ОБЪЕКТИВНЫЕ ПРИЗНАКИ ПРЕСТУПЛЕНИЙ ПРОТИВ ЧЕСТИ И ДОСТОИНСТВА ЛИЧНОСТИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Ёкубжонов Алишер Шерзод угли
Самостоятельный соискатель Ташкентского государственного юридического университета
E-mail: alish2022abdukadirov@gmail.com
https://doi.org/10.5281/zenodo.17800078

ARTICLE INFO

Received: 27th November 2025
Accepted: 28th November 2025
Online: 29th November 2025

KEYWORDS

частная жизнь, информация, неприкосновенность прайвеси, персональные данные, тайна личной жизни, тайна переписки

ABSTRACT

В статье автором с уголовно-правовой точки зрения исследуются объективные признаки преступлений против чести и достоинства личности в информационном пространстве. В частности, отмечается, что общественная опасность киберпреступлений становится на современном этапе одним из важнейших причин противодействия киберпреступности против чести и достоинства личности, проанализированы некоторые нормы уголовного законодательства касательно охраны частной жизни в информационном пространстве, при этом разработаны соответствующие предложения и выводы

В современных условиях развития информационных технологий и телекоммуникаций уголовно-правовая борьба с преступлениями в данной сфере представляет особую актуальность. Первый Президент Республики Узбекистан И.Каримов отмечал, что «...нет необходимости говорить о том, что в век информации, коммуникационных и компьютерных технологий, когда Интернет с каждым днем все шире и глубже входит во все сферы нашей жизни, и когда борьба за умы и умонастроения людей приобретает решающее значение, – все эти задачи сегодня становятся для нашего общества актуальными и приоритетными»[1].

Проблема киберпреступности переросла в масштабы мирового сообщества. Для разработки комплексного научного подхода к решению этой проблемы необходима ее формализация: выделение основных объектов и определение принципиальных свойств рассматриваемого явления.

Во всем современном мире, характеризующемся развитием информационно-коммуникационных технологий, киберпреступления в странах достигают гигантских масштабов.

Статистика показывает, что посягательства на безопасное функционирование информационных технологий являются одними из самых распространенных угроз в различных информационных системах, включая банковскую и корпоративную систему. Ущерб от киберпреступлений в Узбекистане только за первое полугодие 2025 года превысил 1,2 триллиона сумов[2].

По прогнозам Cybersecurity Ventures, ущерб от вымогательских и хакерских атак составит в 2025 году 10,5 триллиона долларов США. Ущерб предприятий от каждой украденной записи базы данных составляет в среднем 158 долларов США, средний объем

потерь компаний от утечки данных – 4 миллиона долларов на один инцидент, в США эта цифра составляет 7 миллиона долларов США (на состояние 1 января 2024 года)[3].

Данный статистический анализ еще раз наводит на мысль о необходимости адекватного реагирования и совершенствования уголовно-правовых механизмов, обеспечивающих разновекторные сферы жизнедеятельности государства, общества и личности, охраняющих общественно-политическую, социально-экономическую и правовую сферу. Само непосредственно обеспечение процесса информатизации, который связан со всеми сферами, влечет за собой также проблемы по охране информационной безопасности.

В научно-практической литературе существуют различные мнения касательно определения круга общественных отношений в сфере информационной безопасности как объекта киберпреступлений.

Роберт Хаббард, Петер Браути и другие отмечают, что «мнения западных ученых позволяет разделить киберпреступность на две категории:

1. «Чистые компьютерные преступления», где компьютер или иная информационная система (сеть, коммуникационный ресурс) является объектом преступления. Эта категория включает некоторые новые преступления, которые представляют угрозу для компьютерных систем и сетей, например, взломы, DOS-атаки, и злонамеренное распространение компьютерных вирусов.

2. Поддерживаемые компьютером преступления, где компьютер является инструментом, используемым при совершении преступления. Эта категория включает использование компьютера для совершения таких традиционных преступлений как распространение порнографии, сетевой шантаж, кибермошенничество и незаконный оборот наркотиков»[4].

Вызывает особый интерес мнение Брэдфорда Рейнса, который отмечает, что киберпреступления классифицируются по трем категориям в зависимости от следующих объектов посягательства:

Частное лицо. Этот тип киберпреступления может быть в форме киберпреследования, торговли людьми, распространения порнографии, клеветнических или оскорбляющих сведений. Сегодня правоохранительные органы относятся к этой категории киберпреступлений очень серьезно и прилагают все усилия на международном уровне для привлечения к ответственности виновных лиц.

Собственность. Точно так же, как в реальном мире, где преступник может совершить хищение, и в киберпространстве преступник может совершить различные виды хищений - кражу или мошенничество. В этом случае преступники могут неправомерно завладеть банковскими реквизитами лица и перевести деньги; неправомерно использовать кредитную карту, чтобы совершить многочисленные покупки в онлайн режиме; совершить мошенничество; использовать вредоносное программное обеспечение, чтобы получить неправомерный доступ к веб-сайту организации или разрушить системы организации. Вредоносное программное обеспечение может нанести ущерб программному и аппаратному обеспечению, точно так же, как вандалы наносят ущерб собственности в реальном мире.

Правительство. Преступления против правительства через компьютерную технику упоминаются как кибертерроризм. Эта категория может нанести ущерб и вызвать панику среди гражданского населения. В этой категории преступники «взламывают»

правительственные веб-сайты, веб-сайты правоохранительных органов или пропагандируют идеи свержения государственного строя. Данная категория преступлений может быть совершена террористическими организациями или специальными службами недружественно настроенных правительств других стран[5].

Подводя краткий итог мнений западных экспертно-аналитических кругов, можно прийти к выводу, что в западной литературе объектом киберпреступлений признаются общественные отношения, которые охраняют права и законные интересы личности, общества и государства в информационном пространстве. Кроме того, следует отметить, что более детальный акцент делается на обеспечении защиты частной собственности, компьютерной информации, информационной безопасности и непосредственно связанном с ними противодействии киберпреступности и другим преступлениям в сфере информационных технологий.

Своеобразная точка зрения бытует среди ученых стран СНГ, которая также заслуживает особого внимания. Так, при определении родового объекта преступлений в сфере информационных технологий существуют некоторые расхождения. Т.М. Лопатина отмечает, что правовое регулирование данных отношений реализуется в двух формах: созданием нового законодательства и распространением существующего на возникшие новые общественные отношения. Эти процессы происходят в государстве не обособленно, наоборот, они взаимосвязаны и неразрывны, что и должно обеспечивать гармонизацию общественных отношений в информационной сфере[6].

Все эти данные показывают крайнюю необходимость системного изучения и определения объекта рассматриваемых преступлений в целом. Ведь именно объект преступления охватывает те общественные отношения, которые следует охранять в уголовно-правовом порядке.

Следует отметить, что первое из вышеприведенных определений является спорным, так как преступления в сфере информационных технологий и безопасности посягают не на компьютерную технику в целом, а на безопасность использования компьютерной информации, базы данных и информационных систем. В случае определения родового объекта преступлений в сфере информационных технологий как безопасности использования ЭВМ, представляется невозможным определить общественную опасность рассматриваемых преступлений и разграничить их от смежных составов преступлений.

Непосредственный объект некоторых киберпреступлений, по мнению Н.В. Карчевского, можно определить как право собственности на компьютерную информацию. Предметом таких преступлений является компьютерная информация[7]. С данным мнением трудно согласиться, так как не всегда преступления в сфере информационных технологий и безопасности посягают на компьютерную информацию в качестве объекта собственности. Допустим, при нарушении правил информатизации вряд ли можно согласиться с тем, что осуществляется посягательство на право собственности на компьютерную информацию. В данном случае речь идет о создании, внедрении и эксплуатации информационных систем без принятия установленных мер защиты.

Большинство ученых на пространстве СНГ рассматривают родовой объект преступлений в сфере информационных технологий через призму процессов обработки компьютерной информации. В качестве преступлений в сфере информационных технологий

принято считать уголовно наказуемые действия, подразумевающие несанкционированное проникновение в работу компьютерных сетей, компьютерных систем и программ, с целью видоизменения компьютерных данных. При этом компьютер выступает в качестве предмета преступления, а информационная безопасность – объекта. К событиям, связанным с преступлением, можно отнести ситуации, при которых компьютер – орудие для совершения преступлений с целью нарушения авторских прав, общественной безопасности, прав собственности, нравственности.

Заслуживает особого внимания позиция ряда авторов. Так, по мнению А.И.Малярова, родовым объектом рассматриваемых преступлений являются общественные отношения по поводу поиска, получения, передачи, производства и распространения компьютерной информации, а предметом преступления - компьютерная информация[8].

Л.А.Прохоров и М.Л.Прохорова полагают, что объектом анализируемой группы преступлений, исходя из законодательного описания составов, являются общественные отношения, складывающиеся в связи с использованием компьютерной информации[9].

В.А.Колобов и В.Н.Ясенев отмечают, что компьютерные преступления направлены против установленного порядка общественных отношений, который регулирует изготовление, использование, распространение и защиту компьютерной информации[10].

Как мы видим, позиция данных авторов связана с предметом преступления, а именно – компьютерной информацией. Следует особо отметить, что мы не должны упускать стержневые моменты по обеспечению безопасности процессов обработки и передачи информации в информационных системах, базах и банках данных. Данное понятие исключает применение рассматриваемого определения объекта в отношении преступлений, связанных с использованием компьютерной техники и информационных технологий.

Кроме того, вышеуказанные авторы при определении родового объекта подходят к решению вопроса более узко и предметно, что не является неверным. Однако при этом в полной мере учитывается системность проблемы, а также основные задачи и функции уголовного кодекса, в которых красной нитью прописаны общепринятые конвенционные нормы по обеспечению интересов личности, общества и государства.

Необходимо отметить, что однозначно сформулировать определение родового объекта компьютерных преступлений не представляется возможным. Это объясняется тем, что в научном мире пока не разработано единого мнения касательно объекта преступлений в сфере информационных технологий и безопасности. Сложность данного вопроса проявляется еще и в неоднозначном толковании понятия указанных преступлений в разных странах, что приводит к практическим проблемам при квалификации преступлений, а также создает определенные трудности в сотрудничестве государств, организаций и общественности по противодействию киберпреступности.

Совершение киберпреступлений связано с компьютерной информацией, что требует и законодательного определения понятия электронной информации, которое шире понятия компьютерная информация. На наш взгляд, электронная информация может быть определена как «любые сведения (сообщения, данные), представленные в электронно-цифровой форме».

Интересным является позиция группы ученых, которые подходят к решению данного вопроса через систему защищенности и обеспеченности процессов обработки и передачи

компьютерной информации и информационных систем. Так, А.С.Михлин отмечает, что объектом преступлений в сфере компьютерной информации является совокупность общественных отношений, связанных с безопасным производством, использованием и распространением информации и информационных ресурсов, а также обеспечением их надлежащей защиты[11].

С учетом существующих разновекторных позиций по определению родового объекта, более интересным, системным, а также устраняющим проблемы при квалификации преступлений, и тем самым для нас практичным и более близким является позиция В.П.Ревина. Автор определяет в качестве родового объекта преступлений в сфере компьютерной информации общественные отношения, которые нарушают формирование и использование автоматизированных информационных ресурсов и средств их обеспечения. По мнению автора, родовой объект преступлений в сфере информационных технологий является сложным, который включает несколько объектов, охватывающих права и законные интересы: а) владельцев (в том числе, собственников) и пользователей информации, компьютеров, их систем и сетей, средств обеспечения; б) физических и юридических лиц, сведения о которых имеются в автоматизированных информационных ресурсах (банках данных); в) общества и государства, в том числе, интересов национальной безопасности. В частности, применительно к гражданам объектом посягательства могут быть здоровье (например, при нарушении правил эксплуатации информационных систем), имущественные права, право на личную тайну и тайну сообщений, честь и достоинства личности[12].

Лаконичным и емким является авторское определение рассматриваемого понятия М.Х.Рустамбаевым, который в качестве объекта преступлений в сфере информационных технологий рассматривает общественные отношения по обеспечению безопасности компьютерной информации и нормальной работы ЭВМ, их систем или сети[13].

Уголовное законодательство отдельных стран не представляет информационные преступления в виде одной самостоятельной главы. В странах АТР, в частности, в УК КНР имеются отдельные статьи, которые устанавливают ответственность за компьютерные преступления в главе «Преступления против общественного порядка и порядка управления». В УК Республики Корея предусмотрена всего лишь одна статья, устанавливающая ответственность за мошенничество с использованием компьютера. В УК ФРГ информационные преступления представлены в виде двух составов преступлений – компьютерное мошенничество и компьютерный саботаж.

В Узбекистане решение данной проблематики осуществлялась поэтапно. Последовательная либерализация уголовного законодательства, дальнейшее совершенствование судебно-правовой системы, особенности национального уголовно-правовой политики явились логическим продолжением проводимых в стране реформ. С момента принятия в 1994 году в УК Республики Узбекистан предусматривалась всего лишь одна специальная статья 174 (нарушение правил информатизации).

Кроме того, имеются смежные составы, которые опосредованно затрагивают вопросы по обеспечению безопасности информации. Так, в частности, статьи 191 и 192 УК предусматривают ответственность за незаконное собирание, разглашение или использование информации, а также дискредитацию конкурента.

Кроме того, в последние годқ УК ответственность за преступления против чести

и достоинства, совершаемые в информационных сетяхИнтернет, предусмотрена в статьях 139 (Клевета), 140 (Оскорбление), а также статьях 141^1 (Нарушение неприкосновенности частной жизни), 141^2 (Нарушение законодательства о персональных данных), 141^3 (Разглашение сведений, ущемляющих честь и достоинство личности и отражающих интимные стороны жизни человека), 143 (Нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений).

Но виды преступлений одно, так как они выступают в качестве непосредственного объекта уголовно-правовой защиты, а что касается родового объекта, то тут здесь возникает некая проблема. Как отмечает

М.С. Жук, институты Особенной части уголовного права представляют собой совокупность сгруппированных в рамки одной главы уголовного закона предписаний об ответственности за преступления, имеющие единый родовой объект. Сложившаяся иерархия объектов уголовно-правовой охраны и основанный на ней порядок (последовательность) институтов Особенной части уголовного права должны быть пересмотрены. В существующей иерархии интересы общей безопасности остаются явно недооцененными, хотя именно они должны быть поставлены во главу угла при решении вопросов о содержании и систематизации уголовного законодательства[14].

С этим мнением нельзя не согласиться, так как разработанная модель УК Республики Узбекистан, по причине развития общественных отношений, часто добавляется новыми статьями, а то и главами. В этой связи порой становится не до конца понятным, к какому родовому объекту относится введенное законом новшество.

Следует отметить, что специфической особенностью построения Особенной части УК Республики Узбекистан является выделение разделов по признаку родового объекта. Это также требовало выделения рассматриваемых преступлений в отдельную категорию преступлений. Поэтому справедливо можно отметить, что следующим прорывным этапом по обеспечению защиты информации, информационной безопасности явилось принятие в 2007 году новой отдельной главы XX^1 «Преступления в сфере информационных технологий». В ней предусмотрено шесть статей, которые объединены общим родовым объектом преступного посягательства, под которым следует понимать общественные отношения, связанные с охраной законом информации, базы данных и информационных систем их обработки в рамках более общих понятий – общественная безопасность и общественный порядок.

Вместе с тем, если провести анализ Главы XX^1 «Преступления в сфере информационных технологий», то его родовым объектом выступают, общественные отношения по обеспечению общественной безопасности и общественного порядка, однако, исходя из сущности статей предусмотренной главы, родовым объектом является обеспечение информационной безопасности личности, общества и государства. Не выделение данного объекта уголовно-правовой охраны в качестве самостоятельного вида заставляет задумываться, как сложится практика рассмотрения уголовных дел, когда речь будет идти об информационных преступлениях.

Между тем основными задачами и функциями УК является обеспечение интересов личности, общества и государства. Согласно статье 19 Закона Республики Узбекистан «Об информатизации» защита информационных ресурсов и информационных систем

осуществляется в целях: обеспечения информационной безопасности личности, общества и государства; предотвращения утечки, хищения, утраты, искажения, блокировки, подделки информационных ресурсов и иного несанкционированного доступа к ним; предотвращения несанкционированных действий по уничтожению, блокированию, копированию, искажению информации и других форм вмешательства в информационные ресурсы и информационные системы; сохранения государственных секретов и конфиденциальной информации, содержащейся в информационных ресурсах[15].

С учетом вышеизложенного нам представляется логически верным, при определении родового объекта преступлений в сфере информационных технологий и безопасности особо обратить внимание на следующие положения:

- во-первых, на данный момент уголовный закон осуществляет защиту компьютерной информации и информационных систем в рамках общественной безопасности и общественного порядка;

- во-вторых, защита информационных ресурсов и систем является составной частью обеспечения информационной безопасности.

Исходя из этих двух значений можно отметить, что объект информационных преступлений должен обеспечивать уголовно-правовую охрану отношений в сфере информационных технологий и информационной безопасности, которые непосредственно связаны и указывают на фундаментальные принципы права по обеспечению информационной безопасности личности, общества и государства в системе и по отдельности.

Принимая во внимание, что в мировом информационном пространстве возникают новые вызовы и угрозы, которые оказывают огромное влияние на сознание и формирование личности, общества, государства – сама информация становится самым «дорогим» товаром, определяющим и влияющим на процессы, происходящие в мире в условиях глобализации. В связи с этим, считаем возможным определить **родовой объект** преступлений в сфере информационных технологий и безопасности как общественные отношения, обеспечивающие безопасность личности, общества и государства в сфере информационной безопасности и технологий. Определение родового объекта позволит не только определить приоритеты уголовно-правовой охраны в информационном пространстве, но и успешно бороться с информационной преступностью. При определении приоритетов стоит подчеркнуть, что, безусловно, ключевым фактором является национальная безопасность.

Безопасность личности существенным образом зависит от обеспечения информационной безопасности. Под информационной безопасностью понимают состояние защищенности информации и информационной среды от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, (в том числе владельцам и пользователям информации)[16] .

Информационная сфера, является системообразующим фактором жизни общества. Свободное движение информации способствует экономическому и социальному развитию, образованию и демократическому управлению общества. Значительный прогресс в разработке и внедрении информационных технологий и телекоммуникационных средств создал новые возможности для преступной деятельности, и, в частности, для преступного

использования информационных технологий. Количество преступлений, совершаемых в информационном пространстве, растет пропорционально числу пользователей компьютерных сетей, и, по оценкам Интерпола, темпы роста преступности, например, в глобальной сети Интернет, являются самыми быстрыми на планете[17]. Динамичное развитие, а также создание и расширение многовекторного производства персональных компьютеров явилось мощным толчком для естественного стремления человечества получить более совершенный доступ к информационным ресурсам.

В настоящее время сфера информационной безопасности человека не в полной мере отвечает существующим вызовам и угрозам современности, а со стороны научно-экспертных и академических кругов не уделяется должного внимания противодействию этой глобальной проблеме национального информационного пространства. Для этого незамедлительно должен быть предпринят комплекс мер по выработке современных подходов с глубоким изучением опыта развитых стран по борьбе с информационными преступлениями, которые будут соответствовать всем нормам, кроме того, необходимо совершенствовать методы научно-аналитических подходов для системного изучения института информационной безопасности.

На сегодняшний день умышленные общественно опасные, но до настоящего времени не наказуемые деяния в сфере телекоммуникаций характеризуются **большим разнообразием способов и целей их совершения**. Ежегодно наблюдается неуклонный рост числа взломов и иных противоправных воздействий на мобильные устройства. Так, в 2021 году эта цифра составляла 200, в 2022 году – 552, в 2023 году – 606. За последние три года были разработаны более 200 вредоносных программ для системы Android. Всего в 2021 году были обнаружены 3,6 миллионов вредоносных программ для мобильных устройств, в 2022 году – 9 миллионов, в 2023 году – 18,4 миллионов программ.

Потребуется 2 минуты для того, чтобы мобильное устройство подверглось противоправному воздействию (взлом, атака)[18].

Проведенный анализ позволяет выделить несколько основных деяний в сфере телекоммуникаций:

1) неправомерный доступ в локальные и глобальные коммуникации под чужими учетными именами и паролями;

2) доступ к информации на мобильных устройствах для ее копирования, блокирования, хищения денежных средств;

3) использование телефонов - «двойников» мобильной связи.

Кроме того, следует отметить, что в эпоху Интернета, чатов, текстовых сообщений и мобильных телефонов подрастающее поколение, больше, чем кто-либо, рискует стать объектом запугивания. Киберугрозы, которые происходят во время пользования Интернетом, могут принимать различные формы - электронные письма с угрозами, угрожающие (неприличные) сеансы мгновенных сообщений, агрессивные сообщения по мобильной связи, отправление сообщения от лица другого человека, пересылка личных сообщений, фотографий или видеосъемок другим пользователям[19].

В этой связи, обеспечение безопасности в процессе использования мобильной связи выдвигается на первый план.

Стоит также отметить, что на современном этапе развития ИКТ на первый план выходят не компьютерные средства, а мобильные устройства, служащие как для развития социальных сетей, так и для осуществления многих иных функций (в том числе, в сфере управления финансами).

Таким образом, в настоящее время само понятие «компьютер» становится размытым, идет процесс слияния мобильных телефонов с сетью Интернет. Специалисты называют это «мобильной революцией». Телекоммуникационные инфраструктуры приспосабливаются к тому, чтобы максимально способствовать перемещению гигантских объемов информации в самой удобной для потребителя форме. Например, в настоящее время компании-производители мобильных телефонов выпускают так называемые «коммуникаторы» и «смартфоны», сочетающие в себе свойства мобильных телефонов и компьютеров[20].

Согласно исследованиям Norton by Symantec за 2024 год около 55 % пользователей мобильных устройств не задумывались о подключении в сеть WI-FI, в связи с чем их устройства стали жертвами онлайн-программ, 25 % пользуются сетью WI-FI без разрешения владельца или собственника, 8 % сетей были взломаны.

Один из шести человек использовал сеть WI-FI для просмотра негативных ресурсов. 60 % пользователей считают себя защищенными при использовании общественной сети WI-FI, при этом 53 % пользователей не могут различить защищенную и незащищенную общественную сеть.

На вопрос, похищение каких данных для Вас является наиболее неприятным, респонденты ответили следующим образом: 48 % - потрясение от утечки банковских данных или финансовой информации; 38 % - гнев от утечки личных или семейных фотографий; 36 % - обеспокоенность от утечки информации о семье, работе или учебе; 21 % - смущение от утечки личной переписки и сообщений[21].

Вместе с тем, считаем нецелесообразным размещать в отдельном разделе (главе) все преступления, совершаемые с использованием информационных технологий, поскольку это не представляется возможным исходя из разнообъектности преступлений и невозможности отражения в единой главе таких разновекторных и разноплановых преступных деяний (копирайтинг, цифровая подделка и прочие преступления, совершаемые с использованием информационных технологий, где основным объектом являются не отношения в сфере компьютерной информации, а иные отношения).

В современных условиях информационных вызовов и угроз, наряду с криминализацией общественно опасных деяний в виде информационных преступлений, одним из перспективных направлений совершенствования предупреждения и профилактики подобных деяний нам видится создание целого ряда административных правонарушений в сфере информационно-коммуникационных технологий.

В частности, на наш взгляд, внесение некоторых статей УК в сфере информационных технологий в Кодекс Республики Узбекистан об административной ответственности, может послужить снижению роста преступности в данной сфере.

Так, в аспекте дальнейшей либерализации уголовной ответственности полагаем целесообразным дополнить Кодекс об административной ответственности нижеследующими статьями, предусматривающими административные взыскания за

правонарушения в сфере информационно-коммуникационных технологий против чести и достоинства лица:

«Статья 46³. Нарушений требований размещения информации в сети Интернет

Нарушение блогером требований по размещению достоверной информации на своем веб-сайте и (или) странице веб-сайта во всемирной информационной сети Интернет, а равно не принятие соответствующих мер по удалению размещенной информации в случае установления ее недостоверности либо запрещенном характере в течение одних суток после предъявления соответствующего представления –

влечет наложение штрафа от десяти до двадцати базовых расчетных величин.

Статья 46⁴. Незаконное собирание сведений, ущемляющих честь и достоинство личности и отражающих интимные стороны жизни человека

Незаконное собирание информации, содержащей фото и (или) видеоизображения обнаженного тела и (или) половых органов лица без его согласия —

влечет наложение штрафа от тридцати до шестидесяти базовых расчетных величин».

Анализ существующих в мире информационных вызовов и угроз заставляет правительства стран всего мира кардинально поменять политико-правовые подходы к решению глобальных информационных проблем, исходящих из различных источников, объединять усилия международных организаций, государств, ТНК, различных сообществ, академических и экспертно-аналитических кругов в противодействии киберпреступности как надвигающейся угрозы уничтожения социально-экономической и общественно-политической инфраструктур, нравственных и идеологических ценностей цивилизаций.

Список использованной литературы:

1.Каримов И.А. Наша главная цель – демократизация и обновление общества, реформирование и модернизация страны // Народное слово, 29.01.2005 г. № 28.
2.https://daryo.uz/ru/2025/11/03/v-uzbekistane-ushcherb-ot-kiberprestupleniy-prichinyonnyy-grazhdanam-prevysil-12-trilliona-sumov/
3.Dell Secure Works: 2024 Underround Hacker Marketplace Report
4.Robert W. Hubbard, Peter M. Brauti and Scott K. Fenton. Wiretapping and Other Electronic Surveillance: Law and Procedure, Vol. 2, Canada Law Book, Aurora, Ont., March 2008. – P. 15-20.
5.Reyns W. The Anti-Social Network: Cyberstalking Victimization among College Students / LFB Scholarly, 2012 (https://www.questia.com).
6.Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности. Диссертация на соискание ученой степени доктора юридических наук. ВНИИ МВД России. Москва, 2006. – 36 с.
7.Карчевский Н.В. Компьютерные преступления: определение, объект и предмет / Доклад на V Международной конференции «Право и Интернет: теория и практика». http://www.ifap.ru/pi/05/ karchev.html
8.Маляров А.И. Объект преступления в сфере электронно-цифровой (компьютерной) информации и вопросы квалификации (российский и зарубежный опыт). «Общество и право», 2008, № 2 http://www.center-bereg.ru/h1461.html
9.Прохоров Л.А., Прохорова М.Л. Уголовное право: Учебник. — М.: Юристъ, 2004. – 300 с.

10.Колобов В.А., Ясенев В.Н. Контртерроризм и информационная безопасность в современном мире. Монография. Нижний Новгород: Финансовый факультет ННГУ, 2004. – 80 с.
11.Уголовное право: Часть Общая. Часть Особенная. Вопросы и ответы (Серия «Подготовка к экзамену»). - М.: Юристъ, 2004. – 244 с.
12.Ревин В.П. Уголовное право России. Общая часть: Учебник. - М.: Юстицинформ. 2016. – 482 с.
13.Рустамбаев М.Х. Курс уголовного права Республики Узбекистан. Особенная часть. Том 5: Преступления против общественной безопасности и общественного порядка. Преступления против порядка несения военной службы. Учебник для ВУЗов. – Т.: Издательство «ТГЮИ», 2008. – 586 с.
14.Жук М.С. Объект преступления как критерий построения системы институтов Особенной части Уголовного права / Общество и право. 2009. № 5. – С. 24-27.
15.Закон Республики Узбекистан «Об информатизации» от 11 декабря 2003 года № 560-II.
16.Амелин Р.В. Обязанности поставщиков информации в федеральные информационные системы, связанные со способом представления информации // Юрист. 2017. № 8. – С. 36-38.
17.Номоконов В.А. Актуальные проблемы борьбы с киберпреступностью // Сборник научных трудов международной конференции «Информационные технологии и безопасность». Выпуск 3. – Киев: Национальная академия наук Украины, 2003. – С. 104-110.
18.http://www.symantec.com/
19.http://www.ruskline.ru/
20.Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы. Владивосток. – 2007. – 276 с.
21.http://www.symantec.com/