ГУМАНІТАРНА-ЭКАНАМІЧНЫ
ВЕСНІК

ГУМАНИТАРНО-
ЭКОНОМИЧЕСКИЙ
ВЕСТНИК

2'2010

УДК 343.13

БОРИЧЕВСКАЯ В.В.

УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

LEGAL AND CRIMINAL ASPECTS OF INFORMATION SECURITY OF THE CENTRE IN THE REPUBLIC OF BELARUS

Статья посвящена проблеме обеспечения информационной безопасности Республики Беларусь. Акцентировано внимание на основные меры обеспечения защиты информации, составной частью которых являются уголовно-правовые меры, направленные на противодействие наиболее опасным посягательствам на информационные общественные отношения. Дан анализ нормативно-правовым актам, которые регулируют информационные отношения, обеспечивают их правовую защиту. В настоящее время в Республике Беларусь система правовых норм, направленная на правовое обеспечение информационной безопасности находится в стадии развития. Наиболее важная роль в регулировании данных отношений принадлежит конституционному законодательству, являющемуся основой для отраслевого законодательства, прежде всего административного, уголовного и уголовно-процессуального. В то же время возникает необходимость формирования или преобразования соответствующих органов и государственных структур по обеспечению информационной безопасности.

The article deals with the problem of ensuring information security of the Republic of Belarus. The attention to basic measures to protect information, which are an integral part of criminal law measures aimed at countering the most dangerous attacks on the news public relations. The analysis of normative legal acts which regulate relations information, provide them with legal protection. Currently in the Republic of Belarus system of law, aimed at legal information security is under development. The most important role in regulating these relations belongs to the constitutional law is the basis for sector-specific legislation, primarily administrative, criminal and criminal procedure. At the same time there is the need to create or convert the relevant authorities and government agencies on information security.

Информационная сфера представляет собой самостоятельную сферу национальной безопасности, в которой необходимо обеспечить защиту информационных ресурсов, систем их формирования распространения и использования, информационной инфраструктуры, реализацию прав на информацию государства, юридических лиц, граждан.

В настоящее время создается разветвленная система общественных отношений, предметом которых является информация, хранящаяся, циркулирующая и обрабатываемая как в отдельных компьютерах, так и сетях ЭВМ. Развивающаяся система информационных взаимосвязей не избежала столкно-

вения с преступностью, использующей современные научно- технические достижения. Осознавая важность информации, общество приходит к пониманию опасности информационной преступности.

Развитие компьютерных технологий и повсеместное их внедрение позволяет совершать различные преступления с помощью компьютера. С использованием ЭВМ совершаются такие неправомерные действия, как не санкционированное копирование, уничтожение, блокирование или модификация информации, находящейся в компьютере. Под угрозой осуществления таких действий совершаются вымогательства денежных средств у банков, предприятий и т.п. Развитие компьютерных сетей позволило более быстро, анонимно и эффективно распространять различного рода негативную информацию (инструкции по изготовлению взрывных устройств, приготовлению наркотиков; призывы к совершению преступлений; порнографию и т.д.). Появились новые способы мошенничества, хищения, причинения имущественного ущерба, нарушения авторских прав и других преступлений, список которых довольно велик и постоянно растет. Особого внимания заслуживает проблема распространения и других вредоносных программ, способных причинить ущерб, исчисляемый в миллионах долларов, и нанести вред тысячам людей. Современный этап характеризуется устойчивой тенденцией роста компьютерных преступлений, как в Беларуси, так и во всем мировом информационном пространстве. В настоящее время в отечественной криминалистической науке не существует сколько-нибудь обобщенных данных для формирования понятий основных элементов характеристики компьютерных преступлений. Все еще не существует четкого определения понятия данного вида преступлений, и дискутируются различные точки зрения по их классификации. Сложность в формулировке этих понятий существует, по-видимому, как по причине невозможности выделения единого объекта преступного посягательства, так и множественности предметов преступных посягательств с точки зрения их уголовно-правовой охраны. Некоторые правоведы считают, что компьютерные преступления представляют собой все преступления, при котором компьютер является орудием, средством или целью их совершения, а другие объединяют под этим термином все противозаконные действия, которые причиняют ущерб имуществу и связаны с электронной обработкой информации. В Германии, например, полиция, использует определение киберпреступности как "все противозаконные действия, при которых электронная информация выступала средством либо объектом."

Обобщая различные точки зрения, можно сделать вывод о том, что в настоящее время существуют два основных течения научной мысли.

Одна часть исследователей относит к компьютерным преступлениям действия, в которых компьютер является либо объектом, либо орудием посягательств.

Исследователи же второй группы относят к компьютерным преступлениям только противозаконные действия в сфере автоматизированной обработки информации. В качестве главного классифицирующего признака, позволяюще-

го отнести эти преступления в обособленную группу, выделяется общность способов, орудий, объектов посягательств.

Иными словами, объектом посягательства является информация, обрабатываемая в компьютерной системе, а компьютер служит орудием посягательства.

Надо отметить, что законодательство многих стран стало развиваться именно по этому пути.

Следует отметить, что относительно объекта преступного посягательства двух мнений быть не может - им, естественно, является информация, а действия преступника следует рассматривать как покушение на информационные отношения общества. Но далее необходимо учесть, что если информация является не объектом, а средством покушения на другой объект уголовно-правовой охраны, то здесь необходимо делать различия в том, была ли это машинная информация, т.е. информация, являющаяся продуктом, произведенным с помощью или для компьютерной техники, либо она имела другой, "некомпьютерный" характер.

Главным этапом в криминализации компьютерных преступлений стало принятие нового Уголовного кодекса Республики Беларусь, в котором 31 глава содержит статьи (ст.ст.349-355), предусматривающие уголовную ответственность за преступления в сфере компьютерной информации.

Сравнивая позиции различных ученых-правоведов, было сформулировано свое понятие преступления в сфере компьютерной информации - предусмотренное уголовным законом, противоправное, виновное нарушение чужих прав и интересов, связанное с использованием, модификацией, уничтожением компьютерной информации, причинившее вред либо создавшее угрозу причинения вреда охраняемым законом правам и интересам физических и юридических лиц, общества и государства.

По мнению В.Н. Черкасова подобные преступные действия возможно осуществить путем: введения в ЭВМ неправильных данных (манипуляции по входу); фальсификации программ (программные манипуляции); изменения первоначально правильных данных (манипуляции по выходу). Причем манипуляции с системными программами могут осуществлять только специалисты узкого профиля - программисты. Проведение противозаконных операций с программами пользователей могли осуществлять только специалисты-аналитики.

Позволим себе не согласиться с мнением о проведении противозаконных операций с программами пользователей только специалистами-аналитиками. В настоящее время имеется множество литературы и компактных магнитных дисков, в которых общедоступным способом показаны возможные незаконные пути выявления паролей на системы защиты разных уровней. Если человек, свободно пользующийся международной системой Internet, обладает средним интеллектом, то он сможет незаконно проникнуть в файлы с чужой информацией, пусть и не охраняемой законом, используя советы более опытных хакеров, либо информацию из книг или компьютерных лазерных дисков.

Неправомерный доступ к охраняемой законом информации привлекал внимание многих исследователей, в частности таких как: Ю.М. Батурин, Н.Н. Безруков, С.В. Бородин, Т.А. Бушуева, В.В. Вехов, А.Г. Волеводз, А.М. Жодзишский, И.А. Клепицкий, В.С. Комиссаров, В.В. Крылов, В.Д. Курушин, В.А. Мазуров, В.А. Минаев, С.А. Пашин, Н.С. Полевой, С.В. Полубинская, А.Н. Попов, К.С. Скоромников, Н.Г. Шурухнов и другие. Большинство данных исследований носят преимущественно криминалистическую или криминологическую направленность.

Возникновение понятия «информационная безопасность» будет правильным соотносить с пониманием информации как важного ресурса экономического и социально-политического потенциала общества и государства. Несомненно, что это понятие распространяется и на жизнеобеспечение, жизнедеятельность личности, так как личность является основным субъектом в отношениях, регулируемых позитивным правом. Высшие приоритеты человека закреплены в Конституции РБ. Конституция, провозгласившая основные свободы человека, в том числе свободу информации (ст. 29, ч. 4), между тем, предусматривает в качестве гарантии их осуществления для каждого, возможные законодательным образом установленное регулирование этих свобод.

Основными мерами обеспечения информационной безопасности выступают правовые средства, составной частью которых являются уголовно-правовые меры, направленные на противодействие наиболее опасным посягательствам на информационные общественные отношения. Признание социальной ценности информации определяет необходимость комплексного уголовно-правового подхода к ее защите.

Важнейшей проблемой уголовно-правовых мер обеспечения информационной безопасности является проблема защиты информации от неправомерного доступа. Наличие данной проблемы заключается в том, что защите от неправомерного доступа подлежит наиболее ценная охраняемая законом информация, а также в том, что неправомерный доступ к охраняемой законом информации влечет, как правило, значительные общественно опасные последствия, в частности, нарушение ее конфиденциальности, целостности и доступности.

Вышеуказанные обстоятельства выступают причиной необходимости разработки системы преступлений в сфере информационных отношений, одной из составляющих которой должен выступить неправомерный доступ к охраняемой законом информации. При этом степень уголовно-правовой защиты информации должна определяться ее содержанием, а не свойствами носителя. Все это требует детальной разработки элементов нового общего состава преступления, заключающегося в неправомерном доступе к охраняемой законом информации.

В белорусском законодательстве предусмотрен достаточно обширный конгломерат норм, направленных на защиту конфиденциальной информации, информационных ресурсов, информации, составляющей государственную и иную тайну. Среди них как государственные правовые акты (кодексы, законы, указы, постановления), так и ведомственные документы (приказы, руководства,

положения, инструкции). Нормы, направленные на защиту информационных ресурсов страны, обеспечение информационной безопасности государства и граждан, которые осуществляют правовое регулирование информационных отношений, закреплены в таких законах Республики Беларусь как: «Об информации, информатизации и защите информации» (от 10.11.2008), «О государственных секретах» (от 04.01.2003),также в «Соглашении об обмене правовой информации» (от 24. 09.1993г.), в Постановлении Совета Министров РБ от 06.11.1992г «Об утверждении положения о коммерческой тайне», в Гражданском кодексе, Уголовном кодексе, а также нормативных актах об органах государственной безопасности, о связи, об информационном обеспечении экономического и социального развития, о патентах, об авторском праве и смежных правах и др.

Определенная «пестрота», широкий разброс правовых норм, сложность структуры законодательства Республики Беларусь в области обеспечения информационной безопасности обусловлен как самой историей формирования этого института права, так и разнообразием предмета ведения — конфиденциальной информацией, то есть документированной информацией, доступ к которой ограничивается в соответствии с законодательством республики, что, естественно, порождает определенные трудности в правоприменении. Конфиденциальная информация, по убеждению таких исследователей данной проблемы как Лукашова А.И. и Мухина Г.Н., - это наиболее широкое по объёму понятие среди иных понятий информации, действующих в сфере закрытых информационных ресурсов. Оно объединяет различные категории сведений, в том числе касающихся тайны личной жизни граждан, тайны голосования, профессиональной тайны, (врачебной, следственной, адвокатской, нотариальной и др.), тайны корреспонденции, телефонных и иных сообщений, коммерческой и банковской тайны, государственных секретов, тайны исповеди и др. [5.с.6]. Ныне действующее законодательство не содержит определения понятия конфиденциальная информация. В самом широком смысле слова конфиденциальная (от лат. confidenta - доверие) информация может быть определена как любая информация, находящаяся в распоряжении отдельного субъекта-носителя данной информации, раскрытие которой иными субъектами может привести к неблагоприятным для ее владельца последствиям[5.с.5]. В узком смысле слова конфиденциальная информация определена как документированная информация, доступ к которой ограничивается в соответствии с законодательством [7.с.212].

Отдельными актами законодательства определена конфиденциальная информация в зависимости от специфики отношений, попадающих под их регулирование. Так, ст. 1 Закона от 9 июля 1999г. «О депозитарной деятельности и центральном депозитарии ценных бумаг в Республике Беларусь» (НРПА. 1999.№ 56.2/61) под конфиденциальной информацией понимаются сведения о состоянии счетов «депо» депонента, сведения об операциях депонента по счетам « депо», адресные данные депонента и данные о его наименовании (фамилия, имя, отчество).

Правилами проведения клинических испытаний лекарственных средств, утвержденными приказом Министерства здравоохранения Республики Беларусь от 13 августа 1999 г. № 254 (НРПА.2000. №6. 8 /781), конфиденциальность обозначена как сохранение в тайне от неуполномоченных лиц информации, принадлежащей спонсору или позволяющей установить личность испытуемого.

Следовательно, конфиденциальная информация – наиболее широкое понятие, охватывающее практически все виды информации ограниченного доступа (включая составляющую государственную, служебную, коммерческую, банковскую, профессиональную, личную тайну), защищаемая в установленном законом порядке.

В Российской Федерации такое положение вызвало необходимость создания единого концептуального правового документа, во-первых, объединяющего результаты общего законотворчества, во-вторых, открывающего перспективы государственной организационной и законодательной политики в области обеспечения информационной безопасности.

Разработанная в 2000 году Советом безопасности «Концепция национальной безопасности РФ» и подписанная Президентом РФ В. Путиным «Доктрина информационной безопасности Российской Федерации» являются теми документами, которые определяют на перспективу содержание данной работы. Документы не только устанавливают границы правовой защиты информации, но и формируют основные методологические аспекты данной проблемы - характер национальных интересов в информационной сфере, виды угроз информационной безопасности, состояние, источники угроз, общие и особенные методы обеспечения информационной безопасности и др.

Понятие безопасности информационной получило достаточно стабильное выражение и правовое закрепление: «Информационная безопасность - состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства» (ФЗ РФ «Об участии в международном информационном обмене», ст. 2). С такой же содержательной основой это понятие вошло в Доктрину информационной безопасности РФ - «Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства» (Гл. 1, п. 1).

На первый взгляд действующее уголовное законодательство достаточно широко охватывает преступления в сфере компьютерной информации. Но это не совсем так. Еще в 1991 году Ю.М. Батурин предлагал внести в административный кодекс РФ нормы о несанкционированном доступе, разработке и использовании компьютерных вирусов, а затем и в уголовный кодекс РФ.

Батурин Ю.М. и Жодзишский А.М. предложили проект Закона "О защите гражданских прав и свобод в связи с компьютерной обработкой информации", состоящий из 4 глав. Думается, что данный закон облегчил деятельность не только правоохранительных органов, но и внес бы существенный порядок в

работу фирм и предприятий различных форм собственности. Однако проект опередил время.

Позднее Ю.М. Батурин предлагает Модель договора о взаимной компьютерной безопасности, направленного на осуществление контроля за компьютеризованными системами стран, подписавших данный договор. Для того чтобы подписание договора стало возможным, необходимо иметь слишком много конкретных данных, которыми автор, по понятным причинам, не обладал. Однако думается, что при наличии доброй воли воплотить эту модель в реальный Договор не является непреодолимой задачей. Основные положения данного Договора актуальны и в настоящее время, они могут регулировать достаточное количество деяний в международных отношениях в области компьютерной информации.

Анализ уголовно-правовых последствий неправомерного доступа к компьютерной информации, создания, использования и распространения вредоносных программ показал наличие достаточных оснований для введения дополнительных квалифицирующих признаков в составы некоторых статей УК Республики Беларусь.

Поскольку информация выступает средством организации самых разных сфер жизнедеятельности общества, то ее понятие уже предполагает отмеченную выше дифференцированность, а значит и некоторую несамостоятельность. Возможно, предположить, что информационная безопасность — это структурная часть более широкой системы. Структурная несамостоятельность понятия информационной безопасности замечена и другими учеными. Она может рассматриваться как составная часть национальной безопасности. Понятие информационной безопасности в теоретическом аспекте перспективнее соотносить с понятием политической безопасности, что открывает возможность оперировать им как политико-правовой категорией. В таком случае становятся очевидными политические приоритеты деятельности по созданию и укреплению системы информационной безопасности личности, общества и государства.

Новые информационные и информационно-телекоммуникационные технологии (ИТТ) открыли уникальные перспективы создания в мире единого информационного пространства, мирового информационного сообщества, создающие новые условия развития экономики, политики, культуры, образования, государственности, гражданского общества, личности.

Значение информации для жизнедеятельности и развития государства и общества (как и мирового сообщества в целом) невозможно переоценить. Она становится основой выработки и принятия решений любого уровня, а, следовательно, и основой управления. И сама информация является одним из основных объектов государственного управления, ибо информационные ресурсы становятся равными иным ресурсам, составляющим политический и экономический потенциал страны.

Однако нельзя не отметить ту особенность современных международных отношений в области информации, что чем прозрачнее, доступнее становится информация общего характера, тем тщательнее охраняются особые ее

сферы, важные для формирования национальной политики, приоритетных областей экономики, свидетельствующие о состоянии и перспективах обороноспособности, новейших промышленных и иных технологий, стратегических природных ресурсов и др. Мировой информационный рынок выступает не только сферой международного сотрудничества, но и конкуренции в том числе. Само собой разумеется, что законодательство любой страны, обеспечивающее участие и регулирующее поведение ее в информационном пространстве мира, должно предусматривать систему норм, обеспечивающих ее информационную безопасность.

Исследовательское внимание привлекает и институт информационной безопасности. Понятно, что его создание происходило на фоне эйфорически-ажиотажного стремления к повсеместному утверждению полной и окончательной свободы слова, информации, выражения мнений, а значит, происходило противоречиво, подчас в ущерб национальным интересам. Информационные ресурсы, наравне с иными важнейшими ресурсами, такими как трудовые резервы, природные ископаемые, финансы, интеллектуальный потенциал, культурные ценности, - есть достояние национального масштаба. Без них невозможно принимать эффективные управленческие и иные решения на всех уровнях власти.

Информационная безопасность структурно выглядит как сложная, но гармонично взаимодействующая, система организационных, технологических, технических, правовых мероприятий, осуществляемых государственными, общественными организациями, коммерческими структурами, ведомствами и отдельными гражданами с использованием методов и способов, не противоречащих действующему законодательству. Объектом защиты является секретная, конфиденциальная информация в ее целостном, то есть неискаженном, виде, а также информация специального назначения, предназначенная для решения задач в той или иной предметной или ведомственной области. Нас же интересуют в первую очередь политические и правовые аспекты указанного рода деятельности, в том числе: юридическое понятие безопасности и ее объекты; субъекты обеспечения информационной безопасности (в основном государство, осуществляющее функции защиты информации через органы законодательной, исполнительной и судебной властей); принципы обеспечения безопасности; основные функции системы информационной безопасности; руководство государственными органами в деле обеспечения информационной безопасности; контроль и надзор за деятельностью по обеспечению информационной безопасности и др.

Доступ к информации по закону есть условие национальной безопасности. Не государственной, в конкретном смысле этого слова, а именно национальной безопасности. В этом случае, подход к проблеме предусматривает интересы не только государства, но всего общества как единого организма с нормальными системами информационного обращения. Отечественные и зарубежные издания и средства массовой информации последних лет наводнены раз-

личными понятиями, обозначающими те или иные новые проявления криминального характера в информационной области.

Постепенно на наших глазах возникла информационная индустрия, чья самостоятельность и перспектива развития целиком и полностью зависели от точного регулирования правоотношений, возникающих при формировании и использовании информационных ресурсов. "Информационная революция" застигла страну в сложный экологический и политический период и потребовала срочного регулирования возникающих на ее пути проблем.

Сейчас, когда создан и принят ряд базовых нормативных актов в области информационных отношений, наступило время для их применения на практике, однако на этом пути неизбежны пробы и ошибки. И если такие ошибки, допущенные, например, в области хозяйственных отношений, могут быть тем или иным образом эффективно исправлены, то ошибки в области уголовно-процессуальных, уголовно-исполнительных отношений отражаются на конституционных правах и свободах конкретных граждан и носят необратимый характер.

Важно, что терминологическая неточность изложения закона или методологической рекомендации по его исполнению может повлечь неправильное его применение, а следовательно, и вышеуказанные негативные последствия. А этого допустить нельзя. Между тем, как известно, правовые механизмы могут быть включены и становятся эффективными лишь тогда, когда общественные отношения, подлежащие регулированию, в достаточной мере стабилизировались. Исходя из выше изложенного, мы можем сделать следующие выводы:

1)основные цели и задачи обеспечения информационной безопасности Республики Беларусь должны быть определены на базе устойчивых приоритетов национальной безопасности, отвечающих долговременным интересам общественного развития;

2)для создания и поддержания необходимого уровня защищенности объектов безопасности в Республике Беларусь должна быть создана система правовых норм, регулирующих отношения в информационной сфере. Система правовых норм, включает в себя совокупность относительно взаимосвязанных и внутренне согласованных основополагающих нормативных правовых актов, которые содержат юридические нормы и принципы, направленные на регулирование общественных отношений в сфере обеспечения информационной безопасности страны. В настоящее время в Республике Беларусь данная система правовых норм, находится в стадии развития. Наиболее важная роль в регулировании данных отношений, как уже было отмечено, принадлежит конституционному законодательству, являющемуся основой для отраслевого законодательства, прежде всего административного, уголовного и уголовно-процессуального;

4) должны быть определены и сформулированы основные направления деятельности органов государственной власти и управления в данной области;

5) возникает необходимость формирования или преобразования соответствующих органов и государственных структур по обеспечению националь-

ной безопасности (в том числе и информационной безопасности как ее составной части);

6) со стороны государства возникает необходимость в обеспечении механизма контроля и надзора за деятельностью соответствующих органов и государственных структур по обеспечению национальной безопасности, в том числе информационной безопасности.

---

1. Доктрина информационной безопасности Российской Федерации//Российская газета, 2000, 28 .09.

2. *Вехов В.Б.* Компьютерные преступления: способы совершения методики расследования. / В.Б.Вехов. - М., 1996. - 182 с.

3. Закон Республики Беларусь от 10.11.2008 № 455-З "Об информации, информатизации и защите информации// НРПА 26.11.2008, № 279, 2/1552,

4. *Копылов В.А.* Информационное право: Учебное пособие. / В.А Копылов - М.: Юристъ, 1997.- 472 с.

5. *Мухин Г.Н.* Конфиденциальная информация и коммерческая тайна: правовое регулирование и организация защиты / Под общей редакцией А.И. Лукашова. Мн., Тесей, 1998. С. 128.

6. *Северин, В.А.* Правовое обеспечение информационной безопасности предприятия : Учеб. - практ. пособие / МГУ им. М.В.Ломоносова. Юрид. фак. - М.: Городец, 2000. - 191 с.

7. *Тихомирова Л.В., Тихомиров М.Ю.* Юридическая энциклопедия. / Под ред. М.Ю.Тихомирова - М.: 1997 - 526 с.

8. *Юзвишин И.И.* Основы информациологии. Изд-е 2./-М.:Международное изд-во «Информациология», «Высшая школа», 2000.-517 с.

9. *.Ярочкин В.И.* Информационная безопасность. / В.И Ярочкин - М.: Междунар. отношения,2000. - 400 с.