ВЕСТНИК ЮГОРСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
2023 г. Выпуск 3. С. 71–78

УДК 343.4
DOI: 10.18822/byusu20230371-78

КРИМИНАЛИЗАЦИЯ НЕВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Должикова Анна Эдуардовна
аспирант кафедры уголовного права, уголовного процесса и криминалистики,
Российский университет дружбы народов
Москва, Россия
E-mail: l_a_buka@mail.ru

Предмет исследования: персональные данные как предмет общественно опасного деяния.

Цель исследования: обоснование необходимости включения в Уголовный кодекс России (далее – УК РФ) нормы об ответственности за невыполнение требований по защите персональных данных.

Методы и объекты исследования: при подготовке настоящей работы применялись индуктивный и дедуктивный методы формальной логики, диалектический метод познания, метод сопоставительного анализа, в т. ч. контент-анализа действующих источников российского и зарубежного права, а также метод экспертных оценок по вопросам общественной опасности незаконных деяний в области обращения персональных данных.

Результаты исследования: доказано, что цифровая трансформация экономики оказывает существенное влияние на все отношения в современном обществе. Поэтому ценность информации о личности значительно повышается. Она становится средством для пользования различными сервисами, в т. ч. обеспечивающими обмен материальными и иными ценностями. Учитывая данное обстоятельство, охрана персональных данных должна быть обеспечена не только гражданским и административным, но и уголовным законодательством. Для этого необходимо введение уголовной ответственности за невыполнение требований по защите персональных данных.

Ключевые слова: персональные данные, уголовная ответственность за невыполнение требований по защите персональных данных, общественная опасность нарушения законодательства о персональных данных, цифровизация экономики, преступления в сфере компьютерной информации, конфиденциальная информация.

CRIMINALIZATION OF FAILURE TO COMPLY WITH PERSONAL DATA PROTECTION REQUIREMENTS

Anna E. Dolzhikova
Postgraduate student of the Department of Criminal Law, Criminal Procedure and Criminology
Peoples' Friendship University of Russia
Moscow, Russia
E-mail: l_a_buka@mail.ru

Subject of research: personal data as the subject of a socially dangerous act.

Purpose of research: to justify the need to include in the Criminal Code of Russia (hereinafter referred to as the Criminal Code of the Russian Federation) a rule on liability for failure to comply with requirements for the protection of personal data.

Methods and objects of research: in the preparation of this work, inductive and deductive methods of formal logic, the dialectical method of cognition, and the method of comparative analysis were

used, incl. content analysis of current sources of Russian and foreign law, as well as a method of expert assessments on issues of the public danger of illegal acts in the field of circulation of personal data.

Main results of research: it has been proven that the digital transformation of the economy has a significant impact on all relationships in modern society. Therefore, the value of information about a person increases significantly. It becomes a means for using various services, incl. ensuring the exchange of material and other values. Taking into account this circumstance, the protection of personal data must be ensured not only by civil and administrative, but also by criminal legislation. This requires the introduction of criminal liability for failure to comply with requirements for the protection of personal data.

Key words: personal data, criminal liability for failure to comply with requirements for the protection of personal data, the public danger of violating the legislation on personal data, digitalization of the economy, crimes in the field of computer information, confidential information.

Введение

Политика государства по цифровизации экономики неизменно приводит к обновлению отношений в каждой сфере жизни человека. На рынке цифровых услуг уже предложено большое количество сервисов, благодаря которым человек без личного участия способен удовлетворить не только материальные потребности: Интернет-магазин, on-line доставка и проч., но и обеспечить реализацию политических прав, заключить/расторгнуть договор с контрагентом, выполнить обязанность налогоплательщика, получить данные о результатах медицинских исследований и т. п. К примеру, по данным Минцифры, в голосовании 8 сентября 2023 года жители различных регионов России могли принять участие дистанционно, предварительно пройдя регистрацию на портале «Госуслуги». Общее количество зарегистрированных избирателей на день голосования составило более 1,2 млн человек [1]. Значительно большее количество пользователей Интернет-ресурсов в настоящее время зарегистрировано на сервисах розничной купли-продажи: Ozon, Wildberries, Joom и др.

Развитие цифровых отношений и активное вовлечение новых участников цифровых отношений, включая сферы, которые ранее даже не рассматривались как объект оцифровки и алгоритмизации [2, с. 193-194], предполагает передачу значительного объема информации о конкретном человеке, т. е. идентифицирующих его сведений. В настоящее время констатируется повышенный интерес представителей криминалитета к базам персональных данных, формируемых различными организациями – операторами обработки персональных данных клиентов. Количество граждан России, персональные данные которых были похищены и предлагаются для продажи, уже исчисляется десятками миллионов человек [3, с. 133].

Появление широких возможностей использования персональных данных как их носителем, так и третьими лицами, создает реальную угрозу для причинения не только морального и имущественного ущерба, но и физического вреда вследствие неправомерного использования персональных данных. В научной литературе высказывается предположение о возможной смене ядерной опасности на цифровую угрозу глобального значения. Ее реализация повлечет за собой техногенные и иные катастрофы, вызванные неправомерным использованием персональных данных для совершения различных преступлений: от мошеннических действий до диверсий и массовых убийств [4, с. 64-65].

Проблема охраны персональных данных, в т. ч. уголовно-правовыми средствами, приобрела значительную актуальность во многих зарубежных государствах. По оценкам исследователей в уголовные законы зарубежных стран активно вносятся изменения, касающиеся установления специальными нормами ответственности за незаконные действия, предметом которых выступают персональные данные граждан. В большинстве случаев эти преступления рассматриваются в качестве разновидности посягательств на частную жизнь личности, а

персональные данные оцениваются в качестве конфиденциальной информации – личной или иной тайны. В той или иной степени специальные уголовно-правовые нормы об охране персональных данных содержатся в законодательстве Дании, Лихтенштейна, Нидерландов, Великобритании и др. [5, с. 65-74]. При этом сфера уголовно-правовой охраны, которая подвергается угрозе нарушения при незаконном использовании персональных данных, сводится к информационной безопасности, неприкосновенности частной жизни личности (переписка, почтовые отправления, телефонные и иные переговоры) и неприкосновенность жилища [6, с. 10, 38-74].

Учитывая кардинальные изменения общественных отношений в части безопасности граждан, обеспечения охраны их прав и интересов имущественного и личного неимущественного характера, необходимо проведение исследования на предмет необходимости включения в действующий УК РФ специальной нормы об ответственности за незаконные действия с персональными данными.

Результаты и обсуждение

Изначально дефиниция «персональные данные» была закреплена Федеральным законом от 20.02.1995 №24-ФЗ «Об информации, информатизации и защите информации» (утратил силу). Под ними понималась конфиденциальная информация о гражданах, касающаяся их частной жизни, личной и семейной тайны, тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Точного перечня персональных данных указанный закон не содержал, но предусматривал запрет на их несанкционированные сбор, хранение, использование и распространение.

В соответствии с действующим законодательством персональные данные представляют собой любую информацию, которая прямо или косвенно относится к определенному или определяемому физическому лицу (п. 1 ст. 3 Федерального закона от 27.07.2006 №152-ФЗ (по сост. на 06.02.2023) «О персональных данных»). Приведенное определение сформулировано чрезмерно широко, что не способствует определению круга общественных отношений, возникающих по поводу обращения и использования персональных данных и нуждающихся в обеспечении уголовно-правовой охраной. Поэтому прав был С.И. Гутник, указавший, что при формулировании определения персональных данных необходимо выделить совокупность трех обязательных признаков соответствующей информации:

- использование персональных данных позволяет обеспечить выделение конкретного физического лица из общей массы иных лиц – обладателей своих персональных данных;
- свободное неконтролируемое обращение сведений о физических лицах создает реальную угрозу для причинения вреда правам и законным интересам личности;
- конфиденциальность сведений, включаемых в содержание термина «персональные данные» [7, с. 10-11].

Учитывая вред, который уже в настоящее время причиняется при неправомерном доступе и/или распространении персональных данных, следует уточнить, что свободное и неконтролируемое обращение персональных данных может не только нарушить права и законные интересы конкретного лица – обладателя, но и третьих лиц, которые находятся в служебных, договорных и иных отношениях с правообладателем.

Несмотря на значительную общественную опасность неправомерных действий с персональными данными, которые в ряде случаев могут повлечь за собой наступление общественно опасных последствий, требующих уголовно-правового реагирования, в действующем УК РФ специальная норма об ответственности за такие деяния отсутствует. Пленум Верховного Суда РФ довольно сдержанно указывает на некоторые преступления, в составах которых могут иметь место персональные данные гражданина. Постановление от 27.12.2002 №29 (по сост. на 15.12.2022) «О судебной практике по делам о краже, грабеже и разбое» содержит

разъяснение (п. 251), что хищение денежных средств с банковского счета или электронных денежных средств, совершенное с использованием конфиденциальной информации владельца, в т. ч. его персональные данные, квалифицируется по п. «г» ч. 3 ст. 158 УК РФ. Если хищение указанных предметов совершается путем обмана или злоупотребления доверием, то при прочих равных условиях оно также квалифицируется как кража (п. 17 Постановления Пленума Верховного Суда РФ от 30.11.2017 №48 (по сост. на 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате»).

В соответствии с п. 3 Постановления Пленума Верховного Суда РФ от 15.12.2022 №37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»», охраняемая ч. 1 ст. 272 УК РФ компьютерная информация, для которой установлен специальный режим правовой защиты, включая отнесение ее к разновидности государственной, коммерческой, служебной, личной, семейной или иной тайны, в том числе и персональные данные. Таким образом, Пленум Верховного Суда РФ указывает, что персональные данные в настоящее время следует рассматривать или как средство, или как предмет для отдельных составов преступлений.

Проблема определения объема информации, который охватывается понятием «персональные данные», а равно – и особенностей юридической защиты этой информации от получения, обработки и использования в нарушение интересов ее обладателя, в научной литературе была обозначена уже в начале текущего столетия. По причине «универсальности» использования персональных данных решение о необходимости обеспечения межотраслевой дифференциации юридической ответственности за совершение неправомерных действий, предметом которых они являются, уже тогда сомнений не вызывало [8, с. 7].

Многие авторы сходятся во мнении о том, что за незаконные действия с персональными данными необходимо установить уголовную ответственность, но при этом предлагают различные варианты в части и вариантов квалификации указанных общественно опасных деяний по уже действующим уголовно-правовым нормам, и видов криминализируемых действий. Так, А.Ю. Волкова, ссылаясь на отдельные вступившие в законную силу приговоры, обосновывает необходимость квалификации незаконных действий с персональными данными граждан по ст. 137 или 272 УК РФ [3, с. 135-136].

С.И. Гутник обосновал необходимость корректировки положений ст. 137 и 183 УК РФ, которые должны применяться в случае «распространения» сведений, которые являются персональными данными. Он указывает, что уголовная ответственность в таких случаях будет возможной, если лицо-правообладатель не давало разрешения на распространения своих персональных данных, а лицо-правонарушитель совершает запрещённые действующим законодательством действия с персональными данными. Аналогичные действия, по мнению автора, не образуют состава преступления, предусмотренного ст. 272 УК РФ [7, с. 12-13].

А.А. Шутова приводит доводы о том, что при совершении незаконных действий с персональными (но не регистрационными) данными, которые включаются в объем банковской тайны, нарушаются три самостоятельных, но взаимосвязанных друг с другом объекта уголовно-правовой охраны: отношения собственности, отношения в сфере охраны компьютерной информации и информационно-экономические отношения. Исходя из этого, автор полагает, что совершение указанных выше действий образует идеальную совокупность преступлений, предусмотренных ст. 158, 183 и 272 УК РФ [9, с. 11, 131].

Б.Н. Кадников полагает, что обеспечение прав и законных интересов граждан в части сохранности и правомерности пользования их персональными данными должно осуществляться в соответствии со специальной нормой Особенной части УК РФ. Общая уголовно-правовая норма (ст. 137 УК РФ) не охватывает перечисленные действия, а равно предусматривает чрезмерно мягкие меры ответственности в сравнении с общественной опасностью незаконных действий – нарушения правил обращения с персональными данными граждан. Поэтому в условиях обеспечения надлежащей охраны персональных данных граждан необхо-

дима более емкая дифференциация уголовной ответственности по увеличению степени строгости наказаний, предусмотренных ст. 137 УК РФ, а также введение специальной уголовно-правовой нормы об ответственности за нарушение правил обращения с персональными данными – конфиденциальной информацией [10, с. 11, 24]. Но, указывая на необходимость введения специальной нормы, автор не предлагает ее содержания и точно не указывает место ее предполагаемого нахождения, исходя из родового объекта общественно опасного посягательства.

Аналогичной позиции придерживается Е.В. Хохлова. Не предлагая конкретного описания диспозиции и санкции специальной уголовно-правовой нормы, она предлагает аргументацию «социально-правового и криминологического» содержания в пользу введения такой нормы в отечественный уголовный закон. Общественная опасность деяний, связанных с нарушением правового режима использования персональных данных, обусловлена высокой ценностью нарушаемых прав и свобод – жизнь, личная/семейная тайна, честь, достоинство, собственность, а также особенностями современных отношений, в которых ключевую роль стала играть глобальная компьютеризированность, виртуализация [11, с. 146].

И.Н. Мосечкин также указывает на необходимость установления специальной нормой уголовной ответственности за посягательства на персональные данные, которые выражаются в их незаконном получении, хранении, обработке, сбыте и использовании. Данные общественно опасные действия указывают на принципиально новое преступление, которое автор предлагает именовать «кражей личности» [12, с. 201], но не раскрывает юридических особенностей и предполагаемых признаков его состава.

Некоторые авторы небезосновательно полагают, что использование в нормах уголовного закона конструкции «похищение личности» нежелательно, т. к. в таком случае человек приравнивается к предмету гражданско-правовых отношений [13, с. 156]. Хищение и иные незаконные действия с персональными данными следует рассматривать в качестве преступления, ответственность за которое предусмотрено отдельной нормой из гл. 19 УК РФ. Авторы также предлагают рабочий вариант диспозиции этой уголовно-правовой нормы: «Незаконное получение цифровых идентификационных данных. Получение цифровых идентификационных данных путем похищения, обмана, шантажа, принуждения, угрозы применения насилия либо иным незаконным способом…». Правда, здесь же делается оговорка, что данное преступление следует квалифицировать по совокупности со статьями иных глав УК РФ в зависимости от посягательства на объект уголовно-правовой охраны [13, с. 155-156]. В этом случае предлагаемое решение нельзя считать окончательным, т. к. во всех случаях совершения преступления, предметом которых являются персональные данные, по мнению авторов, всегда будет требовать дополнительной квалификации и установления идеальной совокупности.

Учитывая приведенные мнения, следует поддержать идею о необходимости разработки специальной уголовно-правовой нормы об ответственности за совершение общественно опасных деяний, нарушающих требования законодательства о персональных данных гражданина. В этой связи возникает ряд задач, связанных с определением общественной опасности такого деяния, которая была бы достаточна для криминализации. Такая задача решается путем осуществления сопоставительного анализа действующих норм об административной ответственности за неправомерные действия с персональными данными, а также моделированием негативных последствий, которые могут наступить в результате совершения таких правонарушений.

Итак, действующее российское законодательство предусматривает различные виды юридической ответственности за нарушение правил обращения персональных данных. КоАП РФ содержит ряд специальных норм об ответственности для физических лиц и организаций за неправомерные действия с персональными данными граждан: ст. 13.11. Нарушение законодательства РФ в области персональных данных и ст. 19.7.9. Непредоставление сведений в автоматизированные централизованные базы персональных данных о пассажирах и персонале транспортных средств.

Оценивая общественную опасность таких действий, а равно – перспективы криминализации, можно предположить, что деяния, перечисленные в частях ст. 19.7.9 КоАП РФ, по своему

содержанию не относятся к предмету настоящего исследования. Описанные в указанной норме деяния не предполагают незаконного получения персональных данных, равно как и иных незаконных действий с их разглашением и/или использованием. Поэтому анализ противоправных действий, которые при стечении определенных обстоятельств могут приобрести повышенную общественную опасность, распространяется только на содержание ст. 13.11 КоАП РФ.

Действие данной нормы распространяется на физических и юридических лиц, подлежащих ответственности за совершение нарушений действующего законодательства о персональных данных. Учитывая, что уголовная ответственность организаций действующим законодательством исключается, следует рассмотреть содержание деяний-правонарушений, ответственность за совершение которых может быть возложена на физическое лицо за утрату или иное несанкционированное распространение персональных данных, а равно – создания условий, при которых будет возможным получение персональных данных третьими, не уполномоченными на то лицами:

- неправомерная обработка персональных данных (ч. 1 ст. 13.11 КоАП РФ);
- обработка персональных данных, произведенная без согласия их правообладателя – субъекта персональных данных (ч. 2 ст. 13.11 КоАП РФ);
- невыполнение обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных (ч. 4 ст. 13.11 КоАП РФ);
- невыполнение обязанности о блокировании или уничтожении персональных данных в случае, если персональные данные были неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки (ч. 5 ст. 13.11 КоАП РФ);
- невыполнение обязанности по соблюдению условий сохранности персональных данных и исключающих несанкционированный к ним доступ, если это повлекло различные «неправомерные действия» в отношении персональных данных (ч. 6 ст. 13.11 КоАП РФ).

Перечисленные в ст. 13.11 КоАП РФ деяния представляют собой частные случаи нарушения установленных действующим законодательством правил обращения персональных данных граждан. Сами по себе они едва ли могут претендовать на статус преступления в виду отсутствия должной общественной опасности. Поэтому криминализация правонарушения, предметом которого являются персональные данные, возможна только в случаях наступления общественно опасных последствий в виде причинения вреда жизни и здоровью, имущественного ущерба или иных тяжких последствий.

Толкование содержания ст. 13.11 КоАП РФ позволяет заключить, что лицо, допущенное в установленном законом порядке, к получению, обобщению, систематизации и иным действиям с персональными данными, может в случае нарушения нормативных требований безопасности создать угрозу для утраты и/или получения третьими неуправомоченными лицами конфиденциальной информации – персональных данных, а равно – их действительная утрата и/или распространение. Поэтому при формулировании уголовно-правовой нормы нет необходимости перечислять все возможные виды нарушений законодательства о персональных данных в качестве общественно опасного деяния – признака объективной стороны. Но все же следует понимать, что общественная опасность такого преступления формируется ввиду несанкционированной передачи или получения персональных данных третьими неуправомоченными лицами, которые, в свою очередь, получают возможность для совершения противоправных действий, направленных против прав, свобод и законных интересов граждан, интересов общества и государства.

Юридическая конструкция состава преступления, предметом которого являются персональные данные, должна предполагать наступление общественно опасных последствий, которые выступают обязательным признаком объективной стороны. Конструирование состава преступления как формального не обеспечит должного уровня общественной опасности для криминализации и сведет описываемое деяние к уровню административного правонарушения. В части видов общественно опасных последствий следует предусмотреть имуществен-

ный ущерб в размерах, сопоставимых с особо крупным размером хищений, т. е. от одного миллиона рублей. Для обеспечения высокого уровня дифференциации ответственности за совершение преступления последствия в виде причинения вреда здоровью, жизни человека, а также иные тяжкие последствия необходимо рассматривать в качестве квалифицирующих обстоятельств по отношению к признакам основного состава преступления.

Заключение и выводы

Результаты, полученные в ходе представленного исследования, могут быть представлены следующими выводами:

1. Официальное определение дефиниции «персональные данные» сформулировано крайне широко, что позволяет признать таковыми любые сведения, так или иначе характеризующие или относящиеся к конкретному физическому лицу. Для установления ответственности за противоправные действия, предметом которых являются персональные данные, необходимо конкретизировать их содержание. Поэтому под персональными данными следует понимать только ту информацию, свободное обращение которой может причинить вред конкретному физическому лицу и/или третьим лицам.

2. Ответственность за незаконные действия по распространению персональных данных следует предусмотреть в отдельной норме действующего уголовного закона. По конструкции состав такого преступления должен быть материальным. Для соблюдения правил построения уголовно-правовых норм при описании деяния следует использовать общие формулировки, указывающие на совершение нарушения законодательства о персональных данных без конкретизации видов таких нарушений. Открытый перечень деяний, предметом которых выступают персональные данные, обеспечит установление ответственности за любые действия, если они повлекли за собой соответствующие последствия. Поэтому описание деяния может быть представлено в следующем виде: «невыполнение требований по защите персональных данных».

3. Общественно опасные последствия как обязательный признак объективной стороны состава преступления должны включать в себя имущественный ущерб в сумме, превышающей один миллион рублей. Для обеспечения высокого уровня дифференциации ответственности за совершение преступления последствия в виде причинения вреда здоровью, жизни человека, а также иные тяжкие последствия необходимо рассматривать в качестве квалифицирующих обстоятельств по отношению к признакам основного состава преступления.

Литература

1. В электронном голосовании приняли участие уже больше половины зарегистрированных онлайн-избирателей / Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. – URL: https://digital.gov.ru/ru/events/46975/?utm_referrer=https%3a%2f%2fyandex.ru%2f (дата обращения: 15.09.2023). – Текст : электронный.

2. Лапшин, В. Ф. Назначение наказания компьютерной программой: правовая инновация или деградация? / В. Ф. Лапшин // Пенитенциарная наука. – 2020. – Т. 14, № 2. – С. 192-198. – Текст : непосредственный.

3. Волкова, А. Ю. Персональные данные как объект уголовно-правовой охраны / А. Ю. Волкова // Уголовное право: стратегия развития в XXI веке. – 2023. – № 3. – С. 132-137. – Текст : непосредственный.

4. Вабищевич, В. В. Социально-правовые и исторические предпосылки криминализации вмешательства в персональные данные / В. В. Вабищевич // Журнал Белорусского государственного университета. Право. – 2020. – № 1. – С. 61-71. – Текст : непосредственный

5. Хохлова, Е. В. Уголовно-правовая охрана персональных данных в зарубежных странах / Е. В. Хохлова // Известия Юго-Западного государственного университета. Серия: История и право. – 2022. – Т. 12, № 4. – С. 62-78. – Текст : непосредственный.

6. Проскурякова, М. И. Защита персональных данных в праве России и Германии: конституционно-правовой аспект : дис. … канд. юрид. наук / М. И. Проскурякова. – СПб., 2017. 193 с. – Текст : непосредственный.

7. Гутник, С. И. Уголовно-правовая характеристика преступных посягательств в отношении персональных данных: дис. … канд. юрид. наук / С. И. Гутник. – Красноярск, 2017. 241 с. – Текст : непосредственный.

8. Просветова, О. Б. Защита персональных данных: автореф. дис. … канд. юрид. наук / О. Б. Просветова. – Воронеж, 2005. – 24 с. – Текст : непосредственный.

9. Шутова, А. А. Уголовно-правовое противодействие информационным преступлениям в сфере экономической деятельности: теоретический и прикладной аспекты : дис. … канд. юрид. наук / А. А. Шутова. – Н. Новгород, 2017. – 264 с. – Текст : непосредственный.

10. Кадников, Б. Н. Уголовно-правовая охрана конституционного права граждан на неприкосновенность частной жизни : автореф. дис. … канд. юрид. наук / Б. Н. Кадников. – М., 2008. – 27 с. – Текст : непосредственный.

11. Хохлова, Е. В. Социальная обусловленность уголовной ответственности за преступления, связанные с персональными данными / Е. В. Хохлова. – Текст : непосредственный // Вестник Тверского государственного университета. Серия «Право». – 2022. – № 3. – С. 141-148.

12. Мосечкин, И. Н. Направления совершенствования уголовно-правовых средств обеспечения защиты персональных данных / И. Н. Мосечкин. – Текст : непосредственный // Научные исследования в современном мире. Теория и практика. Сборник избранных статей Всероссийской (национальной) научно-практической конференции (Санкт-Петербург, 10 января 2022). – СПб.: ГНИИ «Нацразвитие», 2022. – С. 200-202.

13. Зварыгин, В. Е. Похищение «цифровой личности»: проблемы квалификации / В. Е. Зварыгин, А. М. Ахатова. – Текст : непосредственный // Уголовное право: стратегия развития в XXI веке. – 2023. – № 3. – С. 148-157.