

РАЗВИТИЕ НОРМАТИВНОЙ ПРАВОВОЙ ОСНОВЫ, РЕГЛАМЕНТИРУЮЩЕЙ КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Развитие науки и техники все больше внедряют в жизнь человека, общества и государства цифровые технологии. При несомненном положительном эффекте данного процесса он имеет и негативные стороны, заключающиеся в использовании современных технологий в преступных целях. Так, например, по данным Верховного Суда Республики Беларусь, за хищение имущества путем модификации компьютерной информации (ст. 212 Уголовного кодекса Республики Беларусь) за первое полугодие 2023 г. осуждено 549 лиц, в 2022 г. – 1192, в 2021 г. – 1185, в 2020 г. – 1506. Как видим из приведенных статистических данных, хищение имущества путем модификации компьютерной информации в нашей стране имеет стабильный количественный характер.

Обращение к теме преступлений, совершаемых в сфере информационных технологий, свидетельствует о том, что в различных источниках подобные преступления называют компьютерными преступлениями, информационными преступлениями, цифровыми преступлениями, киберпреступлениями и др. Так как это не является предметом данного изучения, для целей нашего исследования и обозначения преступлений, совершаемых в сфере информационных технологий, мы изберем термин «киберпреступность». Проведенное нами исследование указывает на то, что преступления, основанные на современных технологиях, как правило, имеют свой механизм (почерк), отличаются высокой скоростью деяния, технологичностью (использование специального оборудования), носят корыстный или хулиганский мотив, характеризуются квазиместом совершения преступления, профессионализмом преступников, трансграничностью и транснациональностью совершения и сокрытия и т. п. Все описанные характеристики указывают на сложность раскрытия и расследования преступлений с использованием компьютерных технологий.

Является бесспорным, что успешное противодействие преступности, а в частности киберпреступности, невозможно без надлежащей законодательной основы. Наш анализ нормативных правовых актов (далее – НПА) свидетельствует о том, что всю нормативную правовую базу Республики Беларусь, применимую к сфере борьбы с киберпреступностью, можно условно разделить на несколько частей. Первая – это НПА, создающие основу для борьбы с киберпреступностью, включая систему сил национальной безопасности, ведущих с ней борьбу, а вторая – НПА, непосредственно регламентирующие деятельность субъектов уголовного процесса. В рамках данной статьи нас интересуют НПА, непосредственно регулирующие деятельность следователей, сотрудников органов дознания, экспертов и специалистов, а также регулирующие правоотношения, возникающие в сфере судебной экспертизы и криминалистики.

К НПА, создающим основу для борьбы с киберпреступностью, следует отнести Декрет Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики», Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных», Указ Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» и др.

Говоря о второй группе НПА (непосредственно регламентирующие деятельность субъектов уголовного процесса), мы за основу берем то, что такие НПА должны давать криминалистическую возможность поиска, фиксации, сохранения, экспертизы и использование цифровых доказательств, придавая им критерии законности, относимости и допустимости в уголовном процессе. Одними из таких НПА являются Уголовно-процессуальный кодекс Республики Беларусь, Закон Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности», Закон Республики Беларусь от 18 декабря 2019 г. № 281-З «О судебно-экспертной деятельности» и другие НПА.