САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ
МВД РОССИИ

КАЛИНИНГРАДСКИЙ ФИЛИАЛ

Е.Н. ПРОХОРОВА

ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ ПРАВООХРАНИТЕЛЬНОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ В ЦИФРОВУЮ ЭПОХУ

УЧЕБНО-ПРАКТИЧЕСКОЕ ПОСОБИЕ

КАЛИНИНГРАД
2021

УДК 342.5
ББК 67.7

П84 Прохорова Е.Н. Особенности функционирования правоохранительной системы Российской Федерации в цифровую эпоху: Учебно-практическое пособие. - Калининград: Калининградский филиал Санкт-Петербургского университета МВД России, 2021. 48 с.

Сведения об авторае:

Прохорова Евгения Николаевна – доцент кафедры уголовного процесса Калининградского филиала Санкт-Петербургского университета МВД России, кандидат юридических наук.

Рецензенты:

- начальник кафедры уголовно-правовых дисциплин Белгородского юридического института МВД России имени И.Д. Путилина, кандидат юридических наук, доцент А.В. Максименко.;

- врио заместителя начальника СУ УМВД России по Калининградской области А.В. Трофимов.

Учебно-практическое пособие адресовано преподавателям, курсантам, слушателям, адъюнктам и аспирантам, научным сотрудникам, практическим работникам правоохранительных органов, а также всем интересующимся государственно-правовыми проблемами современности в условиях внедрения в общество информационно-цифровых технологий.

Пособие содержит теоретический и практический материалы, которые будут полезны для подготовки всех видов и этапов занятий по учебным дисциплинам «Основы теории национальной безопасности», «Правоохранительные органы», для совершенствования педагогического мастерства преподавателей образовательных организаций МВД России, а также для самостоятельной подготовки курсантов и слушателей.

В учебно-практическом пособии раскрыты особенности функционирования правоохранительной системы в условиях развития информационных технологий, рассматрены организационные и правовые аспекты противодействия современным угрозам безопасности, в том числе кибертерроризму, разработаны ключевые характеристики указанных понятий как специфических форм противоправных деяний, а также даны практические рекомендации по противодействию данным угрозам.

Содержание

Введение

На сегодняшний день особенности функционирования правоохранительной системы Российской Федерации связаны с общемировыми тенденциями и геополитическими процессами, которые в совокупности представляют собой те вызовы, на которые она не может не реагировать.

При этом уже невозможно представить себе генезис общества вне связи с постоянно развивающимися цифровыми технологиями, провоцирующими увеличение роли информации в формировании глобального информационного пространства. Изменения, происходящие в мире, вызванные широким применением новых технологий, отражаются как на качестве правоохранительной деятельности, так и на жизни общества в целом.

Изучение современных вызовов позволяет сделать вывод о наступлении нового цивилизационного этапа, который требует переосмысления функциональных и структурно-содержательных свойств правоохранительной системы для выработки единого, научно обоснованного подхода. В рамках такого подхода можно было бы определить современное состояние и перспективы обеспечения правопорядка в условиях трансформации правоотношений, связанных в том числе с цифровизацией.

В данном пособии освещены особенности функционирования правоохранительной системы Российской Федерации, которая на сегодняшний день испытывает на себе влияние современных информационно-коммуникационных технологий.

Проблема обеспечения правовой защиты личности от информационных угроз является ключевой в современных условиях развития глобального информационного пространства.

Цифровизация всех сфер общественной жизни привела к появлению ранее неизвестных угроз безопасности. Использование информационных технологий террористами вызывает, пожалуй, наибольшую озабоченность. Автором пособия анализируются угрозы безопасности, связанные с масштабной деятельностью террористических организаций, а также с их финансированием путем применения информационных технологий, что подчеркнуто конкретными примерами. Кроме того, в работе актуализировано понятие кибербезопасности в соответствии с современной действительностью, проведен правовой анализ данного явления, а также предложены формы взаимодействия правоохранительных органов, обеспечивающие интеграцию их деятельности.

Обращается внимание на то, что взаимный дефицит доверия между странами мешает работе по борьбе с терроризмом на основе использования телекоммуникационных систем, а также в настоящее время фактически отсутствует механизм трансграничного расследования кибертерроризма. При этом на национальном уровне противодействие осложняется несовершенством нормативно-правовой регламентации, связанной с международной правовой помощью.

Таким образом, актуальность представленного пособия обусловлена потребностью в уточнении и разработке рекомендаций по обеспечению правопорядка и защите населения от информационных угроз, в актуализации и наращивании знаний представителями правоохранительных органов в области обеспечения безопасности Российской Федерации в современных условиях всеобщей цифровизации.

1. Правоохранительная система Российской Федерации: понятие и базовые элементы

Реалии сегодняшней жизни выдвигают в число первоочередных задачу обеспечения безопасности личности, общества и государства. Однако возникновение целого ряда проблем, связанных с выполнением правоохранительной функции государства, например, таких как недоверие к органам, обеспечивающим национальную безопасность, коррупция, наличие пробелов и коллизий в существующем законодательстве, рост организованной преступности, нарастание глобальных террористических угроз, невозможность справедливой защиты своих прав, побуждает к переосмыслению многих правовых категорий, созданию концептуально нового представления о понятии правоохранительной системы, связанного с повышением эффективности организации деятельности правоохранительных структур.

Вне всяких сомнений, правоохранительная система должна выступать одной из самых результативных структур, противодействующих современным угрозам. От форм взаимодействия правоохранительных органов во многом зависит безопасность и стабильность общества. В современных условиях только государство с эффективно функционирующей правоохранительной системой способно реально обеспечивать безопасность личности, общества и государства в случае возникновения и развития военных (вооруженных) конфликтов на его территории.

В действительно же современная российская правоохранительная система не в полной мере соответствует требованиям безопасности и потребностям общества, а также не всегда гарантирует гражданам основные права на жизнь, свободу, безопасность и пр.

Представляется необходимым совершенствование национального законодательства в правоохранительной сфере, для того чтобы исключить риски возникновения критических недостатков в области обеспечения законности. Прежде всего обратимся к рассмотрению теоретических подходов к анализируемому понятию.

Так, в юридической науке не сложилось единого определения правоохранительной системы. Среди ученых-юристов зачастую встречается ошибочная точка зрения, согласно которой правоохранительная система и система правоохранительных органов по сути одно и то же. Однако это далеко не тождественные понятия.

Потребность в единообразном толковании понятия «правоохранительная система» обусловлена необходимостью четкого разграничения ее задач и функций для устранения рассогласованных действий входящих в ее состав структур, что позволит исключить коллизии при решении практических вопросов.

Существуют значительно отличающиеся друг от друга мнения как в отношении элементного состава правоохранительной системы, так и в отношении ее структуры, что обусловливает тезис о множественности структур правоохранительной системы.

Освещая вопрос о структуре правоохранительной системы государства, авторы обращают внимание на само понятие и специфику выполняемых государственных задач. «Чаще всего анализу подвергаются правоохранительная деятельность и правоохранительные органы без упоминания того, что и правоохранительная деятельность, и правоохранительные органы одного государства являются структурно-функциональными элементами правоохранительной системы этого государства»[1].

Автор согласен с позицией, согласно которой понятие «правоохранительная система» шире, чем «система правоохранительных органов», поскольку в него включаются не только специализированные правоохранительные структуры, но и некоторые другие государственные органы, тесно взаимодействующие с правоохранительными, а также правовые нормы, институты и пр.

Рассмотрим имеющиеся в юридической литературе определения правоохранительной системы. Так, по мнению А.Г. Братко,

[1] Баранов В.Л. Правовое регулирование социальной защиты сотрудников правоохранительных органов // Журнал российского права. 2012. № 1. С. 78-88.

правоохранительная система – это «комплекс государственно-правовых средств, методов и гарантий, обеспечивающих защиту общественных отношений от противоправных посягательств»[1].

О.И. Чердаков определяет ее как «сложный институт правовой организации общества, включающий в себя нормативную и правоохранительную подсистемы, многообразие правовых явлений, основанных на правовой поддержке государства»[2].

По мнению В.В. Лазарева, «правоохранительная система – это совокупность государственно-правовых средств, методов и гарантий, обеспечивающих защищенность человека от противоправных нарушений, которая включает следующие составляющие: цели и объекты правоохраны, субъекты правоохраны, правоохранительную деятельность»[3].

Приведенные дефиниции несильно разнятся между собой и, скорее, дополняют друг друга, поскольку анализируемая система характеризуется в них с разных сторон. Поэтому с общей позицией их авторов можно согласиться. Однако упомянутые ученые-юристы не отражают в своих определениях специфичность деятельности правоохранительных структур, следовательно, нужно сделать акцент именно на их функциях с учетом их адаптации к современным условиям.

По мнению А.Г. Братко, в правоохранительную систему включены «три основных элемента: а) объекты правовой охраны; б) субъекты правовой охраны; в) правоохранительная деятельность. Также имеются переменные – правосознание, правовая культура, состояние законности и правопорядка. Последние реалии более подвижны, дискретны»[4].

Сегодня проявляются тенденции к интеграции правоохранительной системы, которая включает в себя новых членов. Она допускает вступление в нее не каких угодно структур и служб, не с каким угодно набором функций, а именно правоохранительных, чтобы не нарушать устойчивость целого.

По мнению автора, в современных условиях со сложной практикой международных отношений целесообразно говорить не о правоохранительных органах, а выделять именно категорию «пра-

[1] Братко А.Г. Правоохранительная система: вопросы теории: автореф. дис. ... д-ра юрид.наук / Академия МВД России. М., 1992. С. 22.

[2] Чердаков О.И. Формирование правоохранительной системы Советского государства в 1917-1936 гг. Историко-правовое исследование / под ред. А.А. Малько. Саратов, 2001. С. 19.

[3] См.: Общая теория права и государства / под ред. В.В. Лазарева. М., 2001. С. 192-193.

[4] Братко А.Г Правоохранительная система: вопросы теории: автореф. дис. ... д-ра юрид.наук / Академия МВД России. М., 1992. С. 11.

воохранительные структуры» (к которой, например, можно отнести российскую военную полицию, функционирующую в Сирии) для организации наиболее эффективного обеспечения правопорядка. Из этого можно сделать вывод о том, что правоохранительная система – сложное комплексное образование, объединяющее совокупность правоохранительных структур, государственных и муниципальных правовых средств.

Однако на сегодняшний день существуют некоторые трудности в согласовании интересов силовых структур. Особенно ярко это проявилось в прокурорской службе, что обусловлено особым статусом органов прокуратуры, каким не обладает никакой другой из правоохранительных органов в общей системе российской государственной власти.

При этом объединение разнообразных структур в единую правоохранительную систему противоречит интересам отдельных служб. В связи с чем правомерно задаться следующим вопросом: не вызовет ли такое объединение осложнения кадровой ситуации в правоохранительной системе?

Так, работники прокуратуры больше дорожат своими классными чинами, чем специальными званиями полиции. Здесь также можно привести в качестве примера ситуацию, возникшую во вновь образованной Федеральной службе войск национальной гвардии, в которой первоначально наблюдалось сращивание различных правоохранительных структур и, как следствие, происходила путаница в осуществлении полномочий и делегировании обязанностей.

Таким образом, попытка привести всех к общему знаменателю не будет способствовать укреплению статуса прокуратуры в качестве координатора всей правоохранительной системы. При этом специфика службы в правоохранительных органах тесно связана функциональными обязанностями и взаимоотношениями, которые устанавливаются не только административно, но и законодательно, в том числе на процессуальном уровне. Тем не менее работа по практическому совершенствованию новой системы службы активно продолжается.

В связи с этим обосновывается необходимость новой концепции правоохранительной системы как комплексного явления, обеспечивающего безопасность российского общества в современных условиях. Она представляет собой обобщенное знание о правоохранительной деятельности, ее содержании, осуществляющих ее субъектах и объектах, подлежащих правовой охране.

Вместе с тем необходимо решить ряд важных теоретических вопросов, среди которых следующие:

- определение понятия правоохранительной системы;
- соотношение различных точек зрения относительно данного понятия;
- раскрытие содержания правоохранительной деятельности;
- рассмотрение содержания и значения интегративных действий сотрудников правоохранительных органов;
- определение критериев отнесения того или иного органа к правоохранительным.

Отметим, что «признаками системы являются множество составляющих ее элементов, единство главной цели для всех элементов, наличие связей между ними, целостность и единство элементов, наличие структуры и иерархичности, относительная самостоятельность и наличие управления этими элементами»[1].

Правоохранительная система обладает присущей ей целостностью элементов – правоохранительных органов, взаимодействующих друг с другом на различных этапах борьбы с преступностью.

Во-вторых, указанные органы осуществляют непосредственное взаимодействие между элементами (или подсистемами) системы, а также с внешними элементами и подсистемами.

При этом система существует как единое целое именно благодаря наличию связей между ее элементами, которые определяют ее интегративные качества. Связи могут быть прямые, обратные, информационные и пр. Вместе с тем внутри системы они должны быть более мощными, чем связи отдельных элементов с внешней средой, так как в противном случае система не сможет существовать.

В-третьих, для системы необходима организация, то есть упорядоченные связи, четко регламентированная структура с определенным порядком и иерархичностью внутри нее.

Таким образом, для становления правоохранительной системы важна правильная структурно-определенная организация. Применительно к рассматриваемой проблеме можно сделать вывод о том, что объединенная, построенная надлежащим образом классификация правоохранительной системы ускоряет развитие входящих в нее суверенных структур.

По мнению автора, в правоохранительной системе можно выделить следующие элементы: «силовой блок» и «обеспечительный блок», которые тесно взаимодействуют друг с другом в части обеспечения правоохранительной функции государства.

«При таком подходе к «силовой» составляющей правоохранительной системы, призванной обеспечивать стратегию государ-

[1] Соловьев В.С. Теория организации социальных систем. Т. 1: Уч. пос. М., 2005. С. 7.

ственного строительства, можно отнести: органы Министерства внутренних дел Российской Федерации, органы прокуратуры Российской Федерации, органы Федеральной службы безопасности Российской Федерации, органы Следственного комитета Российской Федерации, органы Федеральной таможенной службы, подразделения Министерства обороны Российской Федерации, Межведомственную комиссию по противодействию финансирования терроризма, Федеральную службу войск национальной гвардии Российской Федерации»[1].

К «обеспечительному блоку» данной системы автор относит: Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, Федеральную службу исполнения наказаний, органы принудительного исполнения Российской Федерации, Службу внешней разведки Российской Федерации, Федеральную службу по финансовому мониторингу, Федеральную службу охраны Российской Федерации и Федеральную таможенную службу.

Например, «речь может идти об Уполномоченном по правам человека с его рабочим аппаратом, который представляет собой единый государственный орган, независимый и неподотчетный другим государственным органам и должностным лицам, о Росфинмониторинге, осуществляющем функции по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, функции национального центра по оценке угроз национальной безопасности, возникающих в результате легализации (отмывания) доходов, полученных преступным путем, финансирования терроризма и распространения оружия массового уничтожения, по выработке мер противодействия этим угрозам, а также о таможенных органах, которые оказывают существенное влияние на состояние правоохраны в обществе»[2].

Приведенная классификация позволяет адекватно решать задачи, связанные с международными конфликтами, которые происходят в Украине, Сирии, бороться с мировым терроризмом и угрозами распространения влияния «Исламского государства».

Ведущая роль при этом должна отводиться силовой подсистеме, призванной гарантировать приемлемый уровень законности и безопасности личности, общества и государства.

[1] Степанов О.А., Прохорова Е.Н. О «силовой» составляющей правоохранительной системы, обеспечивающей безопасное осуществление государственного строительства в России // Вестник Академии Генеральной прокуратуры Российской Федерации. 2014. № 6(44). С. 14.

[2] Степанов О.А. Теория государства и права: Курс лекций / Академия генеральной прокуратуры РФ. М., 2016. С. 159.

Понятие «правоохранительная система» в категориальном аппарате юридической науки выполняет единую функцию, которую можно рассматривать как системообразующую. Отсюда можно сделать вывод, что правоохранительная система – единая система, а структур у нее может быть несколько в зависимости от того, какие цели и задачи перед ней стоят: «Можно сказать, что при классификации и выделении элементов правоохранительной системы все зависит от конечных целей, которые ставит перед собой классификатор»[1].

С учетом изложенного допустимо дать следующее определение правоохранительной системы: это система государственных и муниципальных структур, осуществляющих специализированные правоохранительные функции в сфере обеспечения законности и безопасности общества в целях защиты прав и свобод граждан, их объединений, государственных институтов от правонарушений различного характера в современных условиях.

Целью правоохранительной системы является прежде всего охрана жизненно важных человеческих ценностей, неотъемлемых прав и свобод человека и гражданина. При этом исполнение правоохранительными органами возложенных на них обязанностей носит публично-правовой характер, то есть осуществление данной функции является их конституционной обязанностью.

Однако при этом стоит учитывать изменение потребностей и интересов общества, необходимость их развития по прогрессивному пути, что отражается в основных направлениях проводимой государственной политики.

Таким образом, необходимо дальнейшее научное переосмысление функциональных и структурно-содержательных свойств правоохранительной системы, связанных с обеспечением безопасности личности, общества и государства с учетом трансформации общественных отношений, особенно в условиях цифровизации. Последнее обстоятельство уже сейчас необходимо учитывать законодателю на стадии подготовки правоохранительной системы к новой – цифровой – форме существования информации.

[1] Бержель Ж.-Л. Общая теория права. М., 2000. С. 99.

2. Обеспечение безопасности личности, общества и государства как цель деятельности правоохранительной системы в современных условиях

В настоящий момент правоохранительная система Российской Федерации функционирует в особых условиях, связанных с действием политических санкций и наличием террористических угроз. Вместе с тем снижение реальных доходов населения, вызванное возникновением сложной ситуации в силу распространения коронавирусной инфекции COVID-19, наряду с таким явлением, как цифровизация современного общества, стали своего рода катализаторами тех негативных явлений, которые отразились на состоянии и динамике всей преступности.

В данных обстоятельствах в теоретическом плане не проработаны некоторые вопросы организации и деятельности правоохранительных органов. Тем не менее правоохранительная система должна адаптироваться к изменяющимся условиям функционирования и развития, а также должна быть восприимчива к воздействию как внутренних, так и внешних факторов, обладать способностью к нейтрализации наиболее неблагоприятных из них (угрозы, вызовы, критические риски) и создавать среду для воздействия благоприятных факторов.

Так, в условиях введения международных санкций, обострения противоречий в международных отношениях, возникновения внутренних конфликтов деятельность правоохранительных органов значительно усложняется. Их цели, задачи, методы и функции наполняются новым содержанием. В связи с этим необходимость поиска новых форм противодействия подобной тенденции усложнения международных отношений очевидна.

Одним из способов повышения эффективности защиты прав и свобод человека и гражданина, на наш взгляд, является развитие интеграции в деятельности правоохранительной системы.

В силу этого необходимо ясно обозначить содержание и структуру правоохранительной системы, изучить ее принципы, формы и методы, что позволит установить основные признаки данной системы, решить проблемы, связанные с обеспечением безопасности личности, общества и государства и соблюдением законности как основной цели деятельности правоохранительной системы.

По мнению автора, правоохранительную систему следует рассматривать с учетом особенностей деятельности правоохранительных структур в современных условиях. Именно анализ «силового блока» правоохранительной системы представляет наибольший

практический интерес, поскольку должностные лица указанных органов законом наделены полицейскими полномочиями. Это особенно актуально в связи с тем, что в последнее время вновь возникла забытая ранее угроза третьей мировой войны.

Многие западные средства массовой информации открыто публикуют материалы, касающиеся плана проведения военных действий США против России. Так, например, по мнению Валентина Василеску, «главная задача НАТО – нанести России быстрое поражение, которое заставит сколлапсировать политическую систему страны»[1].

Двойные стандарты в оценке преступлений против гражданского населения на юго-востоке Украины, нарушение фундаментальных прав человека на жизнь, свободу передвижений, личную неприкосновенность привели к тому, что западные страны закрывают глаза на происходящее в этой стране.

Существует точка зрения политолога В. Третьякова о том, что «США предвидят распад Евросоюза и им нужен новый хозяин новой Европы, например в лице Германии». По его мнению, первая часть этого плана – Украина, вторая – Калининградская область.

По мнению директора Службы внешней разведки Российской Федерации С.Е. Нарышкина, ряд западных политиков опасно совмещает, по сути, поддержку гражданской войны на Украине с заигрыванием с пронацистскими силами.

Стоит отметить, что правовая природа механизма защиты прав и свобод человека и гражданина в значительной мере определяется характером самого процесса реализации этих прав и свобод, в том числе в рамках правоохранительной деятельности.

В таких условиях только государство с эффективно функционирующей правоохранительной системой способно реально обеспечивать безопасность личности, общества и государства в случае возникновения и развития военных конфликтов на его территории.

Именно поэтому изучение общих закономерностей функционирования правоохранительной системы позволит сотрудникам правоохранительных органов в условиях нарастания военной угрозы более успешно решать задачи, стоящие перед ними при исполнении их функциональных обязанностей.

«Реализация идеи безопасности в современном обществе может сводиться к обеспечению максимально возможной свободы человека при защите важнейших параметров среды его обитания, представляющих для него блага либо интерес. С учетом такого под-

[1] Опубликован сценарий грядущей войны США с Россией [Электронный ресурс]. – URL: http://www.politonline.ru/interpretation/22887808.html.

хода, например, деятельность сотрудников правоохранительных органов допустимо ассоциировать с конкретной программой поведения, направленной как на сохранение структурно-функциональной устойчивости государственных институтов, так и на обеспечение защиты личности в условиях изменяющихся параметров состояния ее безопасности»[1].

При этом норма права, как признаваемая государством мера должного поведения, обусловленная государственным принуждением, должна рассматриваться как результат осознания потребности в правовом регулировании правоотношений, связанных с общественной безопасностью.

Следовательно, правоотношения, связанные с обеспечением безопасности личности, общества и государства, допустимо рассматривать как результат реализации нормы, как результат ее воплощения в действиях сотрудников правоохранительных органов.

Однако сотрудники правоохранительных органов в рамках фактического доминирования в обществе идеи «не войны и не преступности» зачастую (как показали события Майдана (2013/2014)) оказываются неготовыми к решению проблем правоохранительной деятельности, подвергая сомнению положение о том, что единственным эффективным средством защиты общества в таких условиях является силовой компонент.

При этом следует подчеркнуть, что хотя лидеры европейских стран высказывают серьезные опасения по поводу продолжения политики международных санкций против российского государства, однако Белый дом оставляет их без должного внимания. По мнению автора, давно пора задуматься, к чему привело и к чему еще может привести фактическое возвращение холодной войны и прекращение работы в области контроля над вооружением.

Другой глобальной проблемой человечества является терроризм, который выступает одним из наиболее сложных, социально опасных и многоаспектных негативных явлений современного общества, влекущим за собой множественные человеческие жертвы по всему миру. Трагические события в Москве, Беслане, Нью-Йорке, Мадриде, Монте-Карло, Лондоне и Париже наглядно это показали. При этом следует учесть, что нынешний терроризм динамично видоизменяет свои формы, что требует иных методов борьбы с ним[2].

[1] См.: Степанов О.А., Тюрина Е.Н. Безопасность как объект правоотношений в современном обществе // Современное право. 2011. № 10. С. 13.
[2] По этому вопросу см. напр.: Котенко И.В., Юсупов Р.М. Информационные технологии для борьбы с терроризмом // Защита информации INCIDE. 2009. № 2. С. 74-79.

Очевидно, что в ходе современного государственного строительства в России важно формировать более глубокое понимание необходимости защиты естественных прав человека, обеспечения его безопасности, в том числе от террористических угроз, к которым можно отнести угрозу распространения влияния и деятельности «Исламского государства» (ИГИЛ – запрещенная в России террористическая организация) на территории России.

Согласно Информационному письму Генеральной прокуратуры Российской Федерации от 10 апреля 2014 г. № 27-26-2014/Ип2063-14 «О проблемных вопросах уголовно-правового обеспечения противодействия терроризму, связанных с запретом деятельности террористических организаций» терроризм представляет собой угрозу международному миру и безопасности, сохранению территориальной целостности и стабильности государств, а также реализации основных прав человека и гражданина, включая неотъемлемые права. Этим и определяется необходимость переосмысления существующей концепции безопасности в части изменения отношения к ней как к состоянию динамического равновесия между деструктивными и стабилизирующими факторами, оказывающими воздействие на систему[1].

В связи с этим в настоящее время осуществляется активная работа по практической реализации мер взаимодействия различных силовых структур Российской Федерации и наделения их соответствующими полномочиями. Так, в целях обеспечения государственной и общественной безопасности, защиты прав и свобод человека и гражданина сотрудники Федеральной службы войск национальной гвардии Российской Федерации наделяются правом давать экспертные заключения по состоянию антитеррористической защищенности охраняемых объектов[2].

Вместе с тем не только российское уголовное право, но и международное уголовное право относит терроризм к одной из опаснейших форм преступного посягательства, в основе которой лежит стремление субъекта посеять в обществе страх, панику, дестабилизировать общественный порядок, парализовать нормальное функционирование органов государственной власти.

[1] Романова Л.М. Национальный суверенитет в условиях глобализации: институционально-правовой анализ: автореф. дис. ... д-ра юрид. наук. Ростов-на-Дону, 2009.

[2] Указ Президента Российской Федерации от 30.09.2016 № 510 «О Федеральной службе войск национальной гвардии Российской Федерации» (вместе с «Положением о Федеральной службе войск национальной гвардии Российской Федерации») // Собрание законодательства РФ, 10.10.2016, № 41, ст. 5802.

Под террористическим актом в Уголовном кодексе Российской Федерации понимается «совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в целях воздействия на принятие решений органами власти или международными организациями» (ст. 205).

Правовую основу противодействия терроризму составляют резолюции Генеральной Ассамблеи ООН и Совета Безопасности[1], конвенции[2], документы Интерпола, федеральные законы Российской Федерации[3], указы Президента Российской Федерации[4] и пр.

По инициативе Российской Федерации Генеральная Ассамблея ООН приняла в декабре 1998 года резолюцию, касающуюся достижений в сфере информатизации и телекоммуникации в контексте международной безопасности[5], согласно которой она призывает государства-члены информировать Генерального секретаря ООН о своих взглядах и оценках относительно:

а) определения основных понятий, связанных с информационной безопасностью;

б) проблем, возникающих по поводу обеспечения информационной безопасности;

в) развития международных принципов, направленных на улучшение в части обеспечения безопасности глобального информационного пространства и телекоммуникаций.

[1] Резолюция 51/210 Генеральной Ассамблеи ООН «Меры по ликвидации международного терроризма» (вместе с «Декларацией, дополняющей Декларацию о мерах по ликвидации международного терроризма 1994 года») (принята 17.12.1996 на 88-ом пленарном заседании 51-ой сессии Генеральной Ассамблеи ООН); Декларация о мерах по ликвидации международного терроризма (принята 09.12.1994 Резолюцией 49/60 на 84-ом пленарном заседании Генеральной Ассамблеи ООН).

[2] Международная конвенция о борьбе с финансированием терроризма (заключена в г. Нью-Йорке 09.12.1999); Концепция противодействия терроризму в Российской Федерации (утв. Президентом РФ 05.10.2009).

[3] Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму»; Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

[4] Указы Президента Российской Федерации от 26.12.2015 № 664 «О мерах по совершенствованию государственного управления в области противодействия терроризму», от 18.11.2015 № 562 «О Межведомственной комиссии по противодействию финансированию терроризма», от 15.02.2006 № 116 «О мерах по противодействию терроризму».

[5] Резолюция Генеральной Ассамблеи ООН A/RES/53/70 от 04.01.1999.

Пресечение террористического акта осуществляется силами и средствами органов Федеральной службы безопасности Российской Федерации, а также создаваемой группировки сил и средств. В ее состав могут включаться «подразделения, воинские части и соединения Вооруженных Сил Российской Федерации, подразделения федеральных органов исполнительной власти, ведающих вопросами безопасности, обороны, внутренних дел, обеспечения деятельности войск национальной гвардии Российской Федерации, юстиции, гражданской обороны, защиты населения и территорий от чрезвычайных ситуаций, обеспечения пожарной безопасности и безопасности людей на водных объектах, других федеральных органов исполнительной власти и федеральных государственных органов, а также подразделения органов исполнительной власти субъектов Российской Федерации»[1].

Мероприятия по противодействию терроризму координируются рядом органов: Национальным антитеррористическим комитетом и Федеральным оперативным штабом, антитеррористическими комиссиями и оперативными штабами в регионах. При этом эффективная работа по противостоянию террористическим угрозам невозможна без тесного взаимодействия с миграционными подразделениями МВД России по направлениям паспортно-визового отдела и иммиграционного контроля.

Стоит отметить, что на сегодняшний день меняется представление о террористе как о субъекте уголовного права. Так, за все время своего присутствия в Сирии США минимально участвовали в борьбе с террористами. Зачастую они, напротив, помогали боевикам (эвакуировали их из осажденных зон, создали в стране очаги для наращивания новых группировок). Желая удержать мировое господство, США находят людей, готовых за щедрое вознаграждение разжигать в своей стране беспорядки, организовывать панику среди населения, используя различные угрозы, телефонный терроризм, погружая свою страну в хаос, тем самым дестабилизируя различные сферы общественной жизни.

Представляется, что в современных условиях террорист понимается как субъект военно-политического характера, то есть это не обязательно наемный головорез, имеющий своей целью месть и установление мусульманского мирового порядка. Сегодня террорист может быть человеком интеллигентным, хорошо образованным, разбирающимся в информационных технологиях и, к сожалению, использующим их не во благо, а во вред национальным интересам какой-либо страны.

[1] Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму» // СПС «КонсультантПлюс».

«Отмечается распространение, с использованием сети интернет, идей национального, религиозного и расового превосходства, размещение видеороликов и других материалов экстремистского характера. В ряде регионов Интернет используется для оповещения и координации участников несанкционированных массовых мероприятий. При этом выявление лиц, совершающих такие правонарушения, их изобличение и привлечение к ответственности затруднено несовершенством нормативной правовой базы, фактической анонимностью пользователей сети и размещением провокационных сайтов преимущественно за пределами юрисдикции российских правоохранительных органов»[1].

В качестве примера можно отметить массовое распространение сообщений неизвестными лицамаи, которые находились за пределами Российской Федерации, о заминированных общественных объектах и зонах большого скопления людей, таких как гипермаркеты, аэропорты, вокзалы и пр.

Сложность расследования такого вида преступлений заключается в латентности звонивших личностей в силу использования ими технических средств и приложений, позволяющих абоненту оставаться анонимным, затрудняющих его идентификацию из-за невозможности определения географического местоположения.

Здесь стоит отметить особенность международного сотрудничества, которая заключается в том, что если абонент установлен за границей, то исполнение международных поручений по проведению в отношении него следственных действий, как показывает практика, может длиться полтора-два года. За это время срок исковой давности за преступления небольшой тяжести уже подойдет к концу. К тому же, если это лицо будет являться иностранным гражданином, то уголовное дело в отношении него будет отправлено в страну постоянного его проживания при наличии принципа двойной инкриминации.

С развитием цифровых технологий стало еще сложнее идентифицировать телефонного террориста и установить его местоположение, так как в распоряжение преступников попал самый широкий арсенал технических средств анонимизации. При этом тактика лжетеррористов тоже видоизменяется, от звонков с угрозами они переходят к рассылке электронных писем, в том числе используя популярные мессенджеры.

В связи с тем, что применение цифровых технологий открывает широкие возможности для преступников, механизм солидар-

[1] Дамаскин О.В. Актуальные вопросы организации противодействия терроризму // Вестник военного права. 2016. № 1. С. 2.

ного функционирования правоохранительных органов тоже должен измениться. Таким образом, правоприменительная деятельность в сфере обеспечения безопасности личности, общества и государства нуждается в разработке четких алгоритмов по квалификации преступлений, совершаемых с использованием информационно-коммуникационных технологий.

Особенностью террористических атак, совершаемых в киберпространстве, является то, что при сравнительно небольших усилиях и средствах можно добиться серьезной дестабилизации ситуации в стране в целях создания возможности захвата власти на основе нанесения ущерба информационным системам безопасности, подрыва социальной и политической стабильности в обществе, массовой вербовки населения, путем оказания психологического давления. Это при наихудшем варианте развития событий может привести к масштабным последствиям, уничтожению линий коммуникаций, инженерной инфраструктуры, атомных и гидроэлектростанций и других особо важных объектов.

Стоит обратить внимание на малоизученный в российской юридической науке феномен. Под кибертерроризмом (кибервойной) принято понимать комплекс противоправных действий террористического характера, применяемых с использованием информационных технологий в киберпространстве и создающих угрозу государственной безопасности, жизненно важным потребностям личности и общества.

В отличие от обычного террориста, который для достижения своих целей использует взрывное устройство, кибертеррорист удаленно использует все возможности современных технологий, в том числе гаджеты, мобильные устройства, программные продукты и др.

Информационный террористический акт отличается и по формам воздействия. Такие акты носят политически мотивированный характер и выражаются в применении насилия по отношению к гражданским целям. Главное в тактике кибертеррориста состоит в том, чтобы кибертеррakt имел опасные последствия, получил широкую общественную огласку и резонанс.

Серьезную обеспокоенность угрозой кибертерроризма выразил и Президент Российской Федерации В.В. Путин, который 15 января 2013 года подписал Указ «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», вступивший в силу в тот же день. Согласно данному указу на ФСБ России возложены полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации

последствий компьютерных атак на информационные ресурсы РФ (информационные системы и информационно-телекоммуникационные сети, находящиеся на территории РФ и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом).

При этом стоит отметить, что любая деятельность террористов, особенно масштабная, не может осуществляться без соответствующей финансовой платформы. Поэтому обратимся к рассмотрению еще одной актуальной проблемы в анализируемой сфере – оплате террористической деятельности биткоинами.

Механизм противодействия указанному явлению пока отсутствует во многом из-за анонимного характера деятельности по выпуску и использованию виртуальных валют неограниченным кругом субъектов.

Согласно информационному сообщению Росфинмониторинга «Об использовании криптиовалют» использование криптовалют при совершении операций является основанием для их рассмотрения как направленных на легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма[1].

Весьма наглядным в данном случае является пример вынесения обвинительного приговора в отношении подростка из Вирджинии Али Шукри Амина с мерой пресечения в виде лишения свободы на 11 лет за то, что он оказывал финансовую поддержку ИГИЛ, используя для этого социальные сети, инструктируя людей, как использовать биткоин. У Амина в Twitter было более 4000 последователей[2].

Террористические группы также проникают в некоммерческие организации, чтобы получить доступ к благотворительным средствам. «Это позволяет террористам получать в виде пожертвований и непосредственной «дани» от откровенного рэкета значительные финансовые ресурсы, «отмывать» полученные средства для создания собственной экономики, которая, по их замыслу, призвана стать основой будущего «единого исламского государства Великий Халифат»[3].

При этом «конечная цель (боевиков) – обеспечить доставку этих средств по назначению. Мелкие или крупные транзакции мо-

[1] Информационное сообщение Федеральной службы по финансовому мониторингу Российской Федерации от 06.02.2014 «Об использовании криптовалют» // СПС «КонсультантПлюс».

[2] В США подростка посадили на 11 лет за помощь ИГИЛ [Электронный ресурс]. – URL: http://www.ntv.ru/novosti/1491556.

[3] Грачев С.И. Контртерроризм: организационные, правовые, финансовые аспекты и вопросы профилактики / под ред. О.А. Колобова. Нижний Новгород, 2010. 166 с.

гут помочь продвинуть планирование терактов на следующий уровень – совершение терактов». В настоящее время можно отследить «источник финансирования, но установить, кто стоит за операцией, очень проблематично»[1].

Правильно расставленные акценты в борьбе с международным терроризмом могли бы значительно усилить ее эффективность, что позволило бы сохранить большое количество жизней и материальных ценностей. По мнению С.И. Грачева, «в данном контексте следует отметить, что российскими спецслужбами регулярно проводятся конкретные операции, связанные с перехватом десятков миллионов долларов. Причем основные средства тратятся не на проведение терактов, требующих незначительных средств, а на организацию вербовки, подготовку террористических групп и вооруженных формирований, создание современной материально-технической базы. Соответствующими ведомствами постоянно обновляется список компаний и организаций, подозреваемых в отмывании денег и финансировании терроризма. Собраны данные на 350 тысяч подозрительных сделок. Заключены соглашения о взаимодействии между всеми правоохранительными структурами, в том числе ФСБ, МВД, Федеральной таможенной службой России»[2].

Данное обстоятельство позволяет говорить о необходимости развития принципиально новой сферы международного сотрудничества, затрагивающей все жизненно важные аспекты информационной безопасности каждого государства, путем повышения эффективности интеграции деятельности правоохранительных органов и специальных служб, в том числе с использованием и внедрением технологии распределенного реестра, которая может обеспечить защиту информации, ее хранение, распространение и передачу ограниченному кругу лиц, имеющих санкционированный доступ от правообладателя.

Блокчейн представляет собой распределенную базу данных, в которой информация, представленная в виде цифровых записей, объединена в установленные блоки, криптографически связана в цепь путем сложных математических алгоритмов. Такая система блоков отвечает современным признакам технологического обеспечения, характеризуется безопасностью, децентрализованностью,

[1] В Юго-Восточной Азии зафиксировали подозрительные транзакции с биткоином [Электронный ресурс]. – URL: https://news.mail.ru/economics/32090152.

[2] Грачев С.И. Контртерроризм: организационные, правовые, финансовые аспекты и вопросы профилактики / под ред. О.А. Колобова. Нижний Новгород, 2010. С. 147.

разными уровнями доступности, отсутствиеи необходимости в наличии третьей стороны для верификации транзакций.

Сама работа шифрования осуществляется большим количеством разнообразных компьютерных систем, работающих в одной сети. Если по результату их расчетов все получают один и тот же исход, тогда блоку присваивается уникальная цифровая сигнатура (подпись).

Когда реестр производит обновление и создается новый блок, в него уже недопустимо внести какие-либо изменения. Благодаря этому подделать его невозможно. В таком случае есть возможность только добавить новую запись.

Общими задачами для блокчейна являются хранение и передача информации. Однако с момента введения информации в сеть у правообладателя возникают два правомочия: ввести информацию в интернет или в блокчейн. При этом не важно, какой будет информация (перевод денег, пост в социальной сети, запись в реестре недвижимости). Благодаря этой технологии информация не может быть потеряна, заблокирована или кем-то исправлена.

В связи с указанным представляется целесообразным внедрение технологии блокчейн в правоохранительную деятельность, поскольку все серверы органов внутренних дел взаимозависимы. Система позволит любому сотруднику, осуществляющему правоохранительную функцию, при наличии доступа, получать сведения из имеющихся интегрированных банков данных по одному запросу. Такой доступ к оперативной информации положительным образом скажется на эффективности правоохранительной деятельности, в том числе на раскрываемости преступлений и сохранности содержащейся информации.

В качестве примера можно упомянуть событие, произошедшее на Гаити в 2010 г., когда в результате землетрясения обрушилось здание реестра прав на недвижимость, в котором размещалась электронная база данных[1]. Однако если персональные данные хранить в блокчейне, то они все подлежат восстановлению даже в случае гораздо более глобального стихийного бедствия.

В блокчейне применяют хеширование. Сформировав из необходимых записей список и вычислив его хеш, сервер разошлет эти данные на все остальные серверы реестра. Такую информацию называют блоком. Каждый новый блок будет присоединяться к предыдущему с учетом совпадения id и на конце будет содержать хеш,

[1] Блокчейн и криптовалюты простыми словами [Электронный ресурс]. – URL: https://golos.io/ru--blokcheijn/@stepanov/blokchein-i-kriptovalyuty-prostymi-slovami.

вычисленный из информации всех блоков цепи. Такую цепь как раз и называют блокчейном (от англ. *block chain* – цепочка блоков).

Следует, что чем больше серверов в блокчейне, чем сильнее серверы распределены в пространстве и чем менее взаимозависимы друг от друга или от какого-либо центра принятия решений, то есть децентрализованы, тем больше обеспечена защита исходных персональных данных.

Также в блокчейне используют токены – технологию, основную на принципе подмены реальных конфиденциальных данных некими значениями. Этот способ считается наиболее безопасным, он обеспечивает сохранение конфиденциальных данных[1]. Токенизация предназначена для закрепления цифровых прав граждан, например, электронного удостоверения личности (конфиденциальных персональных данных, например, клиента, получающего доступ к банковскому счету). Использование токенов представляется эффективным средством в оперативно-служебной деятельности правоохранительных органов.

Следовательно, необходимыми условиями противодействия кибертерроризму правоохранительными органами являются:

- взаимодействие всех правоохранительных органов и спецслужб в рамках внутригосударственных и межгосударственных структур посредством многосторонних механизмов и соглашений по вопросам уголовного расследования кибертерроризма, в том числе совершенствование законодательства, регулирующего уголовно-процессуальные действия;

- участие правоохранительных ведомств в международных конвенциях и договорах по противодействию международному кибертерроризму;

- введение уголовной ответственности и заморозка банковских счетов и других финансовых активов за финансирование кибертеррористических атак;

- в целях предотвращения кибертеррористических актов необходимо повысить скорость обмена оперативной информацией, привлекать высококвалифицированные кадры из информационно-телекоммуникационной сферы, оперативного и следственного аппарата, специализирующегося на выявлении и раскрытии преступлений в данной области, а также IT-специалистов, обладающих умениями и навыками по обнаружению противозаконных действий. Реализация указанных задач позволит обеспечить эффективное противодействие кибертерроризму.

[1] Токенизация. Принципы функционирования и выбор решения [Электронный ресурс]. – URL: http://www.akkamal.kz/info/library/tokenization.

Однако представляется, что усилий лишь одного государства в предупреждении террористических актов недостаточно, требуется координация действий на международном уровне в части обмена значимой информацией и развития возможностей Международного уголовного суда (МУС), введения европейского ордера на арест, пресечения канала финансирования экстремистских организаций и формирования списка террористических организаций.

Международный уголовный суд – первый постоянно действующий институт международной уголовной юстиции. В его компетенцию в настоящее время входит производство по делам о геноциде, преступлениях против человечности, военных преступлениях, преступной агрессии. Отказ Российской Федерации от участия в Римском статуте был заявлен по материально-правовым основаниям, но не по процессуальным. В этом плане следует уделить внимание идее, рассмотренной 30 ноября 2017 г. в ходе работы Научно-консультативного совета в Верховном Суде Российской Федерации, согласно которой в настоящее время то или иное развитие ситуации требует дифференциации порядка производства по уголовному делу[1].

В настоящее время такую идею можно и нужно распространить на международный уровень. Оговоримся, что возможность отнесения международного терроризма к юрисдикции МУС сегодня наталкивается на определенные препятствия, которые состоят в том, что те или иные террористические акты часто совершаются различными группировками, довольно небольшими по численности в сравнении с регулярной армией государства. Кроме того, террористы, как правило, не совершают те или иные преступления систематически и широкомасштабно в трактовке терминов, используемых в Римском статуте. Вместе с тем отдельные террористические группировки сегодня называют себя государством. И если проанализировать историю вопроса по Сирии и Ираку, связанную с захватом и контролем ИГ территории этих стран, то со всей уверенностью можно говорить о том, что такая практика является обычной, против террористов использовались стратегические бомбардировщики, подводные лодки, крейсеры и пр. Более того, другие международные трибуналы рассматривают терроризм как преследуемое уголовным законом деяние (речь идет о Статуте Международного трибунала по Руанде, а также Статуте Специального Суда по Сьерра-Леоне). Последнее утверждение связано, и, на наш взгляд, вполне обоснованно, с тем обстоятельством, что современные войны могут вестись

[1] Заседание Пленума Верховного Суда РФ 30 ноября 2017 года [Электронный ресурс]. – URL: https://vsrf.ru/press_center/news/26093.

латентно, при помощи наемников, которые, в том числе, в качестве метода военных действий могут избрать организацию и проведение террористических актов.

Причем следует заметить, что международные терроризм и наркоторговля были предметом обсуждения в ходе первых совещаний при образовании МУС. Ведь именно проблема международной наркоторговли и неэффективность национальных средств сподвигли Тринидад и Тобаго обратиться к международному сообществу за помощью. В 1994 году Комиссия по международному праву представила Генеральной Ассамблее ООН отчет о работе, проделанной в ходе 46 сессии, в котором был отражен Проект Статута Международного уголовного суда. Между тем именно США активно выступили против распространения юрисдикции МУС на данные преступления, ссылаясь на то обстоятельство, что они весьма успешно справляются с расследованием и пресечением этих преступлений своими силами и тратят на это колоссальные суммы денежных средств[1].

Отметим, что национальные и международные уголовно-правовые средства противодействия террористической деятельности важно рассматривать в их единстве и взаимосвязи. Представляется целесообразным не расширять круг норм, предусматривающих ответственность за совершение террористических действий, а поддержать идею назначения МУС смертной казни за указанный вид преступлений, которая призвана работать на упреждение распространения террористической деятельности как в России, так и в международном масштабе.

Таким образом, механизм солидарного функционирования правоохранительных органов призван эффективно распределять ресурсы при решении общей задачи обеспечения безопасности личности, общества и государства.

В настоящее время увеличиваются связи «силового блока» с «обеспечительным»; укрепление связей между ними является показателем нового объединения, которое основано на правоохранительной идеологии обеспечения прав человека.

В условиях усложнения международных отношений актуальное значение приобретает выбор правильных направлений и средств правового воздействия на общественные и иные процессы, чему способствует «обеспечительный блок» правоохранительной системы. При этом необходимо, чтобы выделенные автором блоки правоохранительной системы взаимодействовали солидарно, то

[1] Vyver J. Prosecuting Terrorism in International Tribunals // Emory International Law Review.

есть появляется необходимость в обеспечении эффективности деятельности силовых структур за счет обеспечительных средств.

На сегодняшний день только сильные государства, с хорошо организованной силовой составляющей правоохранительной системы имеют реальную возможность обеспечения как национальной безопасности личности, общества и государства, так и достойного существования на общественном и индивидуальном уровнях. В случае возникновения чрезвычайных обстоятельств, военных и вооруженных конфликтов только силовая составляющая является перманентно действующей движущей силой любой нации.

Указанные рекомендации позволят сотрудникам правоохранительных органов в конкретных ситуациях более успешно решать вопросы обеспечения безопасности, возникающие при осуществлении сотрудниками функциональных обязанностей в условиях международных экономических санкций и нарастающих угроз со стороны западных держав.

При этом современный период развития правоохранительной системы характеризуется ее цифровой модернизацией и открытием широких возможностей применения цифровых инструментов (блокчейн и искусственный интелект и др.) прогнозируемой четвертой промышленной революции.

3. Современное состояние и перспективы обеспечения правопорядка в условиях цифровизации

В современных условиях важным фактором динамики общественных отношений является цифровизация жизнедеятельности людей. Цифровые технологии изменяют вектор развития социума, что неизбежно отражается на всех сферах его жизни.

Современное общество находится под влиянием сложных процессов, связанных с усилением роли информации, стремительным развитием информационных технологий. В связи с этим значительным и имеющим интерес для сотрудников органов внутренних дел будет рассмотрение такого сложного и многогранного явления, как цифровизация, в том числе и его роли в правоохранительной деятельности.

При этом в научной литературе последних лет появился целый ряд терминов, с помощью которых ученые пытаются дать название отрасли права, связанной с использованием цифровых технологий, среди которых можно выделить: «право информатики», «компьютерное право», «программное право», «информационно-

компьютерное право», «цифровое право», «телекоммуникационное право», «информационное право» и др.

По мнению автора, наиболее целесообразным будет использование понятия «цифровое право», обусловленное массовым распространением цифровых отношений и появлением в связи с этим специальных норм, регулирующих их.

В настоящий период многие правоотношения связаны с использованием информационно-электронных ресурсов, которые раньше отсутствовали. Например, создаются электронные банки данных, происходит переход на электронный документооборот, внедрение системы искусственного интеллекта, оптимизируются государственные услуги и системы аутентификации личности, в результате чего можно дистанционно записаться на прием к врачу, подать процессуальные документы, получить справочную информацию, отправить обращения и жалобы.

При этом важно обратить внимание на то, что в связи с развитием в обществе правоотношений, основанных на цифровом взаимодействии, обостряется потребность в правовом регулировании таких отношений, а также возникающих на их основе пробелов и коллизий.

Процессы цифровой трансформации оказывают влияние не только на формы, сущностное содержание, субъектно-объектный состав различных правоотношений, но и, в том числе, на рост преступности в киберпространстве, транснациональной преступности, терроризма, включая преступления, совершаемые с использованием информационных технологий. С этим утверждением согласуется мнение академика В.Н. Кудрявцева о том, что информационные технологии сегодня используются как правоохранительными органами, так и преступниками. При этом он справедливо полагал, что «постоянно совершенствующиеся методы пресечения преступлений и технические возможности правоохранительных органов не стали основой тотального контроля над населением, чреватым вмешательством в личную жизнь людей, а значит, и нарушением фундаментальных прав человека»[1].

Таким образом, мы видим, что цифровые технологии, с одной стороны, представлены в широком спектре и созданиют большие преспуктивы для своего использования правоохранительными органами по обеспечению безопасности, а, с другой стороны, их использование развязывает руки криминалитету, что приводит к логическому выводу о необходимости придания упреждающего характера «цифровому праву».

[1] Кудрявцев В.Н. Стратегии борьбы с преступностью. - Изд. 2-е. испр. и доп. М., 2005. С. 69.

Этим обстоятельством обусловлена и необходимость переосмысления существующих подходов к обеспечению и защите прав человека; российская правоохранительная система должна соответствовать целям и задачам, которые ставятся в сфере обеспечения внутренней безопасности страны, ее регионов и граждан.

Так, одним из направлений совершенствования правоохранительной системы является внедрение электронных систем и технологий в деятельность правоохранительных органов. Применение цифровых информационно-коммуникационных технологий открывает большие перспективы в сфере борьбы с преступностью. Представляется необходимым исследование и развитие цифровых механизмов правоохранительной деятельности с учетом опережающих технологий управления данной сферы. Благодаря современным информационным технологиям у правоохранительных органов появится много новых возможностей, например, в сфере обеспечения безопасности дорожного движения, защиты банковских операций в режиме онлайн от несанкционированного доступа, разглашения персональных данных пользователя, пресечения незаконного оборота запрещенных веществ и предметов и пр. Однако стоит отметить, что на сегодняшний день правоприменительная практика сильно отстает от настоящих реалий современного общества в сфере цифровых технологий.

Сущность деятельности правоохранительной системы Российской Федерации определяется прежде всего теми объективными социальными условиями, в которых она формируется и развивается. Повышение эффективности функционирования правоохранительной системы Российской Федерации заключается в упорядочении деятельности по реализации возложенных на нее задач всех силовых структур.

Но, как мы видим, у органов правопорядка существует ряд значимых проблем, которые затрудняют, а иногда и делают невозможным раскрытие преступлений. Среди них – большой объем бумажного документооборота. Сотрудники буквально зарываются в огромном количестве документов, что порой и не является обоснованной необходимостью. В связи с этим целесообразно использование электронного документооборота.

В будущем ожидается перевод уголовного судопроизводства в электронный формат. Это позволит ускорить и улучшить ведение уголовных дел для скорейшего раскрытия преступлений, изобличения виновных и применения к ним справедливого наказания.

Успешный перевод уголовного судопроизводства в электронный формат был произведен в Саудовской Аравии более десяти лет

назад. В этой стране преступления раскрываются намного быстрее, чем в Российской Федерации. В некоторых странах полностью отказались от уголовного судопроизводства в бумажном виде, а в других допускается его ведение как в бумажном, так и в электронном виде, например, в России.

Ожидания общества и перспективы развития цифровых технологий значительны и связаны с расширением онлайн-доступа к различным процессуальным действиям. На сегодняшний день уже имеются возможности, позволяющие в необходимых случаях избежать поездок в суды, например, посредством использования видеоконференц-связи.

В настоящее время в Российской Федерации происходит создание и усовершенствование правовой основы и нормативной правовой базы в области цифровизации, что подтверждается содержанием Послания Президента Российской Федерации Федеральному Собранию Российской Федерации, в котором был анонсирован переход государства к цифровой экономике[1]. После чего началась работа над национальной программой с аналогичным названием, принятой в соответствии с Указом Президента Российской Федерациии от 07 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года».

В ноябре 2017 года Департаментом проектной деятельности Правительства Российской Федерации была представлена Концепция поэтапной цифровизации правовой системы, а спустя две недели на конференции LegalTech в Сколково состоялось первое масштабное профессиональное обсуждение вопросов цифровой трансформации права в России. После этого последовал ряд нормативных правовых актов в области цифровизации, некоторые из которых еще не вступили в законную силу[2].

На заседании правительственной комиссии по цифровому развитию Д.А. Медведев заявил, что «Министерство внутренних дел является одним из ключевых участников национальной программы «Цифровая экономика». В банках данных МВД, полиции содержатся весьма востребованные сведения. Причем количество запросов по ним – как от ведомств, так и от людей – стремительно растет. Понятно, что с увеличением нагрузки на информационные ресурсы процессы выполняются дольше. А это вопрос не только эффективности работы ведомства, но и в первую очередь – обеспечения по-

[1] Послание Президента Российской Федерации В.В. Путина Федеральному Собранию Российской Федерации от 1 декабря 2016 г. [Электронный ресурс]. – URL: http://www.kremlin.ru/acts/bank/41550.

[2] Сайт Государственной Думы Федерального Собрания Российской Федерации [Электронный ресурс]. – URL: http://duma.gov.ru.

рядка, безопасности. Поэтому нужно думать о модернизации технической инфраструктуры МВД. Это потребует создания центров хранения и обработки информации. Нужно проработать вопрос о том, на какой технологической площадке они будут размещаться. Нужны новые цифровые платформы и гибкая система, которая способна работать с большими данными. Также нужно развивать современные сети связи здесь, как и в других местах. И необходимо, естественно, позаботиться о том, чтобы все данные были надежно защищены, включая защиту от киберпреступности»[1].

Цифровая трансформация правоохранительных органов проводится в рамках государственной политики по созданию необходимых условий для развития цифровой экономики Российской Федерации. Осуществление данной задачи необходимо в целях:

- создания среды электронного взаимодействия с гражданами;
- исключения бумажного документооборота;
- оптимизации деятельности, выраженной в повышении скорости работы и ее упрощении;
- создания принципиально новых каналов взаимосвязи между правоохранительными структурами, а также между правоохранительными структурами и гражданами;
- интеграции правоохранительных систем противодействия преступности;
- противодействия коррупции;
- решения кадровой проблемы;
- развития цифровой инфраструктуры на базе использования российских информационно-телекоммуникационных технологий.

Таким образом, итог теоретико-правовой оценки современного состояния и перспектив развития правоохранительной системы в информационно-цифровую эпоху сводится к предложению совершенствования законодательства в области регулирования отношений, складывающихся по поводу использования цифровых технологий и внедрения их в правоохранительную деятельность.

В настоящее время уголовно-процессуальное законодательство допускает внедрение в работу цифровых технологий в ходе производства по уголовному делу. Например:

1. В соответствии с ч. 2 ст. 474 УПК РФ процессуальные документы могут быть выполнены типографским, электронным или иным способом.

[1] Медведев Д.А. Заседание Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности [Электронный ресурс]. – URL: http://government.ru/news/36818.

2. В ч. 3 ст. 474.1 УПК РФ говорится, что копия судебного решения, изготовленная в форме электронного документа, заверенная усиленной квалифицированной электронной подписью, по просьбе либо с согласия участника уголовного судопроизводства может быть направлена ему с использованием информационно-телекоммуникационной сети «Интернет».

3. Часть 2 ст. 393 УПК РФ говорит о том, что копия обвинительного приговора направляется судьей или председателем суда в то учреждение или в тот орган, на который возложено исполнение наказания. Для исполнения приговора, определения, постановления суда в части имущественных взысканий вместе с копиями приговора, определения, постановления суда судебному приставу-исполнителю направляется исполнительный лист. Исполнительный лист вместе с копиями приговора, определения, постановления суда может направляться судом для исполнения судебному приставу-исполнителю в форме электронного документа, подписанного судьей усиленной квалифицированной электронной подписью в порядке, установленном законодательством Российской Федерации.

Уже действуют ведомственные приказы, позволяющие применять в деятельности субъектов уголовного судопроизводства современные информационно-цифровые технологии. Одним из них является приказ МВД России от 29 августа 2014 г. № 736 «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях». Данный приказ позволяет принимать заявления о преступлении в электронной форме посредством официальных сайтов, при помощи специального программного обеспечения, которое предусматривает заполнение специальных реквизитов.

Совершенствование данного направления делает необходимым внесение в УПК РФ изменений, касающихся ряда процессуальных действий. К их числу можно отнести: подписание процессуальных документов при помощи электронной подписи; перевод уголовного судопроизводства в электронный формат; использование новых понятий, необходимых при осуществлении цифрового уголовного судопроизводства; упорядочение порядка уведомления участников уголовного процесса о различных процессуальных действиях (например, о вызове на допрос); взаимодействие участников уголовного судопроизводства в электронном виде; допуск участников уголовного дела к материалам уголовного дела в части, их касающейся; порядок составления ходатайств и жалоб в электронном

формате; порядок получения судебной санкции при производстве следственных действий, требующих согласия судьи, и осуществление контроля за действиями следователя при ведении уголовного дела в электронном формате.

Внедрение в уголовное судопроизводство вышеуказанных функций позволит ему выйти на новый уровень, повысить эффективность, качество и сократить сроки осуществления процессуальных действий и принятия решений.

Что касается современного состояния и перспектив обеспечения внутренней безопасности, то не следует забывать практику правоохранительных органов в Белоруссии и Украине, поскольку сценарий гипотетически может повториться и в Российской Федерации. Следует констатировать, что политические события, происходящие сегодня в указанных странах, создают угрозы не только всей системе международных отношений, но и внутреннему правопорядку. Следовательно, является актуальным вопрос: что нужно сделать, чтобы не допустить развития неблагоприятных событий, возникших спонтанно?

Опыт общественного развития показывает, что если внутренним вызовам безопасности не уделяется достаточно внимания на ранних стадиях, то миротворческие усилия, направленные на постконфликтное урегулирование, могут оказаться напрасными. Так, в нестабильных государствах из-за того, что система действенного управления фактически не функционирует, а верховенство закона отсутствует, возникает размытость понятий «преступность» и «война». В этих условиях на сознание сотрудников правоохранительных органов воздействует идея «не войны и не преступности», порождающая недоверие к праву и государству, коррумпированность государственных органов, невозможность справедливой защиты прав человека, его чести и достоинства, что побуждает граждан к самозащите, способами, порой дискредитирующими власть, к насилию и произволу[1].

В связи с этим именно правоохранительный аспект приобретает особую актуальность и значимость. При этом он самым непосредственным образом связан с развитием теоретико-правовых воззрений, направленных на повышение эффективности деятельности силовой компоненты правоохранительной системы, исследование которой позволит определить дальнейшие перспективы деятельности правоохранительных структур, минимизировать риск утраты

[1] Степанов О.А., Прохорова Е.Н. «Силовая» составляющая правоохранительной системы в рамках осуществления государственного строительства в России // Современное право. 2015. № 3. С. 30.

контроля над правопорядком с тем, чтобы противостоять возникающим угрозам правопорядку и безопасности.

В современных условиях правоохранительные органы Российской Федерации должны быть готовы к успешному решению задач по обеспечению общественного порядка и безопасности в условиях применения новых «протестных технологий». Прежде всего это касается наиболее уязвимых территорий, которые в случае возникновения непредвиденных актов агрессии или социальной напряженности, связанных с вооруженным сопротивлением осуществлению государственной деятельности путем управления через «протестные технологии», становятся уязвимыми с точки зрения общественной безопасности ввиду фактической оторванности их от основной территории.

Масштабные протестные компании способны вызвать как позитивные, так и негативные процессы в обществе. Стоит отметить, что под «протестными технологиями» следует понимать меры, направленные на отдельные социальные группы с целью изменения их эмоциональных и психических состояний, суждений, мнений, оценки и поведения в интересах организатора проведения операции.

Следовательно, формы и методы работы сотрудников правоохранительных органов должны трансформироваться с учетом новых потребностей общества по защите прав и обеспечению правопорядка на более профессиональном уровне, связанном с адекватным и соразмерным использованием сил и средств.

Так, в качестве способа ненасильственной политической борьбы можно отметить использование электронных сетей и смартфонов, с помощью которых создаются Telegram-каналы, выступающие в качестве технологии организации и физического управления протестом, призывающие к выполнению тех или иных действий, выгодных сторонникам оппозиционных движений, препятствовать осуществлению законной деятельности государственных органов. Через них пользователям поступает информация о проведении мероприятия, его дате, времени, местах сбора, маршрутах движения, возможных опасностях для активистов, связанных с перемещениями полиции и пр.

Действия призывающих носят организованный характер, а отличительными признаками являются операторы с профессиональным оборудованием и активисты, стимулирующие участников и управляющие толпой. Одного «информационного вброса» достаточно для того, чтобы ложная информация распространилась в обществе, что может привести к хаосу и беззаконию. Следовательно, организовать политические акции стало проще и быстрее.

Наиболее тяжелыми последствиями реализации таких акций являются разлад в обществе, недоверие к власти, развал экономики, человеческие жертвы и пр. События в Белоруссии можно также проанализировать с точки зрения динамики политических инноваций, где подобные технологии активно использовались для координации действий и передачи информации о местоположении сил ОМОНа.

Чтобы понять суть использования информационных технологий для организации беспорядков, оценить степень угрозы общественной безопасности, нужно рассмотреть ее особенности.

В частности, к особенностям информационной сферы, связанным с организацией и управлением беспорядками, можно отнести отсутствие явного лидера, высокую степень анонимности и латентности действий, трудность в выявлении актора и используемых коммуникационных технологий.

Новые форматы воздействия очень пластичны, легко меняют свои контуры, обеспечивают быструю скорость обмена информацией. Используемые коммуникационные технологические площадки становятся штабами координации, провоцирующими сценарии, выгодные организаторам атаки.

Еще одной особенностью является то, что отсутствуют четкие границы в проведении операции. При ее проведении могут одновременно охватываться не только локальные, но и глобальные районы.

К особенностям также следует отнести массовый охват аудитории и возможный огромный масштаб последствий, который может выражаться в смене политического лидера, представителей органов государственной власти, государственного режима, провоцировании конфликтов между государствами, разжигании ненависти и пр.

Конечной целью такого воздействия являются массовые выступления для свержения неудовлетворяющего режима. Достижение целей протестной кампании зависит от ресурсов и мобилизационных возможностей, которыми располагает актор.

Соответственно, можно сделать вывод о возникновении новой, неведомой ранее угрозы установления цифровой диктатуры как формы организации человеческой деятельности, которая возникает путем манипулирования новыми информационно-коммуникационными технологиями.

Наглядным примером применения такого воздействия является давление на сотрудников силовых структур правоохранительных органов, связанное с угрозой разглашения в киберпространстве персональных данных (дата рождения, имена, номер телефона, адрес проживания, сведения о занимаемой должности и пр.). Права

сотрудников рассматриваются как инструмент манипулирования, используемый «киберпартизанами» в своих интересах.

Угрозы, которые поступают от организаторов протестных движений о том, что они знают адреса сотрудников силовых ведомств и готовы оказывать давление на их близких, приводят к высочайшему психологическому стрессу и срывам. На сотрудниках начинает сказываться усталость, что приводит к увольнениям, а то и вовсе к переходу на сторону противника.

Однако стоит отметить, что в нынешних условиях практически отсутствует правоохранительный механизм защиты от актов информационного воздействия.

В целях защиты персональных данных следует обратить внимание на использование в деятельности правоохранительных органов интегрированных банков данных, позволяющих обеспечить запросы по различным направлениям оперативно-служебной деятельности.

В каждом подразделении существует своя информационная система конфиденциальных данных ограниченного доступа и их защита. При этом имеются открытые банки данных, доступ к которым не запрещен сотрудникам всех государственных структур, например, база данных Федеральной миграционной службы Российской Федерации, и банки данных с ограниченным доступом, к которым относится, например, международный информационный банк данных ГИАЦ МВД России.

Интеграция действий правоохранительных органов в сфере защиты конфиденциальных данных, несомненно, позволяет повысить эффективность их деятельности. Информационная система, включающая в себя интегрированные банки данных, обеспечивающая предоставление оперативной информации в интересах всех подразделений, предусматривает решение следующих задач: обеспечение запросов по различным направлениям оперативно-служебной деятельности; информационный обмен между различными правоохранительными подразделениями; сбор, обработка и анализ информации; информационная поддержка расследований, проводимых различными службами и ведомствами.

Реализованные технические решения по интеграции информационных ресурсов позволяют максимально сократить сроки проведения поиска в банках данных федерального и регионального уровней, содержащих сведения о лицах, судимых и находящихся в розыске, утерянном и украденном оружии, автомототранспорте, а также по ряду иных объектов учета, что в конечном итоге способствует оперативному раскрытию преступлений.

В решении задач по организации противодействия нетрадиционным методам организации беспорядков, связанным с психоэмоциональными факторами, должны активно участвовать все силы и средства правоохранительной системы, деятельность которых в той или иной мере связана с решением указанных проблем.

Одним из возможных способов противодействия информационным угрозам и повышения эффективности защиты прав человека является создание механизма информационного противодействия в деятельности правоохранительных органов. Изменение форм обеспечения правопорядка в современных условиях требует разработки более гибкой стратегии организации управления правоохранительными органами, включающей доктрину информационного противодействия, ведения информационных операций, связанных с обеспечением внутреннего правопорядка.

Необходимо изменение существующего подхода к противодействию современным угрозам. Например, психологическое воздействие через современные информационные технологии для подавления сил противника может использоваться не только как специфический метод нелетального поражения, но и как самостоятельная форма привлечения правоохранительных органов к обеспечению правопорядка.

Психологические операции могут выступать в роли фактора, существенно повышающего эффективность правоохранительной деятельности. Способами противодействия протестному информационному воздействию являются регулирование деятельности средств массовой информации, военно-политическая цензура, а также ликвидация самих источников информации. К последним можно отнести разработку и применение средств блокирования информационных каналов связи путем выведения из строя технологических систем управления и контроля.

Ключевое место в таком взаимодействии занимает обмен значимой оперативной информацией в целях обеспечения внутреннего правопорядка, своевременного информирования о готовящихся актах, что способствует предупреждению, пресечению и расследованию преступлений с использованием современных технологий.

Другое направление взаимодействия заключается в проведении совместных мероприятий по созданию условий, способствующих успешной реализации государственной политики в сфере безопасности и охраны правопорядка, защиты жизненно важных интересов личности, общества и государства.

И, наконец, третье направление касается решения кадрового вопроса, связанного с организацией подготовки специалистов в ин-

формационной сфере для обеспечения правопорядка и общественной безопасности с целью противодействия киберугрозам. При этом данных сотрудников необходимо обучать умению оценивать степень информационных угроз и определять допустимые риски, анализировать и оценивать уязвимость информационных систем, принимать меры по нейтрализации таких угроз.

Следовательно, необходимо исследовать и развивать цифровые механизмы правоохранительной деятельности с учетом опережающих технологий управления данной сферы. Благодаря современным информационным технологиям у правоохранительных органов появится много новых возможностей, например в сфере обеспечения безопасности дорожного движения, защиты банковских операций в режиме онлайн от несанкционированного доступа, разглашения персональных данных пользователя, пресечения незаконного оборота запрещенных веществ и предметов и пр.

Взаимодействие между правоохранительными органами должно осуществляться с четким определением места и роли каждой из сторон и каждого сотрудника. При этом важно наладить механизм взаимодействия правоохранительных органов с институтами гражданского общества, который в России пока носит декларативный характер (особенно в субъектах Российской Федерации).

Гражданское общество является одной из важнейших составляющих демократического государства и важнейшим звеном системы сдержек и противовесов. Свое влияние гражданское общество оказывает на правоохранительные органы в целях усовершенствования их деятельности, пресечения их незаконной деятельности, а также для защиты прав и свобод человека и гражданина.

Различные «формы сотрудничества общественных формирований с полицейскими органами, начиная от совместного патрулирования и организации опорных пунктов дежурства по охране правопорядка до внедрения специализированных программ социальной профилактики и предупреждения правонарушений и криминальных явлений, используются при осуществлении правоохранительной деятельности в Великобритании, ФРГ, Канаде»[1].

Анализ зарубежного и отечественного опыта электронного взаимодействия показывает, что на первый план выдвигаются проблемы удовлетворенности граждан доступом к правоохранительным ресурсам и их доверия правоохранительной системе.

Однако в российском законодательстве и практике пока не выработаны четкие механизмы, которые бы обеспечивали контроль

[1] Нижник Н.С. Полиция и гражданское общество: поиск вектора взаимодействия // Полицейская деятельность. 2018. № 5. С. 59.

институтов гражданского общества за процессами принятия и реализации государственно-властных решений.

Как выясняется, даже при наличии такой возможности граждане не используют свое право обращаться в правоохранительные органы с сообщениями и заявлениями. Например, согласно приказу МВД России от 31 декабря 2012 г. №1166 «Вопросы организации деятельности участковых уполномоченных полиции», участковый уполномоченный полиции обязан вести прием граждан и рассматривать их обращения. В действительности, граждане не пользуются предоставленным им правом в силу неосведомленности или нежелания взаимодействовать с государственными органами, что зачастую и является причиной наступления негативных последствий.

Представляется целесообразным развивать данное взаимодействие посредством использования современных технических средств, так как подобное общене граждан с представителями органов внутренних дел не требует посещения опорного пункта полиции.

Совершенствование порядка взаимодействия правоохранительных органов с гражданским обществом должно заключаться в создании конкретных механизмов контроля, обеспечении открытости и гласности деятельности органов государственной власти, ограничении влияния интересов отдельных групп на осуществление правоохранительной функции государства.

Сущностью контроля граждан за правоохранительной деятельностью является установление правового порядка, исключающего коррупцию, ставящего на первое место открытость и гласность при осуществлении правоохранительной функции.

Одним из современных методов контроля за правопорядком и обеспечения безопасности является использование камер видеонаблюдения как сотрудниками правоохранительных органов, так и представителями гражданского общества. Широкая сеть видеокамер рассчитана на опознание преступников, а также на превентивные меры, направленные на снижение вероятности совершения преступления.

В связи с этим интересен опыт Великобритании по использованию камер видеонаблюдения в качестве средства фиксации совершенного правонарушения. Компания DigitalBridge сразу после терактов 2005 года учредила новый местный телеканал Shoreditch TV, на который стекается информация с 12 камер видеонаблюдения. Это позволяет гражданам оперативно сообщать о происшествиях, подозрительных личностях, например, сравнивая их с портретами лиц, находящихся в розыске или недавно вышедших из тюрьмы. Таким образом, каждый гражданин имеет возможность отправить

электронное сообщение напрямую в полицию, не выходя из дома[1].

Этот пример весьма наглядно подчеркивает положительную сторону использования современных технических возможностей и подтверждает наличие механизма взаимодействия правоохранительных органов с институтами гражданского общества.

Однако не всегда подобные методы вызывают положительный отклик со стороны общества. С противоположной стороны проявил себя опыт использования систем видеонаблюдения в г. Сан-Франциско. Общественность высказала мнение о том, что применение данной технологии может привести к нарушению неприкосновенности частной жизни и гражданских прав жителей. Критики системы распознавания лиц утверждают, что эта технология недостаточно надежна и не должна использоваться правоохранительными органами, так как ошибки в системе могут привести к тому, что в полицейские расследования будут вовлечены невинные люди[2].

Таким образом, выработались две противоположных точки зрения: граждане либо готовы сотрудничать с сотрудниками правоохранительных органов и претерпевать определенные ограничения, либо настроены против систем видеонаблюдения, охватывающих личные стороны жизни людей.

Модель взаимодействия российского гражданского общества с правоохранительными органами должна соответствовать реалиям, то есть должна быть основана на партнерских взаимоотношениях правоохранительных органов с институтами гражданского общества не за счет подавления индивида государством, а посредством создания некоторых барьеров, в пределах которых на данном конкретном этапе возможно введение инноваций.

К обеспечению внутренней защищенности общества целесообразно применить такой подход, где безопасность – это компромисс между правоохранительными целями социальной системы и действиями, предпринимаемыми правоохранительными органами.

Здесь главным фактором является создание системы доверительных отношений между гражданами и сотрудниками правоохранительных органов, что подчеркивается в Стратегии развития России на 2018-2024 годы[3]. В основе формирования партнерской модели

[1] Невидимое оружие Скотленд-Ярда. Как относятся лондонцы к жизни под прицелом видеокамер [Электронный ресурс]. – URL: https://www.moscowtorgi.ru/news/bolshaia_ dvadtcatka/64.

[2] Власти Сан-Франциско запретили использование технологий распознавания лиц [Электронный ресурс]. – URL: https://hitech.vesti.ru/article/1207598.

[3] Указ Президента Российской Федерации от 07.05.2018 № 204 (ред. от 19.07.2018) «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // СПС «КонсультантПлюс».

таких взаимоотношений находится положительный имидж сотрудника правоохранительных органов.

Сложившаяся отечественная модель организации правоохранительной деятельности безнадежно устарела. В настоящий момент правоохранительная система должна быть существенным образом переформатирована путем усиления оперативного информационного взаимодействия «силовых» и «обеспечительных» блоков правоохранительной системы и их сотрудников при расширении механизмов координирующего управления данными органами.

В качестве шага, позволяющего повысить эффективность осуществления правоохранительной функции государства с учетом взаимодействия с гражданами для обеспечения законности и правопорядка, может рассматриваться высокотехнологичный надзор[1], сущность которого заключается в создании на основе комплексной оптимизации единой цифровой платформы управления и функционирования правоохранительных органов всех уровней.

В связи с этим необходимо адаптировать правоохранительную систему к новым цифровым реалиям с учетом существующих возможностей для цифровизации, лучших практик государственного управления и растущих ожиданий со стороны граждан.

В части повышения эффективности действий правоохранительных органов и взаимодействия их с населением в области безопасности данные положения соответствуют «Основным направлениям деятельности Правительства Российской Федерации на период до 2024 года»[2], которые предусматривают внедрение в практическую деятельность цифровых технологий и платформенных решений, направленных на предупреждение и противодействие угрозам в киберпространстве, оперативное взаимодействие с правоохранительными структурами по фактам совершения противоправных действий в киберсреде, обеспечение доступа граждан к информации, о случаях использования их персональных данных и др.

Основными задачами высокотехнологичного надзора являются:

- повышение эффективности надзора путем внедрения современных информационно-коммуникационных технологий обработки информации во все виды правоохранительной деятельности;

- совершенствование правового и технологического обеспечения оценки качества правоохранительной деятельности;

[1] Информационные технологии в Генпрокуратуре РФ [Электронный ресурс]. – URL: http://www.tadviser.ru/index.php.

[2] Документ рассмотрен и одобрен на заседании Правительства 27 сентября 2018 года [Электронный ресурс]. – URL: http://government.ru/news/34168.

- расширение возможностей граждан по защите их прав в условиях цифровой среды взаимодействия;

- усиление оперативности реагирования на совершение каких-либо правонарушений;

- сокращение временных затрат на поступающие обращения;

- обеспечение противодействия высокотехнологичным угрозам путем межведомственного взаимодействия правоохранительных структур;

- меры превентивного характера;

- обеспечение оперативного, в том числе дистанционного, получения актуальной и своевременной информации о работе сотрудников правоохранительных органов по профилактике правонарушений и преступлений, состоянии законности.

Высокотехнологичный надзор связан с созданием такой цифровой инфраструктуры, которая предусматривает введение единой межведомственной цифровой онлайн-платформы управления данными для сотрудников правоохранительных органов, которая улучшит качество и доступность межведомственного взаимодействия, ускорит обмен информацией между государственными структурами в процессе оказания услуг гражданам, а также обеспечит прозрачность правоохранительной деятельности.

Представляется, что данная платформа объединит информацию из множества государственных систем, реестров и баз данных, в том числе систематизирует данные Единого государственного реестра юридических лиц, Государственного реестра транспортных средств, Единого государственного реестра недвижимости и др.

Так, в средствах массовой информации уже анонсировали запуск новых суперсервисов на портале государственных услуг, среди которых «Уведомление и обжалование штрафов за нарушение ПДД онлайн», «Правосудие онлайн», «Трудовая миграция онлайн».

Единая цифровая платформа правоохранительной деятельности должна будет объединить все существующие профильные цифровые проекты, например, от выдачи электронного заключения эксперта до получения процессуального решения с использованием возможностей искусственного интеллекта.

Фактически речь идет о совершенствовании правоохранительной деятельности путем создания единой цифровой платформы для обеспечения дистанционного взаимодействия граждан с правоохранительными органами или межведомственного взаимодействия, призванного повысить эффективность правоохранительной деятельности, обеспечить гласность, прозрачность и законность действий правоприменителей.

С одной стороны, внедрение цифровых инструментов в правоохранительную деятельность позволяет решить внутриведомственные задачи правоохранительной системы, а с другой стороны, создает новые возможности для удовлетворения потребностей граждан в защите их прав.

Создание цифровой среды управления правоохранительными ресурсами, обеспечивающей взаимодействие с институтами гражданского общества, позволит преодолеть недостатки правоохранительной реформы, в ходе которой пока не получили должной правовой регламентации вопросы цифрового взаимодействия между правоохранительными органами и гражданами, не решены организационные проблемы межведомственного взаимодействия, которые позволили бы оптимизировать осуществление правоохранительной деятельности.

С учетом внедрения единой цифровой правоохранительной платформы меняется парадигма создания систем поддержки решений, в которых в настоящее время основной акцент делается на обработке количественной и статистической информации, содержащейся в банках данных. Информация, поступающая от непосредственных участников событий, жителей, экспертов, дающих качественные оценки произошедшему, перестает быть наиболее значимым источником информации при принятии решений.

Во многих областях правоохранительной деятельности важную роль также играет межведомственная интеграция. Например, для защиты национальных границ перспективным является сотрудничество таможенных органов с иными государственными органами и должностными лицами с использованием безопасных инструментов совместной работы. Стороны могут быстро обмениваться разведывательными данными и другой оперативной информацией, позволяющей пресекать такие виды преступлений, как контрабанда наркотиков, торговля людьми и нелегальная миграция. Вместе с тем вся необходимая информация будет доступна для руководителей на местах и удаленных командных центрах в дистанционном режиме[1].

Решение по созданию цифровой платформы значительно облегчает связь с гражданами, которые, используя современные информационно-коммуникационные технологии, могут сообщать информацию онлайн, заполняя формы электронных документов.

Применительно к проблеме защиты прав личности это обстоятельство важно рассматривать через призму справедливой оценки

[1] См.: Голованова Н.А., Гравина А.А., Зайцев О.А. Уголовно-юрисдикционная деятельность в условиях цифровизации: монография. М.: ИЗиСП при Правительстве РФ; ООО Юридическая фирма контракт, 2019. С. 8.

обществом действий личности, по крайней мере, пока не появится программно-аппаратное обеспечение, сравнимое по мощи с разумом человека.

Данная модель должна развиваться с учетом перспектив внедрения системы искусственного интеллекта в правоохранительную практику, когда возможности машинного интеллекта будут использоваться для генерации возникающих правоохранительных правоотношений и поиска оптимального решения на основе введенных алгоритмов. Автоматизация процесса обработки сообщения о преступлении исключила бы неправомерный отказ в приеме и регистрации заявления о преступлении, а также ошибки, которые могут быть допущены человеком.

Анализируемый процесс облегчает процедуру поиска необходимого документа, открывает к нему удаленный доступ в режиме реального времени, значительно экономит ресурсы (например, снижает затраты на транспортировку документов, их хранение), сокращает трудоемкость процессов, исключает ошибки, обеспечивает прозрачность соблюдения прав граждан, формирует среду доверия, нацеленную на обеспечение защиты интересов граждан, повышает качество правосудия и его эффективность.

К тому же если говорить о преимуществах искусственного интеллекта, то стоит отметить, что он способен функционировать круглосуточно, без перерыва на сон и отдых, также он способен к быстрому и эффективному обучению. При этом он никогда ничего не забывает, не путает информацию в силу субъективных причин.

Так, по мере того как робот-диспетчер получает нужную информацию, он может передавать сведения полиции или иным сотрудникам правоохранительных органов, то есть он имеет исключительную возможность собственными действиями вызвать наступление определенных последствий, связанных с возникновением, изменением или прекращением правоотношений. По результатам рассмотрения сообщений о преступлении граждане незамедлительно уведомляются в автоматическом режиме.

Только искусственный интеллект способен обеспечить невиданные ранее масштабы защиты нарушенного права в удобном, дистанционном режиме. Роботизация правоохранительной сферы сможет обеспечить высокие показатели качества и эффективности рассмотрения обращений в минимальные сроки.

Скорейший переход к цифровой платформе функционирования правоохранительной деятельности требует проведения многочисленных организационных, технологических и нормативных мероприятий. Для реализации указанной задачи требуется провести

огромную работу, которая включает в себя создание нормативной правовой базы, регулирующей деятельность как представителей гражданского общества, так и сотрудников правоохранительных органов; необходимо решение вопроса об уполномоченных лицах из числа гражданского общества, которые могли бы выступать от имени граждан, осуществлять контроль за деятельностью правоохранительных органов; со стороны государства требуется финансирование создания данной платформы, необходимой для более эффективного решения задач по обеспечению правопорядка и безопасности.

Перспективы разработки цифровой платформы управления правоохранительными ресурсами предполагают внедрение эффективных механизмов межведомственного взаимодействия на пути совместных организационных действий со всеми смежными структурами и организациями; совершенствование организационно-технических, нормативных правовых и иных основ разработки, внедрение, эксплуатацию и развитик существующих и вновь создаваемых элементов цифровой среды правоохранительных ресурсов; создание и развитие безопасной информационно-телекоммуникационной инфраструктуры, использующей защищенные средства связи и передачи данных.

Указанное заслуживает самого пристального внимания ученых и практиков, которые призваны учитывать необходимость совершенствования форм и методов осуществления правоохранительной деятельности на основе использования современных информационных систем и технологий в режиме реального времени.

Таким образом, необходимо дальнейшее совершенствование нормативного правового регулирования и технического обеспечения правоохранительной деятельности в части, касающейся обеспечения правопорядка, которое связано с внедрением в практику единой цифровой платформы управления правоохранительными ресурсами. Данный вопрос необходимо в неотложном порядке включить в дорожную карту реформирования правоохранительных органов Российской Федерации, в которой внедрение цифровых технологий сопровождалось бы значительной проработкой изменений процессуального права, что требует тесного сотрудничества правоохранительных органов и органов исполнительной власти, ответственных за внедрение в Российской Федерации цифровых платформ и механизмов.

Заключение

На сегодняшний день угрозы национальной безопасности представляют собой серьезную проблему, встающую перед правоохранительными органами. В таких условиях должна повышаться роль международного взаимодействия и признания общих нормативных установок на основе развития правовой гармонизации. Такой процесс может рассматриваться как рациональный инструмент правового регулирования в современных условиях имеющихся угроз и кибератак.

В связи с этим правоохранительная система может характеризоваться как комплексное явление, связанное с идеями обеспечения законности и безопасности личности, общества и государства и включающее силовую и обеспечительную подсистемы. При этом в рамках международного сотрудничества должны быть интегрированы действия всех правоохранительных структур, гарантирующих обеспечение прав и свобод человека и гражданина, связанных с их безопасным существованием и сохранением стабильного политического порядка в мире.

Также можно констатировать, что развитие информационно-электронных технологий характеризуется постоянным ростом количества киберпреступлений. В связи с этим создание реестров персональных данных на основе блокчейнов может отвечать признакам современности технологического обеспечения, информационной безопасности, защиты от несанкционированного доступа, неправомерного копирования, распространения и использования значимой информации. Кроме того, правообладатель будет иметь возможность отследить использование своих персональных данных, что имеет большое значение для функционирования правоохранительной системы и противодействия современным угрозам в условиях цифровизации.

Предлагаемые в пособии практические рекомендации призваны оказать положительное влияние на работу правоохранительных органов, обеспечивающих безопасное существование личности, общества и государства, связанное с выявлением правонарушений, установлением лиц, их совершивших, и предотвращением событий, создающих угрозу национальной безопасности.

Список использованных источников

Законы, нормативные правовые акты и иные официальные документы:

1. Международная конвенция о борьбе с финансированием терроризма (заключена в г. Нью-Йорке 09.12.1999).

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 05.04.2021, с изм. от 08.04.2021) // Собрание законодательства РФ, 17.06.1996, № 25, ст. 2954.

3. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» (ред. от 30.04.2021) // Собрание законодательства РФ, 14.07.2003, № 28, ст. 2895.

4. Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму» (ред. от 08.12.2020) // Собрание законодательства РФ, 13.03.2006, № 11, ст. 1146.

5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 09.03.2021, с изм. и доп., вступ. в силу с 20.03.2021) // Собрание законодательства РФ, 31.07.2006, № 31 (ч.1), ст. 3448.

6. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности» (ред. от 09.11.2020)// Собрание законодательства РФ, 03.01.2011, № 1, ст. 2.

7. Указ Президента Российской Федерации от 15.02.2006 № 116 «О мерах по противодействию терроризму» (ред. от 25.11.2019) // Собрание законодательства РФ, 20.02.2006, № 8, ст. 897.

8. Указ Президента Российской Федерации от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (ред. от 22.12.2017) // Собрание законодательства РФ, 21.01.2013 г., № 3, ст. 178.

9. Указ Президента Российской Федерации от 18.11.2015 № 562 «О Межведомственной комиссии по противодействию финансированию терроризма» // Собрание законодательства РФ, 23.11.2015, № 47, ст. 6576.

10. Указ Президента Российской Федерации от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ, 04.01.2016, № 1 (часть II), ст. 212.

Научная литература и материалы периодической печати:

11. Баранов В.Л. Правовое регулирование социальной защиты сотрудников правоохранительных органов // Журнал российского права. 2012. № 1. С. 78-88.

12. Бержель Ж.-Л. Общая теория права. М., 2000.

13. Братко А.Г. Правоохранительная система: вопросы теории: автореф. дис. ... д-ра юрид.наук / Академия МВД России. М., 1992.

14. Дамаскин О.В. Актуальные вопросы организации противодействия терроризму // Вестник военного права. 2016. № 1. С. 67-76.

15. Голованова Н.А., Гравина А.А., Зайцев О.А. Уголовно-юрисдикционная деятельность в условиях цифровизации: монография. М.: ИЗиСП при Правительстве РФ; ООО Юридическая фирма контракт, 2019. 212 с.

16. Грачев С.И. Контртерроризм: организационные, правовые, финансовые аспекты и вопросы профилактики / под ред. О.А. Колобова. Нижний Новгород, 2010. 166 с.

17. Котенко И.В., Юсупов Р.М. Информационные технологии для борьбы с терроризмом // Защита информации INCIDE. 2009. № 2. С. 74-79.

18. Кудрявцев В.Н. Стратегии борьбы с преступностью. - Изд. 2-е. испр. и доп. М., 2005.

19. Нижник Н.С. Полиция и гражданское общество: поиск вектора взаимодействия // Полицейская деятельность. 2018. № 5.

20. Общая теория права и государства / под ред. В.В. Лазарева. М., 2001.

21. Прохорова Е.Н. Трансформация механизмов функционирования правоохранительных органов в условиях цифровизации // Российский журнал правовых исследований. 2019. № 3(20). Том 6. С. 174-178.

22. Романова Л.М. Национальный суверенитет в условиях глобализации: институционально-правовой анализ: автореф. дис. ... д-ра юрид. наук. Ростов-на-Дону, 2009.

23. Соловьев В.С. Теория организации социальных систем. Т. 1: Уч. пос. М., 2005.

24. Степанов О.А. Теория государства и права: Курс лекций / Академия генеральной прокуратуры РФ. М., 2016.

25. Степанов О.А., Прохорова Е.Н. О «силовой» составляющей правоохранительной системы, обеспечивающей безопасное осуществление государственного строительства в России // Вестник Академии Генеральной прокуратуры Российской Федерации. 2014. № 6(44).

26. Степанов О.А., Тюрина Е.Н. Безопасность как объект правоотношений в современном обществе // Современное право. 2011. № 10.

27. Трунцевский Ю.В. Вынужденное пособничество террористической организации как обстоятельство, исключающее преступность деяния // Уголовное право: стратегия развития в XXI веке: материалы XV Международной научно-практической конференции. М., 2018. С. 510-513.

28. Чердаков О.И. Формирование правоохранительной системы Советского государства в 1917-1936 гг. Историко-правовое исследование / под ред. А.А. Малько. Саратов, 2001.

29. Шувалов И.И., Хабриева Т.Я., Фэн Цзинжу и др. Киберпространство БРИКС: правовое измерение: монография. М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, 2017. 336 с.

Электронные ресурсы:

17. McConnell K. Best Practice for Bitcoins: Regulatory, legal and financial approaches to virtual currencies in a hesitant, global enviroment // Digital currency. Submission 22. P. 1-65. URL: https://ru.scribd.com/document/350794076/22.

18. Совещание с членами Правительства Российской Федерации. URL: http://kremlin.ru/events/president/news/50401.

19. В Юго-Восточной Азии зафиксировали подозрительные транзакции с биткоином. URL: https://news.mail.ru/economics/32090152.

20. Европол и Интерпол удвоят усилия по борьбе с отмыванием денег через криптовалюты. URL: https://bitnovosti.com/2018/02/01/evropol-i-interpol-udvoyat-usiliya-po-borbe-s-otmyvaniem-deneg-cherez-kriptovalyuty.

21. С.К. Шойгу назвал главные угрозы для России. URL: http://www.mk.ru/politics/2018/04/04/shoygu-nazval-glavnye-ugrozy-dlya-rossii.html.

22. Опубликован сценарий грядущей войны США с Россией. URL: http://www.politonline.ru/interpretation/22887808.html.

23. Токенизация. Принципы функционирования и выбор решения. URL: http:// www.akkamal.kz/info/library/tokenization.

24. Блокчейн и криптовалюты простыми словами. URL: https://golos.io/ru--blokcheijn/@stepanov/blokchein-i-kriptovalyuty-prostymi-slovami

25. Информационные технологии в Генпрокуратуре РФ. URL: http://www.tadviser.ru/index.php.

26. В США набирают популярность камеры видеонаблюдения. URL: https://www.bbc.com/russian/society/2013/04/130429_usa_cctv_surveillance.

27. Невидимое оружие Скотленд-Ярда. Как относятся лондонцы к жизни под прицелом видеокамер. URL: https://www.moscowtorgi.ru/news/ bolshaia_ dvadtcatka/64.

28. В Сан-Франциско запретили технологии распознавания лиц. URL: https://hitech.vesti.ru/article/1207598.

Редактор - М.А. Дмитриева.

Сдано в набор - 06.10.2021. Подписано в печать - 22.10.2021.
Формат 60х90 1/16.
Тираж - 100 экз. Объем - 3,0 усл. п.л. Заказ № 394.

Научно-исследовательское и редакционно-издательское отделение
Калининградского филиала
Санкт-Петербургского университета МВД России.
236006, г. Калининград, ул. Ген. Галицкого, 30.