Литература

1. *Боков, В. А.* Основы экологической безопасности : учеб. пособие / В. А. Боков, А. В. Лущик. — Симферополь : СОНАТ, 1998. — 352 с.

2. Дополнительный протокол к Женевским конвенциям, касающийся защиты жертв международных вооруженных конфликтов [Электронный ресурс] : Конвенция ООН, 12.08.1949 // Сайт ООН. — 1958. — Режим доступа: http://www.un.org/ru/humanitarian/law/geneva.shtml. — Дата доступа: 15.03.2015.

А.В. Щекочихин
И.М. Цуба
БГЭУ (Минск)
Научный руководитель — кандидат философских наук И.П. Мамыкин

КИБЕРКРИМИНАЛ

Информация стала ключевым ресурсом новейшего времени. Неограниченная информатизация общества предопределила его закономерное отклонение от установленных законодательно принципов права. Так, преступность перешагнула из гражданского социума в сеть Интернет.

Понятие компьютерных преступлений тождественно термину киберкриминал.

В гл. 31 Уголовного кодекса Республики Беларусь (далее — УК РБ) указан перечень преступлений, связанных с компьютерными преступлениями или преступлениями против информационной безопасности. Согласно УК РБ выделяются следующие типы компьютерных преступлений: несанкционированный доступ к компьютерной информации, модификация компьютерной информации, компьютерный саботаж (уничтожение информации), неправомерное завладение компьютерной информацией, разработка, использование либо распространение вредоносных программ, нарушение правил эксплуатации компьютерной системы или сети, изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети.

Рассмотрим основные виды преступлений, связанных с незаконным доступом к информации, ее модификацией, саботажем, а также разработкой вредоносных программ. Опасность компьютерных преступлений или преступлений против информационной безопасности рассмотрим на примере кардинга.

Кардинг — это использование платежной карты без согласия на то держателя карты. Широкое распространение получил такой вид кардинга, как скимминг, т.е. незаконная установка в картоприемник банкомата считывающего устройства, фиксирующего данные при пользовании картой, для последующего доступа к находящимся на ней средствам.

Мерой профилактики для борьбы с данными преступлениями является уведомление граждан о возможном наличии считывающих устройств около каждого пункта дистанционного денежного оборота, подробные инструкции по распознаванию и предупреждению механизма размещения преступного программного обеспечения. Стоит отметить, что данное предложение не является новшеством, однако для более успешного закрепления мер борьбы с компьютерными преступлениями и обеспечения информационной безопасности необходимо активизировать правотворческую деятельность в этой части в связи с принципиальной важностью указанных прав для общества и государства.

Представляются возможными следующие направления борьбы с рассмотренными видами компьютерных преступлений в Республике Беларусь:

- ужесточение санкций;
- расширение и детализация существующего законодательства;
- правовая информатизация населения;
- учет экспертного мнения при решении вопросов информационной безопасности государства и общества.

Соблюдение данных и введение дополнительных мер способно качественно улучшить правовое регулирование информационной безопасности Республики Беларусь.

Литература

Уголовный Кодекс Республики Беларусь [Электронный ресурс] : Кодекс Респ. Беларусь, 9 июля 1999 г. № 275-З : в ред. Закона Респ. Беларусь от 29.01.2015 г. № 245-З // КонсультантПлюс: Беларусь / ООО «Юр-Спектр», Нац. центр правовой информ. Респ. Беларусь. — Минск, 2015.