КАЛИНИНГРАДСКИЙ ЮИ МВД РОССИИ

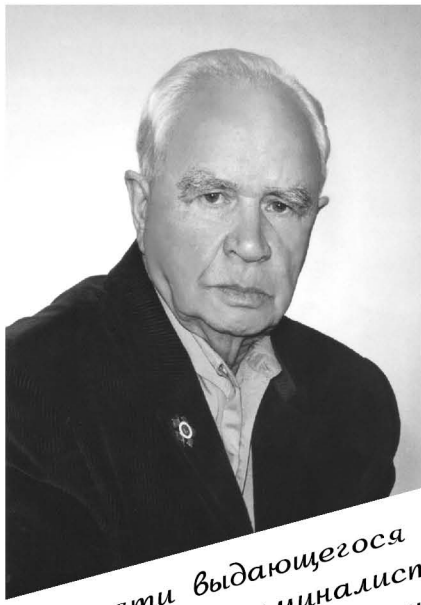
ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ: ПРОБЛЕМЫ, ТЕНДЕНЦИИ, ПЕРСПЕКТИВЫ

СБОРНИК НАУЧНЫХ СТАТЕЙ

КАЛИНИНГРАД, 2007

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ: ПРОБЛЕМЫ, ТЕНДЕНЦИИ, ПЕРСПЕКТИВЫ

СБОРНИК НАУЧНЫХ СТАТЕЙ



Памяти выдающегося российского криминалиста профессора Р.С. Белкина посвящается

Калининград – 2007

УДК 34
ББК 67
И 74

И 74 **Информационное обеспечение правоохранительной деятельности: проблемы, тенденции, перспективы.** Сборник научных статей. – Калининград: Калининградский ЮИ МВД России, 2007. – 244 с.

ISBN 5-93919-031-6

В предлагаемом сборнике научных статей, посвященном памяти выдающегося криминалиста современности, заслуженного деятеля науки РФ, доктора юридических наук, профессора Р.С. Белкина, исследуются современные проблемы, тенденции и перспективы развития информационного обеспечения правоохранительной деятельности в России и за рубежных странах.

Предназначен для научных работников, преподавателей, аспирантов и адъюнктов учебных заведений МВД России, юридических вузов и факультетов, а также для работников правоохранительных органов.

ISBN 5-93919-031-6

УДК 34
ББК 67

В.В. БОРИЧЕВСКАЯ
Гродненский государственный
университет имени Я.Купалы

В.С. СОРКИН
кандидат юридических наук, доцент
Гродненский государственный
университет имени Я.Купалы

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

В статье дается теоретико-правовой анализ научных концепций и положений, регламентирующих состояние вопроса об информационной безопасности. Терминологическая неточность изложения закона или методологической рекомендации по его исполнению может повлечь неправильное его применение, а следовательно, и негативные последствия.

The article presents theoretical-legal analysis of the scientific concepts and proviso regulating the issue of information safety. Terminological imprecision in interpretation of the law or in methodological recommendations on its enforcement may lead to the incorrect application of same and, hence, to negative consequences.

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.

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.

Определенная «пестрота», широкий разброс правовых норм, сложность структуры законодательства Республики Беларусь в области обеспечения информационной безопасности обусловлен как самой историй

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. [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].

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, со-

стояние, 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).

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 информа-

ции – 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 услови-

ям эксплуатации настольно-издательских систем с видеотерминальными 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 вредоносных 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 поли-

тические приоритеты деятельности по созданию и укреплению системы информационной безопасности личности, общества и государства.

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.

СПИСОК ЛИТЕРАТУРЫ

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

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

3. Ярочкин В.И. Информационная безопасность. – М., 2000.

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

5. Юзвишин И.И. Основы информациологии. – М.: «Высшая школа», 2000.

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

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

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

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

СВЕДЕНИЯ ОБ АВТОРАХ

АВДЕЕВА Г.К. – кандидат юридических наук, ведущий научный сотрудник Института изучения проблем преступности Академии правовых наук Украины;

АРЕФЬЕВ А.Ю. – кандидат юридических наук, доцент, доцент кафедры оперативной работы ОВД Нижегородской академии МВД России;

БОРИЧЕВСКАЯ В.В. – соискатель кафедры криминалистики и уголовного процесса Гродненского государственного университета имени Я. Купалы;

БУЛГАКОВ В. Г. – кандидат технических наук, доцент, доцент кафедры криминалистической техники Волгоградской академии МВД России;

ВИНИЦКИЙ Л.В. – доктор юридических наук, профессор, профессор кафедры криминалистики Смоленского филиала Московского университета МВД России;

ВОЛЧЕЦКАЯ Т.С. – доктор юридических наук, профессор, заведующая кафедрой уголовного процесса, криминалистики и правовой информатики Российского государственного университета имени И. Канта;

ГАЕВОЙ А.И. – кандидат юридических наук, доцент, доцент кафедры предварительного расследования Краснодарского университета МВД России;

ГРИГОРЬЕВ А.Н. – кандидат юридических наук, старший преподаватель кафедры информационного обеспечения ОВД Калининградского юридического института МВД России;

ГУРЬЯНОВ К.В. – кандидат технических наук, доцент, доцент кафедры информатики и применения компьютерных технологий в раскрытии преступлений Саратовского юридического института МВД России;

ДРОНОВА О.Б. – кандидат юридических наук, преподаватель кафедры криминалистической техники Волгоградской академии МВД России;

ЖУК М.Г. – кандидат юридических наук, доцент, декан юридического факультета Гродненского государственного университета имени Я. Купалы;

ЗГАДЗАЙ О.Э. – кандидат физико-математических наук, доцент, начальник кафедры экономики, правовой статистики, математики и информатики Казанского юридического института МВД России;

ЗОТЧЕВ В.А. – кандидат юридических наук, доцент кафедры криминалистической техники Волгоградской академии МВД России;

СОДЕРЖАНИЕ

АВДЕЕВА Г.К. Использование специальных знаний в борьбе с преступностью с целью повышения эффективности фиксации доказательственной информации 4

АРЕФЬЕВ А.Ю. Функционирование подразделений оперативно-розыскной информации в системе предупредительного воздействия на преступность (теоретико-прикладной аспект) 10

БОРИЧЕВСКАЯ В.В., СОРКИН В.С. Теоретико-правовой анализ научных концепций и положений, регламентирующих состояние вопроса об информационной безопасности 16

БУЛГАКОВ В.Г. Применение информационных технологий в криминалистическом исследовании динамических признаков человека 23

ВИННИЦКИЙ Л.В., КУЗНЕЦОВА И.В. К вопросу о своевременности расследования незаконной порубки деревьев и кустарников (на примере Челябинской области) 28

ВОЛЧЕЦКАЯ Т.С. Особенности криминалистической характеристики торговли людьми 34

ГАЕВОЙ А.И. К вопросу об использовании современных информационных технологий в борьбе с хищениями нефти и нефтепродуктов из трубопровода 41

ГРИГОРЬЕВ А.Н. Методологические аспекты формирования криминалистической концепции информации 47

ГУРЬЯНОВ К.В. Производство контрафактных экземпляров компьютерных программных продуктов как разновидность организованной экономической преступности 60

ДРОНОВА О.Б. Направление развития криминалистического учета поддельных денежных знаков 68

ЖУК М.Г. Информационно-аналитические подходы к обеспечению экономической безопасности 73

ЗГАДЗАЙ О.Э. Информационные технологии в оперативно-служебной деятельности органов внутренних дел по Республике Татарстан: история и перспективы развития 79

ЗОТЧЕВ В.А. Информационная и криминалистическая характеристика цифрового фотографического процесса 87

ИВАНОВ Н.А. Использование специальных программных и аппаратных средств для обеспечения доступа к компьютерной информации 93

ИШИН А.М. К вопросу об информационном обеспечении борьбы с терроризмом 99

КАРЕТНИКОВ М.К. Особенности оборота специальных информационных технологий 106

КОЛОТУШКИН С.М., САФОНОВ А.А. Концепция создания и использования информационно-аналитической базы следов применения огнестрельного оружия в раскрытии и расследовании преступлений, связанных с терроризмом 113

КРАВЧУК Л.С., КЮНЭ Э. Информационный менеджмент в образовательной и практической деятельности полиции Германии 117

КРАМАРЕНКО В.П. Основные направления развития информационных криминалистических технологий в борьбе с транснациональной преступностью 124

КУЗНЕЦОВА О.Д., ПЕРСИЧКИНА Н.В. Компьютерные технологии при рассмотрении судом уголовных дел 130

КУРИН А.А. Геоинформационные технологии в функционировании системы криминалистической регистрации ... 136

МАРКОВИЧЕВА Е.В., КОНИН В.В. Возможности получения и использования информации о личности обвиняемого на стадии предварительного расследования 143

МЕШКОВ В.М. Взаимосвязь достоверной криминалистической информации и учения о временных связях в деятельности следователя 146

НОВИКОВ А.А. Исторические предпосылки появления института специалиста в уголовном судопроизводстве России 151

ПАНЬКИНА И.Ю. Основные элементы внесудебного способа разрешения уголовно-процессуального конфликта 157

САФОНОВ А.А., ИСАЧЕНКО Н.П., КОЛЕСНИЧЕНКО П.Г. Влияние информационных потоков на организацию дактилоскопических учетов 163

СИМИНЯГИН А.Ю. Отдельные вопросы выявления компьютерных данных, представляющих оперативный интерес 168

СИМИНЯГИН Д.Ю. Актуальные проблемы борьбы с кибернетической преступностью и некоторые вопросы информационного обеспечения специальных подразделений 173

СМУШКИН А.Б. К вопросу о доказательственной информации, получаемой при задержании 177

СРЕТЕНЦЕВ Д.Н. Некоторые результаты анализа научных подходов по вопросу информационного обеспечения судебно-экспертной деятельности 183

ТЕЛЕГИНА Т.Д. О возможности признания правовых знаний специальными в уголовном процессе России 190

ФАДЕЕВА В.В. Подготовка специалистов ОРД МВД России в условиях современного информационного общества 196

ХИЛЮТА В.В. Информационное обеспечение деятельности по расследованию «кредитных» преступлений и проблемы доказывания 199

ХОЛОПОВА Е.Н. Информационное обеспечение деятельности экспертов-психологов: проблемы теории и практики 207

ЧЕНГАЕВА Р.В. Основной элемент состязательного уголовного процесса (информационный компонент) 212

ШАБАНОВ В.Б., КАШИНСКИЙ М.Ю. Правовые проблемы совершенствования предупреждения аутодеструктивного поведения в учреждениях уголовно-исполнительной системы 215

ШЕПИТЬКО В.Ю. Типовые тактические операции в системе информационного обеспечения следственной деятельности 223

ШОШИН С.В. Некоторые проблемы информационного обеспечения деятельности органов МВД России на современном этапе 229