осуществлении своих полномочий они нередко вступают в конфликты с подчиненными, разрешают возникшие противоречия с помощью административно-командных методов.

Подавляющее большинство лиц, совершающих подобные мошенничества, в целом характеризуются положительно. Как правило, лишь небольшой процент от общего числа лиц, совершивших мошенничество, связанного с получением кредита в банке, имели отрицательные характеристики, и то после совершения преступления.

При этом зачастую отсутствует информация о причастности к преступлениям лиц, склонных к алкоголизму и наркомании, либо страдающих теми или иными видами психических расстройств.

Финансовые институты не прилагают достаточных усилий для защиты от нечистых на руку сотрудников. Это характерно для всего мирового сообщества. В докладе Ernst & Young, составленном на базе опроса 100 немецких финансовых институтов, отмечается, что проблемой мошенничества в рядах своих собственных работников серьезно занимаются лишь 37% банков. Наиболее притягательными для мошенников являются подразделения для торговли ценными бумагами (61% опрошенных) и банковская розница (56%). При этом 29% респондентов считают, что за последние годы риски мошенничества возросли [8].

Заключение. Сведения о свойствах личности субъекта кредитных мошенничеств являются важным элементом характеристики данного вида преступлений, а проблемы в отсутствии законодательного определения субъекта данного состава позволяют сделать вывод о том, что законодательство требует изменений, а правоприменительная практика остается несовершенной и требует доработки. На наш взгляд, необходимо создать эффективный организационно-правовой механизм регулирования финансово-кредитного сектора экономики, который позволил бы кредиторам использовать на законных основаниях различные средства защиты от мошенничеств.

Список источников

1. Криминология : учеб. для вузов / под ред. проф. В. Д. Малкова. — 4-е изд., перераб. и доп. — М. : Юстицинформ, 2011. — 86 с.
2 Официальный сайт Федеральной службы государственной статистики РФ (Росстат) [Электронный ресурс]. — Режим доступа: http://www.gks.ru . — Дата доступа: 17.11.2016.
3. *Данилов, Д. А.* Мошенничество в кредитно-банковской сфере / Д. А. Данилов // Пробелы в рос. законодательстве. — 2014. — № 1. — С. 206—209.
4. *Кочерга, В. В.* Криминологические и уголовно-правовые меры противодействия преступлениям, посягающим на интересы кредиторов : автореф. дис. … канд. юрид. наук : 12.00.08. / В. В. Кочерга. — М., 2011. — 25 с.
5. Бизнес. Толковый словарь экономических терминов [Электронный ресурс]. — Режим доступа: http://www.bibliotekar.ru /biznes-15/ . — Дата доступа: 17.11.2016.
6. *Отряхин, В. И.* Методика расследования хищений в сфере банковской деятельности : дис. … канд. юрид. наук : 12.00.09 / В. И. Отряхин. — М., 2001. — 62 л.
7. *Полянский,* А. Ю. Уголовно-правовые аспекты мошенничества в сфере кредитования / А. Ю. Полянский // Вестн. Омского ун-та. — 2014. — № 1 (38). — С. 124—127.
8. Ernst & Young [Electronic resource]. — Access mode: http://www.ey.com/ . — Date of access: 17.11.2016.

УДК 343.53

Ю. В. Харчейкина
Национальный центр законодательства и правовых исследований Республики Беларусь, Минск

ТОЛКОВАНИЕ ПОНЯТИЯ «НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ СИСТЕМЕ»

Введение. Интенсивное развитие информационного общества обусловило появление в УК Республики Беларусь, введенном в действие с 1 января 2001 года, главы 31, закрепившей в семи статьях уголовную ответственность за преступления против информационной безопасности, ранее неизвестные белорусскому законодательству.

В настоящее время указанные преступления хотя и занимают незначительную долю в общей структуре преступности, однако имеют устойчивую тенденцию к ежегодному росту, что ставит перед правоохранительными органами задачу их раскрытия, расследования и правильной правовой оценки.

Изучение уголовных дел свидетельствует о наличии проблемных аспектов, связанных с отсутствием однообразного подхода к квалификации деяний, подпадающих под признаки составов преступлений, предусмотренных ст. 349—355 УК Республики Беларусь. Одной из причин является использование законодателем бланкетных диспозиций, что в свою очередь влечет отсутствие у органов уголовного преследования единого понимания и определения сущности используемых в уголовном законе узкоспециальных технических терминов и понятий.

Основная часть. При криминализации деяний в сфере информационной безопасности в уголовный закон были включены термины, не свойственные для традиционного уголовно-правового описания способов действия. К их числу относится термин «несанкционированный доступ» [1, с. 140].

В ст. 349 УК Республики Беларусь несанкционированный доступ к компьютерной информации выступает в качестве общественно опасного деяния, а в ч. 2 ст. 350 и ч. 2 ст. 351 «несанкционированный доступ к компьютерной системе или сети» выступает в качестве квалифицирующего признака модификации компьютерной информации и компьютерного саботажа. Отметим, что несанкционированный доступ к компьютерной информации и несанкционированный доступ к компьютерной системе не равнозначные понятия.

Исходя из определения информации в ст. 1 Закона Республики Беларусь от 10 ноября 2008 года «Об информации, информатизации и защите информации», а также содержания диспозиции ч. 1 ст. 349 УК Республики Беларусь, компьютерную информацию можно определить как сведения о лицах, предметах, фактах, событиях, явлениях и процессах, хранящиеся в компьютерной системе, сети или на машинных носителях.

Законодательное разъяснение термина «компьютерная система» отсутствует. В ст. 1 Закона Республики Беларусь «Об информации, информатизации и защите информации» дано лишь определение информационной системы, под которой понимается совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств [2].

Техническая литература к компьютерной системе относит совокупность аппаратных средств, управляемых ПО (операционной системой) как единый модуль [3]. В международном праве компьютерная система описана как любое устройство или группа взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных [4].

Комментарий к УК Республики Беларусь предлагает под компьютерной системой понимать организационно упорядоченную совокупность массивов информации и ИТ, реализующую информационные процессы, образующим элементом которой является хотя бы одна ЭВМ [5, с. 762].

Таким образом, в широком смысле компьютерная система является совокупностью трех составляющих элементов: аппаратного обеспечения, ПО и информации.

Несанкционированным в юридической литературе и правоприменительной деятельности понимается доступ, совершенный с несоблюдением, невыполнением установленных правил, т. е. с нарушением системы защиты. Результатом подобных действий применительно к компьютерной системе будет успешное преодоление программной, аппаратной или комплексной защиты, получение возможности управления компьютерной системой, ознакомление лица с хранящейся в ней компьютерной информацией, совершение с нею любых действий по усмотрению виновного лица.

При этом получение доступа к информации осуществляется правонарушителем в несколько этапов. На первом этапе решаются задачи получения тем или иным способом доступа к аппаратным и программным средствам компьютерной системы. На втором этапе решаются задачи внедрения аппаратных или программных средств в целях воздействия на информацию.

В то же время современные компьютерные системы многофункциональны, зачастую высоконагружены, могут иметь одновременно много пользователей с регламентацией прав доступа и сложную архитектуру с точки зрения построения систем, включают множество компонентов и подсистем. При этом доступ может быть осуществлен лишь к части компьютерной системы, к ее элементу либо к защищенной компьютерной информации при открытой системе, либо правомочным пользователем с нарушением его прав доступа к определенному компоненту системы и т. п.

Анализ следственно-судебной практики показывает, что при многообразии способов совершения преступления единый подход к определению содержания понятия «несанкционированный доступ к компьютерной системе» не выработан.

В одних случаях, исходя из определения компьютерной системы как устройства, в качестве несанкционированного доступа к компьютерной системе рассматривался лишь взлом компьютерной системы с его управляющей консоли, т. е. физический непосредственный доступ к компьютеру без разрешения на то собственника, владельца или законного пользователя аппаратного средства; в других случаях несанкционированным доступом являлся и удаленный доступ к системе управления компьютера; в-третьих, несанкционированный доступ к компьютерной системе рассматривался как понятие, тождественное доступу к информации, и охватывал несанкционированный доступ к любым отдельным элементам системы.

Так, приговором суда Октябрьского района г. Гродно от 29.08.2016 К. осужден по ч.1 ст. 351 УК Республики Беларусь. Установлено, что он, используя принадлежащую ему компьютерную технику и доступ к глобальной компьютерной сети Интернет, располагая сведениями о реквизитах входа на страницы двух потерпевших на сайте по адресу www.vk.com, заменил пароли, что повлекло за собой невозможность использования потерпевшими принадлежащих им страниц до момента инициации процедуры восстановления доступа. Действия К. квалифицированы как умышленное блокирование компьютерной информации.

В то же время судом Лидского района 15.02.2016 С. осужден по ч. 2 ст. 351 УК Республики Беларусь. Он признан виновным в том, что используя в качестве орудия преступления личный персональный компьютер, имеющий доступ к глобальной компьютерной сети Интернет, в результате несанкционированного доступа к компьютерной системе ООО «ВКонтакте», находящейся по адресу: Российская Федерация, г. Санкт-Петербург, Лиговский проспект, 61 литер А, получив доступ к информации, содержащейся в учетной записи потерпевшей на странице в социальной сети «ВКонтакте», осуществил блокирование содержащейся на ней

компьютерной информации, выразившееся в установлении нового пароля, изменив таким образом реквизиты доступа к учетной записи, что повлекло невозможность использования ее законным владельцем.

Действия С. получили юридическую оценку как умышленное блокирование компьютерной информации, сопряженное с несанкционированным доступом к компьютерной системе.

Возражением избранной в последнем случае позиции может являться то, что сайт «ВКонтакте» не относится к закрытому сетевому ресурсу. Регистрация пользователя на сайте является бесплатной, добровольной и общедоступной. Выбранные пользователем при регистрации логин и пароль — способ защиты информации его личной страницы, а не компьютерной системы ООО «ВКонтакте».

Приведенные примеры наглядно иллюстрируют отсутствие единообразных подходов при квалификации общественно опасных деяний, сопряженных с несанкционированным доступом к компьютерной системе.

Заключение. В силу широкого использования компьютерной техники во многих сферах деятельности, многообразия способов и видов компьютерных преступлений, в целях успешного выявления и пресечения противоправных деяний в рассматриваемой сфере представляется необходимым глубокое теоретическое осмысление практики применения законодательства об информационных отношениях и совершенствование на этой основе уголовно-правовых норм противодействия преступности, в том числе путем правового толкования понятий и терминов, применяемых при описании правонарушений против информационной безопасности.

Обоснованным является вывод о том, что без решения этой, казалось бы, сугубо формальной задачи невозможно однозначно формулировать любые соображения в данной области. В противном случае из-за различной трактовки понятий и терминов любые замечания и предложения будут пониматься неоднозначно [6, с. 295].

Список источников

1. *Ахраменка, Н. Ф.* Проблемные вопросы судебной практики по квалификации преступлений против информационной безопасности / Н. Ф. Ахраменко // Судебная практика в контексте принципов законности и права : сб. науч. тр. / редкол.: В. М. Хомич (гл. ред.) [и др.]. — Минск : Тесей, 2006. — С. 138—147.

2. Об информации, информатизации и защите информации [Электронный ресурс] : Закон Респ. Беларусь, 10 нояб. 2008 г., № 455-З : в ред. Закона Респ. Беларусь от 11.05.2016 г. № 362-З // Национальный правовой Интернет-портал Республики Беларусь, 17.05.2016, 2/2360.

3. ГОСТ Р ИСО/МЭК ТО 10032-2007 : Эталонная модель управления данными [Электронный ресурс] // Федеральное агентство по техническому регулированию и метрологии. — Режим доступа: http://www.gost.ru/wps/portal/pages/main. — Дата доступа: 30.01.2017.

4. Конвенция о преступности в сфере компьютерной информации, 23 ноября 2001 г. [Электронный ресурс]. — Режим доступа: http://base.garant.ru/4089723/ . — Дата доступа: 17.11.2016.

5. Научно-практический комментарий к Уголовному кодексу Республики Беларусь / Н. Ф. Ахраменка [и др.] ; под общ. ред. А. В. Баркова, А. В. Хомича. — Минск : ГИУСТ БГУ, 2007. — 1007 с.

6. *Быков, В. М.* Преступления в сфере компьютерной информации: криминологические, уголовно-правовые и криминалистические проблемы : монография / В. М. Быков, В. Н. Черкасов. — М. : Юрлитинформ, 2015. — 328 с.

УДК 343.415

С. А. Цюга

Учреждение образования «Брестский государственный университет имени А. С. Пушкина», Брест

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ИЗБИРАТЕЛЬНОГО ЗАКОНОДАТЕЛЬСТВА (НА ПРИМЕРЕ РЕСПУБЛИКИ БЕЛАРУСЬ И РЯДА ЗАРУБЕЖНЫХ СТРАН)

Введение. Важнейшим политическим правом гражданина является право избирать и быть избранным, позволяющее участвовать в осуществлении государственной власти. Это право должно быть обеспечено высокой степенью защиты, так как является гарантией реализации гражданами прав и свобод в избирательном процессе.

Изучение института уголовной ответственности за преступления против избирательных прав граждан Республики Беларусь, Российской Федерации и ряда зарубежных стран будет полезным для совершенствования норм УК Республики Беларусь. В силу того, что избирательные процедуры происходят с определенной периодичностью, накопление опыта уголовно-правовой охраны в данной сфере конституционных правоотношений представляется особо актуальным.

Основная часть. В Республике Беларусь в настоящее время идет активный процесс совершенствования избирательного законодательства, в том числе и в области правовой регламентации ответственности за совершение в ходе проведения избирательных кампаний правонарушений различного характера. «Проблема обеспечения конституционной законности в реализации избирательных прав граждан, установленного порядка выборов от преступных посягательств, выстраивания уголовного законодательства в соответствии с конституционными принципами является постоянной составляющей уголовной политики, в том числе и связанной