию для общественности и правительств экономическое влияние COVID-19. Таким образом, складываются идеальные условия для потенциальных киберпреступлений» [16, с. 4].

Как мы видим, существенной проблемой является вольность и безответственность интернет-пользователей, в первую очередь, блогера-злоумышленника. Свободное пользование средствами ИКТ и сетью Интернет может повлечь за собой определенные негативные последствия. К примеру, особое негативное влияние это оказывает на простых пользователей. Как и любое государство, Республика Узбекистан также намерена решить вопрос предупреждения распространения негативного контента. Проблематичность

данного вопроса заключается в отсутствии конкретных мер ответственности за неправомерное использование сети Интернет. При этом законодательство предусматривает запреты на «использование» Интернета в негативном смысле согласно Закону Республики Узбекистан «Об информатизации». В частности, владелец веб-сайта и/или страницы веб-сайта, в том числе блогер, обязан не допускать использование своего веб-сайта и/или страницы веб-сайта во всемирной информационной сети Интернет, на которых размещается общедоступная информация, в целях распространения негативного контента и совершения других действий, влекущих за собой уголовную и иную ответственность в соответствии с законом [17]. В этой связи важной задачей является установление ответственности за неправомерное использование сети Интернет со стороны злоумышленников.

При анализе детерминантов киберпреступлений существенное значение имеет анализ личности преступника в сфере информационных технологий и безопасности. Черты преступников в сфере информационных технологий и безопасности позволяют нам выделять следующие типы:

1. «Новичок». Данная категория личности совершает правонарушения впервые и характеризуется использованием различных информационных технологий (персональный компьютер, ноутбук) для личных потребительских целей: для загрузки музыки, игр или приложений. В основном это – подростки или молодежь в возрасте 15-25 лет. Пол – в подавляющем большинстве случаев мужской. Образование – среднее, среднее специальное или высшее.

2. «Любитель». Данная категория личности представляет собой лиц, которые периодически совершают правонарушения в компьютерной сети, в основном – это технический персонал (системные администраторы, технические консультанты). В данную группу входят лица мужского пола (реже женского) в возрасте от 20-30 лет. Формирование «любителей» происходит от навыков прошлого в качестве «новичка» или в связи с жизненными обстоятельствами (выполнение поручений и «заказов»).

3. «Профессионал». Данная категория профессиональных лиц, на профессиональной основе занимающихся неправомерной деятельностью и именуемых хакерами. Это – класс образованных

лиц, знающих все азы компьютерного программирования и технической работы. Возраст – 25-40 лет. Пол – в большинстве случаев мужской. Д. Букин справедливо отмечает, что высокая техническая подготовленность – их основная черта, высокая латентность преступлений – основа их мотивации, внутренняя предрасположенность – основное условие вступления на преступный путь и социально-экономическая ситуация в стране – основная причина окончательного выбора [18, с. 28].

Исходя из вышеперечисленных групп, можно утверждать, что киберпреступник характеризуется технической подготовленностью, обладает набором методов, позволяющих ему осуществлять различные махинации (получение несанкционированного доступа, взлом ключей безопасности и т. д.). В большинстве случаев это выпускник (или студент старших курсов) технического вуза, имеющий свой персональный компьютер или ноутбук. В подавляющем большинстве случаев – это мужчины в возрасте 15-40 лет. Как правило, изучаемые лица имеют замкнутый характер, зачастую депрессивны, склонны к личностным переживаниям, обидчивы. Их успехи в школе не были блестящи, но основы информатики и математику они учат хорошо. В большинстве своем они, возможно, имеют неполную семью, где царит сложная психологическая атмосфера. Согласно статистическим данным, 72,2 % хакеров жили в момент совершения преступления с одним из родителей, в 51,3 % случаев основной успех хакеров в обучении был в точных науках, 33,1 % начинали свою деятельность с желания испробовать технику компьютерного взлома [19]. Для киберпреступников характерны правовой нигилизм и завышенная самооценка, в большинстве случаев они, чувствуя свою безнаказанность и неуязвимость, пренебрегают требованиями норм закона и считают вполне нормальным самостоятельно определять моральность и правильность тех или иных правовых норм, исходя из собственных критериев. Часто проявляют инфантилизм, безответственность, бескомпромиссность, непонимание возможных последствий своих действий, нередко игнорируют общественное мнение и интересы. В подобных случаях «оценка ситуации осуществляется не с позиций социальных требований, а исходя из личных переживаний, обид, проблем и желаний» [20, с. 104]. В качестве мотивов пре-

ступления – различных побуждающих факторов, которые способствуют совершению киберпреступлений – можно отнести корысть (большинство киберпреступлений совершается из корыстных побуждений), политические и религиозные взгляды, хулиганство.

Сегодня Интернет стал важным и значимым ресурсом в жизни молодежи, практически незаменимой средой коммуникации, в связи с чем в последнее время стали распространяться атаки со стороны юных хакеров – школьников и подростков. В сети Интернет каждый пользователь может найти соответствующую информацию для формирования навыков и умений хакера. В начале это становится для пользователя забавой, что в последующем может стать причиной совершения правонарушений, а также преступлений в сети Интернет. Поэтому растет количество юных киберпреступников. Ярким примером может служить Джонатан Джозеф Джеймс, который начал взламывать информационные системы с самого раннего возраста. Он взламывал серьезные организации, включая Агентство по сокращению военной угрозы, которое является одним из подразделений Министерства обороны США. После этого он получил доступ к именам пользователей и паролям, а также возможность просматривать конфиденциальную информацию. 29 и 30 июня 1999 г. Джеймс атаковал НАСА, в то время ему было 15 лет. Ему удалось получить доступ, взломав пароль сервера, принадлежащего правительственному учреждению, расположенному в штате Алабама. Джеймс смог свободно бродить по сети и украсть несколько файлов, включая исходный код международной орбитальной станции. По заявлению НАСА, стоимость украденного Джеймсом программного обеспечения оценивается в 1,7 млн долл. После обнаружения взлома НАСА пришлось отключить систему для проверки и приведения ее в рабочее состояние, что обошлось в 41 тыс. долл. Поймали Джеймса быстро, так как НАСА сделало все, чтобы его остановить. Джонатан стал широко известен благодаря тому, что стал первым несовершеннолетним, отправленным в тюрьму за хакерство в США в возрасте 16 лет [21].

Зачастую юные хакеры совершают киберпреступления для демонстрации своих умений, возможностей перед сверстниками. Так, в Германии

мальчик по имени Линус Хенце (Linus Henze) обнаружил брешь в системе MacOS, которая позволяет выкрасть все пароли, сохраненные на устройстве. Об этом он сообщил в своем Twitter и выложил видео взлома на YouTube [22]. Благодаря использованию этого маневра можно было получить доступ к более чем 2 млн логинам и паролям пользователей.

Ответственность за киберпреступления предусматривается главой XX¹ Уголовного кодекса Республики Узбекистан, именуемой «**Преступления в сфере информационных технологий**». Уголовные санкции на национальном уровне еще не обеспечивают надежной защиты от киберпреступности, потому что в существующих нормах права нет достаточного правового регулирования ответственности за преступления в сфере информационных технологий и безопасности. Так, Концепцией совершенствования уголовного и уголовно- процессуального законодательства, утвержденной Постановлением Президента Республики Узбекистан от 14 мая 2018 года № ПП-3723, предусмотрен пересмотр норм, касающихся ответственности в сфере информационных технологий с учетом технологического прогресса, в том числе расширения категорий преступлений, связанных с киберпреступностью.

Одной из существенных проблем является также **недостаточная организация работы по профилактике правонарушений в сфере информационных технологий и безопасности**. Закон Республики Узбекистан «О профилактике правонарушений» не уделяет должного внимания вопросам изучения причин и условий, способствующих совершению преступлений в сфере информационных технологий и безопасности. Так, в качестве меры виктимологической профилактики указана организация веб-сайтов, блогов, чатов во всемирной информационной сети Интернет с целью организации всеобщего обсуждения проек-

тов профилактических программ и мероприятий, выявления и устранения проблем и недостатков при их проведении. Однако информационные технологии должны быть использованы и при общей, и при специальной профилактике правонарушений. В свою очередь, следует включить в круг субъектов профилактики органы Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан.

С учетом изложенного, а также принимая во внимание особую актуальность проблематики в сфере информационных технологий, обеспечения безопасности динамично нарастающей информатизации общества и развивающихся в связи с этим новых форм и методов киберпреступлений, научно-практические и академические круги серьезно задумываются о том, чтобы объединить усилия по международному сотрудничеству, взаимодействию соответствующих специализированных органов, осуществляющих борьбу в данной сфере. В частности, по нашему мнению, следует осуществить следующие мероприятия:

1. Необходимо совершенствование уголовно-правовых норм, предусматривающих ответственность в сфере информационных технологий с учетом технологического прогресса, в том числе расширение категорий преступлений, связанных с киберпреступностью.

2. Следует усилить институциональные основы профилактики киберпреступлений и правонарушений в сети Интернет, а именно предусмотреть в качестве общей меры профилактики использование достижений науки и техники, возможностей современных информационно-коммуникационных технологий.

3. Следует наделить Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан правом осуществления профилактики правонарушений в сети Интернет.

Список использованной литературы

1. <http://www.itu.int/>
2. <http://www.itweapons.com/>
3. <https://podrobno.uz/cat/tehnp/kolichestvo-internet-polzovateley-v-uzbekistane-sostavlyaet-22-milliona-chelovek/>

4. Указ Президента Республики Узбекистан «О Стратегии действий по дальнейшему развитию Республики Узбекистан» от 7 февраля 2017 года № УП-4947 (Собрание законодательства Республики Узбекистан, 2017 г., № 6, ст. 70).
5. Постановление Президента Республики Узбекистан «О мерах по кардинальному совершенствованию системы уголовного и уголовно-процессуального законодательства» от 14 мая 2018 года № ПП-3723 (Национальная база данных законодательства, 15.05.2018 г., № 07/18/3723/1225, 01.10.2018 г., № 06/18/5547/1975).
6. <https://www.internetworldstats.com/top20.htm>
7. Гладких В.И. Криминология: учебник (бакалавриат и магистратура). – М.: Юстиция, 2019. – 422 с.
8. Абдурасулова Қ.Р. Криминология. Дарслик. Масъул муҳаррир: М.Х. Рустамбаев. – Т.: «Адолат», 2007. – 216 б.
9. Криминология. Учебник. Коллектив авторов. Отв. редактор: М.Х. Рустамбаев. – Т.: ТГЮИ, 2008. – 586 с.
10. Кабулов Р., Абдурахманов Э.С. Преступления в сфере информационных технологий: Учебное пособие. – Т.: Академия МВД Республики Узбекистан, 2009. – 80 с.
11. <https://ria.ru/20190805/1557194818.html>
12. <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf>
13. <https://www.bankinfosecurity.com/interpol-a-14778>
14. <https://www.healthcareinfosecurity.com/insights-from-interpol-on-using-threat-intelligence-a-14649>
15. <https://abcnews.go.com/Technology/wireStory/reports-sharp-increase-cybercrime-pandemic-72228287>
16. Доклад Управления Организации Объединенных Наций по наркотикам и преступности «Киберпреступность и коронавирус COVID-19: риски, угрозы и ответные меры» (источник доступен по ссылке: https://www.unodc.org/documents/Advocacy-Section/Russian_-_UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf).
17. Закон Республики Узбекистан «Об информатизации» от 11 декабря 2003 года № 560-II (Ведомости Олий Мажлиса Республики Узбекистан, 2004 г., № 1-2, ст.10; Собрание законодательства Республики Узбекистан, 2014 г., № 36, ст. 452).
18. Кардава Н.В. Киберпространство как новая политическая реальность: вызовы и ответы // История и современность. 2018. №1-2. – С. 27-28.
19. <http://www.psyfactor.org/>
20. Антонян Ю.М., Еникеев М.И., Эминов В.Е. Психология преступника и расследования преступлений. – М.: Юрист, 2006. – 190 с.
21. https://ru.wikipedia.org/wiki/Джонатан_Джозеф_Джеймс
22. <https://lenta.ru/news/2019/02/07/vzломshik/>
23. Salaev. N. (2017) «Differentiation, individualization, execution of criminal punishments and its goals: way to success» Review of law sciences: Vol. 1: ISSN, Article 25.
24. Очиллов Х.Р. Некоторые суждения о проблемах квалификации хищения чужого имущества с использованием компьютерных средств в условиях нынешних судебно-правовых реформ. Review of law sciences. (2020) 205-210. <https://cyberleninka.ru/article/n/nekotorye-suzhdeniya-o-problemah-kvalifikatsii-hischneniya-chuzhogo-imuschestva-s-ispolzovaniem-kompyuternyh-sredstv-v-usloviyah>.