АННОТАЦИЯ

Тема: Уголовные правонарушения в сфере информатизации и связи (уголовно-правовые и криминологические аспекты)

Целью исследования - является комплексный анализ состава уголовных правонарушений, исторических аспектов, вопросов правоприменительной практики в сфере информатизации и связи, а также выработка предложений по совершенствованию законодательства и повышению эффективности борьбы с уголовными правонарушениями.

Для достижения этой цели в работе определены следующие **задачи**:

1.Изучить исторические аспекты ответственности за уголовные правонарушения в сфере информатизации и связи.

2.Раскрыть современное формирование понятия уголовных правонарушений в сфере информатизации и связи и провести теоретический анализ.

3.Анализ нормативной правовой базы, регулирующей ответственность за уголовные правонарушения в сфере информатизации и связи, и выявление ее недостатков.

4.Дать криминологическую характеристику уголовных правонарушений в сфере информатизации и связи.

5.Сравнительный анализ зарубежного опыта борьбы с уголовными правонарушениями в сфере информатизации и связи.

6.Разработка и обоснование предложений по совершенствованию мер профилактики уголовных правонарушений и законодательства в сфере информатизации и связи.

Объект исследования: общественные отношения в сфере уголовных правонарушений в сфере информатизации и связи.

Предмет исследования: уголовно-правовые и криминологические аспекты правонарушений в сфере информатизации и связи.

Методы исследования. Методика исследования уголовных правонарушений в сфере информатизации и связи основана на комплексном подходе, объединяющем историко-правовые, логические, статистические, сравнительно-правовые, теоретические и эмпирические методы анализа. Одним из основных методов является анализ нормативной документации, позволяющей изучить действующее законодательство, регулирующее сферу информационных технологий и коммуникаций. Метод предполагает детальное изучение Уголовного кодекса, специальных законов, подзаконных актов, а также анализ судебной практики и принятых решений. Цель анализа-выявление правовых пробелов, противоречий и оценка эффективности нормативных правовых актов в борьбе с киберпреступностью. Использование статистических данных правоохранительных органов и научно-исследовательских институтов позволяет оценить масштаб проблемы, выявить наиболее распространенные виды уголовных правонарушений и

оценить эффективность принятых мер по их предупреждению и раскрытию. Кроме того, сравнительный анализ международного опыта играет важную роль в изучении эффективных методов и методов регулирования и борьбы с киберпреступностью в разных странах. Этот метод позволяет определить успешные стратегии, которые могут быть адаптированы и применены в контексте других юрисдикций, тем самым способствуя улучшению международного сотрудничества в борьбе с уголовными преступлениями в области информатизации и коммуникации.

Теоретические и методологические основы исследования. Изучение теоретических и методологических основ уголовных правонарушений в сфере информатизации и связи предполагает анализ понимания, классификации и уголовно-правовых аспектов данных уголовных правонарушений с учетом их исторического развития и международного сотрудничества. В криминологическом аспекте позволяет понять причины и условия, способствующие киберпреступности, и разработать эффективные профилактические меры. Методика исследования основана на комплексном использовании теоретических и эмпирических методов, обеспечивающих всесторонний анализ проблемы и способствующих выработке рекомендаций по совершенствованию законодательства и повышению эффективности борьбы с уголовными правонарушениями в сфере информатизации и связи.

Научная новизна исследования. Научная новизна данного исследования заключается в формулировании и разработке новых научных принципов, связанных с анализом и дифференциацией уголовных правонарушений в сфере информатизации и связи. В ходе работы были выявлены и систематизированы основные аспекты, определяющие признаки и механизмы совершения таких уголовных правонарушений, что позволило обновить теоретические подходы в уголовном праве и криминологии. Исследование способствует развитию теоретических основ юридической науки путем детального анализа влияния информационно-технического прогресса на изменение характера и структуры уголовного правонарушения, а также обоснования необходимости адаптации правовой системы к новым задачам.

Теоретическая и практическая значимость исследования.

Теоретическая значимость исследования заключается в разработке методических подходов по изучению и борьбе с уголовными преступлениями в области обогащения и расширения существующих знаний о киберпреступности, а также информатизации и связи. Исследование предлагает новую классификацию киберпреступлений, которая способствует более точному пониманию их природы и, как следствие, большей эффективности правоохранительных органов. Работа также расширяет границы криминологической теории и вводит аспекты, связанные с цифровизацией общества и информационной безопасностью.

Практическая значимость исследования. Практическая ценность диссертации связана с разработкой и представлением конкретных предложений по совершенствованию законодательства и практики его применения в борьбе с уголовными правонарушениями в сфере информатизации и связи. В ходе исследования предложены пути укрепления нормативной правовой базы, направленные на устранение имеющихся пробелов в законодательстве и совершенствование механизмов межведомственного и международного сотрудничества уголовных правонарушений в области информатизации и связи. Кроме того, в ходе работы были выработаны рекомендации по повышению эффективности деятельности органов внутренних дел путем внедрения современных технологий и методов расследования, а также по обучению и повышению квалификации сотрудников, отвечающих требованиям цифровой эпохи.

Основные рекомендуемые формулировки защиты:

1. С учетом реализации Концепции правовой политики Республики Казахстан до 2030 года и Концепции кибербезопасности автором дано авторское определение уголовного правонарушения в сфере информатизации и связи теоретического характера.

В условиях стремительного развития инновационных цифровых технологий правонарушители применяют новые способы совершения уголовных правонарушений, а также возникают дополнительные уголовные угрозы для многих сфер общественной жизни, в том числе и для свободы предпринимательской деятельности, в таких условиях требуется полноценное определение уголовного правонарушения в сфере информатизации и связи.

Уголовные правонарушения в сфере информатизации и связи — это «уголовные правонарушения, совершаемые путем незаконного использования информационных систем, баз данных и сетей телекоммуникаций, компьютерных коммуникаций, с целью доступа к частным и государственным данным, их изменения или уничтожения».

2. В ходе дифференциации уголовных правонарушений в сфере информатизации и связи выявлены недостатки в понятийном аппарате. В целях устранения недостатков в данном направлении предлагаем ввести следующие понятия. Необходимо ввести пункт 3 статьи 41-1 Уголовного кодекса Республики Казахстан и дополнить следующими понятиями: «*киберпреступление*», «*компьютерная коммуникация», «кибербезопасность»*. «*Киберпреступление*» – действия незаконного владения и использования информационных технологий, компьютерных систем, конфиденциальной информации, персональных данных в киберпространстве. «*Компьютерная коммуникации*» — это процесс использования различных сетевых технологий, таких как Интернет, локальные (LAN) и беспроводные сети, для передачи и приема данных между компьютерами», *«кибербезопасность*-это меры и процессы для защиты

компьютерных систем, сетей и данных от несанкционированного доступа, атак и угроз». При изучении уголовных правонарушений в сфере информатизации и связи возникает необходимость четкого и своевременного выявления посредством дефиниций основных признаков общественно опасных действий и бездействия, а также возможных или реально возникающих тяжких и особо тяжких последствий. Такие дефиниции позволяют классифицировать уголовные правонарушения, совершенствовать правоприменительную практику и применять эффективные правоохранительные меры против таких действий. В этом контексте важную роль играет своевременное выявление и четкое описание уголовных правонарушений, поскольку они способствуют правильному поведению правоохранительных органов и обеспечению информационной безопасности.

Также предлагается внести изменения в статьи 3 пункт 38 УК РК в дополнение статьями 205, 206, 208 УК РК, т. е. стоимость имущества или размер ущерба, превышающий месячный расчетный показатель в одну тысячу раз, как крупный ущерб и крупный размер. Дело в том, что понятия крупный ущерб и крупный размер позволяют объективно оценить степень вреда, который уголовное правонарушение наносит обществу. Таким образом, четко определить тяжесть уголовного правонарушения и обеспечить правильное поведение правоохранительных органов. Наличие выявленных пределов облегчает правоохранительным органам и судам процесс выявления и оценки уголовных правонарушений. В международной практике наиболее распространенной практикой является уточнение размера имущественного ущерба и убытков. Эти изменения обеспечат соответствие международным стандартам и улучшат правовую систему.

3. Как показывает следственная и судебная практика, в объективных или субъективных признаках уголовных правонарушений в сфере информатизации и связи наблюдаются законодательные недостатки. Согласно исследованиям, рост числа таких правонарушений связан с расширением сферы применения информационных технологий. Основные инфраструктуры, такие как финансовые институты, энергетические системы и государственное управление, становятся основными целями киберпреступников и требуют эффективных кибербезопасных и уголовно-правовых мер. В процессе технологического прогресса и оцифровки общества возникает необходимость обновления уголовного законодательства. Это, в свою очередь, позволяет поддерживать баланс между информационной безопасностью и инновациями. Таким образом, возрастает необходимость усиления мер по борьбе с информационными уголовными правонарушениями. Повышение достоверности законодательных актов и совершенствование правоприменительной практики способствуют своевременному выявлению уголовных правонарушений, их классификации и эффективному реагированию правоохранительных органов. В этом контексте для борьбы с

информационными правонарушениями необходимо внедрение современной политики и методик, а также совершенствование правового регулирования. Эти действия представляют собой важные шаги, направленные на обеспечение правовой безопасности и усиление защиты от киберугроз.

Поэтому рекомендуются следующие изменения и дополнения:

-Часть 4 статьи 205 УК РК предлагается изложить в следующей редакции «умышленный неправомерный доступ к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или сеть телекоммуникаций, повлекший существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, повлекшие по неосторожности тяжкие последствия, совершенные неоднократно, по предварительному сговору группы лиц» - «наказывается штрафом в размере до двух тысяч месячных расчетных показателей с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до четырех лет или без него, либо исправительными работами в том же размере, либо общественным трудом на срок до шестисот часов, либо ограничением свободы на срок до шести лет, либо лишением свободы на тот же срок»

- Предлагается дополнить диспозицию части 1 статьи 206 Уголовного кодекса РК понятием «*компьютерная коммуникация*». Это связано с тем, что Неправомерные уничтожение или модификация информации передаются через сеть компьютерных коммуникаций. Часть 1 статьи 206 УК РК представляется в следующей редакции «Умышленные неправомерные уничтожение или модификация охраняемой законом информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, компьютерных коммуникаций а равно ввод в информационную систему заведомо ложной информации, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства»

- Предлагается дополнить диспозицию части 1 статьи 208 Уголовного кодекса РК понятием «*компьютерная коммуникация*». Дело в том, что попытки Неправомерное завладение информацией осуществляются сетью компьютерных коммуникаций. Часть 1 статьи 208 УК РК представляется в следующей редакции «Умышленное неправомерное копирование или иное неправомерное завладение охраняемой законом информацией, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства»

-Предлагаем внести изменения и дополнения в подпункт 7-1 статьи 1 принятого Закона Республики Казахстан от 24 ноября 2015 года № 418 - V «Об

информатизации», Основные понятия, используемые в настоящем Законе: «*кибербезопасность* - это совокупность мер и процессов, направленных на защиту компьютерных систем, сетей и данных от несанкционированного доступа, атак и угроз» справка предлагаем дополнить понятием. Это связано с тем, что введение в законодательство понятия кибербезопасности является важным шагом, направленным на цели уточнения правовой ответственности, повышения уровня информационной безопасности, обеспечения соответствия международным стандартам, укрепления экономической и национальной безопасности.

4. Сравнительный анализ отечественного и зарубежного опыта борьбы с уголовными правонарушениями в сфере информатизации и связи показывает, что мы предлагаем следующие мероприятия по борьбе с уголовными правонарушениями в сфере информатизации и связи:

- *Укрепление международного сотрудничества.* Закрепление международным соглашением обязательства к активному международному сотрудничеству в борьбе с киберпреступностью, включая обязательный обмен информацией и проведение совместных операций с иностранными партнерами. Предлагаем ратифицировать международные соглашения и Конвенции, направленные на борьбу с трансграничной киберпреступностью. В связи с этим предлагается присоединиться к международным соглашениям, таким как Будапештская конвенция, которая является первым международным договором об уголовных правонарушениях, заключаемым через компьютерные сети и через интернет. Здесь существует ряд процессов и полномочий, таких как поиск, перехват компьютерных сетей, поэтому мы считаем, что это предложение очень важно. Ратификация Будапештской конвенции о киберпреступности позволит Республике Казахстан присоединиться к системе международного сотрудничества в борьбе с киберпреступностью. Это позволит укрепить правовую базу для борьбы с киберпреступностью, обеспечить эффективное сотрудничество с другими странами и улучшить защиту граждан и организаций от киберугроз. Кроме того, ратификация Конвенции предоставит доступ к международной сети для обмена информацией о киберугрозах и инцидентах, что позволит быстрее реагировать на новые угрозы.

- *Внедрение системы профилактического мониторинга.* В условиях стремительного развития технологий и роста киберпреступлений данный принцип предполагает создание специализированных центров, оснащенных современными средствами анализа информации и контроля информационной среды для правоохранительных органов, что позволяет правоохранительным органам оперативно реагировать. Для обеспечения информационной безопасности предлагается создать на базе «Государственной технической службы» Центр мониторинга раннего выявления киберугроз. Этот центр будет оснащен современными технологиями для анализа информации и раннего

выявления угроз. Такие центры позволяют оперативно реагировать на трансграничные киберугрозы и осуществлять меры по предупреждению уголовных правонарушений на стадии планирования.

- *Разработка учебной программы*. Правоприменительная практика показывает, что сейчас существует требование их подготовки в отношении отсутствия профессионалов, расследующих уголовные правонарушения в данной сфере. Поэтому разработка обязательных учебных программ направления «Киберследователь» для обучения сотрудников правоохранительных органов расследованию киберпреступлений и цифровой экспертизе. Данная учебная программа должна включать новейшие методы выявления и расследования современных кибератак, а также нормы международного права.

- *Повышение цифровой грамотности населения.* Важно установить тесные отношения между правительством и гражданским обществом с целью повышения осведомленности общественности о безопасности в интернете. Массовые информационные кампании, тренинги и образовательные программы по цифровой безопасности позволяют защитить самих граждан и их данные от киберугроз. Повышение осведомленности граждан о безопасности в интернете важно для поддержания правопорядка, так как это увеличивает шансы на предупреждение правонарушений и принятие мер против них. Расширение понимания прав и обязанностей граждан посредством тренингов и образовательных программ по цифровой безопасности повышает их правовую ответственность. Эти меры также способствуют сокращению количества жалоб на киберпреступность, поступающих в правоохранительные органы.

Обсуждение и внедрение результатов исследования:

Диссертационное исследование подготовлено, рецензировано и обсуждено на кафедре уголовно-правовых дисциплин юридического факультета» «Alikhan Bokeikhan University». По диссертационному исследованию опубликовано 5 научных статей:

2 статья в научных изданиях, входящих в международный информационный ресурс Scopus (Elsevier): «Revista de Direito, Estado e Telecomunicacoes» (Brazil), ISSN 1984-9729, Topical Issues in the Fight Against Criminal Offences in the Field of Informatisation and Communications // Revista de Direito, Estado e Telecomunicacoes. – 2023. – Vol. 15, Iss. 1. - p. 177-190.

Revista de Direito, Estado e Telecomunicacoes» (Brazil), ISSN 1984-9729, Measures to Prevent Criminal Offences in the field of Informatisation and Communications in the Republic of Kazakhstan // Revista de Direito, Estado e Telecomunicacoes. – 2024. – Vol. 16, No 2. – P. 276-294.

3 статья в журнале Комитета по обеспечению качества в области науки и высшего образования Министерства науки и высшего образования Республики Казахстан:

Некоторые теоретические аспекты борьбы с уголовными правонарушениями в сфере информатизации и связи, научный журнал «Вестник Академии правоохранительных органов» №2 (24) 2022 г. стр. 58.

International cooperation in combating criminal offences in the field of informatization and communications, научный журнал «Вестник Академии правоохранительных органов»№ 2 (28) 2023 г. с. 74.

Криминологическая характеристика личности киберпреступника / / журнал «Вестник — вестник» Карагандинской академии МВД Республики Казахстан № 3 (77) от 30 сентября 2022 года № 139-144

Структура исследовательской работы: диссертация состоит из 171 страниц, введения, 3 глав, заключения и списка литературы, содержащего источник.

Результаты исследования показывают необходимость внедрения новых механизмов по обеспечению кибербезопасности и защите информационной инфраструктуры в Республике Казахстан. Кроме того, в работе даются конкретные рекомендации по совершенствованию правовых норм и повышению эффективности деятельности правоохранительных органов.

В целом данная диссертация представляет собой комплексное исследование, направленное на решение правовых и организационных проблем, встречающихся в современном информационном обществе.