СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ ОПЫТА ЗАРУБЕЖНЫХ СТРАН ПО ОБЕСПЕЧЕНИЮ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Кулматов Шароф Асадович

uziivacademy@gmail.com

Начальник факультета послевузовского образования Академии МВД Республики Узбекистан, доктор юридических наук (DSc), профессор

O‘zbekiston Respublikasi IIV Akademiyasi Oliy ta’limdan keyingi ta’lim fakulteti boshlig‘i yuridik fanlar doktori (DSc), professor

Head of the Faculty of Postgraduate Education Academies of the Ministry of Internal Affairs of the Republic of Uzbekistan, Doctor of Law (DSc), Professor

Саъдуллаев Гайратжон Абдужаббор угли

uziivacademy@gmail.com

Ведущий научный сотрудник отдела организации научно-исследовательской деятельности Академии МВД Республики Узбекистан

O‘zbekiston Respublikasi IIV Akademiyasi Ilmiy-tadqiqot faoliyatini tashkil etish bo‘limi yetakchi ilmiy xodimi

Leading Researcher at the Department of Organization of Scientific and Research Activities of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

Аннотация. *В данной статье на основе сравнительно-правового анализа изучен опыт зарубежных государств по уголовно-правовой защите информационной безопасности личности. В ходе исследования проанализированы законодательные системы и правоприменительная практика ряда развитых стран, выявлены их преимущества и недостатки в борьбе с киберпреступностью. Также рассмотрены международные стандарты и их интеграция в национальное законодательство. Выдвинуты предложения и рассмотрены возможности применения зарубежного опыта для обеспечения информационной безопасности личности в Узбекистане.*

Ключевые слова: *информационная безопасность, киберпреступность, преступления против личности, правовая защита, профилактика.*

SHAXSNING AXBOROT XAVFSIZLIGINI JINOYAT-HUQUQIY MUHOFAZA QILISH BO‘YICHA XORIJIY DAVLATLAR TAJRIBASINING QIYOSIY-HUQUQIY TAHLILI

Annotatsiya. *Ushbu maqolada shaxsning axborot xavfsizligini jinoyat-huquqiy muhofaza qilish bo‘yicha xorijiy davlatlar tajribasi qiyosiy-huquqiy tahlil asosida o‘rganilgan. Tadqiqot davomida bir qator*

rivojlangan davlatlarning qonunchilik tizimi va huquqni qo‘llash amaliyoti tahlil qilinib, ularning kiberjinoyatchilikka qarshi kurashdagi afzallik va kamchiliklari o‘rganildi. Shuningdek, xalqaro standartlar va ularning milliy qonunchilikka integratsiya qilinishi tahlil qilingan. Maqolada O‘zbekistonda shaxsning axborot xavfsizligini ta’minlashda xorijiy tajribani qo‘llash imkoniyatlari va takliflar ilgari surilgan.

Kalit so‘zlar: *axborot xavfsizligi, kiberjinoyatchilik, shaxsga qarshi jinoyatlar, huquqiy himoya, profilaktika.*

COMPARATIVE LEGAL ANALYSIS OF THE EXPERIENCE OF FOREIGN COUNTRIES IN ENSURING CRIMINAL LAW PROTECTION OF PERSONAL INFORMATION SECURITY

Abstract. *Based on a comparative legal analysis, this article examines the experience of foreign countries in criminal law protection of personal information security. The study analyzed the legislative systems and law enforcement practices of a number of developed countries, identified their advantages and disadvantages in the fight against cybercrime. International standards and their integration into national legislation are also considered. The article presents proposals and considers the possibilities of applying foreign experience to ensure personal information security in Uzbekistan.*

Keywords: *information security, cybercrime, crimes against the person, legal protection, prevention.*

Введение / Introduction

Современный этап развития общества отмечается значительным ростом роли информационной сферы, которая включает в себя не только информацию, но и инфраструктуру, технологии и субъекты, задействованные в процессе сбора, обработки, распространения и использования данных [14]. Это динамично развивающееся направление также сопровождается расширением системы правового регулирования, которая охватывает все более сложные общественные отношения, возникающие в этой области.

Особенно важно подчеркнуть, что стратегически значимым для страны является развитие высокотехнологичной телекоммуникационной отрасли. В современном мире невозможно представить повседневную жизнь без использования компьютерной техники, информационных технологий, Интернета и сотовой связи, которые стали неотъемлемой частью глобальной коммуникационной среды и обеспечения национальной безопасности.

Свободный обмен информацией способствует развитию экономики, общества, образования и поддерживает демократические процессы в управлении. Однако прогресс в области информационных технологий и телекоммуникаций также создал новые возможности для преступной деятельности, в частности, для незаконного использования этих технологий. Развитие технологий, обеспечивающих глобальную коммуникацию и обмен данными, открыло путь для различных форм киберпреступлений, что требует усиления правовой защиты и разработки эффективных методов борьбы с подобными угрозами.

Рост преступлений в киберпространстве требует особого внимания со стороны правовых и правоохранительных органов, так как традиционные методы борьбы с преступностью зачастую оказываются неэффективными в условиях цифровой среды. В этом контексте важным становится не только развитие законодательных инициатив, но и совершенствование международного сотрудничества, так как киберпреступления часто имеют транснациональный характер. Преступники могут совершать преступления из любой точки мира, что усложняет процесс их выявления и задержания.

Кроме того, проблема киберпреступности касается не только экономической безопасности, но и личной безопасности граждан. Современные виды преступлений, такие как кража персональных данных, фишинг, кибербуллинг и интернет-мошенничество, могут наносить

значительный ущерб как физическим, так и юридическим лицам. Поэтому важно разрабатывать и внедрять меры защиты на всех уровнях – от индивидуальной безопасности пользователей до создания эффективных правовых механизмов для защиты национальной безопасности и обеспечения правопорядка в информационном пространстве.

Методология исследования / Methods

В ходе исследования использованы методы сравнительно-правового анализа, формально-юридический метод, а также анализ нормативных актов и правоприменительной практики зарубежных стран. Изучены законодательные акты, а также международные соглашения в сфере кибербезопасности.

По данным статистики, с развитием технологий и глобализацией сети Интернет, количество пользователей значительно увеличилось за последние десятилетия. В 2010 году сетью Интернет пользовались всего 1 миллиард 18 миллионов человек. К 2015 году их количество достигло 3 миллиардов 24 миллионов [3]. По состоянию на 2023 год, примерно 5,4 миллиарда человек, или 67% от мирового населения, используют интернет. Это является значительным увеличением на 45% с 2018 года, когда в сети было около 3,7 миллиардов пользователей. При этом около 2,6 миллиардов человек всё ещё не имеют доступа к интернету [4].

По последним данным, большинство пользователей Интернета по всему миру составляют люди в возрасте от 18 до 49 лет, при этом почти 98% взрослого населения в возрасте 30-49 лет и 97% молодежи от 18 до 29 лет имеют доступ к интернету. Однако использование интернета значительно снижается среди старших возрастных групп. Так, только 88% людей старше 65 лет пользуются интернетом. В целом, более 95% пользователей выходят в сеть с мобильных устройств, что подтверждает рост мобильного интернета среди всех возрастных групп [15].

В 2023 году ущерб от киберпреступлений продолжил увеличиваться, достигнув рекордных величин. По данным Федерального бюро расследований США (FBI), киберпреступники нанесли ущерб более чем 12,5 миллиарда долларов только в США, что представляет собой рост на 22% по сравнению с 2022 год. В целом, специалисты считают, что глобальные потери от киберпреступности могут составлять более 500 миллиардов долларов по всему миру. Это свидетельствует о том, что кибер угрозы становятся все более разрушительными, и соответствующие потери увеличиваются пропорционально росту числа пользователей Интернета и уровня их вовлеченности в онлайн-деятельность [10].

Эти цифры подчеркивают стремительное развитие Интернета и его проникновение в повседневную жизнь людей, а также показывают важность обеспечения безопасности в цифровом пространстве, с учетом роста числа пользователей и расширения диапазона онлайн-деятельности.

С момента появления информационных преступлений государства начали принимать меры для уголовной ответственности лиц, совершивших такие деяния. Тем не менее, несмотря на различные национальные подходы, до сих пор не существует универсальной, согласованной модели регулирования. Это подчеркивает необходимость выработки международно-правовых стандартов для борьбы с информационными преступлениями.

Вопросы, связанные с киберпреступностью, требуют координированных действий на международном уровне, так как преступления в сети Интернет не ограничиваются национальными границами. Международное сотрудничество в области информационной безопасности, включая обмен информацией, развитие общего законодательства и принятие универсальных стандартов, имеет решающее значение для эффективной борьбы с кибер угрозами. Важную роль в этом процессе играют такие международные инициативы, как Конвенция Совета

Европы по киберпреступности (Будапештская конвенция), которая является первым юридически обязательным международным инструментом в этой области.

Анализ и результаты / Results

Таким образом, пока не выработан единый глобальный подход, актуальность международного правового регулирования становится всё более очевидной.

За последнее десятилетие наблюдается значительная активность в принятии международных и региональных документов, направленных на противодействие информационной преступности. Эти документы включают как обязательные для выполнения, так и необязательные. В целом можно выделить несколько групп документов, которые были разработаны в контексте или под эгидой следующих организаций:

1. Организация Объединенных Наций (ООН). Включает документы, как «Резолюции Генеральной Ассамблеи ООН» [3], направленные на гармонизацию правовых норм по борьбе с киберпреступностью. Примером является Резолюция 68/167, которая касается защиты личной информации и предотвращения киберугроз.

2. Совет Европы. Наиболее известным документом является Будапештская конвенция по киберпреступности (2001), которая является первым международным юридически обязательным инструментом для борьбы с киберпреступностью. Конвенция устанавливает стандарты для уголовного законодательства в сфере киберпреступлений и предлагает механизмы международного сотрудничества.

3. Европейский Союз. ЕС разработал ряд директив, например, Директиву 2013/40/ЕС по атакам на информационные системы, а также инициировал проекты по защите данных, как Общий регламент о защите данных (GDPR), который активно используется для защиты персональной информации.

4. Группа 7 (G7) и Группа 20 (G20). Эти международные форумы стали площадками для обсуждения и разработки практических шагов в борьбе с киберпреступностью, включая сотрудничество в области кибербезопасности и принятие принципов для обеспечения защиты информационных технологий [14].

5. Международная телекоммуникационная организация (ITU). Организация разработала несколько документов, направленных на глобальную координацию и установление стандартов для защиты от киберугроз в глобальном масштабе.

6. Организация экономического сотрудничества и развития (ОЭСР). ОЭСР активно участвует в разработке рекомендаций и принципов для борьбы с киберпреступностью, в том числе в контексте защиты персональных данных и защиты критической информационной инфраструктуры. Например, в 2011 году была принята Рекомендация по безопасности интернет-услуг.

7. Азиатско-Тихоокеанский регион. В рамках этого региона было разработано несколько соглашений, направленных на улучшение сотрудничества в борьбе с киберпреступностью, включая инициативы Азиатско-Тихоокеанского экономического сотрудничества (АРЕС), направленные на укрепление координации в сфере цифровой безопасности и защиты данных[14].

8. Международная организация по стандартизации (ISO). ISO разработала стандарты, такие как ISO/IEC 27001, которые обеспечивают основы для управления информационной безопасностью на глобальном уровне. Эти стандарты предоставляют рекомендации по внедрению процессов, направленных на защиту данных и предотвращение киберпреступлений.

9. Международная ассоциация правоохранительных органов (INTERPOL). INTERPOL активно развивает механизмы международного сотрудничества в борьбе с киберпреступностью через создание глобальных баз данных, обучение правоохранителей и предоставление аналитической поддержки.

Эти документы способствуют гармонизации национальных законов и стандартов, а также создают механизмы для международного сотрудничества в борьбе с преступлениями, посягающими на информационную безопасность личности.

Основные направления обеспечения стабильной защищенности информационных систем, сетей и ресурсов, а также информационной безопасности личности в зарубежных актах можно подразделить на несколько ключевых групп:

– совершенствование уголовного законодательства и устранение связанных с ним проблем возможно через тщательный сравнительно-правовой анализ уголовных норм, действующих в различных странах. Такой подход способствует перенять положительный международный опыт, включая положения, направленные на установление ответственности за преступления, посягающих на информационную безопасность личности, что позволяет адаптировать эффективные решения к национальной правовой системе.

Попробуем проанализировать ответственность за преступления, посягающие на информационную безопасность личности, разделив законодательство иностранных государств на две группы.

Первая группа включает страны, где законодательством предусмотрена конкретная ответственность за нарушения, непосредственно направленные на информационную безопасность личности. К таким преступлениям относятся несанкционированный доступ к персональным данным, их модификация или уничтожение, а также использование данных с целью нанесения вреда. Эти государства устанавливают четкие критерии, описывающие состав преступления, и разрабатывают специализированные нормы, что способствует эффективному обеспечению защиты информации. Примером может служить законодательство Европейского союза, в частности Общий регламент по защите данных (GDPR), который вводит строгую ответственность за неправомерное использование персональной информации.

Вторая группа охватывает страны, где ответственность за преступления, посягающие на информационную безопасность личности, не выделена как отдельная категория, но признаки этих преступлений могут быть включены в состав более общих преступлений. Например, в некоторых государствах такие действия квалифицируются как мошенничество, кража, шантаж или нарушение частной жизни. Подобный подход может создавать трудности при правоприменении, так как он не всегда позволяет выделить специфику преступлений, связанных именно с информационной безопасностью.

Такое разграничение позволяет оценить, какие подходы к правовому регулированию являются наиболее эффективными и выявить направления для совершенствования национального законодательства в области обеспечения информационной безопасности личности.

Информационные преступления, направленные на нарушение безопасного создания, хранения, использования и распространения компьютерной информации, которая охраняется уголовно-правовыми средствами, охватывают широкий круг стран по всему миру. Это включает страны Северной и Южной Америки, Европы, Азии, а также государства СНГ. В этих странах данные преступления обычно рассматриваются как посягательства на

компьютерную информацию или информационную безопасность личности, что влечет уголовную ответственность.

Например, в Европейском союзе такие преступления охватываются директивой 2013/40/ЕС о киберпреступлениях, которая устанавливает уголовную ответственность за вмешательство в компьютерные системы и сети, а также за несанкционированное распространение вирусов и вредоносных программ. В США подобные преступления регулируются в рамках Закона о киберпреступлениях (CFAA), который включает наказания за несанкционированный доступ к компьютерам и нарушения защиты данных [11].

В странах СНГ информационная безопасность также закреплена в национальных законодательствах. Например, в России Уголовный кодекс предусматривает ответственность за преступления в сфере компьютерной информации, такие как несанкционированный доступ к данным, создание и распространение вирусов, а также угрозы и атаки на информационные системы. Преступления в области информационной безопасности также предусмотрены в законах стран Центральной Азии и Восточной Европы, включая Казахстан, Туркменистан, Беларусь и Украину, где установлены уголовные санкции.

Посягательства на информационную безопасность личности по своему составу и положению в уголовном праве практически идентичны в странах бывшего Союза и нынешнего СНГ, и даже в уголовном праве отдельных государств этот вопрос решается одинаково. Такие общие черты, как нарушение законодательства о персональных данных, являются общим признаком, присущим информационной безопасности личности, предусмотренному уголовным законодательством этих государств.

Причина сходства посягательства на информационную безопасность личности в уголовном праве стран СНГ заключается, во-первых, в том, что история и этапы развития уголовного права этих государств одинаковы, а во-вторых, в том, что для государств СНГ в 1996 году был разработан модельный УК, а ряд государств при разработке своего законодательства опирались на этот документ.

В Модельном УК для государств – участников Содружества Независимых Государств дифференцирована ответственность за нарушения информационной безопасности личности. Например, статья 142. Принуждение в главе 19. Преступления против личной свободы, чести и достоинства, или статья 151 Незаконное собирание и распространение информации о частной жизни в главе 21. Преступления против конституционных прав и свобод человека и гражданина и др. [2].

В этом кодексе за незаконное собирание в целях распространения сведений о частной жизни, составляющих личную или семейную тайну другого лица без его согласия, либо распространение таких сведений в публичном выступлении, публично выставленном произведении или в средствах массовой информации, причинившие вред правам и законным интересам потерпевшего, установлена ответственность. А также установлена ответственность за нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений (статья 153).

Данное преступление разделено на две части, первая и вторая из которых относятся к менее тяжким преступлениям. В качестве отягчающих обстоятельств ответственности установлено совершение преступления с использованием служебного положения.

Отличия уголовного законодательства Республики Узбекистан от Модельного УК заключаются, в основном, в установленной ответственности, например, законодатель Республики Узбекистан за умышленное нарушение тайны переписки, телефонных

переговоров, телеграфных или иных сообщений, устанавливает административную ответственность, только при повторном совершении уголовную. А также обстоятельства, отягчающие ответственность отсутствуют.

В Модельном УК стран СНГ, ответственность за нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений в УК происходит из главы преступлений против конституционных прав и свобод человека и гражданина. Даже в уголовных кодексах некоторых стран (например, Таджикистана, Казахстана, Туркменистана, Азербайджана, Республики Беларусь) нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений регулируется нормами, аналогичными положениям, закрепленным в Модельном Уголовном кодексе для стран СНГ.

Такое сходство обусловлено общей правовой традицией и единым подходом к защите прав граждан на конфиденциальность информации, закрепленной в законодательстве постсоветских государств. Эти нормы направлены на обеспечение права каждого человека на неприкосновенность частной жизни и защиту личной информации от несанкционированного вмешательства.

Подобные статьи предусматривают ответственность за незаконное получение, распространение или использование информации, переданной посредством различных средств связи, что свидетельствует о значимости защиты личных данных и коммуникаций в условиях современных технологий.

В уголовном законодательстве отдельных государств существуют различия в подходах к регламентации состава преступлений, посягающих на информационную безопасность личности, отягчающим обстоятельствам ответственности и степени общественной опасности. Рассмотрим конкретные аспекты этих преступлений в уголовных кодексах Российской Федерации, Киргизской, Молдавской, Эстонской и Армянской республик:

Российская Федерация. В Уголовном кодексе РФ предусмотрена ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ) [12]. Особенностью является установление отягчающих обстоятельств, таких как совершение преступления с использованием служебного положения или в отношении значительного количества граждан. Преступление наказывается штрафами, исправительными работами, лишением свободы в зависимости от обстоятельств.

Киргизская Республика. УК Киргизии включает нормы, аналогичные российскому законодательству, однако уделяет больше внимания вопросам незаконного использования персональных данных. Преступление, связанное с нарушением конфиденциальности информации, может отягощаться обстоятельствами, связанными с использованием технических средств или служебного положения (ст. 193) [6].

Республика Молдова. В молдовском уголовном законодательстве значительное внимание уделяется защите персональных данных и конфиденциальности частной информации. Отягчающими обстоятельствами являются действия, с использованием служебного положения, или специальных технических средств, предназначенных для негласного получения информации, а также в интересах организованной преступной группы или преступной организации (ст. 179), что связано с учетом европейских стандартов защиты данных [7].

Эстония. В Эстонии законодательство строго регламентирует нарушения информационной безопасности. Уголовный кодекс предусматривает серьезные санкции за незаконное использование средств связи и нарушение конфиденциальности электронных

сообщений. Особое внимание уделяется киберугрозам, что отражает высокий уровень цифровизации общества [13].

Республика Армения. Уголовное законодательство Армении (ст. 144, 145, 146 УК Армении) [5] предусматривает ответственность за нарушение тайны переписки и сообщений, а также за несанкционированный доступ к информационным системам. Отягчающими обстоятельствами выступают повторные действия или причинение значительного ущерба. Также Армения активно совершенствует свое законодательство в контексте растущих угроз киберпреступности.

Во всех перечисленных странах защита информационной безопасности личности является значимым аспектом уголовного права, однако степень детализации норм и их фокус варьируются.

Российское и киргизское законодательство схожи по структуре норм, тогда как Эстония и Молдова ориентированы на европейские стандарты.

Армения усиливает ответственность за киберпреступления, активно реагируя на современные вызовы в области информационных технологий.

Эти особенности подчеркивают значимость индивидуального подхода к защите информационной безопасности в условиях различных правовых и социальных систем.

Информационные преступления, связанные с нарушением безопасности персональных данных, являются важной составляющей правовой охраны конфиденциальности в разных странах мира. В США, например, § 2701 Титула 18 Свода законов устанавливает [16] уголовную ответственность за нарушение конфиденциальности электронной почты и речевой корреспонденции на сервере. В Великобритании вопросы защиты персональных данных регулируются Законом о персональных данных 1998 года, который рассматривает нарушения, связанные с противоправным разглашением данных, включая использование компьютерных технологий для таких деяний.

Аналогичные преступления предусмотрены в других странах: в Дании незаконное использование частной информации регулируется § 264d УК [1], в Испании – раскрытие и распространение тайных сведений, в Швеции – нарушение почтовой и телекоммуникационной тайны (статья 8 главы 4), в Швейцарии – незаконное получение личных данных (статья 179). Во Франции и Нидерландах также предусмотрены санкции за незаконное перехватывание, отслеживание или запись данных с использованием различных технических устройств.

Что касается стран СНГ, то ответственность за нарушение прав на персональную тайну в некоторой степени регулируется в Уголовных кодексах Казахстана и Кыргызстана. В Казахстане статьи 147 и 148 УК рассматривают нарушение неприкосновенности частной жизни, а также незаконное вмешательство в переписку и другие сообщения [8]. В Кыргызстане статья 189 УК охватывает нарушение тайны переписки [6].

В УК Республики Узбекистан ответственность за нарушение безопасности персональных данных предусмотрена статьей 141^2(нарушение законодательства о персональных данных) [9].

Заключение / Conclusions

Основной вывод, который можно сделать на основе анализа состава информационных преступлений, предусмотренных в Уголовных кодексах зарубежных стран, заключается в том, что большинство этих стран предусматривают ответственность за более широкий спектр информационных правонарушений, чем это имеет место в Уголовном кодексе Республики

Узбекистан. Это включает не только более детализированные положения о защите персональных данных и информационной безопасности, но и более широкие нормы, касающиеся компьютерных преступлений, неправомерного доступа, вмешательства в электронные коммуникации и киберугроз.

Тогда как в Узбекистане законодательство в этой сфере пока остается более узким и ограниченным, международная практика отражает глобальные угрозы в области информационной безопасности и использования новых технологий.

Сравнительно-правовой анализ уголовных кодексов зарубежных стран и Узбекистана выявил несколько ключевых проблем, которые требуют дальнейшего внимания. Несмотря на положительные аспекты, такие как уникальные статьи, которые присутствуют в законодательстве Узбекистана, но отсутствуют в кодексах других стран, существуют заметные пробелы в области охраны информационной безопасности личности.

Этот вывод подчеркивает необходимость доработки уголовного законодательства Узбекистана, особенно в контексте продолжающихся реформ в судебной и правовой системах страны. В условиях глобализации и активного внедрения новых технологий Узбекистану необходимо разработать более конкретные и расширенные нормы, которые будут эффективно охватывать новые виды преступлений, включая те, что связаны с киберпреступностью.

В заключение, необходимо подчеркнуть, что несмотря на имеющиеся успехи, для обеспечения полноценной безопасности в информационном пространстве и защиты прав личности от киберугроз, Узбекистану предстоит еще проделать значительный путь, внедряя современные подходы к правовому регулированию информационной безопасности.

Использованные источники / References

1. Аблятипова Н. А., Цыганова Д. С. Проблемы охраны изображения человека в гражданском законодательстве Российской Федерации // Ученые записки Тамбовского отделения РоСМУ. 2019. №14. URL: https://cyberleninka.ru/article/n/problemy-ohrany-izobrazheniya-cheloveka-v-grazhdanskom-zakonodatelstve-rossiyskoy-federatsii (дата обращения: 18.12.2024).
2. Модельный Уголовный кодекс для государств — участников СНГ https://iacis.ru/baza_dokumentov/modelnie_zakonodatelnie_akti_i_rekomendatcii_mpa_sng/modelnie_kodeksi_i_zakoni
3. Расулев А. К. Совершенствование уголовно-правовых и криминологических мер борьбы с преступлениями в сфере информационных технологий и безопасности // 2018 http://diss.natlib.uz/ru-RU/ResearchWork/-OnlineView/43426
4. http://sartraccc.ru/i.php?filename=Pub_inter%2Funodcvscc.html&oper=read_file#1
5. http://www.parliament.am/legislation.php?ID=1349&lang=rus&sel=show
6. https://cbd.minjust.gov.kg/112309/edition/3548/ru
7. https://continent-online.com/Document/?doc_id=30394923#pos=2261;-59
8. https://kodeksy-kz.com/ka/ugolovnyj_kodeks/147.htm
9. https://lex.uz/docs/111457
10. https://rg.ru/2024/05/01/pozhilye-amerikancy-poteriali-34-mlrd-dollarov-iz-za-kiberprestupnosti.html
11. https://sn-law.cfuv.ru/k-voprosu-o-protivodejstvii-kiberprestupnosti-v-usloviyah-novoj-geopoliticheskoj-realnosti/
12. https://www.consultant.ru/document/cons_doc_LAW_10699/
13. https://www.juristaitab.
14. https://www.sechenov.ru/upload/medialibrary/a85/dissertatsiya-myzina-glavnyy_izdatelstvo.pdf
15. https://www.tadviser.ru
16. https://www.unodc.org/e4j/ru/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html