жаппар жан анықталмағандықтан 1291 қылмыстық қаракет тоқтатыла тұрды; 21 қылмыстық шаруа айыпталушының қылмыстық соңына түсу органдарынан жасырынғандығына немесе оның болатын жері анықталмағандығына қатысты тоқтатыла тұрды.

Әдебиеттер тізімі:

1. Джекебаев У.С. Юридическое лицо как субъект преступления. – Заңгер, 2011, № 4 - 49 б.

2. Рогов И.И. Социальная модернизация как приоритетное направление конституционной политики Казахстана. – Заңгер, 2012, № 9. – 9 б.

3. Қоғамов М.Ш. Установление основания уголовной ответственности: вопросы правоприменения в уголовном процессе. Қазақ білім академиясының баяндамалары. Юриспруденция. 2010, № 2. – 131 б.

4. Пермяков Ю.Е. Стандарты научности в юридической теории. – М.: Право и политика. 2011, № 3. – 476-б.

5. Марченко М.Н. Источники права. М., 2006. – 57-б.

6. Прохорова М.Л., Скачко А.В. Контрабанда в законодательстве Республики Казахстан: новые подходы к регламентации уголовной ответственности в условиях членства в Таможенном Союзе. – Международное уголовное право и международная юстиция. М., 2016,

№ 2. – 30-б.

7. Филимонов В.Д. Справедливость как принцип права. – Государство и право. М.,

2009, № 9. – 6-б.

8. Лунеев В.В. Проблемы противодействия экономической преступности. – М., Государство и право, 2014. № 2. – 32-б.

9. Александр Шеслер. Мошенничество: проблемы реализации законодательных новелл. – Уголовное право. М., 2013, № 2. – 67-б.

10. Кленова Т.В. Квалификация преступлений и уголовная политика. – Государство и право. М., 2012, № 4. – 56-б.

ТЕНДЕНЦИИ РАЗВИТИЯ ДЕЙСТВУЮЩЕГО УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА РЕСПУБЛИКИ КАЗАХСТАН В СФЕРЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Володько И.В., магистрант Карагандинской академии МВД РК им. Б. Бейсенова, лейтенант полиции

В своем послании от 01 сентября 2022 года президент Республики Казахстан Касым-Жомарт Токаев отметил, что в ходе модернизации уголовного законодательства страны отдельное внимание следует уделить валу интернет- и телефонного мошенничества. Правоохранительным органам нужно усилить информационно-аналитическую работу по выявлению и нейтрализации подобных угроз.[1].

Для акцентирования внимания именно на данном вопросе имеется несколько причин. Основная причина, по которой была затронута данная проблема, заключается в том, что сейчас во всех странах, в том числе и в Республике Казахстан, активно идет процесс цифровизации. Множество различных сфер жизни вовсю развиваются в киберпространстве – финансы, образование, поиск работы и сам процесс трудовой деятельности. Однако, как и остальные сферы социальной жизни, преступность не стоит на месте, и многие уголовные правонарушения уже перетекли в цифровое пространство.

Второй основной причиной столь острой постановки вышеописанного вопроса является повышенная степень общественной опасности данной категории преступлений, вызванная присущими только ей особенностями, таких, как скрытый характер преступных действий, трансграничный характер и автоматизированность, из-за чего злоумышленники становятся опасными и неуязвимыми.

Особенной опасностью подобной категории преступлений является так называемый трансграничный характер, то есть преступник и его жертва могут находиться в разных странах, при этом у злоумышленника благодаря свободному доступу к информационным технологиям имеется большой объем информации на предполагаемого потерпевшего, а также рычаги воздействия и морально-психологического давления на жертву.

Из-за относительной новизны данного вида преступлений правоохранительные органы Республики Казахстан не всегда оказываются достаточно подготовленными. Это происходит как из-за несовершенства законодательства в регулировании этой области общественных отношений, так и из-за выработки механизма его исполнения.

Также при квалификации преступлений, совершенных в сфере использования информационных технологий, необходимо учитывать наличие специальных знаний в данной области у сотрудников правоохранительных органов и наличие необходимого технического оснащения и экспертных технологий по фиксации подобного рода нарушений и проведению соответствующих экспертиз.

Это, в свою очередь, вызывает необходимость разработки законодательства по противодействию так называемой киберпреступности и поддержанию необходимого уровня информационной безопасности, создания специальных курсов по подготовке специалистов в системе органов внутренних дел, прокуратуре, судебных органов и экспертных учреждений.[2]

Понятие «информационная безопасность» тесно связано с таким термином, как «информатизация». Согласно Закону Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации», информатизация - организационный, социально-экономический и научно-технический процесс, направленный на автоматизацию деятельности субъектов информатизации, а субъекты информатизации - государственные органы, физические и юридические лица, осуществляющие деятельность или вступающие в правоотношения в сфере информатизации.[3]

В вышеуказанном нормативно-правовом акте также прописаны стандарты и механизмы по обеспечению и поддержанию информационной безопасности Республики Казахстан, а именно создаются уполномоченные органы в сфере обеспечения информационной безопасности, порядок и организация деятельности которых регламентируется данным Законом. Также организован Национальный координационный центр информационной безопасности и другие уполномоченные органы, основная работа которых заключается в непрерывном мониторинге цифрового пространства Республики Казахстан с целью выявления и возможной ликвидации угроз поддержания безопасности в информационных сетях, а также оказания поддержки и координации действий органов уголовного преследования, в компетенцию которых входит противодействие уголовным правонарушениям в сфере информационных технологий. Всего, согласно аналитическим данным Электронного Правительства Республики Казахстан, в настоящее время создано и функционирует 12 оперативных центров по информационной безопасности и 6 служб реагирования на компьютерные инциденты.

Однако для того, чтобы понять, для чего необходимо поддерживать информационную безопасность, необходимо определить понятие информационной безопасности в национальном законодательстве.

В статье 4 Закона Республики Казахстан «О национальной безопасности» под информационной безопасностью понимается состояние защищенности информационного пространства Республики Казахстан, а также прав и интересов человека и гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз,

при котором обеспечивается устойчивое развитие и информационная независимость страны.[4]

В уголовном законодательстве информационная безопасность выступает в качестве родового объекта уголовных правонарушений в сфере информатизации и связи и подразумевает под собой общественные отношения, связанные с обеспечением приватности, целостности и доступности охраняемой законом информации, которая хранится на информационном носителе, содержится в информационной системе или передается по информационно-телекоммуникацинным сетям, а также сохранности средств ее хранения, обработки и передачи.

Для предупреждения противоправных деяний в сфере использования информационных технологий в ходе законотворческой деятельности по совершенствованию и изменению уголовного законодательства Республики Казахстан в Уголовный кодекс Республики Казахстан от 03.07.2014 года была добавлена новая глава «Уголовные правонарушения в сфере информатизации и связи», предусматривающая разграничение уголовно-правовых норм, регламентирующих уголовно-правовую характеристику преступлений, совершенных с использованием информационных технологий, в том числе информационно-телекоммуникационных сетей и сети Интернет.

Данная глава под названием «Уголовные правонарушения в сфере информатизации и связи» была введена не только из-за прогресса во всем мире в сфере информационных технологий, но также по причине невозможности квалификации уголовных правонарушений, совершаемых в сфере электронных информационных технологий в связи с тем, что действовавшее тогда уголовное законодательство и Уголовный кодекс Республики Казахстан от 1997 года не предусматривало как ответственности за вышеуказанные преступления, так и уголовно-правовой характеристики и квалификации уголовных правонарушений, совершаемых в отношении пользователей информационной системы, а равно с использованием информационно-телекоммуникационных сетей и других информационных технологий.

В указанную главу были включены основные виды преступлений в сфере информационных технологий, а именно неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций (ст. 205), неправомерные уничтожение или модификация информации (ст. 206), нарушение работы информационной системы или сетей телекоммуникаций (ст. 207), неправомерное завладение информацией (ст. 208), принуждение к передаче информации (ст. 209), создание, использование или распространение вредоносных компьютерных программ и программных продуктов (ст. 210), неправомерное распространение электронных информационных ресурсов ограниченного доступа (ст. 211), предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели (ст. 212) и неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства (ст. 213).[5]

При изучении представленных уголовных правонарушений можно заметить, что большинство из них относятся к категории преступных посягательств, расматриваемой в Конвенции о преступности в сфере компьютерной информации ETS N185, принятой в Будапеште 23 ноября 2001 года, где данный раздел преступных посягательств обозначен под названием «Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем» и включает в себя 5 статей, а именно противозаконный доступ, неправомерный перехват, воздействие на данные, воздействие на функционирование системы и противозаконное использование устройств.

Однако данный перечень уголовных правонарушений не является исчерпывающим, так как чаще всего данные преступления сопутствуют совершению других уголовных

правонарушений, ответственность за которые предусмотрена иными уголовно-правовыми нормами.

Одним из ярких примеров подобного вида уголовных правонарушений является распространенное в настоящее время интернет-мошенничество, ответственность за совершение которого предусмотрена в ст. 190 Уголовного кодекса Республики Казахстан. При том указанный вид преступления относится к уголовным правонарушениям против собственности, так как объектом посягательства по-прежнему являются общественные отношения, регламентирующие права и свободы человека и гражданина на собственность.

Отсюда видно, что далеко не все деяния, предусматривающие совершение уголовных правонарушений в информационном пространстве, охватываются понятием, предусмотренным уголовным законодательством, а именно виновными, противоправными общественно опасными посягательствами на общественные отношения в сфере обеспечения безопасности информации и связи, связанные с обеспечением приватности, целостности и доступности охраняемой законом информации, которая хранится на информационном носителе, содержится в информационной системе или передается по информационно-телекоммуникацинным сетям, а также сохранности средств ее хранения, обработки и передачи.

Согласно аналитическим данным Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан, за прошедший 2022 год по республике было зарегистрировано 85 уголовных правонарушений, регламентируемых главой 7 Уголовного кодекса Республики Казахстан, что превышает показатель зарегистрированных в 2021 году уголовных правонарушений в сфере информатизации и связи на 14,9 процента.

Однако при этом, исходя из статистической информации, представленной на официальном сайте Электронного Правительства Республики Казахстан, Казахстан занимает 31 место в глобальном индексе по кибербезопасности, а 78 процентов населения осведомлено о видах и способах совершения указанных уголовных правонарушений.

Для увеличения уровня кибербезопасности в цифровом пространстве Республики Казахстан и, соответственно, повышения компьютерной грамотности населения страны в 2017 году была разработана и введена в эксплуатацию Концепция кибербезопасности или же «Киберщит Казахстана», основной целью которой является достижение и последующее поддержание высокого уровня защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, обеспечивающего устойчивое развитие Республики Казахстан в условиях глобальной конкуренции.[6]

При этом еще в 2013 году до принятия действующего уголовного законодательства страны в вышеописанной сфере был принят Закон Республики Казахстан от 21 мая 2013 года N 94-V «О персональных данных и их защите», регламентирующий общественные отношения в сфере персональных данных, а также цель, принципы и правовые основы деятельности, связанные со сбором, обработкой и защитой персональных данных. [7]

В ходе совершенствования действующего уголовного законодательства в рамках Концепции сервисной модели полиции по инициативе Межведомственной группы по обеспечению безопасности был создан пилотный проект так называемых «киберволонтеров Казахстана», состоящих из 44 граждан с достаточным уровнем компьютерной грамотности, в число которых вошли IT-специалисты. Целью данного проекта является помощь сотрудникам правоохранительных органов в предотвращении «хакерских атак». Также одно из основных задач данного проекта является повышение цифровой грамотности населения и доступное разъяснение некоторых известных алгоритмов действий киберпреступников.

Главной целью внедрения данных проектов является усиление взаимодействия общественности с органами уголовного преследования для успешной ликвидации

запрещенных законодательством Республики Казахстан действий в информационном пространстве.

Тем не менее, несмотря на стремительный прогресс в области противодействия преступлениям, совершаемым в сфере информационных технологий, перечень уголовно-наказуемых деяний, регламентируемых действующим уголовным законодательством не является исчерпывающим ввиду постоянной модернизации информационных технологий и увеличения количества видов совершаемых в цифровом пространстве уголовных правонарушений. Также важную роль в данном вопросе играет цифровая грамотность общественности и подготовка сотрудников правоохранительных органов к расследованию данной категории преступлений, в том числе умение правильно квалифицировать и дать уголовно-правовую характеристику данным уголовным правонарушениям.

Исходя из вышеизложенного, можно отметить, что в настоящее время в национальной науке уголовного права и криминологии противодействие преступлениям, совершаемым с использованием информационных технологий, имеет особый приоритет и стоит на одном из первых по значимости мест среди проблем действующего уголовного законодательства Республики Казахстан. Предпринимается разработка и организация мер противодействия киберпреступлениям, включающих в себя не только создание, организацию и внедрение структурной и целостной системы обучения, подготовки и переподготовки высококвалифицированных специалистов среди сотрудников правоохранительных органов по борьбе с противоправными деяниями, посягающими на общественные отношения в сфере использования информационных технологий, но и эффективное взаимодействие уполномоченных органов по обеспечению информационной безопасности с населением страны и уполномоченными органами зарубежных стран для повышения уровня координации, мониторинга информационного пространства на основе уже апробированных способов и методов последующей ликвидации результатов деятельности физических и юридических лиц, нарушающей национальное законодательство об информационной безопасности.

Список литературы:

1. Послание Главы государства Касым-Жомарта Токаева народу Казахстана от 01 сентября 2022 года - https://www.akorda.kz/ru/poslanie-glavy-gosudarstva-kasym-zhomarta-tokaeva-narodu-kazahstana-181130.

2. Проблемы компьютерной преступности в Казахстане. Алма Нурпеисова, ст. преподаватель Карагандинский Экономический Университет Казпотребсоюза – 2006 г. - https://eos.ru/eos_delopr/eos_delopr_intesting/112/14849 .

3. Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации». - https://adilet.zan.kz/rus/docs/Z1500000418.

4. Закон Республики Казахстан от 6 января 2012 года № 527-IV «О национальной безопасности». - https://adilet.zan.kz/rus/docs/Z1200000527 .

5. Уголовный кодекс Республики Казахстан от 3 июля 2014 года. - https://adilet.zan.kz/rus/docs/K1400000226#z783 .

6. Концепция кибербезопасности («Киберщит Казахстана») от 30 июня 2017 года. - https://adilet.zan.kz/rus/docs/P1700000407#z154 .

7. Закон Республики Казахстан от 21 мая 2013 года N 94-V «О персональных данных и их защите». - https://adilet.zan.kz/rus/docs/Z1300000094 .