

танням високих технологій; розвідки — забезпечує стратегічну і тактичну розвідку та співробітництво із зарубіжними партнерами; тактичної і технічної підтримки — забезпечує консультативну підтримку та допомогу місцевим правоохоронним агентствам, міжнародним правоохоронним організаціям, уряду і промисловості; цифрових доказів — забезпечує судову підтримку при розгляді злочинів у сфері високих технологій. І, врешті-решт, необхідно зазначити, що, за прогнозами провідних науковців у галузі інформаційної безпеки, вже найближчими роками можливе стрімке зростання кількості кіберзлочинів. Так, за розрахунками компанії Gartner, вже у кінці 2004 р. економічні збитки від них збільшаться у 10—100 разів [12]. Це змушує і уряд США, і Європейське Співтовариство терміново вжити відповідних заходів як на законодавчому, так і організаційному рівнях. Зокрема, урядом США нещодавно прийнята нова Стратегія щодо захисту інформаційних систем у Інтернеті (бюджетом планується виділення близько 60 млрд дол.), у Раді Європи створюється спеціальний Комітет — «Агентство інформаційної безпеки», відповідні заходи вживаються на рівні ООН. Тому, обравши свій шлях розбудови інформаційного суспільства, Україна також повинна здійснювати відповідні кроки щодо своєї інформаційної безпеки, яка згідно з Конституцією є невід'ємною складовою національної безпеки нашої держави.

Література

1. Проблемы развития цифровых информационных технологий в органах внутренних дел // Компьютерные технологии в криминалистике и информационная безопасность. Труды академии МВД РФ. — М., 1997. — С. 3.
2. Иксар В. Компьютерные преступления [электронный ресурс]. — Режим доступа до документа: <http://www.comprice.ru/articles/detail.php?ID=42319>
3. Крылов В. В. Расследование преступлений в сфере информации. — М.: Издательство «Городец», 1998. — С. 264.
4. Козлов И., Карнаухов С. Америка требует выдачи арестованного в Бангкоке 25-летнего жителя Тернополя // Факты и Комментарии. — 31-Май-2003. — С. 10.
5. Карпинский О. Защита информации, виртуальные частные сети (VPN). Технология ViPNet / По материалам компании Infotecs // Gazeta.Ru. — 2001. — 18 июня.
6. Наумов В. Отечественное законодательство в борьбе с компьютерными преступлениями // Computer World Россия. — 1997. — № 8. — С. 17—18.
7. Сайтарлы Т. Россия: статистика компьютерной преступности [электронный ресурс]. — Режим доступа до документа: <http://www.crime-research.ru/news/12.03.2004/2004-03-1202/>
8. За даними маркетингової досліджувальної компанії InMind, [електронний ресурс]. — Режим доступа до документа: <http://itnews.com.ua/analytics/277.html>
9. Хроніка вірусної атаки на Укртелеком, [електронний ресурс]. — Режим доступа до документа: <http://www.ukrtel.net>
10. Гуцалюк М. Безпека банківських інформаційних систем // Страхова справа. — 2002. — № 2(6). — С. 68—70.
11. Гуцалюк М. Координація боротьби з комп'ютерною злочинністю // Право України. — 2002. — № 5. — С. 121—126.
12. Интерпол, [электронный ресурс]. — Режим доступа до документа: <http://www.interpol-assembly2001.com>



В. П. Беленький, аспирант

Одесский национальный университет им. И. И. Мечникова,
кафедра уголовного права, уголовного процесса и криминалистики,
Французский бульвар, 24/26, Одесса, 65058, Украина

СОВРЕМЕННАЯ ИСТОРИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

РЕЗЮМЕ

Статья посвящена истории компьютерных преступлений. Автор приходит к выводу, что преступления в сфере информационных технологий очень часто являются международными, то есть преступники действуют в одном государстве, а их жертвы находятся в другом государстве. Поэтому для борьбы с такими преступлениями особое значение имеет международное сотрудничество.

Ключевые слова: компьютерные преступления, компьютерная безопасность.