УДК 343.4

Виталий Владимирович Вабищевич
аспирант 3 года обучения каф. уголовного права
Белорусского государственного университета
Vitali Vabishchevich
Post-Graduate Student of the Department of Criminal Law of the Faculty of Law
of Belarusian State University
e-mail: r999m@mail.ru

ОСОБЕННОСТИ СОДЕРЖАНИЯ ВИНЫ, ЦЕЛЕЙ И МОТИВОВ ПОСЯГАТЕЛЬСТВ НА ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Рассматриваются вопросы криминализации общественно опасных деяний, направленных на посягательства на персональные данные. Акцентируется внимание на необходимости установления формы вины субъекта потенциальных преступных посягательств на персональные данные, а также целей и мотивов таких посягательств. Проведен анализ практики совершения незаконных действий с персональными данными, а также аналогия с иными преступлениями, которые имеют схожий объект правовой охраны. Сделан вывод о необходимости по общему правилу криминализировать умышленные посягательства на персональные данные. Отмечено, что неосторожная вина может быть установлена только в случае посягательств на наиболее чувствительные персональные данные. Цели и мотивы посягательств на персональные данные должны являться квалифицирующими признаками и основой для разграничения преступных деяний от правонарушений.

Features of the Content of Guilt, Goals and Motives of Attacks on Personal Data

The issues of criminalization of socially dangerous acts aimed at encroaching on personal data are considered. Attention is focused on the need to establish the form of guilt of the subject of potential criminal attacks on personal data, as well as the goals and motives of such attacks. The analysis of the practice of committing illegal actions with personal data, as well as the analogy with other crimes that have a similar object of legal protection. It is concluded that it is necessary to criminalize intentional attacks on personal data as a General rule. It is noted that careless guilt can be established only in the case of attacks on the most sensitive personal data. The purpose and motive of the attacks on personal data have to be aggravating circumstances and the basis for the distinction between criminal acts against infringement.

Введение

В эпоху цифровизации и повсеместного использования персональных данных во всех сферах жизнедеятельности особенно актуальным является выработка конкретных мер защиты персональных данных, а также обеспечение их правовой охраны, в том числе с точки зрения совершенствования Уголовного кодекса (далее – УК) Республики Беларусь в части введения уголовной ответственности за преступные посягательства на персональные данные как на самостоятельный уголовно-правовой объект.

Вопрос целесообразности надлежащей уголовно-правовой охраны персональных данных, считаем, не вызывает сомнений. Тем не менее одним из важнейших элементов, по которым определяется степень криминализации тех либо иных деяний, либо проводится разграничение между видом юридической ответственности за совершенные правонарушения, является субъективная сторона, которая охватывает психическое отношение лица к совершаемому общественно опасному деянию и общественно опасным последствиям этого деяния. При этом следует согласиться с И. О. Грунтовым, который отмечает, что объективные признаки умышленного посягательства при формальной и материальной конструкции состава преступления должны конструироваться в законе таким образом, чтобы психическое и социально-психическое отношение субъекта этого поведения соответствовало законодательной модели умысла, предусмотренной ч. 2 ст. 24, ч. 2 и 3 ст. 22 УК Республики Беларусь [1].

Установление субъективной стороны необходимо рассматривать в контексте реа-

---

Научный руководитель – А. В. Шидловский, кандидат юридических наук, доцент, первый заместитель директора Института переподготовки и повышения квалификации судей, работников прокуратуры, судов и учреждений юстиции Белорусского государственного университета

лизации такого принципа уголовного закона и уголовной ответственности, как принцип субъективного вменения, предусмотренный в ст. 3 УК Республики Беларусь. Согласно данному принципу, лицо подлежит уголовной ответственности только за те совершенные им общественно опасные действия (бездействие) и наступившие общественно опасные последствия, в отношении которых установлена его вина, т. е. умысел или неосторожность. Уголовная ответственность за невиновное причинение вреда не допускается.

Таким образом, в рамках рассмотрения вопросов криминализации общественно опасных деяний, направленных на посягательства на персональные данные, необходимо определить форму вины субъекта преступных посягательств, цели и мотивы таких посягательств.

Настоящее исследование проведено путем анализа сложившейся практики совершения незаконных действий с персональными данными, а также на основании аналогии с иными составами преступлений, которые имеют схожий объект и субъект преступного посягательства. Полученные выводы могут быть использованы при формировании конкретных составов преступлений либо дополнении существующих в части указания на вину при совершении преступления, либо на цели и мотивы как квалифицирующие признаки.

Стоит отметить, что комплексно вопрос об уголовно-правовой охране персональных данных в Республике Беларусь в научной среде не рассматривается, хотя обсуждается отсутствие надлежащей юридической ответственности за посягательства на персональные данные отмечается.

В соответствии со ст. 21 УК Республики Беларусь под виной понимается психическое отношение лица к совершаемому общественно опасному деянию, выраженное в форме умысла или неосторожности.

В субъективную сторону преступления как один из четырех элементов состава преступления также входят такие психологические признаки совершаемого деяния, как мотив и цель преступления, которые указывают на волевую направленность деяния.

А. В. Барков отмечает, что субъективная сторона преступления проявляет себя через объективную сторону преступления. Поэтому изучение субъективной стороны и исследование наличия или отсутствия того или иного ее признака должны осуществляться на основе анализа признаков объективной стороны преступления [2]. Кроме того, указанный ученый говорит о существенном значении субъективной стороны для решения вопросов уголовной ответственности. Во-первых, с ее помощью отграничивают преступное поведение от непреступного. Во-вторых, с помощью субъективной стороны разграничиваются составы преступлений, которые имеют одинаковые по характеру признаки объективной стороны преступления. В-третьих, содержание субъективной стороны преступления указывает на степень общественной опасности преступления и лица, его совершившего. Это учитывается при индивидуализации ответственности, избрании судом вида и размера наказания. Судебная практика исходит из необходимости тщательного исследования содержания и направленности умысла, выяснения действительных мотивов и целей преступления, четкого отграничения умышленных преступлений от совершенных по неосторожности.

Важной проблемой при рассмотрении вопросов криминализации посягательств на персональные данные в целом, а также определение субъективной стороны таких преступлений, является отсутствие в Республике Беларусь единого специализированного нормативного правового акта, регулирующего отношения, связанные с оборотом персональных данных. Регулирование оборота персональных данных осуществляется рядом нормативных правовых актов, которые не охватывают все значимые вопросы и имеют некоторые противоречия. В настоящее время ведется работа над проектом Закона «О персональных данных» (далее – проект закона) [3]. Как следствие, в УК Республики Беларусь отсутствуют специальные составы, имеющие в качестве непосредственного объекта защиту персональных данных. Сегодня количество правонарушений, совершаемых с использованием персональных данных, возрастает. При этом эти правонарушения могут быть направлены на конкретную личность, группу лиц, конкурента при осуществлении предпринимательской деятельности, национальную безопасность.

Действующие редакции статей УК Республики Беларусь, связанные с посягательством на персональные данные, не претерпели существенных изменений с 1999 г., т. е. с момента принятия уголовного закона. Закономерно, что ранее вопрос об информационной безопасности личности, общества и государства не стоял так остро, а посягательства на персональные данные не рассматривались как серьезные общественно опасные деяния, поскольку отсутствовали в таком количестве информационные источники накопления персональных данных, а также технологии, позволяющие их похищать и использовать в преступных целях. В то же время законодатель регламентировал уголовно-правовую охрану некоторых видов информации, находящейся в ограниченном доступе, и обеспечил им надлежащую уголовно-правовую охрану. Например, разглашение тайны усыновления (удочерения) (ст. 177), разглашение врачебной тайны (ст. 178), разглашение коммерческой тайны (ст. 255), нарушение тайны голосования (ст. 192), умышленное разглашение служебной тайны (ст. 375 УК Республики Беларусь) и т. д.

По нашему мнению, наиболее ущемленными в правовой среде стали именно персональные данные, которые могут составлять любой из перечисленных выше видов охраняемой информации, однако не являются непосредственным объектом уголовно-правовой охраны.

Для рассмотрения вопросов о субъективной стороне под потенциальными посягательствами на персональные данные предлагаем понимать деяния, которые, исходя из положений проекта закона, зарубежного опыта, а также международно-правового регулирования, рассматриваются как правонарушения (далее – незаконный оборот персональных данных).

Так, в соответствии с проектом закона ответственность может наступать за непринятие лицом, в том числе должностным, необходимых мер по защите персональных данных, хищение персональных данных с помощью специальных автоматизированных систем, незаконное изменение персональных данных, передачу персональных данных субъектам на территории иностранных государстве, где не установлен надлежащий уровень их защиты [4]. Зарубежный опыт показывает, что объективная сторона преступных посягательств на персональные данные может заключаться в обработке и использовании персональных данных для целей рекламного или маркетингового исследования в случае, когда субъект, которому принадлежат персональные данные, заранее возразил против этого; в нарушении, в том числе при ведении бизнеса, порядка обезличивания персональных данных и их передачи в анонимной форме, что повлекло возможность идентификации конкретных физических лиц; в сборе и передаче персональных данных, раскрывающих идеологию, религию, убеждения, здоровье, расовое происхождение или сексуальную ориентацию субъекта, или если жертва является несовершеннолетним или инвалидом; в нарушении срока хранения персональных данных и непринятии надлежащих мер предосторожности для защиты данных [5].

Незаконный оборот персональных данных, совершенный умышленно. В соответствии со ст. 22 УК Республики Беларусь преступлением, совершенным умышленно, признается общественно опасное деяние, совершаемое с прямым или косвенным умыслом.

Как правило, посягательства на персональные данные совершаются умышленно, как с прямым, так и косвенным умыслом. Проблемным вопросом может являться сознание общественного опасного поступка, поскольку в настоящее время конкретного исчерпывающего перечня персональных данных не существует. Кроме того, персональные данные всегда должны иметь признаки прямой либо косвенной идентификации личности, что является оценочным явлением и требует специального интеллектуального анализа и сопоставления информации. В связи с этим лицо не всегда может понимать, относится та либо иная информация к персональным данным. Усложняется этот процесс отсутствием единого нормативного правового акта в этой области, о чем было указано выше.

Степень сложности данного вопроса, очевидно, значительно ниже при совершении незаконного оборота персональных данных специальными субъектами, как правило, должностными лицами, которые ответственны за сбор персональных данных либо за ведение баз таких данных, включая государственные, и осведомлены о правилах

сбора персональных данных, подписывают соответствующие документы об ознакомлении с ответственностью за их нарушение. В качестве аналогии можно привести коммерческую тайну, когда в ст. 15 Закона Республики Беларусь «О коммерческой тайне» прямо указано об обязанности ознакомить всех работников с перечнем сведений, составляющих коммерческую тайну.

Незаконный оборот персональных данных имеет свои особенности, поскольку сами персональные данные, по нашему мнению, имеют разнообъектный характер, включающий посягательства на конституционные права, на информационную безопасность, личную свободу, честь и достоинство, порядок управления и осуществления власти. Данная характеристика влияет и на умысел при незаконном обороте персональных данных, например, в случае осуществления контроля со стороны родителей в отношении детей, просмотра их социальных сетей, когда родитель не воспринимал свои действия как общественно опасные [6]. Так, органы прокуратуры Беларуси заявили, что военкомат нарушил законодательство при публикации в газете личных данных «уклонистов» [7]. В связи с этим, считаем, крайне важно отношение правонарушителя к общественно опасным последствия своего деяния, т. е. предполагаемый состав преступления о незаконном обороте персональных данных должен иметь материальный состав.

Согласно ст. 179 УК Республики Беларусь, наказываются незаконное собирание либо распространение сведений о частной жизни, составляющих личную или семейную тайну другого лица, без его согласия, повлекшие причинение вред правам, свободам и законным интересам потерпевшего. Исходя из указанной диспозиции, полагаем, что незаконное собирание может быть совершено как с умыслом, так и по неосторожности. Важным является наличие вреда правам, свободам и законным интересам потерпевшего.

Для сравнения: в Российской Федерации, как указывают некоторые авторы, собирание и распространение информации о частной жизни может быть совершено только умышленно, что исключает проявление неосторожности [8, с. 403].

В статьях 177, 178, 203, 255, 373, 375 УК Республики Беларусь прямо предусмотрено, что уголовным признаются указанные там деяния, совершенные только умышленно. Многие из перечисленных выше статей имеют квалифицирующие признаки, а также указания на необходимость наличия определенных тяжких последствий либо причинения ущерба в крупном и особо крупном размерах. Как правило, умысел является определенным (конкретизированным) и заранее обдуманным.

Незаконный оборот персональных данных, совершенный по неосторожности

Согласно ст. 23 УК Республики Беларусь, преступлением, совершенным по неосторожности, признается общественно опасное деяние, совершенное по легкомыслию или небрежности. Как было указано ранее, полагаем, что содержание ст. 179 УК Республики Беларусь может подразумевать совершение противоправных деяний по неосторожности, но только если эти деяния повлекли причинение вреда правам, свободам и законным интересам потерпевшего. Также ст. 374 УК Республики Беларусь преступлением признает разглашение государственной тайны по неосторожности. Такой подход законодателя в данной статье, по нашему мнению, вполне целесообразен, поскольку государственная тайна имеют крайне повышенную ценность и меры ее охраны должны быть максимально жесткими.

Таким образом, полагаем, что незаконный оборот персональных данных, по общему правилу, должен подлежать криминализации только в случае наличия умышленной вины у соответствующего субъекта, на что должно быть отдельное указание в самой диспозиции состава преступления.

При этом возможно рассмотреть подход о признании незаконного оборота персональных данных преступным, когда речь идет о совершении посягательства по неосторожности лицом, имеющим доступ к определенным видам наиболее чувствительных персональных данных, нарушения установленных правил обращения с ними.

Под наиболее чувствительными данными можно понимать биометрические либо генетические данные. Например, ответственное лицо передало по ошибке базу данных с отпечатками пальцев вместо другого, незначительного документа. На практике часто встречаются случаи неумышлен-

ной передачи ненадлежащих источников информации (например, перепутаны флешкарты, диски и т. п.). Конструкция предполагаемой диспозиции связана с повышенной ответственностью определенных лиц в отношении наиболее важной информации персонального характера, поскольку даже легкомысленные или небрежные поступки приведут или могут привести к тяжким последствиям.

В состав субъективной стороны также входит мотив, т. е. то, что побудило лицо совершить преступление, а также цель – преступный результат, достичь которого стремилось такое лицо. Эти элементы крайне важны, поскольку они не только могут содержаться в самих диспозициях и являться линией разграничения преступного деяния от иных, но и в соответствии со ст. 62 УК Республики Беларусь влияют на степень индивидуализации уголовного наказания.

Профессор Т. И. Довнар отмечает, что «матыў злачынства амаль не ўплываў на ступень небяспекі і каральнасці, аднак у шэрагу артыкулаў заканадаўца звяртае ўвагу на яго як абцяжарваючыя або змягчаючыя адказнасць акалічнасці» [9, с. 143].

В качестве основного мотива незаконный оборот персональных данных осуществляется исходя из корыстных побуждений. Персональные данные являются основным ключом для осуществления хищения, как правило, денежных средств.

Нередко встречаются ситуации, когда незаконный оборот персональных данных вызван чувством ревности, желанием установить контроль над личностью, возможно, унизить человека (контроль за передвижениями, социальными сетями, владение данными об интимной жизни и т. п.). Зачастую незаконный оборот персональных данных совершается таким специальным видом субъектов, как компьютерные преступники, которые совершают посягательства на персональные данные с желанием показать свое превосходство, профессионализм и т. д. Такой мотив можно рассматривать хулиганским в случае, например, массовых атак на информационные системы, извлечения из них персональных данных и их всеобщей публичной огласке. Считаем, что в данной ситуации можно говорить о стремлении компьютерного преступника проявить явное неуважение к обществу и продемонстрировать пренебрежение к общепринятым правилам общения.

Е. П. Ищенко выделяет следующие группы «компьютерных преступников»:

1) хакеры – лица, рассматривающие меры защиты информационных систем как личный вызов и взламывающие их с целью получения контроля за информацией независимо от ее ценности;

2) шпионы – лица, взламывающие защиту информационных систем для получения информации, которую можно использовать в целях политического влияния;

3) террористы – лица, взламывающие информационные системы для создания эффекта опасности, который можно использовать и в целях политического влияния;

4) корпоративные налетчики – служащие компании, взламывающие компьютеры конкурентов для экономического влияния;

5) воры – лица, вторгающиеся в информационные системы для получения личной выгоды;

6) вандалы – лица, взламывающие системы с целью их разрушения;

7) нарушители правил пользования ЭВМ, совершающие противоправные действия из-за недостаточного знания техники и порядка пользования информационными ресурсами;

8) лица с психическими аномалиями, страдающие новым видом заболеваний – информационными болезнями, или компьютерными фобиями [10, с. 726–727].

Еще одним мотивом может являться стремление подорвать доверие и авторитет власти. Например, номера телефонов, адреса и банковские данные более 400 немецких политиков, в том числе и личные данные канцлера Германии Ангелы Меркель, были опубликованы хакерами в сети [11]. В данном случае можно отметить, что специальным субъектом совершения подобного незаконного деяния являются журналисты.

Особое место в классификации занимают чувствительные персональные данные, незаконный оборот которыми может совершаться по мотивам расовой, национальной, религиозной вражды и розни, плитической или идеологической вражды. Например, эксперт по вопросам кибербезопасности и нормативно-правовой базы в сфере IT Виктор Дубров сообщил о трех убийствах граждан, персональные данные которых

были похищены и пред-ставлены как неугодные потенциальным преступникам на известном украинском портале «Миротворец» [12].

Цель совершения преступления позволяет отграничить преступное деяние от непреступного, а также правильно квалифицировать те либо иные действия правонарушителя. Отсутствие доказательств целей совершения преступлений признает отсутствие общественной опасности совершенных деяний.

В результате анализа статей УК Республики Беларусь, содержащих цель как квалифицирующий признак, можно сделать вывод, что к основным видам целей совершения преступлений можно отнести следующие:

1) сокрытие другого преступления или облегчение его совершения (например, внесены изменения в персональные данные либо они удалены, не сохранены, обезличены и т. д.);

2) вызов агрессии одной страны против другой, провокация международных осложнений или войны (например, международный эксперт по вопросам информатики Д. Паркер считает, что на смену опасности возникновения ядерной катастрофы может прийти угроза развязывания войны, которая примет новые формы. Это будет борьба, направленная против стран, обладающих передовой технологией, в целях создания хаоса в информационных структурах и порождения экономической катастрофы [13, с. 3].);

3) получение трансплантата или использования его частей, либо изъятие органов или тканей для трансплантации;

4) утаивание или искажение информации о человеке, его местонахождении, передвижениях и т. д.

5) получение каких-либо выгод, не связанных с получением денежных средств;

6) возбуждение у индивидуально неопределенного круга лиц решимости совершить самоубийство;

7) трансграничная передача персональных данных иностранному субъекту;

8) воспрепятствование деятельности должностных лиц либо принуждение к изменению характера этой деятельности;

9) терроризирование;

10) шантаж (например, из судебной практики Российской Федерации можно привести случай, когда пользователи социальный сетей похищают персональные данные, а затем вымогают денежные средства или шантажируют потерпевших под угрозой распространения сведений личного характера [14, с. 145]);

11) искажение данных отчетности;

12) уклонение от воинской службы.

Как видно, целями совершения незаконного оборота персональных является широкий круг видов преступного результата, имеющих отношении ко многим составам преступлений, имеющих различные объекты уголовно-правовой охраны. Стоит отметить, что одним из видов квалифицирующих признаков является совершение определенных деяний в целях совершения иных преступлений.

Например, по ст. 294 УК Республики Беларусь преступным признается хищение огнестрельного оружия, его составных частей или компонентов, боеприпасов, взрывчатых веществ или взрывных устройств (далее – хищение оружия). Часть 4 этой статьи квалифицирует совершение хищения оружия в целях совершения таких преступлений, как акт международного терроризма (ст. 126), геноцид (ст. 127), создание незаконного вооруженного формирования (ст. 287), захват заложника (ст. 291), диверсия (ст. 360).

Незаконный оборот персональных данных, как правило, совершается в определенных целях, поэтому считаем целесообразным его квалифицировать в зависимости от желания субъекта посягательств совершить то либо иное преступление (например, незаконный оборот персональных данных в целях вмешательства в деятельность сотрудника органов внутренних дел (ст. 365)).

Как справедливо отмечает А. В. Шидловский, социальная опасность существенно повышается там, где деяние имеет направленность на совершение другого социально опасного деяния. Следовательно, мотив и цель не только неразрывно связаны с деянием, но и могут влиять на уровень его общественной опасности [15, с. 34].

Также в практике встречаются такие целевые установки при совершении незаконного оборота персональных данных, как личные неприязненные отношения, желание умалить репутацию человека, нанести ему нравственные страдания, сформировать негативное отношение к потерпевшему со сто-

роны его близких. Одним из мотивов получения информации с ограниченным доступом С. В. Баринов называет необдуманное желание оказать помощь посторонним лицам [14, с. 147].

Кроме этого, необходимо отдельно рассматривать незаконный оборот персональных данных, если он не охватывается самостоятельным состав преступления, в качестве стадии приготовления к совершению любого преступления. Так, в соответствии со ст. 13 УК Республики Беларусь приготовлением к преступлению признается приискание или приспособление средств или орудий либо иное умышленное создание условий для совершения конкретного преступления.

Заключение

В результате анализа посягательств на персональные данные, а также субъективной стороны преступлений, предусмотренных УК Республики Беларусь и имеющих схожий уголовно-правовой объект, считаем необходимым по общему правилу криминализировать умышленные посягательства на персональные данные, т. е. совершенные с прямым либо косвенным умыслом, при наличии тяжких последствий либо причинения ущерба в крупном и особо крупном размерах. При этом неосторожная вина может быть установлена только в случае посягательств на наиболее чувствительные персональные данные и при условии, что субъект нарушил определенные правила обращения с ними.

Цели и мотивы посягательств на персональные данные должны являться квалифицирующими признаками и основой для разграничение преступных деяний от правонарушений. Криминализации может подлежать незаконный оборот персональных данных без последствий, однако в случае доказанной цели в совершении иного преступления.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Грунтов, И. О. К вопросу о содержании принципа личной виновной ответственности в уголовном законе / И. О. Грунтов // Совершенствования правового регулирования и механизмов функционирования системы противодействия преступности : ма-териалы междунар. науч.-практ. конф., Минск, 18–19 окт. 2013 г. / Белорус. гос. ун-т. – Минск : БГУ, 2013. – С. 32–35.

2. Белорусская юридическая энциклопедия : в 4 т. – Минск, 2007–2013. – Т. 3: П–С. – 2010. – С. 587–588.

3. Правовой форум Беларусь [Электронный ресурс]. – Режим доступа: http://forum-pravo.-by/forums/npa.aspx?forum=15&topic=10297/. – Дата доступа: 01.02.2020.

4. Вабищевич, В. В. Общественно опасные посягательства на персональные данные как основание криминализации / В. В. Вабищевич // Право.by. – 2019. – № 1 (57). – С. 58–62.

5. Вабищевич, В. В. Зарубежный опыт уголовно-правовой охраны персональных данных / В. В. Вабищевич // Журн. Белорус. гос. ун-та. Право. – 2019. – № 1. – С. 72–80.

6. В Чечерске мужчина влез в аккаунт дочери в соцсети – и теперь ему грозит пять лет [Электронный ресурс]. – Режим доступа: https://news.tut.by/society/638687.html. – Дата доступа: 04.04.2020.

7. Прокуратура: Военкомат нарушил закон при публикации в газете личных данных «уклонистов» [Электронный ресурс]. – Режим доступа: https://news.tut.by/soci-ety/590846.html. – Дата доступа: 04.04.2020.

8. Сапранкова, Т. Ю. Особенности субъективной стороны нарушения неприкосновенности частной жизни / Т. Ю. Сапранкова // Балт. гуманитар. журн. – 2016. – Т. 5, № 4 (17). – С. 403–406.

9. Доўнар, Т. І. Гісторыя дзяржавы і права Беларусі / Т. І. Доўнар. – Мінск, 2011. – 549 с.

10. Ищенко, Е. П. Криминалистика : учебник / Е. П. Ищенко, А. А. Топорков / под ред. Е. П. Ищенко. – М. : КОНТРАКТ : Инфра-М, 2006. – 784 с.

11. Хакеры выложили в сеть данные сотен немецких политиков [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/technology_and_media/04/01/2019/5c2f174-69a794736a28c6-47f. – Дата доступа: 04.04.2020.

12. «Закон работает, и это – факт»: Роскомнадзор защитил 90 млн человек от кражи персональных данных [Электронный ресурс]. – Режим доступа: http://inforeac-tor.ru/98875-zakon-rabotaet-i-eto-fakt-roskomnadzor-zashchitil-90-mln-chelovek-ot-krazhi-personalnyh-dannyh. – Дата доступа: 03.04.2020.

13. Березюк, Л. П. Организационное обеспечение информационной безопасности : учеб. пособие / Л. П. Березюк. – Хабаровск : Изд-во ДВГУПС, 2008. – 188 с.

14. Баринов, С. В. Криминалистическая характеристика личности преступника, совершающего преступные нарушения неприкосновенности частной жизни / С. В. Баринов // Актуал. проблемы рос. права. – 2018. – № 1 (86). – С. 142–150.

15. Шидловский, А. В. Назначение наказания по уголовному праву Беларуси / А. В. Шидловский. – Минск : БГУ, 2015. – 295 с.

Рукапіс паступіў у рэдакцыю 27.05.2020