Дипломная работа на тему:

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ПРОТИВОДЕЙСТВИЮ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Теоретический вывод:

- В области уголовно-правовой борьбы с преступлениями, при совершении которых используются информационные технологии и компьютерная техника, отсутствует единое мнение о том, какие деяния считать такими преступлениями и каким должно быть их юридическое определение. Указанные преступления в уголовно-правовой литературе имеют самое разное название – «информационные преступления», «компьютерные преступления», «виртуальные преступления», «киберпреступления», «преступления в сфере информационных (компьютерных, высоких и др.) технологий», «преступления информационного характера», «преступления в сфере компьютерной информации», «интернет-преступления» и т.д. При этом термин «преступления в сфере высоких технологий» применительно к указанным преступлениям не является в научной литературе самым популярным.

Теоретические выводы:

- Преступления в сфере высоких технологий следует понимать в широком и узком смысле.
- В широком смысле под преступлениями в сфере высоких технологий следует понимать все уголовно наказуемые деяния, совершаемые с использованием информационных и компьютерных технологий. Использование данного термина в широком значении позволяет охватить весь спектр преступлений, совершаемых в сфере использования технических средств обработки информации или данных, а также компьютерной техники. В данном значении понятие преступлений в сфере высоких технологий синонимично понятиям «компьютерные преступления», «киберпреступления» и другим.
- В узком смысле под преступлениями в сфере высоких технологий следует понимать преступления, предусмотренные ст. 212 и главой 31 УК, организацию борьбы с которыми осуществляет УРПСВТ МВД Республики Беларусь.

Теоретические выводы:

- Типологии преступлений в сфере высоких технологий зависят от понимания состава данных преступлений – в их широком или узком смысле.
- Наиболее компактная типология преступлений в сфере высоких технологий в их широком понимании выделяет: 1) преступления против информационной безопасности («собственно компьютерные преступления»), представляющие собой совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния; 2) преступления, связанные с компьютерами («смежные компьютерные преступления»), к которым относятся совершённые с помощью информационных технологий и компьютерной техники, традиционные по характеру преступные деяния.
- Типология преступлений в сфере высоких технологий в их узком понимании выделяет: 1) преступления, связанные с противоправными посягательствами на компьютерную информацию либо с созданием условий для таких посягательств (ст.ст. 350-354 УК); 2) преступления, связанные с нарушением установленного порядка использования компьютерных систем или сети (ст.ст. 349, 355 УК); 3) преступление, связанное с хищением путём использования компьютерной техники (ст. 212 УК).

Теоретические выводы:

- В последние годы спектр преступлений в сфере высоких технологий значительно расширился. Объясняется это тем, что преступники стали активнее использовать в своей противоправной деятельности новейшие достижения науки и техники. Новинки компьютерной техники и информационных технологий используются ими как для непосредственной подготовки, совершения и сокрытия преступлений, так и для организации преступной деятельности в целом (обмен информацией на качественно новом технологическом уровне).
- Анализ статистических данных о преступности в сфере высоких технологий за последние годы в Беларуси показывает тенденцию её роста: в 2011 г. их было выявлено 2 171, в 2012 г. – 2 040, в 2013 г. – 2 558, в 2014 г. – 2 290, в 2015 г. – 2 440, в 2016 г. – 2 471, в 2017 г. – 3 099.

Теоретические выводы:

- В обширном спектре преступлений в сфере высоких технологий правоохранительные органы выделяют два наиболее распространённые из них: 1) хищения путём использования компьютеров; 2) преступления против информационной безопасности.
- Основные особенности корыстных преступлений путём использования компьютерной техники (хищений) заключаются в том, что: 1) доля таких хищений (ст. 212 УК) от общего числа выявленных преступлений в сфере высоких технологий очень велика и на протяжении последних лет составляет не менее 3/4 от всех указанных преступлений; 2) темпы прироста преступлений корыстной направленности по сравнению с другими преступлениями против информационной безопасности возрастают более интенсивно.

Предложения по совершенствованию законодательства:

1. Часть 3 ст. 349 «Несанкционированный доступ к компьютерной информации» УК считать частью 4.

Статью 349 УК дополнить частью 3 в следующей редакции:

«3. Действия, предусмотренные частями 1 и 2 настоящей статьи, совершённые с использованием глобальной компьютерной сети Интернет, –

наказываются штрафом или лишением права занимать определённые должности или заниматься определённой деятельностью, или арестом, или ограничением свободы на срок до 3 лет, или лишением свободы на тот же срок.»

Статью 349 УК дополнить частью 5 в следующей редакции:

«5. Действия, предусмотренные ч. 4 настоящей статьи, совершённые с использованием глобальной компьютерной сети Интернет», –

наказываются ограничением свободы на срок до 5 лет или лишения свободы на срок до 7 лет.»

Предложения по совершенствованию законодательства:

2. Диспозицию ч. 2 ст. 350 «Модификация компьютерной информации» УК изложить в следующей редакции:

«2. Модификация компьютерной информации с использованием глобальной компьютерной сети Интернет, либо сопряжённая с несанкционированным доступом к компьютерной системе или сети либо повлекшая по неосторожности последствия, указанные в части 3 статьи 349 настоящего Кодекса, – ...».

3. Диспозицию ч. 2 ст. 351 «Компьютерный саботаж» УК изложить в следующей редакции:

«2. Компьютерный саботаж, совершённый с использованием глобальной компьютерной сети Интернет, либо сопряженный с несанкционированным доступом к компьютерной системе или сети либо повлекший тяжкие последствия, – ...».

Предложения по совершенствованию законодательства:

4. Статью 352 «Неправомерное завладение компьютерной информацией» УК дополнить частью 2 в следующей редакции:

«2. Действия, предусмотренные ч. 1 настоящей статьи, совершённые с использованием глобальной компьютерной сети Интернет, –

наказываются штрафом, или арестом, или ограничением свободы на срок до 3 лет, или лишением свободы на тот же срок.»

5. Диспозицию ч. 2 ст. 354 «Разработка, использование либо распространение вредоносных программ» УК изложить в следующей редакции:

«2. Те же действия, повлекшие тяжкие последствия, либо совершенные с использованием глобальной компьютерной сети Интернет, – ...».

6. Диспозицию ч. 3 ст. 201 «Нарушение авторского права, смежных прав и права промышленной собственности» УК изложить в следующей редакции:

«3. Действия, предусмотренные частями 1 или 2 настоящей статьи, совершенные с использованием глобальной компьютерной сети Интернет, либо повторно, либо группой лиц по предварительному сговору, либо должностным лицом с использованием своих служебных полномочий, либо повлекшие причинение ущерба в крупном размере, – ...»;

Предложения по совершенствованию законодательства:

7. Пленуму Верховного Суда Республики Беларусь следует разработать и принять постановление о практике рассмотрения судами уголовных дел по преступлениям в сфере высоких технологий, что будет способствовать единообразию следственно-судебной практики;

8. Ввести в действующее законодательство нормы о страховании информационных рисков, которые бы закрепляли страхование компьютерной информации, а также средств её хранения, обработки и передачи, информационно-телекоммуникационных сетей и оконечного оборудования от несанкционированного уничтожения, блокирования, модификации либо копирования. Перед заключением страхового договора следует обязать собственника / владельца компьютерной информации или средств хранения, обработки, передачи охраняемой компьютерной информации, информационно-телекоммуникационных сетей и оконечного оборудования установить программное обеспечение по антивирусной защите компьютерной информации и предупреждению несанкционированного доступа.

Практическое предложение:

- Республика Беларусь до настоящего времени не является участницей Конвенции Совета Европы о киберпреступности 2001 г., что создаёт определённые трудности в деятельности белорусских правоохранительных органов при расследовании преступлений в сфере высоких технологий. На наш взгляд, Республике Беларусь следует присоединиться к указанной Конвенции. Присоединение нашей страны в Конвенции Совета Европы о киберпреступности будет способствовать положительной оценке международным сообществом деятельности нашего государства в сфере обеспечения информационной безопасности и противодействия компьютерной преступности.

СПАСИБО ЗА ВНИМАНИЕ!