Сравнительный анализ киберпреступлений в России и зарубежных странах.

Ступень Мария Викторовна
магистрант направления подготовки 40.04.01 Юриспруденция
ФГБОУ ВО «Красноярский государственный аграрный университет»
E-mail: stupe16@mail.ru

С момента появления компьютерных технологий появилась и проблема защиты информации, попадающей в сеть. XXI век особо остро поставил проблему сохранности данных, касающихся как коммерческой и личной информации, так и защиты банковских данных. С проблемами защиты информации и киберпреступлениями сталкивается каждая страна.

Для сравнительного анализа киберпреступлений выбраны страны с разными правовыми системами, а именно США, Европейские страны (Германия, Испания), Япония и Российская Федерация. Выбор этих стран позволит отследить какие конкретно кибепреступления совершаются в определенном государстве и какие законодательные методы использует государство для борьбы с ними.

Для начала стоит отметить, что на сегодняшний день не существует единого подхода к пониманию киберпреступления и информационного пространства, что в свою очередь ведет к разному пониманию однородных преступлений в законодательстве различных стран.

Рассматривая уголовное законодательство разных стран в сфере борьбы с киберпреступлениями можно отметить целый ряд сходств и различий. По данным американского Центра стратегических исследований за 2015 год мировая экономика потеряла от киберпреступности 500 млрд. долларов США, что превышает даже сумму, полученную от незаконного оборота наркотических средств, которая является одной из самых высоких в мире [1, с. 145]. Судя по намечающейся тенденции эти суммы будут только увеличиваться.

Так, уголовное законодательство США подвергается быстрому и постоянному изменению. Связано это с несколькими причинами, среди которых адаптивность англосаксонской системы, позволяющая реагировать на быстро изменяющуюся ситуацию, а также особенность финансовой системы США, где большая часть денег находится в безналичном формате. Кредитные карты имеет практически каждый житель США. С этим связана статистика, говорящая о том, что 44 % всех киберпреступлений приходится на кражу денег с кредитных карт и только 16% на кражу секретной информации [2, с. 47] Такая статистика привела к изменению уголовного закона штатов и ужесточению наказания. Основным преступлением стало мошенничество, связанное с незаконным использованием кредитных карточек с использованием компьютерных технологий. Кредитная система России гораздо моложе, чем кредитная система США и некоторые механизмы защиты в ней еще не созданы или работают недостаточно эффективно. Поэтому с появлением как одиночек, так и преступных групп, совершаемых неправомерные действия с кредитными картами, стало для России одним из новых видов преступлений. По официальной статистике МВД ущерб от преступлений, связанных с кредитными картами с использованием компьютерных технологий за 2015 г. достигает 150 млн. руб. Поэтому по сравнению с американской системой уголовных наказаний российская гораздо мягче. Так, например, ст. 159.6 УК РФ за мошенничество в сфере компьютерной информации, совершенное в крупном размере предусматривает максимальное наказание в виде ограничения свободы до полутора лет, а по Своду законов США за данное преступление, ущерб которого достигает более 2000 долларов, предусмотрено лишение свободы

до семи лет.

Европейские страны тоже ужесточили ответственность за совершение преступлений в сфере высоких технологий. При этом стоит отметить, что преступлений, связанных с кражей денег с кредитных карт в этих гораздо меньше, чем в США. А вот незаконный сбыт компьютерных программ и несанкционированный доступ к чужому компьютеру совершается гораздо больше. Например, Уголовный кодекс Германии акцентирует внимание на следующие виды киберпреступлений: компьютерный шпионаж, компьютерный саботаж и компьютерные манипуляции, целью которых являются компьютерные данные как объект защиты [3, с. 50] Компьютерный шпионаж расположен в разделе 15 УК ФРГ «Нарушение неприкосновенности тайны частной жизни», что говорит о том, что данный вид преступления включен в защиту личных прав и свобод. Само понятие «данные» в законе не раскрывается. Отсутствие этого понятия свойственно европейскому праву. Уголовный кодекс России компьютерные преступления относит к имущественным преступлениям, а не к защите личных прав и свобод.

Уголовный кодекс Испании предусматривает иную классификацию киберпреступлений. Законодатель не выделяет конкретные виды компьютерных преступлений, а идет по пути «дополнения, расширения границ составов более традиционных, „некомпьютерных“ преступлений» [3, с. 51] Так, преступления в сфере компьютерной информации могут охватываться следующими нормами: нарушение прав, связанных с интеллектуальной собственностью (ст. 270 УК); завладение или разглашение коммерческой тайны (ст. 278 УК); сбор, разглашение, искажение или уничтожение информации с ограниченным доступом (ст. 598 УК) и др. [4] Преступления в сфере компьютерной информации по Уголовному кодексу РФ объединены в главе 28.

В Японии разработана собственная классификация киберпреступлений, которая позволяет определить конкретный вид преступления в сфере высоких технологий, а также статистику совершения данных преступлений.

Первая группа преступлений связана с проникновением в компьютеры. К ним относятся: компьютерное мошенничество; повреждение записей и создание помех бизнесу; преступления, связанные с платежными картами; несанкционированный доступ к компьютеру. Вторую группу составляют преступления, связанные с использованием сети Интернет: мошенничество; нарушение авторских прав; рассылка писем непристойного характера; распространение материалов, связанных с детской порнографией [1, с. 144]. По второй группе преступлений, предусмотренных японским законодательством, можно найти существенные отличия с российским законодательством. В первую очередь, это касается самого понятия «преступления, связанные с использованием сети Интернет». В российском уголовном праве отсутствует такой квалифицирующий признак. Вместо него существует термин «совершение преступлений в сфере компьютерных технологий». Вторым отличием является отношение к авторскому праву. В японском законодательстве нарушение авторского права с использованием сети Интернет предусматривает уголовную ответственность, тогда как в российском законодательстве нарушение авторского права защищается сферой гражданского законодательства. При этом квалификация создания и распространения порнографии даже через сеть Интернет имеет отношение к другой главе, связанной не с компьютерной информацией, а преступления против здоровья населения и общественной нравственности. Тем самым осознавая всю общественную опасность подобных преступлений, российский законодатель вносит их в отдельную главу и не привязывает только к компьютерным преступлениям.

Анализ зарубежного законодательства и законодательства России показывает, что в современных условиях государства по-разному подходят к решению вопроса борьбы с преступлениями в сфере компьютерной информации. Различия можно проследить в способах

криминализации киберпреступлений в разных странах. Так, например, в США за часть посягательств ответственность установлена специальными нормами, а часть преступлений охватывается общими составами. В Испании предусмотрен способ расширения границ действующих составов «некомпьютерных», более традиционных преступлений. Россия ближе всего относится к первому способу криминализации преступлений в сфере компьютерных технологий.

Прогностическая функция сравнительного исследования киберпреступлений в разных странах позволяет сделать следующие выводы. Во-первых, стремление каждого государства создать собственную классификацию компьютерных преступлений приводит к затруднению международного сотрудничества в области борьбы с данными преступлениями, что, в свою очередь, приведет к значительному росту киберпеступлений на международном уровне. Во-вторых, законодательный приоритет определяется наиболее повторяющимся типом преступлений в сфере компьютерных технологий, что приводит к тенденции ужесточения уголовной ответственности за наиболее многочисленные преступления, оставляя без внимания другие киберпреступления. Главной проблемой всех стран явилось то, что на сегодняшний день не существует общепризнанного определения киберпреступлений ни в национальном законодательстве, ни в международном. Это приводит к отсутствию единого подхода к определению оснований отнесения противоправных деяний к таким преступлениям.

Литература:

1. Морозов Н.А., Борьба с компьютерной преступностью в Японии // Общество и право. 2014. № 2 — С. 141-145
2. Несмеянов А. А. Основные проблемы борьбы с преступлениями в сфере высоких технологий // Вестник Восточно-Сибирского института МВД России. 2014. № 4 — С.43-48.
3. Рудик М.В., Евтушенко И.И., Обзор уголовного законодательства западноевропейских стран и США в сфере создания с целью использования, распространения или сбыта вредных программных или технических средств // Вестник КРУ МВД России. 2015. № 2 — С.49
4. Уголовный кодекс Испании URL: http://law.edu.ru/norm/norm.asp
5. Уголовный кодекс ФРГ: пер. с нем. М., 2000.