Розділ II. ПРОБЛЕМИ ТЕОРІЇ ТА ПРАКТИКИ ЗАСТОСУВАННЯ ЗАКОНОДАВСТВА

УДК 343.533:004.5:34

Н.В. Карчевский

ЗАКОНОДАТЕЛЬСТВО ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ И СОВРЕМЕННЫЕ ТЕНДЕНЦИИ ИНФОРМАТИЗАЦИИ: ОСНОВНЫЕ НАПРАВЛЕНИЯ КОРРЕСПОНДЕНЦИИ

Робиться спроба дослідити рівень відповідності чинного кримінального законодавства соціальним тенденціям інформатизації.

Ключові слова: *інформатизація, злочин, суспільна небезпечність.*

Предпринимается попытка исследовать уровень соответствия действующего уголовного законодательства социальным тенденциям информатизации.

Ключевые слова: *информатизация, преступление, общественная опасность.*

We attempt to investigate the level of compliance of existing penal laws social trends of informatization.

Key words: *informatization, crime, public danger.*

Сегодня наиболее динамичной социальной сферой являются отношения информатизации. Скорость, с которой развиваются компьютерные технологии, а также расширяется сфера их применения, актуализирует проблематику соответствия правового регулирования уровню информатизации общества. Одним из дискуссионных вопросов здесь является обеспечение эффективной уголовно-правовой охраны. Цель данной работы – попытка определения степени соответствия действующего законодательства об уголовной ответственности за преступления в сфере использования информационных технологий современным тенденциям и уровню информатизации общества, а также формулирование, в случае необходимости, основных направлений его совершенствования.

Необходимо уточнить содержание понятия "преступление в сфере использования информационных технологий". Как отмечалось ранее, обеспечение уголовно-правового стимулирования положительных и минимизации негативных социальных последствий информатизации, предполагает определение в качестве самостоятельного объекта уго-

ловно-правовой охраны системы общественных отношений, обеспечивающих реализацию информационной потребности. Для обозначения этой системы предлагается использовать термин "информационная безопасность", ее структуру составляют отношения в сфере формирования информационного ресурса, обеспечения доступа к информации, а также отношения в сфере использования информационных технологий. При этом социальная значимость отношений информационной безопасности, а следовательно и целесообразность их уголовно-правовой охраны, определяются значимостью тех отношений, в пределах которых возникает информационная потребность[10]. В свою очередь, информационная технология представляет собой организованную совокупность информационных процессов с использованием средств вычислительной техники, которые обеспечивают высокую скорость обработки данных, быстрый поиск информации, передачу данных, доступ к источникам информации независимо от места их расположения [6]. Таким образом, преступления в сфере использования информационных технологий, являясь одним из видов преступлений в сфере информационной безопасности, представляют собой *предусмотренные законодательством об уголовной ответственности, общественно опасные, виновные, совершенные субъектом преступления деяния, причиняющие вред обеспеченным средствами вычислительной техники отношениям в сфере реализации информационной потребности.* Анализ действующего УК позволяет прийти к выводу, что к таким преступлениям следует относить посягательства, предусмотренные *ч. ч. 11, 12 в. 158, ст. ст. 361, 361-1, 361-2, 362, 363, 363-1, 376-1 УК*[1].

[1] Нельзя обойти стороной вопрос о том, что наряду с предлагаемым понятием ("преступление в сфере использования информационных технологий") в уголовно-правовом дискурсе достаточно активно используются следующие: "компьютерное преступление", "киберпреступление", "интернет-преступление" и т.д. Объем данных понятий определяется по-разному. Достаточно распространенным является отнесение к компьютерным преступлениям всех общественно опасных посягательств, при совершении которых компьютеры используются как технические средства [7, с. 14; 1, с. 72; 3, с. 65; 2, с. 11; 12, с. 243; 4, с. 39 – 40; 11, с. 87; 14]. При таком понимании, любое преступление, совершенное с использованием компьютерной техники (мошенничество, шпионаж, незаконное распространение наркотических средств и т.д.), должно считаться компьютерным. Недостатком данного подхода является его несоответствие основному принципу структурирования законодательства об уголовной ответственности – систематизации уголовных законов на основе классификации посягательств по объекту. Определение новой группы преступлений всегда должно производиться на основе признаков, характеризующих объект посягательства. Именно поэтому в пределах уголовно-правового дискурса необоснованным следует считать определение компьютерных преступлений на основе признаков, характеризующих способ, орудие или средство посягательства. Такой подход недопустим и потому, что не обеспечивает четкого определения предмета дискурса. Вместе с тем, следует признать, что определение компьютерных преступлений как группы посягательств, характеризующейся общими признаками способа, орудия или средства, может быть востребовано. Речь идет об установлении особенностей методики раскрытия или расследования преступлений, специфики фиксации следов и т.д. Возможно, решением проблемы является ограничение применения понятия "компьютерное преступление" в широком смысле в пределах уголовно-правового дискурса.

Проведенный анализ законодательства об уголовной ответственности и практики его применения позволяет следующим образом определить *основные* направления решения поставленной задачи:

1) обоснование целесообразности выделения специальных норм об уголовной ответственности за посягательства в сфере использования компьютерных систем особого назначения;

2) формулирование чётких законодательных критериев общественной опасности преступлений в сфере использования информационных технологий.

Целесообразность выделения *специальных норм об уголовной ответственности за посягательства на работу компьютерных систем особого назначения*. Речь идет о преступлениях, предусмотренных ч. ч. 11, 12 ст. 158 и ст. 376-1 КК. Прежде всего, нельзя не обратить внимания на практически одинаковые санкции, предусмотренные действующим УК за несанкционированное вмешательство в работу компьютерной техники (ст. 361), несанкционированное вмешательство в работу Государственного реестра избирателей (ч. ч. 11, 12 в. 158 КК) и незаконное вмешательство в работу автоматизированной системы документооборота суда (ст. 376-1 КК). Такое законодательное решение, несомненно, свидетельствует в пользу отмены названных специальных запретов. Кроме того, в контексте наличия указанных специальных норм трудно объяснить, почему отсутствуют подобные нормы относительно использования информационных технологий стратегического значения [13, с. 46] или, например, в атомной энергетике, управлении движением воздушного транспорта и т.д. Бесперспективность установления специальных уголовно-правовых запретов в данной сфере подтверждается и тем, что количество социально значимых информационных систем будет постоянно возрастать, однако это не означает, что каждая такая система должна быть обеспечена "собственным" уголовно-правовым запретом. Скорее наоборот, стабильность законодательства об уголовной ответственности обеспечивается лучшим образом тогда, когда появление новых видов компьютерных систем особого назначения не требует дополнения УК новыми нормами.

Относительно *чётких законодательных критериев общественной опасности преступлений в сфере использования информационных технологий* следует отметить следующее. Аксиоматичным является положение о том, что эффективность уголовно-правового регулирования пребывает в прямой зависимости от чёткости нормативных критериев общественной опасности посягательств, предусмотренных уголов-

ным законодательством. Чем четче законодательное разграничение преступных и непреступных проявлений, тем эффективнее применение уголовного закона. Представляется, что критерием отнесения определённых деяний к преступлениям в сфере использования информационных технологий следует считать вред, причиняемый той социально значимой деятельности, для осуществления которой применяется компьютерная техника. Очевидно, что уничтожение информации, обрабатываемой в компьютерной системе, опасно настолько, насколько социально значимой является задача, для решения которой используется определенный компьютер. Тем не менее, национальное законодательство об уголовной ответственности не учитывает такой специфики. Судя по решению, принятому законодателем, утечка, потеря, подделка, блокирование информации, нарушение установленного порядка ее маршрутизации или искажение процесса ее обработки (ст. 361, 362 УК Украины) признаются общественно опасными сами по себе. Лишь на уровне квалифицирующих признаков мы встречаем зависимость уголовной ответственности от наступления "существенного вреда". Необходимо отметить, что аналогичные выводы могут быть сделаны и относительно содержания ст. ст. 272 и 273 УК РФ; ст. 268 УК Польши; ст. 9с Главы 4 УК Швеции. Не лишены указанного недостатка и положения Конвенции о киберпреступности. Подобная ситуация приводит к вполне ожидаемым проблемам: из-за отсутствия в законодательных определениях "компьютерных" преступлений четких критериев общественной опасности под уголовно-правовой запрет и, соответственно, в сферу действия уголовной юстиции попадают не только деяния, которые действительно являются общественно опасными, но и не являющиеся таковыми. Это приводит к существенному снижению эффективности уголовно-правового противодействия данным преступлениям [10].

Исправление ситуации в первую очередь предусматривает включение в диспозиции соответствующих уголовно-правовых норм четких положений относительно критериев общественной опасности посягательств. Одним из возможных и наиболее оптимальных решений является обращение к законодательным конструкциям, свойственным преступлениям с производными последствиями. Структура объективной стороны преступлений в сфере использования компьютерной техники должна включать: 1) основные последствия - различные формы нарушения информационных отношений, выступающих непосредственными объектами (уничтожение, блокирование, наруше-

ние целостности информации и т.д.); 2) производные последствия - нарушение отношений в сфере реализации прав и свобод отдельных физических лиц, государственных или общественных интересов, деятельности юридических лиц. Лишь при наличии совокупности таких последствий совершенное посягательство следует считать преступлением в сфере использования информационных технологий.

Показательным здесь будет пример встроенных компьютерных систем. Современные технологии позволяют разрабатывать и широко применять специализированные электронно-вычислительные машины, предназначенные для управления разнообразными устройствами и оборудованием. Это средства на основе управления, контроля, диспетчеризации в системах тепло и энергосбережения, компьютерные системы управления производством, кассовые аппараты, аппаратура диагностики, бытовые приборы и т.д. [5]. Для обозначения таких электронно-вычислительных машин употребляются термины "встроенная система" (англ. embedded system) или "встроенная компьютерная система". Определить данную систему можно следующим образом: специализированная компьютерная система управления, которая конструктивно соединена, является частью, того устройства, управление которым обеспечивает.

В настоящее время активно внедряются счетчики электроэнергии, тепла, воды, оборудованные встроенными компьютерными системами. Фальсификация показаний таких устройств осуществляется путем несанкционированного вмешательства в их работу [8]. Поскольку встроенные компьютерные системы представляют собой электронно-вычислительные машины по определению, несанкционированное вмешательство в работу таких систем, при наличии соответствующих оснований, может быть квалифицировано как преступление, предусмотренное ст. 361 КК Украины.

Собственно пример заключается в следующем. Частный дом А. был оборудован счетчиком воды с вмонтированной компьютерной системой, частный дом Б. - механическим счетчиком воды. А. и Б. совершили фальсификацию показаний указанных устройств. А. - путем несанкционированного вмешательства, Б. - путем механического воздействия. Допустим, что объемы воды, полученной, но неоплаченной вследствие фальсификации работы измерительных приборов, у А. и Б. одинаковы. Какой может быть уголовно-правовая квалификация их действий? С позиций преступлений против собственности, при условии причинения ущерба превышающего 50 необлагаемых налогом минимумов, действия и А. и Б. могут быть квали-

фицированы по ст. 192 УК. В случае причинения меньшего ущерба, необходимо констатировать отсутствие признаков состава преступления в действиях Б. В свою очередь, действия А., в таком же случае, могут быть квалифицированы как несанкционированное вмешательство в работу электронно-вычислительной машины (ст. 361 УК). При этом, нельзя не обратить внимания на тот факт, что наиболее суровое наказание за преступление предусмотренное ч. 1 ст. 192 УК до 6 месяцев ареста, тогда как ч.1 ст. 361 УК – до 3-х лет лишения свободы. Справедлива ли такая правовая оценка, соответствует ли она общественной опасности посягательства? В свою очередь, реализация приведенных ранее законодательных предложений позволила бы эффективно решать подобные задачи.

В данном контексте следует обратить внимание и на проблему уголовно-правовой оценки мошенничества, совершенного путем незаконных операций с использованием электронно-вычислительной техники (ч.3 ст. 190 УК). И хотя данное посягательство, являясь преступлением против собственности, не относится к преступлениям в сфере использования информационных технологий, пример важен поскольку демонстрирует определенную тенденцию развития уголовного законодательства. На момент появления нормы (12 лет назад) применение компьютерной техники для осуществления мошенничества действительно могло свидетельствовать о повышенной общественной опасности посягательства. Степень распространенности систем дистанционного банковского обслуживания была незначительной. Пользовались ими крупные хозяйствующие субъекты. Поэтому положения ч.3 ст. 190 УК достаточно четко очерчивали круг деяний, которые обосновано было рассматривать как *особо квалифицированный вид мошенничества*, близкий по степени общественной опасности к мошенничеству в крупных размерах. Однако стремительные темпы проникновения информационных технологий в финансовую сферу обусловили качественное изменение рассматриваемого вида мошенничества. Уже сейчас правоохранительные органы фиксируют ощутимое количество таких преступлений, сопряженных с причинением вреда, соответствующего признакам простого или квалифицированного мошенничества (ч. 1, ч. 2 ст. 190 УК). Можно ли считать обоснованной, а именного этого требует толкование нормы, уголовно-правовую оценку таких действий по ч. 3 ст. 190 УК? Вопрос скорее риторический. В современных условиях нет оснований утверждать, что использование электронно-вычислительной техники в процессе осуществления мошенничества настолько повышает уровень общественной опасности совершенного деяния. Сравним два гипотетических примера: с

целью завладения имуществом путем обмана Т. сообщает в рекламной газете заведомо неправдивые сведения о продаже определенного оборудования, а В. сообщает такие сведения использую электронную доску объявлений или интернет аукцион. Понятно, что степень общественной опасности таких деяний определяется главным образом предметом посягательства, а использование электронно-вычислительной техники не может рассматриваться как признак, фактически приравнивающий простое мошенничество к особо квалифицированному. Здесь нельзя не вспомнить пример Б.Г. Розовского о том, что УК РСФСР 1927 года, предусматривал такой квалифицирующий признак кражи как "использование технических средств" (ст. 162). Очевидно, развитие уголовного законодательства в данной части прошло аналогичные стадии. На этапе формулирования указанной нормы использование технических средств, в силу их чрезвычайно ограниченного применения, действительно свидетельствовало о повышенной общественной опасности совершенной кражи. С дальнейшей индустриализацией общества рассматривать применение технических средств как квалифицирующий признак кражи уже не было необходимости. С учетом изложенного, целесообразным представляется отказ от нормативного закрепления рассматриваемого квалифицирующего признака. В условиях стремительного расширения сферы применения информационных технологий, положения ч.3 ст. 190 УК приобретают характер таких, которые не обеспечивают адекватного уголовно-правового отражения объективного уровня развития общественных отношений[1].

Пример ч.3 ст. 190 УК был приведен после описания специфики уголовно-правовой оценки несанкционированного вмешательства в работу встроенных компьютерных систем в связи с тем, что указанные проблемы имеют общее происхождение: формализованные в

[1] Рассмотрение сложившейся ситуации было бы неполным без анализа еще одной стороны проблемы. Исходя из содержания ст. 246 УПК Украины большинство негласных следственных (розыскных) действий проводится исключительно в уголовных производствах по тяжким или особо тяжким преступлениям (ч. 3 ст. 190 УК предусматривает наказание до восьми лет лишения свободы). При этом, специфика мошенничества, совершаемого с использованием электронно-вычислительной техники, обуславливает необходимый характер таких действий. В частности, результативное расследование данной категории преступлений практически неосуществимо без снятия информации с электронных информационных систем. Имеем абсурдную ситуацию: существование в УК нормы, которая не соответствует социальным тенденциям и не отражает объективной опасности предусмотренного деяния, позволяет "срабатывать" нормам УПК, правоохранительные органы имеют основания проводить необходимые негласные следственные (розыскные) действия. Очевидно, что приведенные положения не стоит рассматривать как аргумент в пользу сохранения ч. 3 ст. 190 УК в действующей редакции. Скорее, сложившуюся ситуацию следует рассматривать как еще одно свидетельство необоснованности законодательного ограничения сферы применения негласных следственных (розыскных) действий, нецелесообразности зависимости возможности их проведения от тяжести совершенного преступления.

соответствующих нормативных предписаниях представления законодателя об общественной опасности данных посягательств не соответствуют фактическому уровню развития отношений информатизации, вследствие этого в сфере действия законодательства об уголовной ответственности оказываются деяния, которые безосновательно рассматривать как преступления. Являясь видом преступлений против информационной безопасности, преступления в сфере использования информационных технологий общественно опасны настолько, насколько значима реализация определенной информационной потребности. Использование данного положения как принципиального при дальнейшем совершенствовании законодательства позволит обеспечить повышение его эффективности, будет способствовать предупреждению злоупотребления уголовным правом в данной сфере.

Таким образом, можно сформулировать следующие основные положения о соответствии действующего законодательства об уголовной ответственности за преступления в сфере использования информационных технологий современным тенденциям и уровню информатизации общества:

1) преступления в сфере использования информационных технологий, являясь одним из видов преступлений в сфере информационной безопасности, представляют собой *предусмотренные законодательством об уголовной ответственности, общественно опасные, виновные, совершенные субъектом преступления деяния, причиняющие вред обеспеченным средствами вычислительной техники отношениям в сфере реализации информационной потребности;*

2) наметившуюся тенденцию расширения специальных уголовно-правовых запретов в сфере применения компьютерных систем особого назначения (ч.ч. 11, 12 ст. 158, ст. 376-1 УК) следует считать бесперспективной, поскольку в условиях дальнейшей информатизации стабильность законодательства об уголовной ответственности следует считать обеспеченной лучшим образом тогда, когда появление новых видов компьютерных систем особого назначения не требует дополнения УК новыми нормами;

3) повышение эффективности уголовно-правовой охраны отношений в сфере использования информационных технологий предполагает включение в соответствующие законы четких положений относительно критериев общественной опасности посягательств, обеспечивающих применение средств уголовной юстиции только в тех случаях, когда имеет место обусловленное посягательством в сфе-

ре информационных технологий существенное нарушение отношений в сфере реализации прав и свобод отдельных физических лиц, государственных или общественных интересов, деятельности юридических лиц.

Использованная литература:

1. Азаров Д. С. Порушення роботи автоматизованих систем – злочини у сфері комп'ютерної інформації / Д. С. Азаров // Право України. – 2000. – № 12. – С. 69–73.

2. Батурин Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. – М. : Юридическая литература, 1991. – 157 с.

3. Біленчук П. Д. Комп'ютерна злочинність : навчальний посібник / Петро Дмитрович Біленчук, Володимир Васильович Бут, Владислав Данилович Гавловський, Михайло Васильович Гуцалюк, Руслан Леонідович Колпак. – К. : Атіка, 2002. – 240 с.

4. Голубєв В. О. Правові проблеми захисту інформаційних технологій / В. О. Голубєв // Вісник Запорізького юридичного інституту. – 1997. – № 2. – С. 35–40.

5. Грицай Д. Д. Особливості побудови комп`ютерної системи тестування цифрових пристроїв на базі soft-процесорів / Д. Д. Грицай, А. І. Роговенко // Вісник Чернігівського державного технологічного університету. "Технічні науки". – 2011. – №2(49) [Електронний ресурс]. – Режим доступу: http://archive.nbuv.gov.ua/portal/natural/vcndtu/2011_49/

6. Закон України "Про національну програму інформатизації" від 04.02.1998 р. [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=74%2F98-%E2%F0.

7. Калюжный Р. А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект) : автореф. дис. … доктора юрид. наук: 12.00.02 / Ростислав Андрійович Калюжний. – К., 1992. – 47 с.

8. Каргапольцев В.П. О фальсификациях при прибором учете тепла и воды [Электронный ресурс]/ В. П. Каргапольцев // Архив Теплопункта. – Режим доступа: http://www.glavbukh.ru/art/19724

9. Карчевский Н.В. Основные направления совершенствования уголовного законодательства в контексте социальных тенденций информатизации / Н.В. Карчевский // NB: Вопросы права и политики. – 2013. – № 6 [Электронный ресурс]. – Режим доступа: http://e-notabene.ru/lr/article_8317.html.

10. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія / М. В. Карчевський ; МВС України, Луганський державний університет внутрішніх справ імені Е. О. Дідоренка. – Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. – 528 с.

11. Лісовий В. "Комп'ютерні" злочини: питання кваліфікації / В. Лісовий // Право України. – 2002. – № 2. – С. 86–88.

12. Правовая информатика и кибернетика : учебник / Г. А. Атанесян, О. А. Гаврилов, П. Дёри, А. Г. Каблуков, А. К. Караханьян, И. Ковачич, К. Ковачичне, В.В. Крылов, А. Малиновский, М. Г. Мальковский, Г. О. Матюшкин, Я. Петцель, Н. С. Полевой, Л. Д. Самыгин, Д. Д. Хан-Магомедов, И. Ханец, С. И. Цветков, Н. П. Яблоков ; [под ред. Н. С. Полевого]. – М. : Юридическая литература, 1993. – 528 с.

13. Скулиш Є. Д. Проблеми створення системи кримінально-правової охорони державної безпеки України / Є. Д. Скулиш // Основні напрями розвитку кримінального права та шляхи вдосконалення законодавства України про кримінальну відповідальність : матеріали міжнар. наук.-практ. конф., 11 12 жовтня 2012 р. / редкол.: В. Я. Тацій (голов. ред.), В. І. Борисов (заст. голов. ред.) та ін. – Х. : Право, 2012. – С. 41–46.

14. Супруненко А.М. Кіберзлочинність як особливий вид протиправної діяльності / А.М. Супруненко, М.С. Гожий // Боротьба з інтернет-злочинністю : матеріали міжнародної науково-практичної конференції (м. Донецьк, 12-13 червня 2013 р.). – Донецьк : ДЮІ МВС України, 2013. – С. 55–57.

УДК 343.86 (477)

Є.В. Літвінов

КРИМІНОЛОГІЧНИЙ ПОРТРЕТ ОСОБИ, ЯКА ВЧИНЯЄ ЗЛОЧИНИ У СУДОВІЙ СИСТЕМІ

Виконано аналіз концептуальних засад, поглядів та ідей щодо розуміння сутності структури особистості яка вчиняє злочини у судовій системі.

Ключові слова: *особистість, соціально-демографічні ознаки, морально-психологічні риси, запобігання, судова система.*

Выполнен анализ концептуальных основ, взглядов и идей относительно понимания сущности структуры личности, совершающей преступления в судебной системе.

Ключевые слова: *личность, социально-демографические признаки, морально-психологические черты, предотвращение, судебная система.*

The analysis of the conceptual framework of views and ideas on the understanding of the structure of the person who commits a crime in the judicial system.

Key words: *personality, socio-demographic characteristics, moral and psychological traits, the prevention of the judicial system.*

Поняття особистості злочинця є ключовим у теорії кримінології, оскільки саме воно надає практичну відповідь: чи обов'язково люди-