способа совершения преступлений, с применением традиционных методов становится неэффективным, а в ряде случаев невозможным. Полагаем, что назрела необходимость вырабатывать новые механизмы реагирования на преступления с учетом их специфики. При этом относительно рассматриваемых нами преступлений выработка таких механизмов должна осуществляться на международном уровне, не ограничиваясь национальным законодательством, поскольку борьба с такими преступлениями является актуальной не только для одного государства.

Гасанова Я. Р.

ТРАНСГРАНИЧНОСТЬ ПРЕСТУПЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ВИРУСОВ

Гасанова Яна Рамиловна, студентка 3 курса Белорусского государственного университета, г. Минск, Беларусь, yana.gasanova99@mail.ru

Научный руководитель: кан. юрид. наук, доцент Захилько К. С.

Согласно ст. 354 Уголовного кодекса Республики Беларусь (далее – УК) уголовно наказуемыми являются разработка, использование, распространение либо сбыт компьютерных программ или специальных программных средств, которые предназначены для нарушения системы защиты сети или машинного носителя, несанкционированного уничтожения, блокирования, модификации компьютерной информации или неправомерного завладения компьютерной информацией либо нарушения работы компьютерной системы, сети или машинного носителя. Компьютерные вирусы являются одним из видов вышеперечисленных вредоносных программ. Вирусы имеют такую функциональную характеристику, как способность самовоспроизводиться, размножаться, присоединяться к другим программам. Более того, они обладают способностью дистанционного заражения компьютеров.

Преступление, предусмотренное ст. 354 УК, относится к одним из наиболее общественно опасных и сложных преступлений в этой сфере, поскольку имеет высокую степень латентности (многие компьютерные вирусы самоуничтожаются) и сложность в плане технического выявления правоохранительными органами. Соответственно, возникают проблемы при необходимости установлении обстановки совершения преступления, а именно места совершения. Установление места совершения преступления необходимо для выяснения вопроса о принципах действия уголовного закона в пространстве.

В подобных преступлениях можно выделить несколько вариантов мест их совершения:

рабочее место, где обрабатывается информация, являющаяся предметом преступного посягательства;

место постоянного хранения или резервирования информации, т. е. сервер или стример;

место использования средств для несанкционированного доступа к предмету преступления (может совпасть с рабочим местом, но находиться в другом с помощью внешнего удаленного сетевого доступа);

место подготовки преступления (например, разработка вирусов).

Особенность определения места совершения рассматриваемого преступления заключается в том, что все вышеперечисленные места могут находиться на разных территориях. Одно совершенное преступление может быть начато на территории одного государства, а продолжено и окончено на территории других государств.

В таком случае остается неразрешенным вопрос о том, в юрисдикции какого государства находится расследование совершенного преступления и уголовный закон какого государства подлежит применению.

Согласно ч. 2 ст. 5 УК преступление признается совершенным на территории Республики Беларусь, если оно начато, или продолжалось, или было окончено на ее территории, или совершено в пределах Республики Беларусь в соучастии с лицом, совершившим преступление на территории иностранного государства. Аналогичные нормы предусмотрены и в других государствах. В связи с этим, а также тем обстоятельством, что вред от рассматриваемого преступления может затрагивать различные государства, проблема выбора уголовного закона, подлежащего применению, может обостряться и выходить на политический уровень.

Учитывая то, что подобные преступления становятся все менее ограничены лишь территорией одного государства, как было указано на десятом Конгрессе ООН по предупреждению преступности и обращению с правонарушителями, т. е. являются трансграничными, считаем, что вопрос определения подлежащего применению закона или порядок его определения должен найти отражение в международном праве. Например, в ст. 22 Конвенции Совета Европы о киберпреступности от 2001 г. вопрос решен следующим образом: государствам в таких ситуациях необходимо провести взаимные консультации для установления наиболее подходящей юрисдикции для осуществления судебного преследования.

Заметно, что ни на международном, ни на национальном уровне единых и универсальных специальных положений о юрисдикции преступлений против компьютерной информации, которые могут позволить однозначно установить подсудность компьютерных преступлений с учетом специфики их совершения, не содержится.

Показательным примером разрешения проблемы определения места совершения преступления является закон Великобритании «Computer Misuse Act 1990». В соответствии с его нормами под юрисдикцию компетентных органов и судов Великобритании подпадает любое преступление в сфере компьютерных преступлений, при совершении которого хотя бы один из элементов состава преступления имел место на территории страны.