Романов Владимир Анатольевич

магистрант

ФГБОУ ВО «Бурятский государственный университет»

г. Улан-Удэ, Республика Бурятия

АКТУАЛЬНЫЕ ПРОБЛЕМЫ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЯХ

***Аннотация**: в данной статье проводится анализ по преступлениям в так называемой «информационной безопасности», способы их защиты и ответственность за противоправные действия с точки зрения уголовного кодекса.*

***Ключевые слова**: компьютерные преступления, информация, преступления, уголовный кодекс, защита информации, министерство внутренних дел.*

Современный мир уже невозможно себе представить без использования информационных ресурсов. Использование информационных технологий диктуется стремительным развитием информационного общества, широким распространением технологий нового тысячелетия, таких как сеть «Интернет», мобильных приложений банковской системы, предоставления государственных услуг по средствам личного кабинета и еще бесконечное множество других различных услуг по средствам компьютерной коммуникации. Моментальные способы передачи информации в наши дни являются одним из самых привлекательных объектов деятельности людей по всему миру, одни способы используются в коммерческих целях и приносят прибыль, другие способы применяются в области государственной и исполнительной власти, когда информацию нужно передать максимально быстро. Однако, как и многие сферы ведения хозяйственной деятельности, компьютерные технологии нуждаются в защите. Стремительное развитие, создание и внедрение информационных систем во все сферы экономики – все это дает благоприятные условия, для совершения неправомерных действий, развития мошенничества в режиме «инкогнито» и количество данных преступлений растет не только в нашей стране, но и повсеместно во всем мире.

При сборе информации о преступлениях в сфере компьютерной информации можно оттолкнуться от данных ГИЦ МВД России, так в период 1996–1997 годов было зарегистрировано всего 12 правонарушений в сфере компьютерной информации, в 2005 году составило 10214 случаев, а в 2014 году официально зарегистрировано 11000 преступлений [1]. Но в ходе опроса компанией Digital Security, реальное количество киберпреступлений в России минимум в несколько раз больше [2]. Ведь люди крайне редко обращаются в органы правопорядка, пишут заявления о попытках взлома личной почты, кражи логинов и паролей, а они в свою очередь тоже считается киберпреступлениями. Все это дает неточную информацию в сводках официальной отчетности правоохранительных органов.

Главный объект преступных замыслов – компьютерная информация и ее безопасность. Дополнительные объекты – законное право на информацию ее владельцев, так как это является их собственностью.

Предмет посягательств – компьютерная информация на любом электронном носителе.

Задача уголовного законодательства в этой связи – обеспечить грамотную и современную защиту. Следует отметить, что в данной сфере уголовное право оказалось не вполне готовым к быстротечному развитию компьютерной техники и ее внедрению в повседневную жизнь общества.

Анализируя наше отечественное законодательство, оно предусматривает уголовную ответственность не только за компьютерные преступления, но и за киберпреступления в целом. Нормы по данным преступлениям отображены в трех статьях УК РФ, выделенных в самостоятельную главу 28 УК РФ.

Статья 272 УК РФ. Неправомерный доступ к компьютерной информации [3, с. 177].

Под компьютерной информацией понимаются сведения находящиеся в памяти компьютера, а также на электронных, переданных по средствам связи (интернет) или иных носителях сведения, которые могут прочитаться машинами ЭВМ.

Статья 273 УК РФ. Создание, использование и распространение вредоносных компьютерных программ [3, с. 178].

Статья 274 УК РФ. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей [3, с. 178].

В данных статьях уголовного кодекса описаны преступления в сфере компьютерной информации и ответственность за их нарушения.

Но, к сожалению, компьютерные злодеяния являются информационными преступлениями, зачастую отличаются оригинальностью и совершенные на значительном расстоянии, а данные нормы и статьи очень сильно ограничены в области применения, часто правоохранительные органы не в компетенции завести уголовное дело в рамках производства по таким преступлениям. С внедрением более современных технологий развиваются все более изощренные способы преступности, к примеру, взлом приложений «мобильного банка» через сотовые телефоны или кража «личных персональных данных» с последующим использованием в противоправных целях, дополнительно стимулируют развитие криминальных талантов у определенных лиц. Все вышесказанное подтверждает необходимость обновления норм УК РФ, устанавливающих ответственность за преступления в сфере компьютерной информации.

Список литературы

1. Официальный сайт Министерства Внутренних Дел РФ. 2016. МВД России [Электронный ресурс]. – Режим доступа htpp://МВД.рф

2. Сайт Digital Security. 2003–2016, Москва [Электронный ресурс]. – Режим доступа: htpp://dsec.ru

3. Уголовный кодекс Российской Федерации. – М.: Проспект КноРус, 2016. – 240 с.

4. Уголовно-процессуальный кодекс Российской Федерации. – М.: Проспект КноРУс, 2016. – 256 с.

5. Криминалистика: Учебник / Под ред. Е.П. Ищенко. – М.: Проспект, 2014. – 504 с.