

ПРОБЛЕМА ОПРЕДЕЛЕНИЯ И ЛАТЕНТНОСТИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

В.Г. Стаценко

Витебск, ВГУ имени П.М. Машерова

Противодействие преступности в сфере информационно-коммуникационных технологий (далее - ИКТ) является составной частью международной и национальной безопасности и стратегии защиты важнейшей информационной инфраструктуры.

Вместе с тем, борьба с преступностью в сфере ИКТ существенно осложняется тем обстоятельством, что современные технологии внедряются в преступную среду гораздо быстрее, чем в правоохранительные органы. Последнее значительно затрудняет процессы выявления преступлений и сбора доказательственной базы. Негативную роль играет также отсутствие универсальных правовых международных стандартов в рассматриваемой области.

Целью исследования является выявление существующих проблем в официальной фиксации преступлений, относящихся к преступности в сфере ИКТ и характеристика латентности данного вида преступности.

Материал и методы. Материалом исследования являются международные и национальные правовые источники, определяющие преступные деяния в информационно-коммуникационной сфере, эмпирические материалы, в частности, соответствующие статистические данные МВД Республики Беларусь, публикации по теме исследования.

В работе использовались общенаучные методы, а также сравнительный метод.

Результаты и их обсуждение. В различных правовых системах к преступности в информационно-коммуникационной области относят самые различные противоправные деяния, так или иначе связанные с использованием компьютерных технологий.

Европол подразделяет рассматриваемые преступления на «киберзависимые преступления», под которыми понимается «любое преступление, которое может быть совершено только с использованием компьютеров, компьютерных сетей или других форм информационно-коммуникационных технологий» и «преступления, совершаемые посредством кибертехнологий», т.е. традиционные преступления, совершаемые с помощью информационно-коммуникационных технологий [1]. Большинство исследователей киберпреступности [2, с. 54], разделяют этот подход.

В последние годы вся совокупность данных преступлений объединяется термином «киберпреступность». В правовой доктрине понятие «киберпреступность» чаще всего употребляется наряду с такими понятиями, как «компьютерная преступность», «преступления в сфере компьютерной

информации», «Интернет – преступность», «преступления в сфере высоких технологий», «преступления, сопряженные с компьютерными технологиями» [3, с. 32].

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 также не имеет. 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.

Отсутствие содержательно универсального определения преступности в сфере информационно-коммуникационных технологий, учитывая актуальность и все возрастающую, по мере развития коммуникационных технологий значимость противодействия преступности в этой области, развивающейся во всем мире прямо пропорционально развитию ИКТ, создает все большие проблемы для всех государств, особенно тех стран, в которых информационно-телекоммуникационная инфраструктура определяет сегодня все направления развития социума.

Анализ официальной статистики МВД Республики Беларусь [4] показывает, что на протяжении последних лет в стране наблюдается скачкообразность динамики регистрируемых киберпреступлений – с 2,3 тысяч в 2014 году – до 25,5 тысяч в 2020 году – рост киберпреступлений, т.о., более чем десятикратный (для ср.: в РФ за тот же период число рассматриваемых преступлений возросло с 44 тыс. до 510,5 тысяч, т.е. в той же, примерно, пропорции). Удельный вес киберпреступлений составил в 2020 году порядка четверти всех зарегистрированных в Республике Беларусь преступлений. В 2021 году статистика показала существенное снижение показателя объема и удельного веса киберпреступлений – было зарегистрировано 15,5 тыс. преступлений, что составило 18% всех зарегистрированных преступлений.

Следует отметить, что в структуре киберпреступлений преобладают, составляя свыше 90%, преступления, относящиеся к т.н. «хищениям путем модификации компьютерной информации» (ст.212 УК Республики Беларусь), в которых компьютерная техника выступает не предметом хищения, а орудием его совершения.

Неопределенность правового регулирования в рассматриваемой сфере правоотношений усиливает с неизбежностью и без этого свойственную преступности естественную латентность, проявляющуюся в том, что регистрирующие органы не фиксируют значительную часть совершаемых преступлений в сфере ИКТ, а официальная статистика не отражает реальное состояние дел.

Данные официальной статистики, фиксирующей непредсказуемые «скачки» показателей регистрируемых киберпреступлений, свидетельствуют не столько о реальном состоянии преступности, сколько о качестве работы правоохранительных органов. Преступления, совершаемые с использованием ИКТ, в силу их виртуальности и технологичности относятся к деяниям, где во многих случаях нет явно выраженной жертвы (либо она не сознает себя таковой) и, следовательно, обладают высоким уровнем естественной латентности.

В настоящее время не существует ни релевантной статистики, отражающей реальную картину состояния киберпреступности, ни надежных методов сбора таких данных. Значительная часть киберпреступлений остается вне поля зрения правоохранительных органов.

Заключение. Как показывает анализ тенденций и динамики киберпреступности важнейшее значение приобретает в современных условиях выявление приемов и способов преодоления латентности преступности, с целью установления если не подлинных, то хотя бы приближенных к ним, ее масштабов.

Поскольку общего (универсального) соглашения, регулирующего противодействие преступлениям в сфере ИКТ, до настоящего времени не существует, разнородность правового закрепления составов преступлений с использованием компьютерных технологий в законодательстве отдельных стран с очевидностью определяет необходимость унификации правового пространства на международном уровне.

1. Киберпреступность / Управление ООН по наркотикам и преступности. - Вена, 2019.-С.9 [Электронный ресурс]. - Режим доступа: https://www.unodc.org/documents/e4j/Cybercrime/Cybercrime_Module_1_Introduction_to_Cybercrime_RU.pdf. - Дата доступа: 15.01.2023

2. См.: Саркисян, А. Ж. Криминологическая характеристика преступлений, совершаемых в сфере информационно-коммуникационных технологий / А.Ж.Саркисян // Российский следователь. - 2019.- № 3. -С. 54–59

3. Стаценко, В.Г. Киберкриминология как область криминологического знания: объект исследования и перспективы развития / В.Г.Стаценко // Право. Экономика. Психология. - 2020. - № 3 (19).-С.29-34. URL <https://rep.vsu.by/handle/123456789/24335> Дата доступа: 15.01.2023

4. Сведения о совершенных правонарушениях на территории Республики Беларусь за январь–декабрь 2015-2021 г.г. / Информационный центр МВД Республики Беларусь. – Минск, 2016 – 2022.

ТРЕВОЖНОСТЬ КАК ФАКТОР ОПОСРЕДОВАННОЙ КРИМИНОГЕННОЙ ЗНАЧИМОСТИ

А.А. Сухарев

Витебск, ВГУ имени П.М. Машерава

Повышенная тревожность зачастую оказывает негативное влияние на критическое осмысление складывающейся ситуации, препятствует участнику правоотношений должным образом оценить ситуацию и сознательно принять адекватное решение.