Саттаров Михаил Олегович

НЕКОТОРЫЕ УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ КВАЛИФИКАЦИИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

В настоящей статье проведен уголовно-правовой анализ преступлений в сфере компьютерной информации. Исследованы вопросы квалификации и практического противодействия компьютерным преступлениям. Отмечены основные недостатки законодательного регулирования в данной области. Выявлены ключевые проблемы как теоретического, так и практического характера, возникающие в процессе борьбы с киберпреступлениями. Предложены пути разрешения обозначенных проблем.

Адрес статьи: www.gramota.net/materials/1/2015/10/32.html

Источник

Альманах современной науки и образования

Тамбов: Грамота, 2015. № 10 (100). С. 125-127. ISSN 1993-5552.

Адрес журнала: www.gramota.net/editions/1.html

Содержание данного номера журнала: www.gramota.net/materials/1/2015/10/

ON THE DEGREE OF PRICE-JONES CURVE ASYMMETRY IN HEALTH AND DISEASE

Sarkisyan Grach'ya Pargevovich, Ph. D. in Physical-Mathematical Sciences
A. B. Nalbandyan Institute of Chemical Physics of the National Academy of Sciences of the Republic of Armenia
hrachya_sargsyan@mail.ru

The article is devoted to one of the fundamental problems of hematological science – Price-Jones curve location in health and disease, and the evaluation of the degree of the asymmetry of this curve. The author developed an approach, which allows identifying anisocytosis with different degrees of dispersion and asymmetry. The paper discusses the advantages of the developed mathematical apparatus while processing diffractometric experiment data.

Key words and phrases: Price-Jones curve; anisocytosis; degree of asymmetry; distribution function; laser diffractometry.

УДК 343.3/7
Юридические науки

В настоящей статье проведен уголовно-правовой анализ преступлений в сфере компьютерной информации. Исследованы вопросы квалификации и практического противодействия компьютерным преступлениям. Отмечены основные недостатки законодательного регулирования в данной области. Выявлены ключевые проблемы как теоретического, так и практического характера, возникающие в процессе борьбы с киберпреступлениями. Предложены пути разрешения обозначенных проблем.

Ключевые слова и фразы: уголовное право; уголовная ответственность; уголовное законодательство; компьютеризация; киберпреступления; компьютерные преступления; компьютерная информация.

Саттаров Михаил Олегович
Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)
malevolentmalevolent@gmail.com

НЕКОТОРЫЕ УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ КВАЛИФИКАЦИИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ©

Сегодня важное место в нашей жизни занимают компьютерные системы, позволяющие получить мгновенный доступ к информации и тут же ее обработать. К сожалению, помимо позитивных сторон, у данного явления имеются и негативные. В частности, так называемые киберпреступления, требующие корректной квалификации, эффективного практического пресечения и законодательной регламентации.

Глава 28 раздела IX УК РФ определяет родовой объект данных преступлений как отношения общественного порядка и общественной безопасности [5]. Видовым же объектом является информационная безопасность как специфичный вид общественной безопасности [1].

Предметом данной группы преступлений являются любые сведения, независимо от формы их представления, – информация, легальное определение которой дано в ФЗ «Об информации, информационных технологиях и о защите информации» и коррелирует с определением «компьютерной информации» – сведения, представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи, – данным в Примечании 1 к ст. 272 УК РФ [3; 5]. Последнее было введено в конце 2011 года, что впоследствии устранило внутреннюю непоследовательность и несогласованность российского законодательства.

Нормы о преступлениях в сфере компьютерной информации в целом направлены на правовую охрану компьютерной безопасности как специфичного вида общественной безопасности, что следует принять во внимание при их юридическом толковании и применении.

Начать стоит со статьи 272 УК РФ, предусматривающей наказание за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

В качестве охраняемой законом информации следует понимать любую информацию в чужом компьютере, которая охраняется в соответствии с нормами гражданского права, что вероятно вытекает из права собственности на компьютерную технику, содержащую информацию.

Состав данного преступления материален, хотя вопрос об общественно опасных последствиях – дискуссионный, поскольку законодатель не раскрывает понятия конкретных видов последствий, указанных в диспозиции рассматриваемой статьи [7]. Помимо всего прочего, следует полагать, что потенциально опасные действия (например, просмотр информации), которые не были помещены в диспозицию статьи, состава не образуют. На практике подобное упущение вызывает немало трудностей у сотрудников правоохранительных органов.

Заострить внимание хотелось бы на одном из квалифицирующих признаков, а именно на тяжких последствиях и создании угрозы их наступления. Подобная часть в рассматриваемые статьи добавлена справедливо, поскольку в век быстрого развития информационных технологий возможность нанести колоссальный ущерб информации и гражданам, ею владеющим, возрастает в разы.

Отметим также и особый признак субъективной стороны – корыстный мотив, направленный на извлечение имущественной, зачастую денежной, выгоды.

Следующая статья 273 устанавливает ответственность за создание, использование и распространение вредоносных компьютерных программ, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты.

В настоящее время более популярным становится блокирование информации путем создания препятствий правомерному к ней доступу как со стороны человека, так и со стороны технических устройств. Типичным примером блокирования является DoS или DDoS-атака, когда осознанно организуется масса запросов к системе, которые она заведомо не может обработать, и перегружается [2]. Отследить атакующего или группу атакующих представляется зачастую невозможным, поскольку приходится иметь дело с профессионалами – так называемыми «хакерами», оперирующими программами, способными скрыть местоположение.

На сегодняшний день в арсенале правоохранительных органов отсутствует высокоуровневое программное обеспечение, которое давало бы возможность отследить местоположение злоумышленника.

Состав преступления – формальный. Уголовный закон достаточно строго преследует сам факт создания препятствий доступу к информации [6].

В статье 274 УК РФ предусмотрена ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Состав преступления, предусмотренного ч. 1 ст. 274, – материальный, преступление окончено в случае причинения крупного ущерба, превышающего один миллион рублей. Имеется в виду как реальный ущерб, так и упущенная выгода. Если же ущерб составляет сумму, не превышающую одного миллиона рублей, оценка содеянного будет перенесена в гражданско-правовую плоскость.

Общественно опасные последствия данного состава разбиваются на два уровня. Первый – промежуточный, заключающийся в уничтожении, блокировании, модификации или копировании компьютерной информации, и конечный в виде причиненного крупного ущерба.

Итак, наиболее спорны и непонятны в данной системе преступлений нормы, содержащиеся в ст. 274 УК РФ. Связано это в первую очередь с тем, что на сегодняшний день нет единых правил, которые бы определили особый порядок защиты информации, что подчас влечет неправильную квалификацию. Во избежание подобного рода пробела предлагаем закрепить общие для всех субъектов РФ правила на федеральном уровне.

Киберпреступления – распространенное противоправное явление, их число с каждым днем неизбежно растет. Это связано, как было ранее отмечено, со стремительным развитием компьютерной техники и программного обеспечения, в особенности вредоносного. Следует признать, что с течением времени подобного рода технологии просочатся во все сферы преступной деятельности, и ни одно из преступлений не сможет обойтись без «киберэлемента». Чтобы избежать подобного разворота событий, стоит закрепить квалифицирующий признак «совершение преступления с использованием компьютерных технологий или вредоносного программного обеспечения» в различных составах в рамках общественных отношений собственности, экономической деятельности и др.

Смежные составы в Уголовном кодексе присутствуют, но в малом количестве:

- статья 138 УК РФ – Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений;
- статья 138.1 УК РФ – Незаконный оборот специальных технических средств, предназначенных для негласного получения информации;
- статья 146 УК РФ – Нарушение авторских и смежных прав;
- статья 159.3 УК РФ – Мошенничество с использованием платежных карт;
- статья 159.6 УК РФ – Мошенничество в сфере компьютерной информации;
- статья 187 УК РФ – Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов.

Некоторые шаги в предлагаемом нами направлении сделаны, однако пока их недостаточно.

В заключение приведем следующие меры, принятие которых теоретически поспособствует снижению уровня преступности в данной сфере:

- функциональные меры, которые заключаются в защите от несанкционированного доступа к системе путем резервирования особо важных компьютерных подсистем, установки оборудования и программного обеспечения, способного вычислить и ликвидировать угрозу в кратчайшие сроки;
- меры координационные: подбор и привлечение высококвалифицированных профессионалов в данной области, исключение случаев ведения особо важных работ только одним человеком;
- и, наконец, правовые меры, сущность которых состоит в разработке правовых норм в данной плоскости в соответствии с быстро меняющимися компьютерными устройствами и программным обеспечением.

Конечно, подобные меры, какими бы современными они ни были, не смогут гарантировать абсолютную надежность и сохранность компьютерной информации, но, в то же время, на наш взгляд, снизят риск потенциальных потерь до минимума.

Список литературы

1. **Бытко С. Ю.** Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерных технологий: дисс. ... к.ю.н. Саратов, 2002. 207 с.
2. **Комментарий к Уголовному кодексу Российской Федерации** / С. А. Боженок, Ю. В. Грачева, Л. Д. Ермакова и др.; отв. ред. А. И. Рарог. 10-е изд., перераб. и доп. М.: Проспект, 2015. 952 с.

3. **Об информации, информационных технологиях и о защите информации**: Федеральный закон от 27.07.2006 г. № 149-ФЗ // Собрание законодательства Российской Федерации (СЗРФ). 2006. № 31. Ст. 3448.
4. **Уголовное право. Особенная часть**: учебник для бакалавров / под ред. А. И. Чучаева. 2-е изд., перераб. и доп. М.: Проспект, 2015. 552 с.
5. **Уголовный кодекс РФ** от 13.06.1996 г. № 63-ФЗ (ред. от 13.07.2015 г.) // СЗРФ. 1996. № 25. Ст. 2954.
6. **Ястребов Д. А.** Вопросы отграничения неправомерного доступа к компьютерной информации от смежных составов преступлений // Российский следователь. 2008. № 17. С. 25-26.
7. **Ястребов Д. А.** Общественно опасные последствия неправомерного доступа к компьютерной информации: нарушения работы ЭВМ. 2008 [Электронный ресурс]. URL: http://www.allpravo.ru/library/doc101p0/instrum7225/item7226.html (дата обращения: 14.09.2015).

CERTAIN CRIMINAL AND LEGAL ASPECTS OF QUALIFYING COMPUTER CRIMES

Sattarov Mikhail Olegovich
Kutafin Moscow State Law University
malevolentmalevolent@gmail.com

The article provides a criminal and legal analysis of crimes in the sphere of computer information. The paper analyzes the issues of qualifying and counteracting computer crimes. The author emphasizes the basic shortcomings of the legislative regulation in this sphere, identifies the key problems both of theoretical and practical nature arising on counteracting cybercrimes, and introduces the ways to solve the mentioned problems.

Key words and phrases: criminal law; criminal responsibility; criminal legislation; computerization; cybercrimes; computer crimes; computer information.

УДК 504.064.2:546(470.13)
Науки о Земле

В статье представлены результаты исследования почвенного покрова, техногенного почво-грунта и угольной породы с породных отвалов в зоне деятельности угольных шахт «Комсомольская» и «Воркутинская» города Воркуты Республики Коми. В почвенном покрове были исследованы физико-химические свойства для выяснения наличия или отсутствия их изменения под влиянием деятельности угледобывающего производства. Установлена степень загрязнения почвенного покрова изучаемых территорий.

Ключевые слова и фразы: тяжелые металлы; почвенный покров; угольная порода; угледобывающая шахта; уголь.

Северьянова Елена Николаевна
Ульяновский государственный университет
SeveryanovIV@mail.ru

ЭКОЛОГО-ГЕОХИМИЧЕСКАЯ ХАРАКТЕРИСТИКА ПОЧВЕННОГО ПОКРОВА В ЗОНЕ ДЕЯТЕЛЬНОСТИ УГЛЕДОБЫВАЮЩЕГО ПРЕДПРИЯТИЯ НА ПРИМЕРЕ ГОРОДА ВОРКУТЫ РЕСПУБЛИКИ КОМИ©

Республика Коми является одним из основных топливно-энергетических регионов России. Топливно-энергетические ресурсы Республики представлены промышленными запасами коксующихся и энергетических углей Печерского угольного бассейна [5]. Запасы каменного угля Печерского бассейна, второго по величине в России, обеспечивают отработку трех крупных месторождений [9] и составляют около 7,8% общероссийской добычи, в том числе до 20% коксующихся углей [10].

Основными потребителями коксующихся углей Печерского бассейна являются ОАО «Северсталь», ОАО «Носта», ОАО «Мечел», Новолипецкий, Нижнетагильский, Магнитогорский металлургические комбинаты, Московский коксогазовый завод. Угли энергетических марок поступают на предприятия лесной, целлюлозно-бумажной и деревообрабатывающей промышленности, предприятия системы Минэнерго РФ, Министерства путей сообщения РФ Ленинградской, Архангельской области, Карелии, г. Череповца, Республики Коми.

Угледобывающая отрасль является источником загрязнения окружающей среды вследствие производства, использования, хранения, утилизации, обращения различных машин, оборудования [11].

Необходимо отметить, что при добыче каждой тысячи тонн угля шахтным способом на поверхность поступает в среднем 100-115 м^3 породы, а при карьерной добыче требуют размещения 3,6 тыс. м^3 вскрышных пород [4]. При этом любые нарушения техногенного массива могут привести к непредсказуемому загрязнению окружающей среды [3; 8].

В результате добычи ископаемых углей происходят высвобождение тяжелых металлов и их поступление в окружающую среду. Основным источником являются отвалы вскрышных пород. Например, вскрышные породы Экибастуза содержат (в процентах): меди – 0,2; кобальта – 0,005; свинца – 0,03; цинка – 0,08; молибдена – 0,003; никеля – 0,002; марганца – 0,7; хрома – 0,3, что на 1-2 порядка выше кларка этих металлов в осадочных породах.