Аманжолова Б. А., доцент кафедры уголовного права и криминологии КарГУ им. Е. А. Букетова, кандидат юридических наук;

Кенжебаев А., магистрант юридического факультета КарГУ им. Е.А.Букетова

ПРИЧИНЫ И УСЛОВИЯ, СПОСОБСТВУЮЩИЕ СОВЕРШЕНИЮ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

В экономике Казахстана все быстрее идут рыночные преобразования, из года в год увеличивается количество акционерных, совместных, частных предприятий, инофирм и фермерских хозяйств. В связи с этим в республике наблюдается резкое увеличение интереса к безопасности вычислительных систем. Без сомнения, это объясняется в первую очередь развитием банковского бизнеса и широким внедрением современных вычислительных и коммуникационных средств в государственные структуры.

Развиваются новые технологии, компьютерная инфраструктура, растет объем получаемой и передаваемой по компьютерным коммуникационным сетям информации, зачастую составляющей новые технологические разработки. Поэтому логичным будет предположение о том, что эта информация будет и уже становится объектом пристального внимания криминальной среды, особенно для завоевания новых сфер влияния.

Ключевым моментом при рассмотрении данной проблемы является исключительная важность и необходимость использования системного подхода к ее решению. Это объясняется тем обстоятельством, что безопасное функционирование системы в целом обусловливается безопасностью самого слабого звена. Этих слабых звеньев может быть очень много, перечислим только некоторые из них. Во-первых, абсолютная защита компьютерной сети от проникновения в нее сделает вычислительную систему практически недоступной и непригодной для использования; во-вторых, не все возможные пути преодоления систем защиты вычислительных сетей могут быть известны, и, следовательно, не всем угрозам может противостоять применяемая система обеспечения безопасности; в-третьих, очень многое зависит от «человеческого фактора», а людям свойственно ошибаться. Отсюда вытекает принципиальная важность рассмотрения данной проблемы в комплексе, в противном случае принимаемые меры уголовно-правовой борьбы с компьютерными преступлениями окажутся малоэффективными.

Для упреждения подобных явлений «впервые в уголовном законодательстве Казахстана введена уголовно-правовая защита компьютерной информации, так как преступления в этой сфере направлены, прежде всего, против той части установленного порядка общественных отношений, который регулирует изготовление, использование, распространение и защиту компьютерной информации».

Наиболее типичными причинами и условиями совершения преступлений в сфере компьютерной информации являются:

- рост числа ЭВМ и, как следствие, увеличение объемов информации, обрабатываемой и хранимой в ЭВМ;
- недостаточность мер по защите ЭВМ, систем ЭВМ и их сетей;
  недостаточность защиты программного обеспечения;
- рост информационного обмена через мировые информационные сети;
- отступление от технологических режимов обработки информации;
- отсутствие, несовершенство или отступление от правил эксплуатации программ для ЭВМ, баз данных и аппаратных средств обеспечения сетевых технологий;
  отсутствие или несоответствие средств защиты информации ее категории;
  нарушение правил работы с охраняемой законом компьютерной информацией;
- низкий уровень специальной подготовки должностных лиц правоохранительных органов, которые должны предупреждать, раскрывать и расследовать преступления в сфере компьютерной информации;
- отсутствие государственной политики в сфере обеспечения информационной безопасности.

Наряду с вышеперечисленными, специалистами выделяются следующие причины, способствующие совершению преступлений данного вида:

- недостаточная защита средств электронной почты;
- небрежность в работе пользователей ЭВМ;
- непродуманная кадровая политика в вопросах приема на работу и увольнения;
- нарушение технологического цикла проектирования, разработки, испытаний и сдачи в промышленную эксплуатацию компьютерных систем;
- совмещение функций разработки и эксплуатации программного обеспечения в рамках одного структурного подразделения;
- нарушение сроков изменения паролей пользователей;
- нарушение установленных сроков хранения копий программ и компьютерной информации, а иногда полное их отсутствие;
- необоснованность использования ЭВМ в конкретных технологических процессах и операциях;
- отсутствие должного контроля со стороны администрации за деятельностью своих работников, задействованных на чувствительных этапах обработки компьютерной информации;
- психологически неправильные межличностные взаимоотношения должностных лиц с подчиненными и другими работниками.

Известно, что компьютерные преступления характеризуются очень высокой степенью латентности. Данное обстоятельство во многом определяет тенденцию к постоянному росту количества совершенных преступлений в сфере компьютерной информации.

По оценкам специалистов, 85 % зарегистрированных уголовных дел в сфере компьютерной информации остаются нераскрытыми, а факты обнаружения некорректной работы оборудования и попыток незаконного доступа к информационным ресурсам зачастую носят случайный характер.

Нельзя обойти стороной и социальный аспект совершения преступлений в сфере компьютерной информации. Существуют следующие социальные условия и факторы совершения компьютерных преступлений.

1. Различие между уровнем социального развития общества и технологическим уровнем. Технологическая развитость не сопровождается моральным развитием, не формируются в достаточной мере понятия и нормы ответственности.

2. Страна решает одновременно задачи модернизации и постмодернизации при наличии активных компонентов традиционного общества. В разных ситуациях общественной жизни проявляются те или иные компоненты: постмодернизация — в активном использовании компьютерной техники, а элементы предшествующих стадий развития — в примитивном воровстве и низменных мотивах. Для условий информационного общества формируется ответственность организаций. В органической информационной среде это происходит органично, при наличии модемного и традиционного общества — наоборот.

3. Аномия, слабость норм. Нет необходимых нравственных образцов; универсальные стандарты поведения не всегда соответствуют требованиям информационного общества. Для решения этой проблемы необходим этический кодекс компьютерного сообщества, который бы закрепил нормы обращения с компьютерной информацией, сформировал основы корпоративной морали и информационной ответственности организаций.

Для выяснения криминогенной ситуации в стране, кроме изучения данных официальной статистики, можно использовать еще и информацию из таких альтернативных источников, как: виктимологический мониторинг (опрос) лиц, ставших жертвами преступлений; самоотчеты правонарушителей; выводы и экспертные оценки специалистов и в целом общественного мнения о состоянии преступности и эффективности деятельности правоохранительных органов. Как свидетельствует мировая практика, обзор уголовной виктимизации дает возможность узнать о действительных масштабах преступности, выявить ее латентную часть и скрытую уголовную виктимизацию населения, наметить и активизировать меры по усилению борьбы с преступностью в сфере компьютерной информации и противодействию уголовной виктимизации населения.

Түйін

Мақалада компьютерлік қылмыстарды жасауға мүмкіндік туғызатын себептер мен жағдайлар қарастырылады.

Resume

In the article examined reasons and terms, assisting the feasance of cyber crimes.