УДК 002.5/6+347.775

ЗАЩИТА ЭЛЕКТРОННОЙ ИНФОРМАЦИИ В СОЮЗНОМ ГОСУДАРСТВЕ: ПРАВОВОЙ АСПЕКТ

***А.А. Сидорович**, 1 курс*
*Научный руководитель – **Ю.А. Степанчук**, к.филол.н.*
Филиал Российского государственного социального университета в г. Минске

С каждым днем во всем мире увеличивается число пользователей всемирной компьютерной сети Интернет. В Союзном государстве темпы "интернетизации" настолько велики, что даже трудно делать долгосрочные прогнозы, касающиеся развития этого явления.

Однако наряду с положительными сторонами технический прогресс всегда влечет и негативные последствия. Не является исключением и развивающийся стремительными темпами мир компьютеризации. Порожденные им нежелательные явления разнообразны и до настоящего времени не до конца поняты и изучены. Печальное первенство принадлежит проблемам противоправного применения компьютерной техники. В частности, новые информационные технологии стимулировали возникновение неизвестных ранее способов посягательства на охраняемые законом общественные отношения.

Одной из наиболее распространенных проблем остается необходимость обеспечения надежной защиты от несанкционированного доступа к информации. Пользователи электронно-вычислительной техники принимают определенные меры безопасности. Средства массовой информации периодически передают сообщения о начатой спецслужбами войне против хакеров и компьютерных террористов. Однако этого, как правило, оказывается недостаточно, нарушителей не остановить разовыми акциями или техническими мероприятиями. Общественная опасность их противоправных посягательств слишком велика и не должна недооцениваться. По этой причине во многих государствах были разработаны законодательные меры защиты от вредоносного использования компьютерной техники.

Юридическая охрана сферы применения электронно-вычислительных машин стала жизненно необходимой, значительная доля соответствующих обязанностей была возложена на уголовное право. В специальной литературе появился термин "компьютерная преступность", который затем прижился и в средствах массовой информации. В большинстве случаев уголовно наказуемыми признаются такие действия, как несанкционированный доступ к информации, ее копирование и уничтожение, введение в систему компьютерного вируса, модификация компьютерных программ. В уголовные кодексы многих стран стали вноситься статьи, предусматривающие уголовную ответственность в сфере компьютерной информации, несущие повышенную общественную безопасность.

Действующим российским и белорусским уголовными законодательствами достаточно подробно регламентирована ответственность и наказуемость деяний в рассматриваемой сфере. Уже сам факт уголовно-правовой защиты общественных отношений, регулирующих изготовление, использование, распространение и защиту компьютерной информации, имеет профилактическое, предупредительное значение.

Однако анализ текста законов позволяет констатировать, что ситуация все-таки не совсем благополучна. То, что криминализированы некоторые общественно опасные деяния в сфере компьютерной информации в определенной мере поможет предотвратить или значительно ослабить их негативное влияние. Но процесс совершенствования уголовного законодательства не должен останавливаться. Обусловлено это тем, что компьютерная преступность не знает границ. Интернет позволяет электронно-вычислительным системам, находящимся в различных точках земного шара, взаимодействовать друг с другом.

"Всемирная паутина" облегчила жизнь не только правопослушных граждан. Свою выгоду извлекают также представители криминального мира. С учетом существующих технических возможностей и тенденций развития преступности можно прогнозировать осложнение ситуации. Уже сейчас место расположения компьютера, с помощью которого совершается посягательство, крайне редко совпадает с местом расположения объекта посягательства.

Однако изменение законодательства входит в компетенцию государственных органов, да и процесс этот довольно длительный. Вопросы международного сотрудничества в сфере борьбы с преступностью - также прерогатива государства.

Руководителям же предприятий и сотрудникам приходится постоянно уделять внимание вопросам безопасности, в том числе компьютерной. Отказаться от контроля этого направления деятельности опасно. Чтобы эффективно противостоять преступлениям, в которых, так или иначе, задействованы компьютерные сети, надо, прежде всего, проанализировать потенциальную угрозу подобных деяний для каждого конкретного объекта охраны. Это поможет оценить степень защиты, которую необходимо обеспечить.

Если предприятие все же стало жертвой компьютерного преступления следует учитывать, что находящиеся там компьютеры могли использоваться злоумышленниками в качестве орудия преступления либо могли сохранить любую информацию, которая позволит восстановить обстоятельства дела, выявить виновных и их соучастников. Поэтому до прибытия компетентных должностных лиц следует подготовить (а лучше постоянно иметь) следующую документацию и информацию:

а) нормативные документы, регламентирующие деятельность предприятия вообще и касающиеся использования компьютерной техники в частности;

б) документы, с использованием которых было совершено преступное посягательство, либо в которых оно нашло отражение;

в) наличие и комплектация используемой вычислительной техники;

г) списки лиц, имеющих допуск к работе с указанной техникой, краткие характеристики последних с данными о профессиональных навыках владения компьютерной техникой.

Кроме того, надо предотвратить несанкционированное уничтожение компьютерной информации (при необходимости организовать охрану компьютеров, отключить от телефонной и иных линий связи).

Сотрудники правоохранительных органов в процессе следственных действий могут осматривать и изымать как полностью компьютеры, так и отдельные их устройства и блоки. Целесообразно, чтобы при этом присутствовал не просто представитель предприятия, а благонадежный сотрудник, обладающий специальными знаниями.

В случае изъятия названного оборудования должны быть соблюдены требования уголовно-процессуального законодательства, касающиеся протоколирования процедуры и результатов следственного действия. В числе прочего следует обращать внимание на то, чтобы в протоколе указывались заводские или серийные номера изымаемых объектов, а также иные сведения, необходимые для их точной идентификации.

Список использованных источников

1. Ляпунов, Ю.В. Ответственность за компьютерные преступления / Ю. Ляпунов, В. Максимов // Законность. – 1997. – N 1. – С.11.

2. Медведев, А.М. Пределы действия Уголовного кодекса Российской Федерации. / А.М. Медведев. – М., 1998. – С.104.

3. Об электронной и цифровой подписи : федеральный закон от 10 января 2002 г. № 1 – ФЗ // Кодекс [Электронный ресурс] / Консорциум "Кодекс". – М., 2010.

4. О федеральной целевой программе «Электронная Россия (2002-2010 гг.) : постановление Правительства Российской Федерации, 28 января 2002 г., № 65 // Кодекс [Электронный ресурс] / Консорциум "Кодекс". – М., 2010.

5. Об электронном документе : Закон Республики Беларусь от 10 января 2000 г. № 357-З // Национальный реестр правовых актов Республики Беларусь.- 2000. – № 7.

6. Инструкция по делопроизводству в государственных органах и организациях Республики Беларусь: постановление Министерства юстиции Республики Беларусь от 19.01.2009 № 4 // Консультант Плюс: Беларусь Технология 3000 [Электронный ресурс] / ООО "ЮрСпектр", Нац. реестр правовой информ. Респ. Беларусь. – Минск, 2010.