УДК 343.28

Челмодеева И.О.,
Донецкая академия внутренних дел
Министерства внутренних дел
Донецкой Народной Республики
Chelmodeeva I.O.,
Donetsk Academy of Internal Affairs
of the Ministry of Internal Affairs
of the Donetsk People's Republic

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УГОЛОВНОМ ЗАКОНОДАТЕЛЬСТВЕ ЗАРУБЕЖНЫХ ГОСУДАРСТВ

В статье рассмотрены вопросы обеспечения информационной безопасности в уголовном законодательстве зарубежных государств. Аргументирована необходимость закрепления отдельных статей, предусматривающих уголовную ответственность за преступления против информационной безопасности, в главе уголовного законодательства Донецкой Народной Республики, выделив информационную безопасность в качестве родового объекта преступления.

Ключевые слова: информационная безопасность, кибербезопасность, информационные ресурсы, уголовно-правовая охрана информационной безопасности, компьютерные преступления.

ENSURING OF INFORMATION SECURITY IN THE CRIMINAL LEGISLATION OF FOREIGN STATES

The article defines the features of ensuring of information security in the criminal legislation of foreign states. The need to consolidate certain articles providing for criminal responsibility for crimes against information security in the chapter of the criminal legislation of the Donetsk People's Republic is argued, highlighting information security as a generic object of crime.

Key words: *information security, cybersecurity, informational resources, criminal informational security, computer crimes.*

Постановка проблемы в общем виде и ее связь с важными научными или практическими заданиями. Становление правового регулирования сферы информационной безопасности началось в конце XX века. Это связано с осознанием угроз, возникающих в связи с развитием информационных технологий, социально-экономических, военных и политических последствий последней информационной революции, имевшим место в странах, которые первыми начали активную трансформацию в направлении построения информационного общества. Одними из первых государств, которые начали разработку национальной информационной политики и политики в сфере информационной безопасности стали Соединенные Штаты Америки (далее – США) и Япония, а вслед за ними – подавляющее большинство развитых стран мира.

Для современного периода характерен значительный прогресс в развитии информационно-коммуникационных технологий и информационной инфраструктуры в целом. В то же время наблюдается обострение общественных отношений внутригосударственного или трансграничного уровня во время их активного использования. В частности, речь идет о нарушении права на частную жизнь, защите персональных данных, информационных конфликтах и информационных войнах и тому

подобное. В связи с этим актуальными становятся вопросы обеспечения информационной безопасности.

Для Донецкой Народной Республики вопрос обеспечения информационной безопасности приобретает особенно важное значение в сложившихся общественно-политических условиях. Наряду с существующими внешними проблемами и угрозами (военно-политические процессы, отсутствие международного признания), имеет место ряд внутренних проблем (обеспечение информационно-коммуникационными технологиями и уровня развития информационной инфраструктуры, активные миграционные процессы). При данных условиях растет количество совершаемых преступлений, в том числе и против информационной безопасности, которая является одной из составляющих государственной безопасности.

Вышеуказанное требует надлежащего правового обеспечения информационной безопасности, в том числе уголовно-правовыми средствами.

Анализ последних исследований и публикаций, в которых начато решение данной проблемы и на которые опирается автор. Вопросы обеспечения информационной безопасности в уголовном праве нечасто являлись предметом исследования. Так, уголовно-правовым аспектам охраны информационных отношений (в том числе, компьютерной информации) были посвящены работы В.Н. Додонова, А.Ф. Жигалова, Р.В. Жубрина, У.В. Зининой, О.С. Капинус, Л.Р. Клебанова, В.А. Мазурова, Н.И. Пикурова, А.А. Рожнова, И.В. Смольковой, А.А. Фатьянова, С.П. Щербы, И.А. Юрченко и других. Непосредственно уголовно-правовой охране информационной безопасности были посвящены работы Л.А. Букалеровой, Д.А. Калмыкова, Е.А. Красненковой.

Вместе с тем, остались неразрешенными ряд вопросов как на практическом, так и на теоретическом уровне, одним из которых является определение видов преступлений, которые могут быть совершены путем посягательства на информационную безопасность.

Нерешенные ранее части общей проблемы, которым посвящается обозначенная статья. До сегодня не решен вопрос о том, какие посягательства следует относить к преступлениям против информационной безопасности, в связи с чем актуальность приобретает проведение сравнительного анализа обеспечения информационной безопасности в уголовном законодательстве зарубежных государств.

Формулировка целей статьи. Целью данной статьи является сравнительный анализ обеспечения информационной безопасности в уголовном законодательстве зарубежных государств с целью совершенствования отечественного законодательства на основе учета и заимствования положительного зарубежного опыта.

Изложение основного материала исследования с полным обоснованием полученных научных результатов. Анализ законодательных актов зарубежных государств свидетельствует о том, что информационная и сетевая безопасность понимается в большинстве государств как способность сети или системы противостоять с определенным уровнем надежности аварии или злонамеренным действиям, которые могут нарушить доступность, целостность и конфиденциальность информации, которая хранится или передается, а также услуг, предоставляемых посредством сети или информационной системы. Соблюдение безопасности определяется как доступность, идентификация, целостность, конфиденциальность информации. Особое внимание при этом уделяется законодательной базе, которая охватывает вопросы перехвата и дешифровки информации [1, с. 8].

При этом выбор направлений политики обеспечения информационной безопасности и форм их закрепления в национальных правовых системах существенно отличается и обусловлен рядом исторических, культурных, правовых и экономических факторов. Так, например, в США внимание акцентируется на технологических аспектах, в

Европе – на социальных измерениях. Все государства-члены Евросоюза имеют собственные программы национальной политики по построению информационного общества, а также кибербезопасности; кроме того, имеются общие директивы Европейского Союза (далее – ЕС) по исследуемым вопросам. Сегодня быстрыми темпами начал развиваться рынок информационных технологий в азиатских странах – Республике Корея, Тайване, Гонконге и Сингапуре. Канада пытается максимально сохранять культурное разнообразие и национальную идентичность перед угрозой информационной экспансии США.

Российская Федерация и другие страны постсоветского пространства почти за 30 лет сформировали собственные подходы к информационной политике, которые отличаются как по содержанию, так и по формам и степени реализуемости. Как отмечает Е.В. Лебедева, позиции государств Содружества Независимых Государств (далее – СНГ) свойственен комплексный подход к рассмотрению вопросов информационной безопасности: изучаются как техническая сторона вопроса, так и идеологическая (или информационно-психологическая). В частности, акцентируется внимание на необходимости демилитаризации сферы безопасности, на недопущении использования информационных технологий в военных целях, на принятии правил поведения, гарантирующих свободное и безопасное использование информационной среды. В свою очередь, взгляды западных коллег по диалогу по информационной безопасности имеют существенные отличия: акцент ставится на борьбе с киберпреступностью, безопасностью информационных структур и сетей, на вопросах защиты информации, имеющей ограничения в доступе, также на предотвращении попадания новейших информационных разработок в руки к преступным группировкам и криминальным элементам [2, с. 505].

Что касается обеспечения информационной безопасности в уголовном законодательстве зарубежных государств, то оно характеризуется преимущественно отсутствием системного подхода к уголовно-правовой охране информационной безопасности [3, с. 131]. В качестве родового или видового объекта преступления информационная безопасность, как правило, не выделяется. Исключением является Уголовный кодекс Польши, предусматривающий в статьях 265-269 главы XXXIII преступления против охраны информации, которые устанавливают уголовную ответственность за: нарушение конфиденциальности государственной тайны; ответственность за незаконные действия в отношении нескольких видов информации с ограниченным доступом; незаконные действия в отношении профессиональной и служебной тайн; нарушение тайны переписки; уничтожение, повреждение, удаление или изменение записи на компьютерном носителе информации, имеющей значение для обороноспособности государства, безопасности связи, функционирование правительственной администрации, иного государственного органа или администрации органа самоуправления или нарушения или предотвращения автоматизированного сбора или передачи такой информации; уничтожение или замену носителя информации либо уничтожение или повреждение устройства, служащего автоматизированному преобразованию, сбору или передаче такой информации [4, с. 200-201].

В других зарубежных странах преступления против информационной безопасности установлены отдельной главой уголовного закона, однако они включают в себя только уголовно-правовые нормы, предусматривающие ответственность за преступления против безопасного использования информационно-телекоммуникационных технологий. При этом они либо выделяются в самостоятельный раздел или главу, либо рассредоточены по различным разделам или главам.

Например, в США на федеральном уровне установлена уголовная ответственность за преступления в сфере компьютерной информации, а именно – в Акте о подделке средств доступа, компьютерном мошенничестве и злоупотреблении (Counterfeit Access

Device and Computer Fraud and Abuse Act). Этот акт с 1984 года многократно дополнялся и в действующей редакции как § 1030 в Титуле 18 Свода законов США устанавливает ответственность за семь основных противоправных деяний, которыми признаются:

- компьютерный шпионаж;
- несанкционированный доступ к информации из правительственного ведомства США с любого защищенного компьютера;
- воздействие на компьютер, находящийся в исключительном пользовании правительственного ведомства США;
- мошенничество с использованием компьютера;
- умышленное или неосторожное повреждение защищенных компьютеров;
- мошенничество путем торговли компьютерными паролями или аналогичной информацией, позволяющее получить несанкционированный доступ;
- угрозы, вымогательство, шантаж и другие противоправные деяния, совершенные с использованием компьютерных технологий [5, с. 82-83].

Ответственность за компьютерные преступления в информационном пространстве установлена и другими пунктами Свода законов США, в частности, за торговлю похищенными или поддельными устройствами доступа, которые могут быть использованы для получения ценностей (денег, товаров или услуг); за умышленное повреждение имущества, оборудования, контактных пунктов, линий или систем связи (§ 1029 Титула 18).

Предусмотрена также ответственность за перехват и разглашение сообщений, переданных по телеграфу, устно или с использованием компьютеров (§ 2511 Титула 18) за нарушение конфиденциальности электронной почты путем незаконного доступа к сохраненным сообщениям, а также за создание препятствий для санкционированного доступа к таким сообщениям (§ 2701 Титула 18).

Ответственность за другие преступления с использованием компьютерной информации или составляющих информационного компьютерного пространства предусматривает § 1343 Титула 18 Свода законов США. Его нормами, в частности, предусмотрена возможность привлечения к уголовной ответственности за передачу полностью или частично проволочными средствами связи, по радио или телевидению сообщения с целью использования для дальнейшего совершения мошенничества. Предписания § 1343 подлежат применению в случаях, когда терминалы, используемые для ведения мошеннических действий, обмениваются информацией с помощью каналов электросвязи.

Во всех без исключения странах Европейского союза вопросам правового обеспечения информационной безопасности уделяется особое внимание. При этом первостепенное значение приобретают вопросы противодействия киберугрозам, которые являются составляющими процесса обеспечения информационной безопасности. С 1999 года реализуются программы «Безопасный Интернет» (Safer Internet), в рамках которых осуществляются мероприятия, направленные на борьбу не только с вредным контентом, но и с опасным поведением в сети.

Уголовный кодекс Нидерландов в разделе XXVII «Уничтожение или причинение вреда» предусматривает ответственность за разрушение, порчу, приведение в негодность или неисправность, уничтожение компьютера или системы для хранения и обработки данных, телекоммуникационного прибора, предназначенных для использования населением или для национальной обороны (статьи 351, 351bis) [6, с. 309].

Уголовный кодекс Франции предусматривает ответственность за действия, совершенные с компьютерной информацией в ущерб интересам государства. Перечень данных составов преступлений также достаточно велик: сбор или передача содержащейся в памяти ЭВМ или картотеке информации иностранному государству, уничтожение,

хищение, изъятие или копирование данных, носящих характер секретов национальной обороны, содержащиеся в памяти ЭВМ или в картотеках, а также ознакомление с этими данными посторонних (ст.ст. 411-7, 411-8, 413-9, 413-10, 413-11) [7, с. 423].

Анализ Уголовного закона ФРГ позволяет отнести к преступлениям в сфере информационной безопасности: антиконституционный саботаж (§ 88), нарушение конфиденциальности разговора (§ 201), нарушение тайны переписки (§ 202), нарушение тайны почтовой и телекоммуникационной тайны (§ 206), компьютерное мошенничество (§ 263a), изменение данных (§ 303a), компьютерный саботаж (§ 303b), вмешательство в работу телекоммуникационных установок (§ 317) [8, с. 300-350].

В Австрии, Финляндии и Ирландии, как и в других странах ЕС, значительное внимание уделяется проблемам кибербезопасности, очерченным в документе Европейской комиссии «На пути к общей политике в сфере борьбы с киберпреступностью», где последняя определяется как уголовные действия, совершенные с использованием электронных коммуникационных сетей и информационных систем или против таких сетей и систем, а именно:

традиционные формы преступления (мошенничество и подделки в электронных коммуникационных сетях и информационных системах);

публикации незаконного контента в электронных медиа;

специфические преступления в электронных сетях (атаки на информационные системы, хакерство и т.д.) [9, с. 126].

В Беларуси отсутствуют специальные законы о киберпреступности, но некоторые аспекты, регулирующие отношения, защищены Уголовным кодексом и нормативными актами, регулирующими интернет. Согласно официальной статистике, более 90% киберпреступности в Беларуси имеют финансовый характер, а также имеют место: несанкционированный доступ к данным; диверсионные акты; незаконное получение электронных данных; нарушение правил использования компьютерных систем; создание, использование или распространение вредоносного программного обеспечения компьютерных устройств. Серьезной проблемой в Беларуси является создание и распространение порнографии, включая детскую порнографию, особенно учитывая тенденцию быстрого распространения информации в соцсетях [10, с. 182].

Учитывая изложенное, можно сделать вывод, что преступления против информационной безопасности в уголовных законах практически всех зарубежных стран не выделены в отдельную главу. Уголовные законы некоторых стран в качестве родового объекта преступлений предусматривают безопасное использование информационно-телекоммуникационных технологий.

Следует отметить, что защита информации от неправомерного доступа тесно связана с категорией «тайна», в связи с чем важным является исследование вопросов криминализации данного преступления в зарубежных странах.

Общественные отношения, возникающие в сфере оборота информации с ограниченным доступом в зарубежных странах, охраняются отдельными уголовно-правовыми нормами. Анализ законодательства зарубежных стран, которое предусматривает уголовную ответственность за указанные посягательства, дает основания считать, что преступления, предметом которых является информация с ограниченным доступом, в зависимости от владельца информации можно разделить на две группы. К первой группе следует отнести преступления, предметом которых признается информация, являющаяся собственностью государства. Вторую группу составят преступления, предметом которых выступает информация, являющаяся собственностью физических и негосударственных юридических лиц.

К первой группе преступлений можно отнести шпионаж, разглашение государственной тайны, разглашение служебной тайны, содержащиеся в уголовных

кодексах подавляющего большинства стран. Особенностью шпионажа в законодательствах зарубежных стран является то, что, во-первых, адресатом передачи информации являются иностранные государства, иностранные организации или их представители; во-вторых, субъектом этого преступления признается иностранный гражданин или лицо без гражданства; в-третьих, сведения могут быть использованы для нанесения вреда суверенитету, территориальной целостности или внешней безопасности страны. Предметом шпионажа законодательства указанных стран признают государственную информацию.

В законодательствах ряда стран (например, Республика Казахстан, Эстония, Франция и т.д.) предметом шпионажа признают государственную тайну, а также другие сведения, разглашение которых может нанести ущерб внешней безопасности или суверенитета страны. Законодатели этих стран не отмечают определенный правовой режим информации (за исключением государственной тайны), за передачу или сбор которой наступает уголовная ответственность, а только называют ее «другие сведения». То есть, предметом этого преступления может быть не только информация с ограниченным доступом, но и любые сведения, которые интересуют разведывательные службы иностранных государств, секреты [11, с. 227].

В законодательствах таких стран как Германия, Швейцария, Болгария, Голландия, Латвийская Республика, Республика Узбекистан предметом шпионажа является только государственная информация с ограниченным доступом. Так, например, в Швейцарии дипломатическим шпионажем является разглашение или предоставление доступа иностранному государству или агентуре тайны, хранение которой необходимо для благосостояния Конфедерации [12, с. 248]. В ФРГ шпионской агентурной деятельностью является осуществление в пользу иностранного государства действий, направленных на сбор или сообщение государственной тайны, или предоставление согласия к ведению такой деятельности иностранному государству или ее представителям.

Особого внимания требуют преступления, предметом которых признаются сведения, являющиеся собственностью государства, но не составляющие государственной тайны. В законодательствах разных стран это понятие терминологически имеет разные названия: «официальные акции или сведения» (США), «сведения, не подлежащие оглашению» (Латвия), «информация для внутреннего пользования» (Эстония), «конфиденциальная информация» (Дания), «служебная тайна» (Республика Беларусь, Республика Болгария, Республика Польша, Швейцарская Конфедерация) и другие.

Следует отметить, что информация с ограниченным доступом, которая является собственностью государства, но не составляет государственной тайны, в одних странах охраняется отдельными уголовно-правовыми средствами, а в других – наряду с государственной и другими видами тайн.

В законах об уголовной ответственности таких стран как КНР (ст. 111), Республика Узбекистан (ст. 162), Нидерланды (ст. 98), Республика Таджикистан (ст. 308), Российская Федерация (ст. 276), Азербайджанская республика (ст. 276) уголовная ответственность за незаконные действия с информацией с ограниченным доступом, которая является собственностью государства, но не составляющая государственной тайны, предусмотрена за такие преступления как шпионаж и разглашение служебных секретов [3, с. 99-100].

Согласно ст. 162 УК Республики Узбекистан разглашением государственных секретов является разглашение или передача государственных секретов, то есть, сведений, составляющих государственную, военную или служебную тайну, лицом, которому эти сведения были доверены или стали известны по роду служебной или профессиональной деятельности, при отсутствии признаков государственной измены [13, с. 120]. То есть, предметом этого преступления наряду с государственной тайной являются служебная и военная тайны.

В таких странах как Республика Казахстан, Республика Беларусь, Республика Болгария, Республика Польша государственная информация, не составляющая государственной тайны, но к которой может быть ограничен доступ, называется «служебная тайна». Например, в Республике Казахстан за разглашение служебной тайны уголовная ответственность предусмотрена в ст. 172 УК Республики Казахстан, а за утрату документов, содержащих служебную тайну, а также предметов, сведения о которых составляют служебную тайну – ч. 2 ст. 173 УК Республика Казахстан [14, с. 194-195]. Эти действия указаны в статьях, предусматривающих ответственность за незаконное получение, разглашение государственных секретов и утрату документов, предметов, содержащих государственные секреты, но ответственность за деяния по служебной тайне предусмотрена отдельными частями этих статей.

В Республике Болгария, Швейцарии, Латвийской Республике, Швеции, Республике Узбекистан, КНР, Республике Беларусь, Республике Польша, Дании общественно опасные последствия не являются обязательным признаком объективной стороны разглашения служебной тайны.

Как было отмечено выше, уголовно-правовой охране подлежит не только информация с ограниченным доступом, которая является собственностью государства, но и информация, являющаяся собственностью физических и негосударственных юридических лиц. Уголовная ответственность за незаконное обращение с такой информацией предусмотрена, в частности, ст. 226-13 (нарушение профессиональной тайны) УК Франции, ст. 250.12 (нарушение прайвеси) Примерного УК США, § 353 4 (незаконное разглашение сведений о судебных разбирательствах), § 355 (нарушение налоговой тайны) УК ФРГ, ст. 161-2 (использование конфиденциальной информации, касающейся сделки с ценными бумагами эмитента) УК Эстонии, ст. 321 УК Швейцарии (нарушение почтовой и телекоммуникационной тайны), ст. 157 (посягательство на личную или семейную тайну), ст. 158 (нарушение тайны частных переговоров), ст. 159 (нарушение тайны частной переписки, телефонных переговоров или сообщений, передаваемых другим способом) УК Грузии, ст. 269 (незаконное получение информации, составляющей коммерческую или банковскую тайну), ст. 270 (разглашение коммерческой или банковской тайны), ст. 151 (незаконный сбор и распространение информации о частной жизни), ст. 152 (разглашение медицинской тайны), ст. 153 (нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений) Модельного УК стран-участниц СНГ, ст. 267 УК Польши (получение информации, не предназначенной для него), § 153 (незаконное раскрытие, уничтожение или присвоение письма или посылки или оказание помощи любому другому лицу в осуществлении подобных действий) УК Дании и др. [3, с. 102].

Таким образом, преступления, предметом которых является информация с ограниченным доступом, в зависимости от владельца информации разделены на две группы. К первой группе отнесены преступления, предметом которых признается информация, являющаяся собственностью государства, – шпионаж, разглашение государственной тайны, разглашение сведений, являющихся собственностью государства, но не составляющих государственной тайны. Ко второй группе отнесены преступления, предметом которых является информация, являющаяся собственностью физических и негосударственных юридических лиц.

Выводы по исследованию и перспективы дальнейших поисков в данном направлении. Изучение практики зарубежных стран в построении собственных моделей правового обеспечения информационной безопасности, противодействии киберугрозам позволяет резюмировать отсутствие единой модели национальной системы обеспечения информационной безопасности уголовно-правовыми средствами. Вопросы уголовно-правовой охраны информации и информационной безопасности разрешаются различным

способом. При этом системный подход в данном вопросе отсутствует во всех странах, кроме Польши. Ряд зарубежных государств системно охраняют посредством уголовного закона различные виды тайн.

В целом же, в большинстве зарубежных стран, как и в Донецкой Народной Республике, преступления против информационной безопасности расположены в различных разделах и главах Особенной части уголовного закона зарубежных стран. Преступления, посягающие на компьютерную информацию, как правило, объединены в один раздел или главу. Зарубежные законодатели уделяют повышенное внимание уголовно-правовой охране государственных информационных ресурсов, что определяется в установлении ответственности за посягательство на них не в общих, а в специальных нормах.

Приоритетным направлением является совершенствование законодательства, устанавливающего ответственность за правонарушения, разработка и законодательное закрепление в одном перечне правонарушений и видов ответственности в сфере информационной безопасности. То есть, необходимо закрепить преступления против информационной безопасности в отдельной главе уголовного закона, выделив информационную безопасность в качестве родового объекта преступления.

Список использованной литературы

1. Информационная безопасность: Учебное пособие / В.Н. Ясенев, А.В. Дорожкин, А.Л. Сочков и др. Под общей редакцией В.Н. Ясенева. – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. – 198 с. – Текст: непосредственный.

2. Лебедева, Е.В. Информационная безопасность государств СНГ: этапы реализации / Е.В. Лебедева // Национальная безопасность / nota bene. – 2016. – № 4. – С. 500-508. – Текст: непосредственный.

3. Ефремова, М.А. Уголовно-правовая охрана информационной безопасности: специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»: диссертация на соискание ученой степени доктора юридических наук / Марина Александровна Ефремова. – Москва, 2017. – 427 с. – Текст: непосредственный.

4. Уголовный кодекс Республики Польша / под общ. ред. Н.Ф. Кузнецовой. – Санкт-Петербург: Юридический центр Пресс, 2001. – 234 с. – Текст: непосредственный.

5. Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – Москва: Юрлитинформ, 2001. – 496 с. – Текст: непосредственный.

6. Уголовный кодекс Голландии / [науч. ред. докт. юрид. наук, заслуж. деятель науки РФ, проф. Б.В. Волженкин; пер. с англ. И.В. Мироновой]. – Санкт-Петербург: Юридический центр Пресс, 2001. – 510 с. – Текст: непосредственный.

7. Уголовный кодекс Франции / перевод с французского канд. юрид. наук доцента Н.Е. Крыловой. – Санкт-Петербург: Юридический центр Пресс, 2002. – 648 с. – Текст: непосредственный.

8. Уголовный кодекс Федеративной Республики Германии / под общ. ред. Д.А. Шестакова. – Санкт-Петербург: Юридический центр Пресс, 2003. – 524 с. – Текст: непосредственный.

9. Ступень, М.В. Сравнительный анализ киберпреступлений в России и зарубежных странах / М.В. Ступень // Евразийский научный журнал. – 2016. –№ 12. – С. 125-127. – Текст: непосредственный.

10. Дубко, М.А. Международное сотрудничество в сфере уголовно-правовой борьбы с неправомерным завладением компьютерной информацией / М.А. Дубко //

Вестник Полоцкого государственного университета. Сер. D, Экономические и юридические науки. – Новополоцк: ПГУ, 2012. – № 14. – С. 180-183. – Текст: непосредственный.

11. Азаров, Д.С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження) / Д.С. Азаров. – Київ: Атіка, 2007. – 304 с. – Текст: безпосередній.

12. Уголовный кодекс Швейцарии. Перевод с немецкого / Науч. ред.: Серебрянникова А.В. – Санкт-Петербург: Юридический центр Пресс, 2002. – 350 с. – Текст: непосредственный.

13. Уголовный кодекс Республики Узбекистан / вступ. ст. М.Х. Рустамбаева, А.С. Якубова, З.Х. Гулямова. – Санкт-Петербург: Юридический центр Пресс, 2001. – 338 с. – Текст: непосредственный.

14. Уголовный кодекс Республики Казахстан / предисл. И.И. Рогова. – Санкт-Петербург: Юридический центр Пресс, 2001. – 466 с. – Текст: непосредственный.

Статья поступила в редакцию 30.06.2021