- Ограничение использования подключаемых к компьютеру устройств
- Строгое и чёткое разграничение доступа к информации
- Совершенствование законодательной базы
- Проведение специализированных тренингов для персонала

Литература:

1. Дамир Равилов «Методы классификации внутренних нарушителей» http://infocom.uz/2009/12/16/metodyi-klassifikatsii-vnutrennih-narushiteley/
2. Алексей Комаров «Защита от инсайдера» http://www.osp.ru/text/print/302/5157097.html

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ ПРОТИВ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

(по законодательству Республики Молдова)

Светлана Грищук-Бучка,
Институт истории, государства и права АНМ
(Республика Молдова)

The paper is dedicated to the examination of the categories of crimes against computer safety. This article is based on the analysis of national criminal legislation of the Republic of Moldova.

Противоправные преступные деяния свойственны человечеству с древнейших времен. Однако с развитием цивилизации меняются не только предметы и методы преступного воздействия, но и сам объект преступного посягательства.

Одним из ярких примеров данной категории преступлений являются преступления в сфере компьютерной информации [1]. Активное развитие компьютерных технологий, доступность средств коммуникации, всеобщая информатизация населения стали с одной стороны, еще одной вехой развития цивилизации, а с другой стороны - серьезным испытанием для «права» и правового регулирования. «Наряду с очевидными преимуществами, которые получило человечество от развития информационных технологий, как

отмечает В.И. Волковский, налицо и новые проблемы, ранее нам неизвестные. Существующие сегодня в мире информационные сети позволяют не только обмениваться посланиями, но и проникать в информационные массивы, охраняемые государством» [2]. Соответственно возникает объективная необходимость в правовом регулировании данной сферы общественных отношений.

Законодатель Республики Молдова впервые закрепил уголовную ответственность за данную категорию преступлений в 2002 году в положениях отдельной главы XI Уголовного Кодекса Республики Молдова - «Преступления в сфере информатики». Данная глава содержала три статьи – ст.259-261. В настоящее время в Уголовном Кодексе Республики Молдова (далее УК РМ) данная глава получила новую редакцию и в настоящее время определена как «Информационные преступления и преступления в области электросвязи», и включает 9 статей [3]:

- несанкционированный доступ к компьютерный информации (ст.259 УК РМ);
- неправомерные производство, импорт, продажа или предоставление технических средств или программных продуктов (ст.260 УК РМ);
- неправомерный перехват передачи информационных данных (ст.260[1] УК РМ);
- нарушение целостности информационных данных, содержащихся в информационной системе (ст.260[2] УК РМ);
- воздействие на функционирование информационной системы (ст.260[3] УК РМ);
- неправомерные производство, импорт, продажа или предоставление паролей, кодов доступа или иных аналогичных данных (ст.260[4] УК РМ);
- подлог информационных данных (ст.260[5] УК РМ);
- информационное мошенничество (ст.260[6] УК РМ);
- нарушение правил безопасности информационных систем (ст.261 УК РМ);
- несанкционированный доступ к сетям и услугам электросвязи (ст.261[1] УК РМ).

Правовой анализ состава данных преступлений дает основание сделать следующие выводы, характеризующие их специфику:

Родовым объектом преступного посягательства данной категории преступлений выступают «общественные отношения, обеспечивающие права и законные интересы граждан и организаций, охраняемые законом интересы общества и государства в сфере создания и обращения компьютерной информации» [4; 5].

Объективная сторона компьютерных преступлений может характеризоваться деяниями как в форме действия (например, непра-

вомерный доступ к компьютерной информации – ст.259 УК РМ), так и путем бездействия (например, нарушение … правил защиты информационных систем – ст.261 УК РМ, в частности, виновный не включает систему защиты информации от несанкционированного доступа к ней, оставляет без присмотра свое рабочее место и т.д.) [5].

По конструкции объективной стороны все составы преступлений (за исключением состава, предусмотренного ст.260 УК РМ, 260[1] УК РМ) являются материальными, т.е., включающими в качестве обязательных признаков последствие и необходимую причинно-следственную связь между деянием и последствием. Это означает, что преступление считается оконченным с момента наступления указанных в уголовном законе последствий.

Субъективная сторона характеризуется, как правило, умышленной формой вины в виде прямого умысла.

Субъект компьютерных преступлений – общий – физическое вменяемое лицо, достигшее 16 лет. Согласно положениям ч.2 ст.21 субъектом преступления по ст.206 УК РМ «неправомерное производство, импорт, продажа или предоставление технических средств или программных продуктов» может выступать физическое вменяемое лицо, достигшее на момент совершения преступления 14 лет. Кроме того, положениями ст.261 УК РМ определен специальный субъект как лицо, имеющее в силу своего служебного положения доступ к компьютеру, информационной системе или сети. Следует отметить, что в качестве субъекта данной категории преступлений может выступать так же и юридическое лицо.

Базовые понятия в сфере информатики, такие термины как «компьютерная информация», «информация в компьютерах», «машинные носители», «информационная система», «сеть», «программные продукты», «информационные данные» определяют специфику данного рода преступлений, выступают непосредственными предметами преступного посягательства. «Компьютерная информация» как предмет преступления является обязательным признаком состава анализируемых преступлений [6].

А, соответственно, и подтверждает, тот факт, что данная категория преступлений должна определяться как «компьютерные преступления», «преступления против компьютерной безопасности», а не так как определена в действующем уголовном законодательстве Республики Молдова - «информационные преступления». На лицо подмена понятий, когда «информационная безопасность» рассматривается слишком узко, только лишь с позиции безопасности информации

содержащейся в компьютерах и информационных системах. Ошибочно отождествляются два совершенно разных по своей сущности понятия «защита информации» и «информационная безопасность», хотя на сегодняшний день это совершенно не одно и то же [7]. Кроме того, следует отметить, что и само понятие «информационная безопасность» - многогранно [7]. «Информационная безопасноть не сводится только лишь к компьютерной безопасности … «информационная безопасноть», включающая в себя компьютерную безопасноть в качестве необходимой составляющей распространяется на все социальные процессы современного общества[8]. Именно данное утверждение доктора философских наук Т.Н. Цырдя подчеркивает тот факт, что «в современном обществе информационная безопасность является составной и неотъемлемой частью государственной безопасности любого современного государства, обеспечивающей состояние защищенности личности, общества и государства от угроз в информационной сфере» [7].

Целесообразно, на наш взгляд, внести соответствующие изменения в положения Уголовного Кодекса Республики Молдова и изменить наименование данной главы с целью исключения возможности неверного истолкования категории «информационные преступления», так как в представленной форме это может привести к правовой коллизии и неправильной правовой трактовке и применению уголовно-правовых норм на практике. Более того, из положения самих статей УК РМ, четко явствует тот факт, что речь в данной главе идет именно о «преступлениях против компьютерной безопасности».

Литература:

1. Иван Бабенко. Расследование компьютерных преступлений в сети Internet/ „Securitatea informațională – 2009", conf. intern. (2009; Chişinău). Securitatea informațională – 2009: Conf. intern., 20-21 mai 2009, (ed. a 6-a) /com. org.: Grigore Belostecinic, Vadim Cojocaru, Tatiana Mişova [et al.]; coord. ed.: S. Ohrimenco. – Ch.: ASEM, 2009. – p. 14-18
2. Волковский В.И. Проблемы информационной безопасности //Журнал «Право и безопасность». – № 2-3 . – август, 2002. http://www.dpr.ru/pravo/pravo_3_26.htm
3. Уголовный кодекс Республики Молдова № 985-XV от 18 апреля 2002г.//. Повторно опубликован Monitorul Oficial al Republicii Moldova № 72-74, 2009.
4. Уголовное право. Особенная часть: Учебник/ Под ред.проф. Л.Д. Гаухмана и проф. С.В.Максимова. –2-е изд., перераб., доп. –М.: Изд-во Эксмо, 2005 – с.530-538

5. Лазарева Н. Проблемы квалификации преступлении в области информатики и электросвязи//Закон и жизнь. -2007. -№12. – С.49-56.
6. Лосев В. Преступления против информационной безопасности //Судовы весник. -2002. -№1. – С.40-46.
7. Рыженкова, О.Ю. Информационная безопасность: определение понятия, место в системе национальной безопасности//Закон и право. -2009. -№1. – С.50-51.
8. Теодор Н.Цырдя. Информационная безопасность в условиях информатизации общества http://security.ase.md/publ/ru/pubru06.html

ОРГАНИЗАЦИЯ ПРОГРАММНО- АППАРАТНОЙ ЗАШИТЫ ИНФОРМАЦИИ ОТ ИНСАЙДЕРОВ

Зинаида Гулка, Ольга Гешова,
Славянский университет (Республика Молдова)

In work the problem of distribution of insider trade is considered by the information. The set of software and tools for protection of the data with the short description of functionality of each utility is presented.

Важнейшей проблемой, стоящей перед руководством и службой безопасности любого предприятия, является проблема лояльности сотрудников, или, иными словами, проблема защиты информации от инсайдеров.[1] Существует множество ролей, приписываемых инсайдеру. Например, в финансовой деятельности незаконные инсайдерские торговые операции с ценными бумагами на основе внутренней информации о деятельности компании-эмитента. Обычно инсайдерами являются директора и старшие менеджеры, а также владельцы более 10 % голосов компании. Очевидно, что обиженный или недовольный сотрудник компании, имеющий легальный доступ к сетевым и информационным ресурсам и обладающий определенными знаниями о структуре корпоративной сети, может нанести своей компании гораздо больший ущерб, чем хакер, взламывающий корпоративную сеть через Интернет.

Более того, в результате ошибки или невнимательности инсайдером может оказаться и вполне лояльный сотрудник, который, например, может вынести из офиса диск с конфиденциальной информацией для того, чтобы поработать дома, и