***V.M. Veremeenko**, Candidate of Juridical Sciences, Associate Professor, Associate Professor at the Department of Operational-Investigative activity of the Faculty of Militia of the Academy of the MIA of the Republic of Belarus*

THE SUBJECTIVE SIDE OF THE CRIMES CONCERNING THE BRIBERY: PECULIARITIES OF THE CRIMINAL AND LEGAL CHARACTERISTICS

The subjective side of crimes provided for in Art. 430–432 of the Criminal Code of the Republic of Belarus is analyzed. It discusses various points of view on the topic under study. Particular attention is given to characterizing such signs of the subjective side of the acts being analyzed, as a motive and purpose. Authors own judgments and suggestions on the discussion issues of this problem are expressed.

Keywords: bribery, the subjective side of crimes concerning the bribery, fault, motive and purpose.

УДК 340

***М.А. Дубко**, следователь по особо важным делам управления анализа практики и методического обеспечения предварительного расследования центрального аппарата Следственного комитета Республики Беларусь*
(e-mail: mihail-dubko@tut.by)

СОВЕРШЕНСТВОВАНИЕ УГОЛОВНО-ПРАВОВОЙ РЕГЛАМЕНТАЦИИ ОТВЕТСТВЕННОСТИ ЗА НЕПРАВОМЕРНОЕ ЗАВЛАДЕНИЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИЕЙ (ст. 352 УК)

Рассматриваются теоретические вопросы установления уголовной ответственности за неправомерное завладение компьютерной информацией и направления совершенствования уголовно-правовой регламентации ответственности за данное деяние. Изучаются вопросы криминализации информационных преступлений сквозь призму правового режима информации. Сформулированы предложения по изменению уголовного закона в части ответственности за различные формы противоправного получения информации.

Ключевые слова: информационная безопасность, завладение компьютерной информацией, несанкционированное копирование, криминализация.

Более десяти лет назад в статье Н.Ф. Ахраменка «Преступления против информационной безопасности: краткий реестр проблем» рассматривались проблемные аспекты уголовной ответственности за совершение преступлений против информационной безопасности, связанные с несовершенством норм уголовного закона. При этом автором было высказано мнение, что «действующее законодательство проблему борьбы с компьютерной преступностью уголовно-правовыми методами не сняло, а лишь создало иллюзию ее решения» [1, с. 240].

Сегодня обозначенные недостатки правовой регламентации и практики применения не только сохранили актуальность, но их число значительно увеличилось, в связи с чем можно формулировать самостоятельный «реестр проблем» относительно отдельных норм гл. 31 УК.

Так, с введением в действие белорусского уголовного закона установлена уголовная ответственность за неправомерное завладение компьютерной информацией (ст. 352 УК). В совокупности с недостаточной научной проработкой в целом вопросов уголовной ответственности за различные формы противоправного получения информации трудности при юридической оценке и расследовании деяний, подпадающих под признаки данного общественно опасного деяния, создают особенности законодательной конструкции указанной статьи (насыщенность диспозиции специальными терминами, оценочный характер последствий, нормативная неопределенность формы вины по отношению к ним), а также отсутствие единообразной правоприменительной практики.

Так как законодатели различных государств неодинаково подходят к вопросам криминализации деяний, связанных с неправомерным завладением компьютерной информацией, разобраться в вопросе поможет сравнительный анализ уголовного законодательства государств-участников СНГ. В результате можно выделить два основных подхода к криминализации неправомерного завладения компьютерной информацией в уголовных законах обозначенных государств: прямой уголовно-правовой запрет и придание неправомерному (несанкционированному) копированию компьютерной информации статуса одного из последствий несанкционированного доступа к компьютерной информации. Однако указанные подходы имеют недостатки. Так, криминализа-

ция несанкционированного копирования компьютерной информации, обусловленная только формой ее представления, вызывает конкуренцию с иными нормами уголовного закона. Также при одновременной криминализации копирования компьютерной информации и иного ее завладения возникает диспропорция в степени общественной опасности деяний в рамках одного состава. При последнем подходе соответствующие составы преступлений содержат указание только на копирование компьютерной информации (например, ст. 272 УК Российской Федерации, ст. 334 УК Туркменистана), в то время как при прямом уголовном запрете уголовно наказуемым является не только копирование, но и иное неправомерное завладение, в том числе перехват компьютерной информации. Рассмотрев уголовное законодательство ряда иных европейских государств (Австрия, Бельгия, Германия, Голландия, Республика Польша, Швейцария, Эстонская Республика и др.), также можно говорить и об отсутствии единых подходов в части конструктивных признаков данного деяния, санкций и условий уголовной ответственности за его совершение.

В этой связи по-прежнему актуален вопрос выработки оптимальной модели уголовно-правовой регламентации ответственности за неправомерное завладение компьютерной информацией не только в рамках главы о преступлениях против информационной безопасности, но и в целом системы уголовного закона, так как конструировать норму необходимо в связи с «общим контекстом кодекса» [2, с. 137]. Правовое обеспечение информационной безопасности в современных условиях должно включать использование новых методологических подходов [3, с. 313].

Согласно модельному Информационному кодексу для государств – участников СНГ, принятому постановлением Межпарламентской Ассамблеи государств – участников СНГ от 23 ноября 2012 г. № 38-6, установленный в соответствии с законодательством порядок создания, распространения, использования, хранения и уничтожения информации является правовым режимом информации. В целом правовые режимы вводятся для создания особых подходов к регулированию тех сфер, которые неэффективно или нецелесообразно регулировать в общем порядке [4, с. 42]. При этом установление уголовно-правового запрета в отношении ряда деяний, посягающих на безопасность компьютерной информации, видится одной из характеристик ее правового режима.

Итак, правовой режим различных видов информации кроме Закона Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» (Закон) регламентирован целым рядом иных законодательных актов: Гражданским кодексом, Банковским кодексом, Налоговым кодексом, Уголовно-процессуальным кодексом, Избирательным кодексом, Законами от 19 июля 2010 г. «О государственных секретах», 5 января 2013 г. «О коммерческой тайне», 18 июня 1993 г. № 2435-XII «О здравоохранении» и др. Комплексный анализ названных нормативных документов позволил сформулировать следующие выводы:

перечисленные в ст. 17 Закона виды информации отнесены к информации, распространение и (или) представление которой ограничено, по причине возможности наступления вредных и даже общественно опасных последствий в случае свободного доступа к ней и беспрепятственного ее распространения;

к тому или иному виду информации, распространение и (или) представление которой ограничено, она относится в зависимости от собственного содержания и негативных последствий ее свободного оборота, а не от формы представления (закрепления). Это подтверждает то, что критерием ценности информации служит прогноз негативных последствий, наступающих вследствие завладения ею вероятным противником, конкурентом или злоумышленником [5, с. 14];

в большинстве случаев выделение указанных категорий информации направлено на закрепление определенных гарантий ее защиты и запрета на использование такой информации (необходимость получения согласия лица на использование личных сведений, запрет их разглашения и др.);

в отношении каждого вида информации, распространение и (или) представление которой ограничено, законодательными актами установлен порядок получения, передачи, сбора, обработки, накопления, хранения и предоставления, нарушение которого влечет установленную законодательством ответственность, в том числе уголовную;

одна и та же информация может быть отнесена к различным видам информации, распространение и (или) представление которой ограничено. Так, информация, затрагивающая неприкосновенность частной жизни и ставшая известной на законных основаниях другим лицам,

должна охраняться в зависимости от обстоятельств ее получения в режиме соответствующей профессиональной тайны [6].

Анализ литературных источников (И.Ю. Богдановская, В.С. Бондаренко, Е.А. Войниканис, Л.Н. Мороз, Д.Г. Полещук, Л.К. Терещенко, Е.Н. Яковец и др. [4, 7–11]) также позволяет сделать вывод, что правовой режим информации есть характеристика информации как объекта правоотношений, вытекающая из ее нематериальной природы. На это указывает также дефиниция информации, содержащаяся в ст. 1 Закона. А.В. Полушкин, формулируя определение информационного правонарушения[1], указывает, что им является общественно опасное, противоправное, виновное деяние в информационной сфере и (или) с использованием информационных средств и технологий работы с информацией независимо от ее формы [12, с. 9].

В отечественной литературе в сфере информационного и уголовного права вопросы принципов, условий и иных социально-правовых аспектов установления юридической ответственности, в том числе уголовной, за совершение противоправных действий в отношении компьютерной информации не нашли отражения. Однако на основании анализа норм УК, предусматривающих уголовную ответственность за общественно опасные деяния, предметом которых является информация (сведения, сообщения, данные), можем сделать вывод о том, что основными критериями их криминализации выступают содержание информации, являющейся предметом преступления (различные виды охраняемых законом тайн), и, соответственно, установленный в отношении информации правовой режим. Общественная опасность таких деяний обусловливается причинением (возможностью причинения) существенного вреда в результате неправомерного обладания данной информацией, включая последующее ее использование (разглашение). При установлении уголовной ответственности данный подход в зависимости от вида информации позволяет определить объект данных преступлений (преступление против уклада семейных отношений и интересов несовершеннолетних, против конституционных прав и свобод человека и гражданина, против порядка осуществления экономической деятельности и др.), предусмотреть особенности условий уголовной ответственности (ст. 33 УК) и уголовного преследования за их совершение (ст. 26 УПК).

В то же время в ст. 352 УК криминализировано деяние, где предметом выступает информация по признаку формы представления, которая одновременно по содержанию может являться банковской тайной, тайной личной жизни, государственными секретами. Данное обстоятельство на практике приводит к возникновению спорных вопросов, связанных с выбором нормы, подлежащей применению (например, в случае завладения реквизитами банковских платежных карт). При этом орган уголовного преследования ставится в условия выбора нормы в зависимости от разнородных характеристик информации (содержание и форма). На практике предпочтение отдается форме, что в том числе обусловливается закреплением за специализированными подразделениями «компетенции» по раскрытию и расследованию преступлений в сфере высоких технологий (преступлений против информационной безопасности).

Ранее нами сформулировано основание самостоятельной криминализации данного деяния и названы факторы, обусловливающие общественную опасность несанкционированного копирования компьютерной информации, при этом при дальнейшем совершенствовании уголовно-правовой регламентации ответственности за совершение данного деяния последние необходимо учитывать [13, 14]. Таким образом, логичен вывод о целесообразности дифференциации уголовной ответственности за перечисленные в ст. 352 УК деяния (несанкционированное копирование, иное неправомерное завладение) посредством сохранения в данной статье ответственности только за неправомерное получение компьютерной информации, в том числе путем перехвата, в результате которого обладатель информации либо ее получатель лишаются возможности использовать данную информацию. Одновременно предлагается установить повышенную ответственность за противоправное получение компьютерной информации путем дополнения составов преступлений, предусматривающих уголовную ответственность за противоправное получение сведений безотносительно формы их представления, таким квалифицирующим при-

[1] Разновидностью информационного правонарушения следует считать в том числе компьютерное преступление, киберпреступление и др.

знаком, как сопряженность с несанкционированным доступом к компьютерной информации, компьютерной системе или сети. Данный квалифицирующий признак одновременно указывает на особенности предмета преступления (компьютерную информацию) и отражает значительное увеличение степени общественной опасности запрещаемого деяния в сравнении с деянием, предусмотренным основным составом. В результате несанкционированное копирование компьютерной информации будет полностью охватываться этими нормами.

Основной задачей уголовного закона является охрана прав и свобод человека, что необходимо учитывать при конструировании уголовно-правовых норм. Так, для обладателя информации неважно, какие противоправные действия в отношении информации совершены – уничтожение, модификация, «хищение» информации; основополагающим является их негативный результат – утрата информации либо невозможность ее использования. Как отмечает А.И. Халиуллин, доступность, целостность, конфиденциальность и иные характеристики информации в равной степени определяют ее значимость для субъекта информационного обмена [15, с. 23]. Видится обоснованной унификация законодательной конструкции уголовно-правовых норм гл. 31 УК, предусматривающих ответственность за компьютерный саботаж, модификацию компьютерной информации и неправомерное завладение компьютерной информацией, а также обеспечение согласованности санкций в ст. 350–352 УК и иных составах преступлений, предусматривающих ответственность за противоправное получение информации.

Так, перечисленные выше предложения и выводы формируют элементы новой теоретической модели уголовно-правовой регламентации ответственности за противоправное получение компьютерной информации, которая значительно отличается от существующей в УК и уголовном законодательстве государств – участников СНГ. Ее реализация требует внесения ряда изменений в уголовный закон. При этом с учетом продолжительного действия норм гл. 31 УК и практики их применения некоторые предложения могут быть подвергнуты критике. Это в том числе может быть обусловлено, оперируя экономическим понятием, «эффектом колеи» или QWERTY-эффектом – эффектом победы менее эффективного стандарта над более эффективным за счет относительно случайных обстоятельств момента выбора и последующего закрепления победы менее эффективного стандарта набранной пользовательской базой [16]. Не без оснований Н.Ф. Ахраменка, говоря о несовершенстве конструкций ст. 349–355 УК, одной из таких причин называет некритичное включение в гл. 31 УК соответствующих норм в редакции ст. 286–292 модельного УК государств – участников СНГ [1, с. 240].

На основании изложенного логичен вывод о необходимости совершенствования уголовно-правовой регламентации ответственности за рассматриваемое деяние. В этой связи предлагается выделить определеные направления в обозначенной сфере:

реализация подхода к установлению уголовной ответственности за противоправное получение (собирание, похищение, копирование, завладение, перехват) компьютерной информации, который в качестве основного критерия криминализации выделяет содержание информации, являющейся предметом преступления (различные виды охраняемых законом тайн), и, соответственно, установленный в отношении информации правовой режим;

дифференциация уголовной ответственности за различные способы неправомерного завладения компьютерной информацией;

унификация законодательной конструкции уголовно-правовых норм, закрепляющих ответственность за компьютерный саботаж, модификацию компьютерной информации и неправомерное завладение компьютерной информацией, а также обеспечение согласованности санкций в ст. 350–352 УК и иных составах преступлений, предусматривающих ответственность за противоправное получение информации.

Список использованных источников

1. Ахраменка, Н.Ф. Преступления против информационной безопасности: краткий реестр проблем / Н.Ф. Ахраменка // Право и демократия. – Минск, 2007. – Вып. 18. – С. 239–249.

2. Наумов, А. Уголовная статистика: преступность и ее стабильность / А. Наумов // Уголов. право. – 2008. – № 4. – С. 134–137.

3. Информационное право : учеб. пособие / Г.А. Василевич [и др.]; под общ. ред. Г.А. Василевича и Д.А. Плетенева. – Минск : Адукацыя і выхаванне, 2013. – 352 с.

4. Терещенко, Л.К. Правовой режим информации : автореф. дис. ... д-ра юрид. наук : 12.00.14 / Л.К. Терещенко; Ин-т законодательства и сравнительного правоведения при Правительстве Рос. Федерации. – М., 2011. – 54 с.

5. Яковец, Е.Н. Основы правовой защиты информации и интеллектуальной собственности : учеб. пособие/ Е.Н. Яковец. – 2-е изд., доп. и перераб. – М. : Юрлитинформ, 2013. – 440 с.

6. Саванович, Н.А. Личная информация граждан [Электронный ресурс] / Н.А. Саванович // Консультант Плюс. Беларусь. Технология 3000 / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2016.

7. Право на доступ к информации. Доступ к открытой информации / отв. ред. И.Ю. Богдановская. – М. : Юстицинформ, 2009. – 344 с.

8. Бондаренко, В.С. Сохранность информации при автоматизированной обработке / В.С. Бондаренко. – М. : Знание, 1981. – 64 с.

9. Войниканис, Е.А. Информация. Собственность. Интернет: традиция и новеллы в современном праве / Е.А. Войниканис, М.В. Якушев. – М. : Волтерс Клувер, 2004. – 176 с.

10. Мороз, Л.Н. Информационное право. Общая часть / Л.Н. Мороз. – Минск : Право и жизнь, 2007. – 276 с.

11. Полещук, Д.Г. Понятие и объект преступления против информационной безопасности / Д.Г. Полещук // Право.by. – 2016. – № 6. – С. 87–92.

12. Полушкин, А.В. Информационные правонарушения: понятие и виды : автореф. дис. … канд. юрид. наук : 12.00.14 / А.В. Полушкин; Ур. гос. юрид. акад. – Екатеринбург, 2009. – 25 с.

13. Дубко, М. А. Основание и причины криминализации неправомерного завладения компьютерной информацией / М.А. Дубко // Вестн. Акад. МВД Респ. Беларусь. – 2017. – № 1. – С. 87–91.

14. Дубко, М.А. Несанкционированное копирование как способ неправомерного завладения компьютерной информацией / М.А. Дубко // Законность и правопорядок. – 2017. – № 4. – С. 58–63.

15. Халиуллин, А.И. Неправомерное копирование как последствие преступления в сфере компьютерной информации / А.И. Халиуллин // Рос. следователь. – 2015. – № 8. – С. 23–26.

16. Калеев, С.В. «Эффект блокировки» в практике принятия управленческих решений [Электронный ресурс] / С.В. Калеев // Экономика и менеджмент инновационных технологий. – Режим доступа: http://ekonomika.snauka.ru/2015/03/7846. – Дата доступа: 09.04.2018.

Дата поступления в редакцию: 09.04.18

***M.A. Dubko**, Investigator (serious crime), Investigative Committee of the Republic of Belarus*

IMPROVEMENT OF THE CRIMINAL-LEGAL REGULATION OF LIABILITY FOR THE COMPUTER INFORMATION MISAPPROPRIATION (ART. 352 OF THE CRIMINAL CODE)

Theoretical questions of establishing criminal liability for misappropriation of computer information and directions for improving criminal-legal regulation of responsibility for the act. The issues of criminalization of information crimes through the prism of the legal regime of information are considered. As a result, proposals have been formulated to amend the criminal law with regard to liability for various forms of unlawful receipt of information.

Keywords: information security, computer information misappropriation, unauthorized copying, criminalization.

УДК 343.8

***А.А. Жук**, адъюнкт научно-педагогического факультета Академии МВД Республики Беларусь*
(e-mail: alex.zhuk82@gmail.com)

ЗАРОЖДЕНИЕ И СТАНОВЛЕНИЕ ЛИШЕНИЯ СВОБОДЫ КАК ВИДА УГОЛОВНОГО НАКАЗАНИЯ НА БЕЛОРУССКИХ ЗЕМЛЯХ (вторая половина XVI в. – начало XX в.)

Осуществляется попытка проанализировать процесс зарождения и развития тюремного заключения и лишения свободы как вида уголовного наказания на белорусских землях во второй половине XVI – начале XX в. Рассматривается исторический аспект возникновения понятия «тюрьма», зарождения тюрем и тюремного заключения как вида наказания на белорусской территории. Анализируются основные положения нормативных документов, явившихся правовой основой карательной системы на белорусских землях в рассматриваемый период.

Ключевые слова: тюрьма, лишение свободы, Статут ВКЛ, труд заключенных.