распрацоўваецца і выкарыстоўваецца для павышэння эфектыўнасці іх выяўлення, раскрыцця, расследавання і папярэджання.

Асноўнымі структурнымі элементамі крыміналістычных характарыстык махлярстваў (раскраданняў шляхам злоўжывання службовымі паўнамоцтвамі) у сферы РПЗ з'яўляюцца: суб'екты ўчынення злачынства (службовыя і іншыя асобы) і іх намеры, абстаноўка ўчынення злачынства, вызначаная парадкам рэалізацыі праваадносін па РПЗ, спосаб учынення і ўтойвання злачынства, тыповыя сляды.

Структуры крыміналістычных характарыстык махлярстваў і раскраданняў шляхам злоўжывання службовымі паўнамоцтвамі ў сферы РПЗ маюць пэўныя адрозненні, абумоўленыя перш за ўсё складам суб'ектаў і спосабам учынення злачынстваў.

Спіс выкарыстаных крыніц

1. Александров, А. И. Криминалистическая характеристика краж с проникновением в жилище и их расследование : автореф. дис. ... канд. юрид. наук : 12.00.09 / А. И. Александров ; Ленингр. гос. ун-т им. А. А. Жданова. – Л., 1985. – 19 с.

2. Белкин, Р. С. Криминалистика: проблемы сегодняшнего дня : Злободневные вопросы российской криминалистики / Р. С. Белкин. – М. : Норма, 2001. – 240 с.

3. Ермолович, В. Ф. Криминалистическая характеристика преступлений / В. Ф. Ермолович. – Минск : Амалфея. – 2013. – 304 с.

4. Жердев, В. А. Криминалистическая характеристика краж, грабежей и разбойных нападений: методика расследования и методы раскрытия групповых преступлений : автореф. дис. ... канд. юрид. наук : 12.00.09 / В. А. Жердев ; Сарат. гос. акад. права. – Саратов, 2001. – 22 с.

5. Каменецкий, Ю. Ф. Расследование хищений путем злоупотребления служебными полномочиями в бюджетной сфере : монография : в 2 ч. / Ю. Ф. Каменецкий, В. П. Шиенок. – Минск : СтройМедиаПроект, 2017. – Ч. 1 : Теоретические основы и информационное обеспечение. – 248 с.

6. Капіца, П. А. Аб выкарыстанні судовай практыкі па грамадзянскіх справах пры распрацоўцы крыміналістычнай методыкі расследавання раскраданняў у сферы інфарматызацыі дзяржаўных органаў і арганізацый / П. А. Капіца // Право.by. – 2020. – № 3. – С. 78–83.

7. Колесникова, Т. В. Криминалистическая характеристика преступных групп, совершающих вымогательство : автореф. дис. ... канд. юрид. наук : 12.00.09 / Т. В. Колесникова ; Сарат. юрид. ин-т МВД России. – Саратов, 2000. – 23 с.

8. Колесниченко, А. Н. Криминалистическая характеристика преступлений : учеб. пособие / А. Н. Колесниченко, В. Е. Коновалова. – Харьков : Юрид. ин-т, 1985. – 93 с.

9. Криминалистическая методика : учеб. пособие : в 2 ч. / М. П. Шруб [и др.] ; под общ. ред. М. П. Шруба. – Минск : Акад. МВД, 2018. – Ч. 2. – 343 с.

10. Рубцов, И. И. Криминалистическая характеристика преступлений как элемент частных методик расследования : дис. ... канд. юрид. наук : 12.00.09 / И. И. Рубцов. – СПб., 2001. – 225 л.

11. Шебалин, А. В. Расследование хищений средств сотовой связи : автореф. дис. ... канд. юрид. наук : 12.00.09 / А. В. Шебалин ; Сарат. гос. акад. права. – Томск, 2010. – 23 с.

Дата паступлення ў рэдакцыю: 17.05.2022

УДК 343.985.8 + 004:34(476)

***Д. Н. Лахтиков**, кандидат юридических наук, доцент, начальник кафедры информационного права факультета криминальной милиции*
Академии Министерства внутренних дел Республики Беларусь
e-mail: it@amia.by

ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СФЕРЕ

Анализируются проблемные аспекты, связанные с трансформацией преступности в современных условиях. Акцентировано внимание на том, что достаточно остро стоят вопросы обеспечения нацио-

нальной безопасности в информационной сфере, связанные с преступностью. Предлагается рассматривать преступления, совершаемые с использованием информационно-коммуникационных технологий, как угрозу национальной безопасности, определяются отдельные источники этой угрозы.

Ключевые слова: информационная безопасность, информационная сфера, киберпреступность, национальная безопасность, преступность, преступления, совершаемые с использованием информационно-коммуникационных технологий, угроза национальной безопасности

***D. N. Lahtikov**, Candidate of Juridical Sciences, Associate Professor, Head of the Department of Information Law of the Faculty of Criminal Militia of the Academy of the Ministry of Internal Affairs of the Republic of Belarus*
e-mail: it@amia.by

CRIMES COMMITTED USING INFORMATION AND COMMUNICATION TECHNOLOGIES AS A THREAT TO NATIONAL SECURITY IN THE INFORMATION SPHERE

The article analyzes the problematic aspects associated with the transformation of crime in modern conditions. Attention is focused on the fact that the issues of ensuring national security in the information sphere related to crime are quite acute. It is proposed to consider crimes committed with the use of information and communication technologies as a threat to national security, certain sources of this threat are identified.

Keywords: information security; information sphere; cybercrime; national security; crime; crimes committed using information and communication technologies; threat to national security

Информационная сфера Республики Беларусь характеризуется последовательным развитием информационно-коммуникационных технологий, однако на фоне активного развития науки и технологий, их внедрения в повседневную жизнь сформировался новый, более сложный вид преступлений – преступления, совершаемые с использованием информационно-коммуникационных технологий. Это свидетельствует о том, что преступники достаточно оперативно используют результаты научно-технического прогресса в своих целях. Данная тенденция представляет угрозу общественным отношениям, складывающимся в информационной сфере, поскольку на данном этапе развития информационное пространство и общество уже неотделимы. Из-за своего междисциплинарного характера, специфической природы и повышенной социальной опасности данный вид преступлений с момента своего появления и до настоящего времени является предметом исследования и дискуссий широкого круга специалистов (криминологи, криминалисты, специалисты в области оперативно-розыскной деятельности, информационных технологий и защиты информации) о понятии, природе, видах этих преступлений, мерах противодействия им и др.

В соответствии с Концепцией национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575, угрозой национальной безопасности является потенциальная или реально существующая возможность нанесения ущерба национальным интересам Республики Беларусь.

В свою очередь, в научной литературе отмечается, что вопрос определения угроз национальной безопасности в информационной сфере остается не в полной мере проработанным ни на законодательном, ни на научном уровне [8, с. 35–36].

В настоящее время в законодательстве Республики Беларусь (п. 34 указанной Концепции) «рост преступности с использованием информационно-коммуникационных технологий» определен в качестве внутреннего источника угроз национальной безопасности информационной сфере. Анализ термина «рост преступности с использованием информационно-коммуникационных технологий» позволяет сделать вывод, что он не в полной мере раскрывает сущность и количественную характеристику, отражающую рост соответствующих уголовно наказуемых деяний. Преступность – это прежде всего социальное явление (качественное свойство общества), нарушающее общественные отношения и выражающееся в отклонении поведения отдельных членов общества от норм, установленных уголовным законом. Следовательно, использование по отношению к нему количественных показателей не в полной мере является допустимым. С учетом необходимости акцентуации внимания на числовую характеристику (рост, увеличение, динамика) обозначенного явления действующая формулировка может быть закреплена в следующей редакции: «рост преступлений, совершаемых с использованием информационно-

коммуникационных технологий». Полагаем, что указанный подход не только отражает количественную сущность разбираемой смысловой единицы, но и позволяет охватить совокупность преступлений, перечень которых включает в себя, например, деяния, направленные против компьютерной безопасности; преступления, где информационные технологии используются в качестве орудия либо средства совершения преступления; деяния, предметом посягательства которых являются иные охраняемые законом блага, а информация и компьютерные системы (сети) – лишь одним из элементов объективной стороны состава преступления, выступая в качестве, например, орудия либо составной части способа его совершения или сокрытия.

Рассматриваемое понятие является не столько источником угроз национальной безопасности, сколько непосредственно самостоятельной угрозой. Аргументировать указанную позицию можно следующим образом.

Источник угрозы национальной безопасности – это фактор или совокупность факторов, способных при определенных условиях привести к возникновению угрозы национальной безопасности (п. 4 указанной Концепции). С одной стороны, преступность как сложное социальное явление детерминируется определенными явлениями, факторами, обстоятельствами, которые, в свою очередь, взаимодействуют друг с другом при активном влиянии самой преступности; с другой – преступления, совершаемые с использованием информационно-коммуникационных технологий, охватывают такие преступления, как, например, призывы к мерам ограничительного характера (санкциям), иным действиям, направленным на причинение вреда национальной безопасности Республики Беларусь (ст. 361 Уголовного кодекса Республики Беларусь (УК)); создание экстремистского формирования либо участие в нем (ст. 361^1 УК), финансирование экстремистской деятельности (ст. 361^2 УК); изготовление и распространение порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего (ст. 343^1 УК); незаконный оборот наркотических средств, психотропных веществ, их прекурсоров и аналогов (ст. 328 УК); преступления против компьютерной безопасности (ст. 349–355 УК); вымогательство (ст. 208 УК); мошенничество (ст. 209 УК), в том числе совершение которых сопряжено с преступлениями против компьютерной безопасности, и др. Подобные преступления характеризуются рядом признаков, среди которых можно выделить следующие: взаимосвязь с другими видами преступности; высокотехнологичный характер (совершение с использованием информационно-коммуникационных технологий, средств компьютерной техники, носителей компьютерной информации, которые выступают орудиями и средствами совершения преступлений); высокая степень латентности, обусловленная различными факторами; в отдельных случаях организованный характер или тесная взаимосвязь с организованной преступностью; трансграничность (позволяет преступнику с территории одного государства совершать преступления в отношении лиц, находящихся в другом государстве); постоянное совершенствование существующих и создание новых информационно-коммуникационных технологий, используемых в качестве орудий и средств совершения преступлений. К таким признакам также можно отнести особые структурные характеристики преступных формирований, дистанционный способ совершения преступлений, связь не только с иными видами преступлений, но и с целым рядом негативных социальных отклонений (теневая экономика, проституция и т. п.).

Анализ научной литературы и правоприменительной практики показывает, что преступления, совершаемые с использованием информационно-коммуникационных технологий, способны причинить вред различным охраняемым уголовным законом общественным отношениям. Хотя данный вид преступлений рассматривается в качестве новой специфической формы преступлений, следует отметить, что это довольно широкая категория, которая охватывает значительный круг разнородных деяний в информационной сфере.

Общественная опасность заключается и в том, что негативные последствия приводят к серьезным финансовым потерям, нарушениям функционирования инфраструктур, реальным жертвам и т. д.

В свою очередь, анализ состояния криминогенной ситуации в 2015–2021 гг. свидетельствует о том, что более чем в 10 раз возрос удельный вес преступлений, совершенных с использованием информационно-коммуникационных технологий, в общей структуре преступности. При этом по подавляющему большинству (94,8 %) уголовно наказуемых деяний против компьютерной

безопасности (ст. 349–355 УК) лица, их совершившие, не установлены. Это обусловлено тем, что преступления данного вида, как правило, носят трансграничный характер и большое количество противоправных деяний совершаются иностранными гражданами либо с использованием интернет-ресурсов, компьютерных систем, находящихся за пределами государства.

Для анализируемого периода также характерно некоторое снижение преступлений, связанных с незаконным оборотом наркотических средств, психотропных веществ, их прекурсоров и аналогов. Однако в 2021 г. произошел существенный рост (на 30,7 %) числа указанных уголовно наказуемых деяний, включая случаи сбыта (на 43 %). В большинстве своем данные преступления совершены непосредственно с использованием сети Интернет.

Основными детерминантами преступлений, совершаемых с использованием информационно-коммуникационных технологий, являются: возможность извлечения дохода при минимальных затратах и невысоком риске, при этом размер причиняемого преступлениями ущерба за последние годы многократно вырос; низкий уровень осведомленности в области информационной безопасности у пользователей систем дистанционного банковского обслуживания и иных средств интернет-платежей; определенная степень анонимности пользователей сети Интернет, существование иных анонимных информационно-телекоммуникационных сетей, таких как сеть Tor и других средств и методов анонимизации пользователей; определенная степень анонимности финансовых операций, проходящих в информационно-телекоммуникационных сетях; наличие программных уязвимостей разного уровня в экономически значимых информационных системах сети Интернет, позволяющих нейтрализовать систему защиты, используя вредоносное программное обеспечение [7, с. 10–11].

Указанная совокупность признаков отражает высокую степень общественной опасности данных преступлений и предопределяет потенциальную либо реальную возможность нанесения ущерба национальным интересам Республики Беларусь, т. е. угрозу национальной безопасности.

Отдельные авторы отмечают, что основными целями подобных противоправных действий являются следующие: чаще всего совершаются ради экономических целей (например, причинение материального ущерба в виде хищения денежных средств или конфиденциальной информации); могут совершаться и с политической целью (нанесение ущерба базовым политическим и государственным структурам, подрыв системы властных отношений и, как следствие, доверия к власти со стороны населения); следует отметить также идеологические цели (распространение идей и идеологий с целью вербовки интернет-пользователей в ряды, например, радикальных террористических и экстремистских группировок) [2, с. 233–234]. В свою очередь, некоторыми авторами отмечается, что преступная деятельность направлена на получение личной выгоды за счет причинения вреда иным лицам, при этом интеллектуальные и временные затраты, необходимые для осуществления злонамеренных действий, не идут ни в какое сравнение с подготовкой сотрудника правоохранительных органов или инженера. В большинстве случаев преступник неоднократно применяет одну известную ему технологию или методику психологической манипуляции (которую, как правило, даже не сам придумал, а узнал, общаясь в закрытых группах интернет-мошенников, или же купил соответствующую схему действий в даркнете) [3, с. 20].

Изучение опыта Российской Федерации показывает, что законодатель также осознает значение информационной сферы в рамках обеспечения национальной безопасности. При анализе Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 2 июля 2021 г. № 400, можно встретить упоминания о нарастающих угрозах в этой сфере. В частности, закреплено, что достижение цели обеспечения государственной, общественной и информационной безопасности осуществляется путем реализации государственной политики, направленной на решение такой задачи, как предупреждение и пресечение правонарушений и преступлений, совершаемых с использованием информационно-коммуникационных технологий, в том числе легализации преступных доходов, финансирования терроризма, организации незаконного распространения наркотических средств и психотропных веществ, а также использования в противоправных целях цифровых валют, создания условий для эффективного осуществления такой деятельности. Отмечается, что анонимность противоправной деятельности обеспечивается за счет использования информационно-коммуникационных технологий, которые в том числе облегчают совершение преступлений.

Более детально основные угрозы и основы обеспечения безопасности в информационной сфере представлены в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, которая по своему функционально-практическому характеру является логическим продолжением Стратегии национальной безопасности, но со смещением в информационную сферу. В соответствии с п. 14 Доктрины к основным информационным угрозам отнесен рост компьютерной преступности, прежде всего в кредитно-финансовой сфере, а также преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. Отмечается также, что методы, способы и средства совершения таких преступлений становятся все изощреннее.

Российские исследователи также отмечают, что преступность в информационной сфере является одной из основных угроз информационной безопасности современного российского государства. При этом она наносит колоссальный вред политической, социально-экономической и информационным сферам, причиняя значительный материальный ущерб личности, обществу и государству [2, с. 234].

В свою очередь, необходимо учитывать, что в начале 2000-х гг. информационные технологии только начинали внедряться в деятельность человека, общества и государства в различных сферах и серьезных проблем (угроз) не представляли (характеризовались, скорее, с положительной стороны и несли полезный функционал). В то время вопросы информационной безопасности не были столь актуальны и представляли интерес исключительно для узконаправленных специалистов. За 20 лет информационная сфера очень сильно эволюционировала, став важной составной частью общества и государства, проблемы криминализации в этой сфере приобрели характер национальных и международных [6, с. 161–162].

Можно сделать промежуточный вывод о том, что при переоценке и пересмотре дестабилизирующих факторов, которые могут оказать разрушительное воздействие на личность, общество и государство, а значит, имеют статус угрозы национальной безопасности, следует отметить то обстоятельство, что масштабы преступлений, совершаемых с использованием информационно-коммуникационных технологий, достигли таких размеров, что позволяют называть их на современном этапе угрозой национальной безопасности Республики Беларусь.

Активное распространение информационно-коммуникационных технологий и их применение во многих областях человеческой деятельности, а также активная политика многих государств в области формирования цифровой экономики и информационного общества приводят к неизбежному возникновению новых угроз на всех уровнях. В связи с этим угрозы, связанные с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий, включаются в перечень основных проблем национальной и международной безопасности [5, с. 70]. В оперативной, тактической и стратегической перспективе возможно ожидать дальнейшее нарастание в информационной сфере угроз как во всем мировом сообществе, так и в отдельном государстве. Недостаточная защищенность информационных ресурсов создает угрозы национальной и международной безопасности в целом, может вести к частичной или полной потере государственного информационного суверенитета. Государство должно быть в состоянии эффективно противостоять им, руководствуясь продуманной комплексной стратегией эффективных скоординированных действий по самым различным направлениям, целенаправленно используя весь имеющийся в его распоряжении арсенал сил и средств, что обусловливает необходимость определения не только самих угроз национальной безопасности, но и источников этих угроз [1, с. 36]. При этом национальная безопасность выступает в качестве основного условия жизнедеятельности личности, общества, государства, гарантируя поступательное развитие и обеспечение интересов, и достигается способностью системы обеспечения национальной безопасности к своевременному выявлению изменений во внутренней и внешней обстановке, формирующих угрозы национальной безопасности.

Глобальное информационное пространство и возможности скрытого трансграничного оборота информации все чаще используются для достижения отдельными государствами и организациями геополитических, военно-политических, а также террористических, экстремистских

и криминальных целей в ущерб стратегической стабильности национальной и международной безопасности. Территориальное распределение пользователей национальных доменных зон в сети Интернет выходит за рамки государственных границ, что позволяет преступникам в определенной степени противодействовать преследованию и последующему наказанию за противоправные действия. В этой связи данные виды преступлений создают больше проблем, чем традиционный криминал [4, с. 56].

Среди специалистов принято различать внутренние и внешние источники угроз национальной безопасности. Иными словами, по такому критерию, как расположение источника угрозы относительно самого объекта, их можно классифицировать на внешние и внутренние [8, с. 37].

При этом в гл. 16 Концепции информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1, также подчеркивается, что информационные системы и ресурсы становятся как предметом преступлений, так и средством их совершения. Формируется тотальная зависимость финансового и иных секторов от надежности электронных систем хранения, обработки и обмена данными. В качестве одного из наиболее вероятных источников угроз кибербезопасности рассматривается противоправная деятельность отдельных лиц и преступных групп.

В свою очередь, полагаем необходимым выделить источники угрозы данного вида. К внутренним источникам угрозы роста преступлений, совершаемых с использованием информационно-коммуникационных технологий, можно, например, отнести следующие: активное использование информационно-коммуникационных технологий (средства электронных платежей, дистанционные банковские услуги и пр.), имеющих неэффективную систему обеспечения безопасности; противоречия между потребностями определенной части населения в получении высоких доходов и возможностью их удовлетворения легальными способами. Следует также акцентировать внимание на таком источнике, как преступная деятельность групп, совершающих преступления с использованием информационно-коммуникационных технологий.

К внешним источникам угрозы роста преступлений, совершаемых с использованием информационно-коммуникационных технологий, можно отнести: деятельность иностранных политических, финансовых и информационных структур, направленную против интересов Республики Беларусь, в информационной сфере; деятельность международных террористических и экстремистских организаций; деятельность международных преступных групп в сфере незаконного оборота наркотиков; деятельность международных преступных групп в сфере компьютерной безопасности.

Таким образом, связанные с развитием информационно-коммуникационных технологий трансформации преступности не только обусловливают необходимость совершенствования законодательства, изменения организации и тактики борьбы с преступностью, но и требуют новых подходов к комплексному научному осмыслению соответствующих теоретико-прикладных проблем, уточнения некоторых из сложившихся научных представлений о содержании правоохранительной деятельности.

Анализ основных подходов к рассматриваемой проблеме позволяет предложить рассматривать рост преступлений, совершаемых с использованием информационно-коммуникационных технологий, не в качестве внутреннего источника угроз национальной безопасности информационной сферы, а как самостоятельную угрозу национальной безопасности Республики Беларусь в следующей формулировке: «рост преступлений, совершаемых с использованием информационно-коммуникационных технологий, в том числе против компьютерной безопасности, собственности, экстремистской направленности, против половой неприкосновенности или половой свободы несовершеннолетних».

Список использованных источников

1. Акишев, А. Национальные интересы в информационной сфере как объект информационной безопасности в Республике Казахстан / А. Акишев, И. Калиев // Norwegian J. of Development of the Intern. Science. – 2021. – № 66. – С. 36–39.

2. Гогаева, А. Л. Преступность в информационной сфере как основная угроза информационной безопасности России / А. Л. Гогаева, А. С. Лолаева // Вестн. науч. тр. молодых ученых, аспирантов и магистрантов ФГБОУ ВО «Горс. гос. аграр. ун-т». – Владикавказ, 2017. – Вып. 54. – С. 231–234.

3. Губич, М. В. Проблемные аспекты определения сущности и содержания социальной инженерии в контексте обеспечения информационной безопасности / М. В. Губич // Вестн. Акад. МВД Респ. Беларусь. – 2022. – № 1. – С. 18–23.

4. Ищенко, А. Н. Новая доктрина информационной безопасности Российской Федерации как основа противодействия угрозам безопасности России в информационной сфере / А. Н. Ищенко, А. Н. Прокопенко, А. А. Страхов // Проблемы правоохран. деятельности. – 2017. – № 2. – С. 55–62.

5. Мамаева, Л. Н. Угрозы кибербезопасности в цифровом пространстве / Л. Н. Мамаева, В. В. Бехер // Вестн. Саратов. гос. соц.-экон. ун-та. – 2019. – № 4. – С. 68–70.

6. Парамонов, А. В. Некоторые аспекты обеспечения национальной безопасности в информационной сфере / А. В. Парамонов, В. В. Харин // Актуал. проблемы государства и права. – 2021. – Т. 5, № 17. – С. 161–170.

7. Простосердов, М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : автореф. дис. … д-ра юрид. наук : 12.00.08 / М. А. Простосердов ; Рос. гос. ун-т правосудия. – М., 2016. – 232 с.

8. Чеботарева, А. А. Правовое обеспечение информационной безопасности личности в глобальном информационном обществе : автореф. дис. … д-ра юрид. наук : 12.00.13 / А. А. Чеботарева ; Ин-т государства и права РАН. – М., 2017. – 56 с.

Дата поступления в редакцию: 31.10.2022

УДК 343.9

***И. В. Ломоть**, кандидат юридических наук, начальник факультета повышения квалификации и переподготовки руководящих кадров Академии Министерства внутренних дел Республики Беларусь*
e-mail: lomats_iv@mail.ru

ЮРИДИЧЕСКИЙ ПРОЦЕСС И МЕСТО ОПЕРАТИВНО-РОЗЫСКНОГО ПРОИЗВОДСТВА В НЕМ

Анализируются взгляды на проблему юридического процесса. Акцентируется внимание на сильных и слабых сторонах в аргументации самого наличия юридического процесса, круга процессов и процедур, включаемых в него, а также критериев разграничения правовых явлений на материальные и процессуальные. Перечислены признаки оперативно-розыскного производства, позволяющие рассматривать его в качестве составной части юридического процесса. Поддерживается гипотеза о наличии охранительного правоотношения, реализация которого в полной мере способствует формированию объект-субъектных отношений в оперативно-розыскной деятельности.

Ключевые слова: оперативно-розыскное производство, юридический процесс, правоотношение, охранительное правоотношение

***I. V. Lomots**, Candidate of Juridical Sciences, Head of the Faculty of Training and Retraining of Managerial Personnel of the Academy of the Ministry of Internal Affairs of the Republic of Belarus*
e-mail: lomats_iv@mail.ru

JURIDICAL PROCESS AND THE PLACE OF OPERATIONAL-INVESTIGATIVE PROCEEDINGS IN IT

The article analyzes of views on the problem of the legal process. Strengths and weaknesses are considered in the argumentation of the very existence of the legal process, the range of processes and procedures included in it, as well as the criteria for division of legal phenomena into material and procedural ones. The distinctive features of operational-investigative proceedings are indicated, which allow considering it as an integral part of the juridical process, the hypothesis of the existence of a protective legal relationship is supported, the implementation of which is fully facilitated by object-subject relations in detective activities.

Keywords: operational-investigative proceedings, juridical process, legal relationship, protective legal relationship

Особое место и широкие масштабы применения негласных сил и методов оперативно-розыскной деятельности (ОРД) на отдельных этапах истории нашего государства привели к формированию мнения о чуть ли не тождественности ее средневековому инквизиционному процессу, закрытому завесой секретности и проникающему во все сферы жизни любого индивида.