ПРАВОВОЕ РЕГУЛИРОВАНИЕ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Л. М. САТАНОВА,

канд. юрид. наук, ассоциированный профессор
Академия Кайнар, Алматы, Казахстан

Двадцатый век ознаменовал с собой приход новой эры в развитии науки техники – эры компьютерных технологий и интернета. Коммуникационные возможности человека вышли далеко за пределы возможного еще в первой половине прошлого столетия.

С приходом нового века сфера и возможности интернета, а вместе с ним возможности коммуницировать с любой точкой планеты в режиме онлайн вывели человека на уровень невероятной мобильности относительно всего периода развития человеческого общества в совокупности. Безусловно, такой уровень развития технологий, сделали возможности человека наиболее высокими, жизнь в целом удобной, работу легкой и непринужденной. И на этом развитие в данной сфере, как видно из повседневных наблюдений, останавливаться не собирается.

Значит ли это, что интернет принес с собой исключительно блага для человечества? Вовсе нет! Возможности интернета стали орудием в руках и у правонарушителей, лиц желающих, воспользоваться возможностями интернета для получения легких средств посредством правонарушений. Все страны мира отреагировали на новые виды преступлений путем введения в свои уголовные кодексы такие статьи, которые предполагают совершения преступлений посредством интернета. Казахстан в этом ряду не исключение, так как в Конституции РК прямо записано, что государство охраняет информационную собственность, как и любую другую [1], а Уголовный кодекс Республики Казахстан, содержит статью, связанную с преступлением посредством применения интернета. Подобные деяние влекут уголовную ответственность по статье Уголовного кодекса [2].

Тенденция к росту компьютерных преступлений увеличивается во всем мире. По данным Интерпола, компьютерные преступления неуклонно растут и виды этих преступлений расширяются. Данный факт не может не беспокоить мировое сообщество, так как практически все банковские, и иные денежные операции, секретные программы, сфера обеспечения безопасности, государственные секретные материалы переходят на интернет пространство. И взлом конфиденциальных информаций посредством проникновения

в чужую программу, чреваты тяжелейшими последствиями не только для отдельно взятого субъекта национального или международного права, но и в целом для государственных интересов и интересов международных организаций. В данной связи, предсказания многих ученых об идее мирового преступления с помощью компьютерных технологий, охватывающих сообщества стран и целые континенты может оказаться более чем реальной действительностью.

Высокая опасность компьютерных преступлений заключается в их возможности наносить ущерб масштабно и единовременно. Выяснить источник этих опасных и противоправных действий также бывает достаточно сложно и трудоемко. Все государства мира обязаны объединяться и эти вопросы разрешать сообща, так как интернет не имеет государственных границ, и преступник зачастую может наносить удар далеко за пределами государства, в котором могут пострадать интересы как простых граждан, так и интересы крупных сообществ и государств.

Долгое время считалось, что совершение преступлений на компьютере – это привилегия развитых стран, но оказалось, что это не верный постулат. Террористические организации во всех точках планеты, свои преступные акции совершают посредством компьютерных технологий. Эти организации чаще всего имеют в своем арсенале наиболее оснащенные компьютеры с современными и расширенными возможностями. В руках международных преступных организации интернет становится мощным орудием совершения изощрённых и запутанных преступлений, след которых невозможно отыскать многие годы.

В Казахстане, компьютерные преступления относительно суммарной численности всех преступлений не велики, все же настораживает тот факт, что темпы этих видов преступлений медленно, но верно растут из года в год. Сложившаяся тенденция обязывает государственные органы власти задумываться о степени защиты программ, представляющих государственную важность, а также о защите интересов граждан и юридических лиц в РК.

Двадцатое столетие, а в особенности вторая ее половина, шагнула далеко вперед в развитии информационных технологий. Мир стал мобильнее и гораздо ближе друг к другу, благодаря высоким технологиям и средствам современных коммуникаций. Информационные технологии имеют свои особенности в отличие от других ресурсов, которые сводятся к нескольким фундаментальным показателям, а именно:

1. В отличие от сырьевых и энергетических ресурсов, информационные характеризуются не физическими, а моральными износами.

2. Информационные системы эфемерны и не имеют своего физического носителя.

3. Появление информационных ресурсов позволило человечеству значительно экономить все иные ресурсы, что положительно сказалось на их экономии.

Информационные системы создаются компьютерными техниками [3, с. 26].

Информация в современном мире становится предметом сделок и договоров. Она все более приобретает товарный вид и подвергается купле-продаже, различным манипуляциям в целях зарабатывания денег.

Потребность в информации у современного человека значительно выше по сравнению с предыдущими веками, где добыча необходимой информации составляла большой труд и затрату колоссального количества времени. Так, под емкими аббревиатурами ЭВМ, НИТ скрываются сложные системы хранения, обработки, передачи, консервирования информаций посредством электронной вычислительной техники, телевидения, радио [4, с.146].

НИТ (новая информационная технология) – это суммарная составляющая всей информационной технологии, которая объединяет все способы добычи и распространения информаций посредством технических средств коммуникаций. Более того, человек, а точнее его мозг, сам является информационной системой, в голове которого обрабатывается, анализируется и выдается колоссальное количество информаций.

Информация проникает во все сферы человеческой жизни, общества, государств, мировых сообществ. На почве данной тенденции возникло даже крылатое выражение – «кто владеет информацией, тот владеет миром». Существование информационных воин никто не подвергает сомнению. Мировые конфронтации перешли на новую плоскость противостояний, ранее не известную – информационную. Информация способна не только изменить политическую систему отдельно взятого государства, но и перевернуть мир и определить новое мироустройство.

Информация стала представлять опасность государствам мира и целым сообществам, по причине которой, встал вопрос об организации мер безопасности в ходе добычи, обработки, хранения и передачи информаций. Уголовные законодательства государств включает новый вид преступления как хакерство. Правовая система государств встала на защиту интересов граждан и организаций, обладающих конфиденциальной информацией, взлом которых, является преступлением.

Со времени появления на рынке во второй половине двадцатого столетия компактных и относительно простых и примитивных компьютеров,

практически у каждого человека на планете появилась возможность приобщиться и стать частью мировой информационной паутины.

С тех пор, стал актуальным вопрос о дозированности и подконтрольности информационных потоков, каждый из которых может стать общественным достоянием и оказаться обнародованным для неограниченного количества людей [5, с.246].

Как уже отмечалось выше, уголовные законы стран мира, были вынуждены срочно отреагировать на деяния, которые стали признаваться позже преступлениями, так как действия лиц, направленные на проникновение в пределы чужой информации, стали наносить масштабный ущерб отдельным гражданам и юридическим лицам, а также непоправимый ущерб национальной безопасности.

Так, например, в последнем десятилетии прошлого столетия во французском уголовном кодексе произошли изменения, связанные с проникновением лиц в чужие программы с целью извлечения выгоды. Глава, посвященная преступлениям против собственности, была пополнена новой, связанной со взломом чужих информационных программ, повреждением и извлечением конфиденциальной информации в корыстных целях. С 1992 года французский уголовный закон данные действия признал преступлениями [6, с.189].

Без внимания данную тенденцию не оставили и международные сообщества. Так, Совет Европы нашел крайне важным после тщательного исследования и разработки создать конвенцию, которая бы защищала на международном уровне от действий связанных, со взломом информационных программ.

В Республике Казахстан сфера защиты информации основывается на Конституции страны, в которой прописывается, что конфиденциальная информация охраняется законом. Кроме того, информация как товарный объект регулируется нормами Гражданского кодекса РК [7], а специальный закон РК «Об информации» регулирует непосредственно правовые отношения, связанные с использование и применение информации [8].

Уголовный кодекс РК в главе 7 – «Уголовные правонарушения в сфере информации и связи» регулирует все актуальные на сегодняшний день виды информационных преступлений. Данная глава со временем имеет тенденцию к дополнению и изменению, так как технологии в последние десятилетия развиваются с невероятной скоростью. Законодатель, беря во внимание ускоренные темпы развития технологий, вынужден своевременно вносить соответствующие корректировки с тем, чтобы успевать их регулировать в целях защиты интересов субъектов правоотношений [2].

В то же время, все собственники, владельцы, пользователи технологиями должны предпринимать меры безопасности посредством:

1. Недопущения свободного проникновения в информационную систему.

2. Предотвращение и обнаружение действий, связанных с попытками проникновения в чужую информационную систему.

3. Сведение к минимуму последствия действий правонарушителя.

4. Срочное восстановление операционной системы.

5. Взаимодействовать и своевременно информировать о попытках взлома соответствующие государственные органы, ответственные за информационную безопасность [9, с. 189].

Закон РК «Об информатизации» устанавливает, что все меры, предусмотренные законодательством, в ходе осуществления технического обеспечения безопасности информационных ресурсов не должны причинять ущерб жизни и здоровью граждан, наносить информационный и иной ущерб частным предпринимателям, юридическим лицам, государственным и негосударственным структурам [8].

Кроме вышеперечисленного, названный закон предпринимает меры по защите и обеспечению секретности информационных ресурсов, хранящих личные, индивидуальные данные субъектов до полной их ликвидации и последующего уничтожения.

Органы, уполномоченные осуществлять меры и способы соблюдения защиты информационных систем и в частности – Комитет связи, информатизации и информации, обязаны исполнять требования, установленные законодательством РК в сфере информации.

В современной криминалистической науке нет единого мнения и четкого разграничения того, что называть компьютерным преступлением. Многочисленные разногласия имеют место и в вопросах классификации преступного деяния. Нет возможности как четко очертить круг объектов в данном виде преступления, так и в части множественности предметов посягательства.

Существует две исходные точки, от которых можно оттолкнуться в решении вопроса о компьютерном преступлении. Первая из них относит к данным видам преступления действия, в которых компьютер является объектом или орудием преступления.

Вторая исходная точка гласит, что к компьютерным преступлениям можно отнести только действия в сфере обработки информации. И общим в данном преступном деянии является способ, орудие, объект преступления. Если быть точнее, то объектом преступного посягательства является информация, находящаяся в компьютерной системе, а сам компьютер – это орудие преступления.

Эти два подхода стали основой для развития криминалистической научной мысли не только для Казахстана, но и на международном уровне. Компьютерные преступления находятся на стадии изощренного разветвления и разнообразия. И это связано с быстро и бурно развивающимися технологиями, которые поражают своими возможностями не только в области предоставления технических возможностей для пользователей достижениями науки и техники, но и в не меньшей степени для преступного посягательства, которая в свою очередь, изощряется в своих способах наносить ущерб интересам, защищаемым государством, посредством правовых актов [10, с. 298].

ЛИТЕРАТУРА

1. Конституция РК от 30.08.1995 г.
2. Уголовный кодекс РК от 16.07.1997 г. (введен в действие 1.01.98 г.)
3. Андреев Б. В. Расследование преступлений в сфере компьютерной информации: учеб. пособие / Б. В. Андреев. – М.: МАИК «Наука/Интерпериодика», 2016.
4. Гульбин Ю. А. Преступления в сфере компьютерной информации: учеб. пособие / Ю. А. Гульбин. – М.: «Статут», 2007.
5. Коржов В. К. Право и Интернет: теория и практика: учеб. пособие / В. К. Коржов. – М.: Издательство БЕК, 2015.
6. Кочои С. Н. Ответственность за неправомерный доступ к компьютерной информации: учеб. пособие / Под общ. ред. В. Ф. Яковлева. – М.: Изд-во РАГС, 2004.
7. Гражданский кодекс РК (Общая часть) введен в действие 1.03.1994.
8. Закон РК «Об информатизации» от 8.05.2003.
9. Крылов В.В. Информация как элемент криминальной деятельности: учеб. пособие / В. В. Крылов. – 2012.
10. Крылов В.В. Информационные преступления – новый криминалистический объект: учеб. пособие / В. В. Крылов. – 2013.