3(58), 2007

Веснік

Гродзенскага дзяржаўнага універсітэта
імя Янкі Купалы

Навукова-тэарэтычны часопіс

Серыя 4

Праваznаўства
Псіхалогія

Выдаецца з сакавіка 1999 года адзін раз на квартал

Інфармацыйнае права і заканадаўства

ББК. 67.52

В.В. Боричевская

ТЕОРЕТИКО-ПРАВОВОЙ АНАЛИЗ НАУЧНЫХ КОНЦЕПЦИЙ И ПОЛОЖЕНИЙ, РЕГЛАМЕНТИРУЮЩИХ СОСТОЯНИЕ ВОПРОСА ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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 научным концепциям и положениям, которые регламентируют состояние вопроса об информационной безопасности. Отмечено, что в белорусском законодательстве предусмотрен достаточно обширный конгломерат норм, направленных на защиту конфиденциальной информации, информационных ресурсов, но признание социальной ценности информации определяет необходимость комплексного уголовно-правового подхода к ее защите. При этом степень защиты информации должна определяться ее содержанием, а не свойствами носителя.

Современный период развития цивилизации характеризуется переходом от индустриального общества к обществу информационному. Информация признается все более значимым видом общественных ресурсов, требующим, как и любая другая ценность, принятия соответствующих мер

защиты от неправомерных действий. Все более актуальной становится проблема обеспечения информационной безопасности как одной из составляющих национальной безопасности Республики Беларусь.

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.

Неправомерный доступ к охраняемой законом информации привлекал внимание многих исследователей, в частности таких как: Ю.М. Батурин, Н.Н. Безруков, СВ. 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, СВ. 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.

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 информатизации» (от 06.09.1995), «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 А.И. Лукашова и Г.Н. Мухина, – 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, коммерче-ской и банковской тайны, государственных секретов, тайны исповеди и др. [1, 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 [1, с. 5]. В узком смысле слова конфиденциальная информация определена как документированная информация, доступ к которой ограничивается в соответствии с законодательством [2, 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), защищаемой 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 информационной безопасности все более утверждается в политической, юридической и информациологической литературе. В.И. Ярочкин, ссылаясь на законодательство, определяет ее как «состояние защищенности информационной сферы общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств» [3, с. 6].

В.А. Северин также близок к этому определению. Под информационной безопасностью он понимает состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз. Задачи защиты информационных ресурсов он видит в изучении форм, способов, методов выявления и предупреждения опасности в информационной сфере [4, с. 5].

Подобно Ярочкину, считает и известный российский информациолог И.И. Юзвишин [5, с. 366].

Дальнейшее осмысление безопасности, как научной проблемы, требует уточнений основных понятий, которые тесно взаимодействуют между собой. В ряду вообще существующих понятий безопасности, в основу которых положен видовой принцип, наиболее общим, как нам представляется, является понятие национальной безопасности; содержание его включает (полностью или частично) содержание других видов безопасности, в том числе, безопасности информационной.

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).

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 столкновения 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 несанкционированное 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».

Ю.М. Батурин считает, что компьютерных преступлений как особой группы преступлений в юридическом смысле не существует, однако при этом отмечает, что многие традиционные виды преступлений модифицировались из-за вовлечения в них вычислительной техники и поэтому правильнее было бы говорить лишь о компьютерных аспектах преступлений, не выделяя их в обособленную группу.

Другого, более определенного взгляда придерживается А.Н. Караханьян. Под компьютерными преступлениями он понимает противозаконные действия, объектом или орудием совершения которых являются электронно-вычислительные машины.

Но вот в чем заключается еще одно разногласие – в самом понятии, в определении, как обозначить данный вид преступлений: компьютерный или информационный, а может быть, компьютерно-информационные? Бытуют различные точки зрения. Например, В.В. Крылов считает, что подход, согласно которому в законодательстве следует отражать конкретные технические средства, себя не оправдывает и поэтому нецелесообразно принимать термин «компьютерные преступления» за основу для наименования в криминалистике всей совокупности преступлений в области информационных отношений. Компьютер, по его мнению, является лишь одной из разновидностей информационного оборудования и проблемами использования этого оборудования не исчерпывается совокупность отношений, связанных с обращением конфиденциальной документированной информации. Крылов предлагает рассматривать в качестве базового понятия «информационные преступления», исходя из того, что сложившаяся система правоотношений в области информационной деятельности, позволяет абстрагироваться от конкретных технических средств. Он делает вывод, что преступление в области компьютерной информации, выделенные в отдельную главу УК РФ, являются частью информационных преступлений, объединенной общим инструментом обработки информации – компьютером.

С точкой зрения законодателя не расходится В.Б. Вехов, определяя в своей работе данный вид преступлений как компьютерные преступления. В своих определениях «компьютерного преступления» Вехов четко акцентирует внимание на том, что это «... предусмотренные уголовным законом общественно опасные действия...».

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, позволяющего 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 РБ, в котором 31 глава содержит статьи (349–355 УК РБ), 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.

Весьма важным вопросом является вопрос об объективных границах преступного действия. По мнению И.М. Тяжковой, действие, будучи внешним актом противоправного общественно опасного поведения субъекта, начинается с момента совершения первого осознанного и волевого телодвижения. Такими действиями являются не только действия, «которые направлены на причинение вреда охраняемым общественным отношениям», но и «приготовительные действия, приискание соучастников и пр.

Проблемами способа совершения компьютерных преступлений занимались многие ученые, среди которых хотелось бы выделить следующих: Ю.М. Батурин, В.Б Вехов, В.В. Крылов, С.И. Ушаков и другие.

В настоящее время не существует единых нормативных правил, определяющих порядок защиты информации, которые служили бы основой для действия статьи 349 УК РБ, хотя, по нашему мнению, это необходимое условие правильной квалификации подобных действий. Целый ряд нормативных актов, которые устанавливают общие требования к условиям эксплуатации настольно-издательских систем с видео терминальными устройствами.

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 вре-

доносных программ показал наличие достаточных оснований для введения дополнительных квалифицирующих признаков в составы некоторых статей УК РБ.

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 деятельно-сти, 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 безопасностью 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 различными 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 экологиче-ский и политический период и потребовала срочного регулирования возникающих на ее пути проблем.

Между тем, как известно, правовые механизмы могут быть включены и становятся эффективными лишь тогда, когда общественные отношения, подлежащие регулированию, в достаточной мере стабилизировались.

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-репрессивной 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.

Литература

1. Лукашов, А.И., Мухин, Г. Н. Конфиденциальная информация и коммерческая тайна: правовое регулирование и организация защиты / А.И. Лукашов, Г. Н. Мухин. – Минск.: Тесей, 1998.

2. Тихомирова, Л.В., Тихомиров, М.Ю. Юридическая энциклопедия / Л.В. Тихомирова, М.Ю. Тихомиров. – М., 1997.

3. Ярочкин, В.И. Информационная безопасность / В.И. Ярочкин. – М.: Междунар.отношения, 2000.

4. Северин, В.А. Правовое обеспечение информационной безопасности предприятия / В.А. Северин. – М.: Городец, 2000.

5. Юзвишин, И.И. Основы информациологии / И.И. Юзвишин. – М.: Международное изд-во «Информациология», «Высшая школа», 2000.

6. Вехов, В.Б. Компьютерные преступления / В.Б. Вехов. – М., 1996.

7. Копылов, В.А. Информационное право: учебное пособие / В.А. Копылов. – М.: Юристь, 1997.

8. Доктрина информационной безопасности Российской Федерации // Российская газета. – 2000.

9. Вехов, В.Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов. – М., 1996.

Поступила в редакцию 04.07.2007.

Боричевская Валентина Васильевна, соискатель кафедры криминалистики и уголовного процесса ГрГУ им. Я. Купалы. Научный руководитель – кандитдат юридических наук, доцент кафедры уголовного процесса и криминалистики ГрГУ им. Я. Купалы В.С. Соркин.

An up-to-date period of civilization development is characterized by the transition from industrial to information society. Information is identified as a more and more important kind of social resources, demanding, as any other values taking corresponding protection measures against illegal actions. Realizing information importance, society is coming to the understanding of the information crime danger. The problem of providing information security, as one of the components of national security of the Republic of Belarus is becoming more topical.