УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ. СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Романенко Даниил Андреевич

студент, Белорусский государственный экономический университет, РБ, г. Минск

Истомина Анна Валерьевна

научный руководитель, старший преподаватель кафедры государственно-правовых дисциплин, Белорусский государственный экономический университет, РБ, г. Минск

В современных условиях стремительного развития информационных технологий их роль в жизни общества становится все более значимой. Цифровизация затронула практически все сферы человеческой деятельности: промышленность, транспорт, науку, образование, государственное управление, экономику и культуру. Количество пользователей сети интернет и их сетевая активность демонстрируют устойчивую тенденцию к росту, что создает новые вызовы в сфере обеспечения информационной безопасности.

В современном мире преступления в сфере информационных технологий принято называть «киберпреступность».

Киберпреступления - это такие общественно опасные деяния, которые совершаются с применением средств компьютерной техники (СКТ) в отношении информации, обрабатываемой и используемой в Интернете [1].

В праве Республики Беларусь, термин «киберпреступность» хотя и используется – примером может служить его применение в наименовании главы 19 «Противодействие киберпреступности» Концепции информационной безопасности Республики Беларусь от 18 марта 2019 г., тем не менее правового определения в нормативных правовых актах нет. В белорусском уголовном законодательстве применяется понятие «преступления против компьютерной безопасности». Глава 31 Раздела 12 Уголовного Кодекса Республики Беларусь под этим наименованием включает в себя 5 видов преступлений, содержащихся в соответствующих статьях [2, с. 13].

Киберпреступность становится все более серьезной проблемой для стран, в которых хорошо развита инфраструктура интернета и функционируют платежные системы. Согласно последним оценкам Интерпола угрозы киберпреступности, становятся все более агрессивными и конфронтационными. Это можно наблюдать в различных формах киберпреступности, включая высокотехнологичные преступления и утечку данных [2, с. 16].

В 2019 году Секретариат ООН предложил государствам-членам представить информацию о проблемах, с которыми они сталкиваются в борьбе с использованием информационно-коммуникационных технологий в преступных целях – для подготовки доклада Генерального секретаря ООН на ее семьдесят четвертой сессии [2, с. 16].

Республика Беларусь предоставила такую информацию, где, в частности отмечалось:

– «принимая во внимание модернизацию современной наркопреступности и использование даркнета и криптовалют в целях незаконного оборота наркотиков, Беларусь считает, что одним из приоритетных направлений деятельности государств-членов должна стать

организация обмена информацией, касающейся средств совершения преступлений и методов обнаружения преступной деятельности в даркнете, на наднациональном уровне; подборка и изъятие электронных доказательств; а также разработка и использование конкретных методов расследования преступлений, совершенных в виртуальном пространства [3, с. 13] …

– Одним из способов противодействия использованию информационно- коммуникационных технологий в преступных целях может стать разъяснение сотрудникам правоохранительных органов принципов работы даркнета и индустрии криптовалют [3, с. 14].

– Беларусь подчеркнула важность разработки международно-правового механизма (рекомендаций) о порядке изъятия криминальных криптоактивов и их хранения до принятия решения судом [3, с. 13].

– По мнению Беларуси, разработка и принятие универсального международного документа в рамках Организации Объединенных Наций будет содействовать развитию сотрудничества между компетентными органами государств-членов в борьбе с использованием информационно-коммуникационных технологий в преступных целях» [3, с. 14].

Современное состояние регулирования данной области характеризуется наличием ряда проблем. Существующие методики расследования таких преступлений требуют модернизации, поскольку не соответствуют текущим реалиям.

В Республике Беларусь проводится планомерная и последовательная политика борьбы с преступлениями в сфере информационных технологий. Одной из составляющих эффективной борьбы с преступлениями в сфере информационных технологий является наличие соответствующей законодательной базы, способствующей должному реагированию на все виды этих преступлений [4, с. 109].

В Уголовном кодексе Республики Беларусь (далее УК) предусмотрена ответственность за ряд деяний, которые следует признать преступлениями в сфере информационных преступлений (киберпреступлениями). УК Республики Беларусь содержит ряд статей, предусматривающих ответственность за преступления против собственности (ст. 212 УК) и информационной безопасности (ст. 349-355 УК), совершенные с использованием компьютерных технологий [4, с. 111].

Перспективы развития уголовной ответственности за преступления в сфере информационных технологий - это сложная и динамичная область, которая постоянно развивается в ответ на новые технологические вызовы и изменения в характере киберпреступности. К перспективным направлениям развития уголовной ответственности в этой сфере, можно выделить:

- расширение круга деяний, признаваемых преступными. Появление новых технологий (например, искусственный интеллект, блокчейн) неизбежно приведет к возникновению новых видов киберпреступлений, которые потребуют уголовно-правовой оценки и криминализации. Это может включать преступления, связанные с использованием искусственного интелекта для фишинга, дипфейков, автоматизированных кибератак, а также преступления, связанные с криптовалютами.

- усиление ответственности за существующие виды киберпреступлений. В связи с ростом масштабов и ущерба от киберпреступлений, возможно усиление уголовной ответственности за уже известные виды преступлений.

- совершенствование составов преступлений. Для более эффективного применения уголовного закона необходимо уточнять и конкретизировать составы преступлений в сфере информационных технологий (далее ИТ), чтобы они четко соответствовали современным технологическим реалиям и позволяли однозначно квалифицировать различные виды киберпреступлений.

- необходимо упростить процедуры расследования киберпреступлений, чтобы правоохранительные органы могли более оперативно и эффективно выявлять и пресекать

такие преступления.

- развитие криминологических исследований. Необходимо проводить криминологические исследования для выявления причин и условий, способствующих совершению киберпреступлений, и разработки эффективных мер по их предупреждению.

- повышение уровня правовой грамотности населения. Необходимо проводить информационные кампании для повышения уровня правовой грамотности населения в сфере ИТ, чтобы люди знали о рисках, связанных с использованием информационных технологий, и умели защищать себя от киберпреступлений.

В заключении, стоит отметить, что современный уровень развития информационных технологий требует постоянного совершенствования механизмов противодействия киберпреступлениям. Существующая правовая база, предусматривающая уголовную ответственность за преступления в сфере ИТ, нуждается в регулярном обновлении с учетом появления новых способов совершения противоправных деяний. Перспективное развитие системы уголовной ответственности должно идти параллельно с технологическим прогрессом, обеспечивая своевременное реагирование на появление новых видов преступлений и повышение эффективности их выявления и расследования.

Список литературы:

1. Рассолов И. М. Право и Интернет. Теоретические проблемы. М.: Норма, 2009. С. 132–133; Чекунов И. Г. К вопросу о понятии и системе преступлений, совершаемых с использованием компьютерных сетей // Правовые вопросы связи. 2012. № 1. С. 18.

2. Уголовно-правовые, криминологические и криминалистические проблемы расследования и предупреждения киберпреступлений для специальности II ступени высшего образования (магистратура) 1-24 80 01 Юриспруденция : учебно-методический комплекс по учебной дисциплине / сост.: Т.Ф. Дмитриева, В.Г. Стаценко. – Витебск : ВГУ имени П.М. Машерова, 2022. – 83 с

3. Генеральная Ассамблея ООН. 74 сессия. Противодействие использованию информационно-коммуникационных технологий в преступных целях: Доклад Генерального секретаря [Электронный ресурс]. – Режим доступа: https://www.unodc.org/documents/Cybercrime/SG_report/V1908184_R.pdf - 104 с. – Дата доступа: 05.05.2025.

4. Хлус, А. М. Особенности методического обеспечения борьбы с преступлениями в сфере информационных технологий / А. М. Хлус // Проблемы получения и использования доказательственной и криминалистически значимой информации : материалы Междунар. науч.-практ. конф., 26–27 сентября 2019 г., Мисхор (Большая Ялта) / отв. ред. М. А. Михайлов, Т. В. Омельченко; Крымский федеральный университет имени В. И. Вернадского. – Симферополь : ИТ «АРИАЛ», 2019. – 125 с.