УДК 34

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА СПОСОБОВ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Сергейчева Е. Н.

Научный руководитель: Севастьянов Александр Павлович, кандидат юридических наук, доцент кафедры уголовного права, Юридического института, Сибирского федерального университета.

Юридический институт
Сибирского федерального университета

Процесс информатизации общества наряду с положительными последствиями имеет ряд отрицательных сторон. Объединение компьютеров в глобальной сети, с одной стороны, дало возможность большому количеству людей приобщиться к огромному массиву накопленной в мире информации, а с другой стороны, породило проблемы с охраной интеллектуальной собственности, помещаемой в сеть и хранящееся в ней.

Широкое распространение и внедрение во все сферы жизни общества компьютеров привело к тому, что изменился сам характер многих преступлений, появились новые их виды. К их числу, можно отнести, так называемые компьютерные преступления.

Эти преступления берут истоки от других преступлений. Преступления, связанные с компьютерами не отличаются от преступлений без компьютеров. Компьютер-это только инструмент, который используется для совершения преступления. К примеру, использование компьютера, сканера, графических программ и высоко - качественных цветных лазерных или струйных принтеров для подлога или подделки - это такое же преступление, как и с помощью старомодных печати с чернилами. Кража ноутбука с патентованной информации, хранящейся на жестком диске внутри компьютера, - это такое же преступление, как кража портфеля, содержащего документы с конфиденциальной информацией.

Сам термин "компьютерная преступность" впервые появился в американской, а затем другой зарубежной печати в начале 60-х годов. В 1983 году в Париже группой экспертов ОЭСР было дано криминологическое определение компьютерного преступления, под которым понималось любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных и передачу данных. В литературе до настоящего времени ведется полемика о том, какие действия следует относить к разряду компьютерных преступлений. Несмотря на то, что в большинстве стран уголовное законодательство является достаточно гибким, чтобы квалифицировать правонарушения этого типа, социальные и технические изменения создают все новые и новые проблемы. Поэтому некоторые из известных мировой практике компьютерных посягательств не подпадают под действие уголовного законодательства и в юридическом смысле не могут считаться преступными. Так, существует точка зрения, согласно которой компьютерные преступления как преступления специфических в юридическом смысле не существует и следует говорить лишь о компьютерных аспектах преступлений.[1]

Вместе с тем специалисты в данной области пришли к выводу, что к разряду компьютерных преступлений следует отнести те преступления, у которых объектом преступного посягательства является информация, обрабатываемая и

[1] См:. Батурин, Ю.М. Право и политика в компьютерном круге. – Москва: Наука, 1987. - 112 с.

хранящаяся в компьютерных системах, а орудием посягательства служит компьютер. [1]

Существует множество классификации способов совершения преступлений в сфере компьютерной информации. Они являются разнородными, что не позволяет создать классификацию способов совершения преступлений, которая бы включала в себя способы совершения каждого из трех составов главы 28 УК РФ.

Ю.М.Батурин классифицирует компьютерные преступления в зависимости от способа их совершения. По его мнению, все способы совершения компьютерных преступлений можно объединить в три основные группы: методы перехвата, методы несанкционированного доступа и методы манипуляции.[2]

Способы неправомерного доступа к компьютерной информации можно подразделить на несанкционированное проникновение в ЭВМ, в систему ЭВМ или их сеть и перехват компьютерной информации, передаваемой по каналам связи.

Перехват компьютерной информации производится путем непосредственного подключения прямо к коммуникационным каналам либо узлам передачи данных (непосредственный перехват) или осуществляется по остаточным излучениям тех или иных устройств (дисплея, принтера, систем коммуникаций), причем на достаточном удалении от объекта излучения (электромагнитный перехват).

В специализированной литературе можно встретить множество классификаций способов несанкционированного проникновения в компьютерную систему. Все предложенные классификации не являются исчерпывающими. Это объясняется в первую очередь стремительным развитием информационной сферы - создаются все новые и новые технические средства и программные продукты, что определяет возникновение новых способов несанкционированного проникновения в компьютерную систему.

Во-первых, способы непосредственного воздействия лица на компьютерную информацию. При их реализации проникновение в компьютерную систему осуществляется путем введения различных команд непосредственно в компьютерную систему. При этом следы совершения преступления будут находиться только в ЭВМ, в памяти которой хранится информация, являющаяся предметом преступного посягательства. Непосредственный доступ может осуществляться как лицами, имеющими право доступа к средствам вычислительной техники, так и лицам, специально проникающими в зоны с ограничениями по допуску.

Вторая группа- это способы опосредованного (удаленного) воздействия на компьютерную информацию. К ним можно отнести:

- проникновение в чужие информационные сети путем автоматического перебора абонентских номеров с последующим соединением с тем или иным компьютером;

-проникновение в компьютерную систему с использованием чужих реквизитов идентификации;

- подключение к линии связи законного пользователя (например, к телефонной линии) и получение тем самым доступа к его системе;

- использование вредоносных программ для удаленного доступа к информации и др.

Американский юрист и доктор наук Рональд Стэндлер предложил другую классификацию компьютерных преступлений, которая состоит из трех основных классов:

---

[1] См:. Юрасов, А.В. Электронная коммерция.- Москва: Дело,2003.- 480 с.

[2] См:. Батурин, Ю.М. Проблемы компьютерного права. - Москва: Юриздат, 1991.-272 с.

1. Несанкционированное использование компьютера, которое может привести к краже имени пользователя и пароля, или может включать в себя доступ к компьютеру жертвы через Интернет, через тайный вход который управляется с помощью троянской программы.

2. Создания или запуск вредоносной компьютерной программы (например, компьютерного вируса, " червя", "трояна»).

3. Киберпреследование, т.е. пользование интернетом и другими электронными средствами с целью преследования или запугивания человека, группы лиц или организации. Оно может заключаться в создание ложных обвинений, мониторинге, создание угрозы, хищение, порче данных или оборудования или сбора информации, которая может быть использована для преследования. [12]

[1]"Cyberstalking". Oxford University Press. [Электронный ресурс]. – Режим доступа 2014-03-10.
[2]См:. Ronald B. Standler. Computer crime. [Электронный ресурс]. – Режим доступа: http://www.rbs2.com/ccrime.html 2014-03-10.