NB: Административное право и практика администрирования
Правильная ссылка на статью:
Бегеза В.В. — Организация деятельности органов внутренних дел в условиях появления новых вызовов кибербезопасности России // NB: Административное право и практика администрирования. – 2023. – № 2. DOI: 10.7256/2306-9945.2023.2.39962 EDN: ASFTXL URL: https://nbpublish.com/library_read_article.php?id=39962

Организация деятельности органов внутренних дел в условиях появления новых вызовов кибербезопасности России

Бегеза Виталий Васильевич

ORCID: 0000-0002-5201-520X

Старший преподаватель, кафедра Государственного управления и Национальной безопасности, Российская Академия Народного Хозяйства и Государственной Службы при Президенте Российской Федерации

119602, Россия, г. Москва, пр. Вернадского, 84 с 1

89250240000@mail.ru

Статья из рубрики "Полицейское право"

DOI:

10.7256/2306-9945.2023.2.39962

EDN:

ASFTXL

Дата направления статьи в редакцию:

12-03-2023

Дата публикации:

25-03-2023

Аннотация: В статье рассматривается проблема организации и эффективности правоохранительных органов в обеспечении киберпрбезопасности Российской Федерации. На основании анализа нормативно-правовых актов и результативности деятельности правоохранительных органов. Киберпреступность с каждым годом приобретает все большую популярность и тем самым все большее значение ей придается со стороны правоохранительных органов. Статистика ГИАЦ МВД России о состоянии преступности в РФ за январь - октябрь 2022 года показывает, что количество преступлений, которые совершены с использованием информационных технологий, сократилось на 5,6% . Однако, такая статистика подтверждает лишь то, что правоохранительные органы успешно справляются с выполнением превентивной функции, предупреждая и пресекая преступления в сфере информационных технологий. В то же время статистика не говорит о том, что киберпреступления теряют свою актуальность. Они приобретают новый формат, становясь более изощренными в

техническом плане, что, безусловно, требует от правоохранительных органов большей компетенции и профессионализма в этой сфере. В 2022 году в структуре органов внутренних дел действует новое управление – «Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий» как специализированное управление в структуре МВД России. В качестве причин создания Управления законодатель указывает – рост компьютерных атак, дистанционных хищений денежных средств и активное развитие противоправной цифровой индустрии.

Ключевые слова:

киберпреступность, криптовалюта, преступление, мошенничество, программист, правоохранительные органы, информационные технологии, интернет, национальная безопасность, кибербезопасность

Время, в которое мы живем, уникально прежде всего потому, что мы имеем счастливую возможность наблюдать непрерывный процесс появления новых и самых различных технологий. Каждый год ученые, программисты и энтузиасты придумывают и создают революционные технические решения в цифровой среде, некоторые из которых упрощают нам жизнь, другие могут стать серьезной проблемой, поскольку используются для кибермошенничества. Например, кибермошенничество с криптовалютой, создание фишинговых сайтов, создание фальшивых бирж и многое другое[1].

Киберпреступность с каждым годом приобретает все большую популярность и тем самым все большее значение ей придается со стороны правоохранительных органов. Статистика ГИАЦ МВД России о состоянии преступности в РФ за 2022 год показывает, что по сравнению с 2021 годом удельный вес зарегистрированных киберпреступлений вырос лишь на 0,7%, однако МВД России сообщает, что с использованием информационных технологий совершается каждое четвертое преступление[2].

Статистика подтверждает главенствующую роль МВД России в обеспечении кибербезопасности России – большинство киберпреступлений (98,7%) выявляются органами внутренних дел, и лишь 1,3% следственными органами Следственного комитета РФ и органами Федеральной службы безопасности. При этом раскрываемость преступлений, совершенных с использованием IT-технологий, возросла на 4,4% в 2022 году по сравнению с 2021 годом, что говорит о повышении эффективности раскрытия и расследования преступных деяний названной категории.

Статистика ГИАЦ МВД России о состоянии преступности в РФ за январь 2023 года показывает, что показатели киберпреступности выросли на 14,2%[3]. Такая статистика, показывающая негативную тенденцию увеличения киберпреступности, связана с цифровизацией общественных отношений, открытостью и доступностью информации в сети Интернет, в котором к тому же легко оставаться анонимным.

Еще в 2021 году генеральный прокурор России Игорь Краснов отметил, что киберпреступность становится реальной новой угрозой национальной безопасности как в России, так и странах СНГ[4]. Начальник Главного организационно-аналитического управления Генеральной прокуратуры РФ Андрей Некрасов также сообщил о низкой раскрываемости преступлений в сфере информационных технологий, фиксируемой на уровне не более 25%[5].

В системе правоохранительных органов главенствующую роль в борьбе с киберпреступностью занимают органы внутренних дел, что объясняется, во-первых, установленными законом полномочиями. Во-вторых, их главенствующей ролью в качестве органа, уполномоченного обеспечивать национальную безопасность Российской Федерации (далее – РФ). Главенствующая роль органов внутренних дел в обеспечении национальной безопасности неоднократно подчеркивалась в литературе, например: Жаглин А. В.[6], Мазов С.Г.[7].

Стоит пояснить, что кибербезопасность и национальная безопасность соотносятся как часть и целое соответственно, что следует из анализа Стратегии национальной безопасности Российской Федерации 2021 года[8], в которой говорится не напрямую о кибербезопасности, но об информационной безопасности. В Стратегии указано, что обеспечение информационной безопасности является одним из стратегических национальных приоритетов.

В доктрине российского права некоторые авторы также отмечают, что национальная безопасность – это объединённое название разных видов безопасности, в том числе информационной. Так, И.Б. Кардашова указывает, что «безопасность – родовое понятие для всех видов безопасности»[9], а А.А. Прохожев считает необходимым выделение специальных видов национальной безопасности, которые охватывают всю совокупность общественных отношений[10].

Действительно, кибербезопасность является структурным элементом национальной безопасности государства, при том не менее важным, чем другие виды безопасности. С учетом главенствующей роли МВД России в обеспечении кибербезопасности особое внимание должно быть уделено организации деятельности названного органа, что позволить повысить эффективность и оперативность в выявлении, пресечении и раскрытии киберпреступлений.

С сентября 2022 года в структуре органов внутренних дел действует новое управление – «Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий» (далее – Управление)[11] как специализированное управление в структуре МВД России. В качестве причин создания Управления законодатель указывает – рост компьютерных атак, дистанционных хищений денежных средств и активное развитие противоправной цифровой индустрии.

Так, полномочия по борьбе с преступлениями в сфере цифровой индустрии, электронной коммерции, в том числе с преступлениями, посягающими на информационную безопасность РФ, перешли в ведомость Управления. Предупреждение, выявление, пресечение и раскрытие преступлений и иных правонарушений в сфере информационно-коммуникационных технологий, координация этой деятельности в системе МВД России – главные задачи Управления[12].

В декабре 2022 года МВД России утвердило «Положение об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации» (далее – Положение), в котором определило основные задачи, функции, полномочия Управления, а также указало положения об организации и обеспечении деятельности Управления[13].

Положение ограничило полномочия Управления по организации и участию в выявлении, предупреждении, пресечении и раскрытии преступлений, определив их категорию –

тяжкие и особо тяжкие преступления, которые совершены с использованием информационных технологий или в сфере информационных технологий. Так, Управление берет на себя основную нагрузку в борьбе с киберпреступностью, поскольку, как показывает статистика ГИАЦ МВД России, больше половины киберпреступлений (52,1%) относится к категориям тяжких и особо тяжких[14].

С учетом статьи 15 Уголовного кодекса РФ[15] (далее – УК РФ) такими преступлениями являются следующие преступления 28 главы УК РФ: ч. 4 ст. 272; ч. 3 ст. 272; ч. 3-5 ст. 274.1. Примечательно, что появившийся в 2022 году новый состав преступления, предусмотренный статьей 274.2 УК РФ (нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования сети Интернет)[16] не входит в сферу полномочий Управления, поскольку он относятся к категории преступлений небольшой тяжести.

Помимо этого, Управление полномочно расследовать и такие составы преступлений, в которых непосредственным объектом посягательства выступают жизнь, здоровье, половая неприкосновенность, частная жизнь, тайна переписки, собственность, авторские права и другое. Такие преступления должны быть либо связанны с использованием и распространением запрещенной информации в сети Интернет, либо с неправомерным доступом к компьютерной информации и (или) использования вредоносного программного обеспечения.

Так, фактически в полномочия Управления входит расследование любых преступлений, предусмотренных УК РФ, которые прямо или косвенно связаны с обеспечением кибербезопасности РФ. Сказанное заставляет полагать, что Управление как структурное подразделение в системе МВД России играет ключевую роль в обеспечении кибербезопасности РФ, что говорит о необходимости организации эффективного функционирования Управления.

Стоит отметить, что при кажущейся правовой определенности деятельности Управления и появления Положения, все же некоторые вопросы не раскрыты законодателем и до сих пор остаются нерешенными. В частности, вопросы организации взаимодействия Управления с другими органами государственной власти, которые так же специализируются на обеспечении кибербезопасности.

Предполагается, что Управление будет вынуждено взаимодействовать, в частности, с Министерством цифрового развития, связи и массовых коммуникаций РФ (далее – Министерство) и подведомственным Министерству органом – Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор).

В то же время Положение ограничилось лишь указанием на полномочие Управления по взаимодействию с органами государственной власти субъектов РФ, иными государственными и муниципальными органами. Однако с учетом специфики сферы деятельности Управления, представляется необходимым конкретизировать вопросы его коммуникации как минимум с Роскомнадзором, который осуществляет государственный контроль и надзор в сфере информационных технологий.

Роскомнадзор осуществляет свою деятельность в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию, а также осуществляет ограничение доступа к информации в сети Интернет. Сфера деятельности Роскомнадзора

пересекается с деятельностью Управления, которое полномочно расследовать преступления, связанные с нарушением авторских и смежных прав, совершенных по совокупности с неправомерным доступом к компьютерной информации и (или) использованием вредоносного программного обеспечения[17].

При обнаружении информации, распространение которой запрещено на территории РФ, МВД России может во внесудебном порядке обратиться в Роскомнадзор с просьбой ограничить доступ к информационному ресурсу, на котором такая информация размещена[18]. Однако МВД России может принимать решение об ограничении доступа только к той информации, которая касается наркотических, психотропных и других подобных веществ[19]. МВД России также может обращаться в Роскомнадзор для ограничения доступа к «веб-зеркалам» интернет-сайтов, содержащих экстремистские материалы[20].

При этом законодатель не указал на возможность МВД России принимать решения в части иного противоправного контента и информации, распространение которой запрещено на территории РФ. Например, МВД России, и соответственно Управление, не имеют возможности обратиться в Роскомнадзор за ограничением доступа к информационным ресурсам, на которых размещена информация, создающая угрозу причинения вреда жизни, здоровью и имуществу граждан. Хотя организация пресечения распространения такой информации в сети Интернет относится к ведомости Управления[21].

Решение данной проблемы видится в создании нормативного правового акта, который урегулировал бы вопросы взаимодействия Управления с другими органами государственной власти, в частности с Роскомнадзором. Особое значение стоит уделить вопросам организации ограничения доступа к информации в сети Интернет, представив Управлению полномочия по принятию решений в части информации, создающей угрозу причинения вреда жизни, здоровью и имуществу граждан.

Таким образом, в результате изучения темы был получен материал, анализ которого позволил заключить, что в настоящий момент организация деятельности МВД России в части обеспечения кибербезопасности находится на должном уровне. В связи с созданием Управления видится возможным дальнейшая гармонизация законодательных и локальных нормативных актов в сфере обеспечения кибербезопасности РФ.

Кроме того, в результате изучения законодательства было выяснено, что МВД России не имеет возможности принимать решения по ограничению доступа к противоправной информации, за распространением и размещением в сети Интернет которой МВД России не только следит, но и в отношении которой расследует преступления. В связи с этим представляется необходимым детально исследовать порядок взаимодействия МВД России, в частности Управления, с другими органами государственной власти, в частности с Роскомнадзором.

Представляется необходимым позволить Управлению самостоятельно принимать решения в части ограничения доступа к информационным ресурсам в сети Интернет, на которых размещена информация, создающая угрозу причинения вреда жизни, здоровью и имуществу граждан, и которую Управление выявило посредством мониторинга информационных ресурсов на предмет соблюдения законодательства.

Библиография

1. Жаглин А. В. Органы внутренних дел в системе национальной безопасности Россиӣской Федерации: монография / А. В. Жаглин. – Воронеж: Ин-т ИТОУР, 2008. – 224 с.
2. Информатизация и информационная безопасность правоохранительных органов: сб. трудов XXVI Всеросс. науч. конф. (г. Москва, 07.07.2017). – М: Академия управления МВД России, 2017. – 350 с.
3. Кардашова И. Б. МВД России в системе обеспечения национальной безопасности Россиӣской Федерации: монография / И. Б. Кардашова. М.: ВНИИ МВД России, 2006. – 209 с.
4. Прохожев А. А. Теоретико-методологические основы безопасности России / А. А. Прохожев // Безопасность России в XXI веке. – М.: РИЦ ИСПИ РАН, 2006. – С. 129–140.
5. Мазов С.Г. Роль органов внутренних дел в обеспечении национальной безопасности //Труды Академии управления МВД России. 2012. №2 (22). С. 120-122.
6. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ// Собрание законодательства РФ, 1996 г., № 25, Ст. 2954.
7. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»//Собрание законодательства РФ, 31.07.2006, № 31 (часть I), ст. 3448.
8. Федеральный закон от 14.07.2022 № 260-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации»// Собрание законодательства РФ, 18.07.2022, № 29 (часть II), Ст. 5227.
9. Постановление Правительства РФ от 26 октября 2012 г. № 1101 «О единой автоматизированной информационной системе «Единыӣ реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Россиӣской Федерации запрещено»// Собрание законодательства РФ, 29.10.2012, № 44, Ст. 6044.
10. Приказ МВД России от 29.12.2022 № 1110 «Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации»
11. Указ Президента РФ от 30.09.2022 № 688 «О внесении изменений в некоторые акты Президента Российской Федерации»//Собрание законодательства РФ, 03.10.2022, № 40, Ст. 6787.
12. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации»//Собрание законодательства РФ, 2021, № 27 (ч. II). Ст. 5351.
13. В структуре МВД России создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий [Электронный ресурс] URL: https://мвд.рф/news/item/32844180/ (дата обращения: 10.11.2022)
14. Конференция руководителей прокуратур европейских государств на тему «Роль прокуратуры в защите индивидуальных прав и публичного интереса в свете требований Европейской Конвенции по правам человека» (Санкт-Петербург, 6–9 июля 2021 г.) [Электронный ресурс]. – Режим доступа: https://epp.genproc.gov.ru/web/gprf/activity/international-cooperation/rus (дата

обращения: 19.12.2022).
15. В Генпрокуратуре заявили, что киберпреступность стала представлять угрозу нацбезопасности [Электронный ресурс]. – Режим доступа: https://tass.ru/obschestvo/11451173 (дата обращения: 19.12.2022).
16. Кибермошенничество в России: факты, тенденции и анализ [Электронный ресурс]. – Режим доступа: https://crypto.ru/kibermoshennichestvo-v-rossii/ (дата обращения: 19.12.2022).
17. Статистика ГИАЦ МВД России состояния преступности в Российской Федерации за январь-октябрь 2022 года [Электронный ресурс] URL: https://мвд.рф/reports/item/33913311/ (дата обращения: 20.11.2022).

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предмет исследования. Статья "Организация деятельности органов внутренних дел в условиях появления новых вызовов кибербезопасности России" в качестве предмета исследования имеет организационно-правовые основы деятельности специальных подразделений МВД России в сфере киберпреступлений.
Методология исследования. Полагаем, что автором использован исключительно прием описания организационно-правовых основ деятельности специальных подразделений МВД России (скорее одного структурного подразделения - «Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий") в сфере киберпреступлений. Предприняты некоторые попытки проведения анализа, но в конечном счете, автор ограничился обзором разных точек зрения на предмет исследования. Представляется, что методологический аппарат не разработан в данной работе.
Актуальность исследования. В условиях глобальной цифровизации и формирования информационного общества, а также роста числа киберпреступлений, тема этой работы представляется весьма актуальной.
Научная новизна исследования. По причине совершенствования организационно-правовых основ деятельности органов внутренних дел Российской Федерации в условиях появления новых вызовов кибербезопасности тема, выбранная для исследования, недостаточно разработана в российской правовой науке и отличается научной новизной.
Стиль, структура, содержание. Работа носит описательный характер. Автором допускаются терминологические ошибки (например, автор использует "нормативно-правовой акт" вместо "нормативный правовой акт" или "новый состав статьи..." вместо "новый состав преступления, предусмотренный статьей ..." и др.). Автор пишет что: "С сентября 2022 года в структуре органов внутренних дел действует новое управление – «Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий» (далее – Управление)", а в заключительной части делает вывод что: "Кроме того, в результате изучения законодательства было выяснено, что МВД России и Управление соответственно не имеют возможности...", "В связи с этим представляется необходимым детально исследовать порядок взаимодействия МВД России и Управления...". Представляется такие выводы нелогичными, поскольку Управление входит в структуру МВД России. Автором предпринята попытка структурировать свою работу, хотя формально она на части не разделена. Полагаем, что по содержанию работа уже, чем заявленная автором

тема. Поэтому нельзя сказать, что тема раскрыта. Вызывают сомнения приведенные автором статистические данные о сокращении количества преступлений, которые совершены с использованием информационных технологий, на 5,6% (по состоянию на октябрь 2022 г.). Уже есть опубликованная статистика за 2022 год. Так, со ссылкой на официальный сайт МВД России можно отметить: "На 14,2% возросли показатели киберпреступности. Больше зафиксировано фактов сбыта наркотиков с использованием информационно-телекоммуникационных технологий на 85,1%. Сохраняются тенденции роста числа IT-мошенничеств на 12%. При этом снизилось число IT-краж на 13,1%, а также преступлений, связанных с использованием компьютерной техники – на 10,3% и расчетных пластиковых карт – на 7,7%" (https://мвд.рф/reports/item/35396677/).

Библиография. Автором изучено недопустимо мало источником по заявленной теме, отсутствуют в списке библиографии ссылки на публикации последних лет (самая поздняя публикация в списке 2017 год). В ходе написания работы автор не обращался к мнениям таких авторитетных ученых как С.В. Овчинский, А.А. Смирнов, Т.А. Полякова и др., которые занимаются вопросами информационной безопасности, в том числе, проблемами противодействия киберпреступлениям и совершенствования системы правоохранительных органов, обеспечивающих кибербезопасность.

Апелляция к оппонентам. В статье присутствует обзор нескольких мнений (точнее двух) по вопросу соотношения понятий "информационная безопасность" и "кибербезопасность". Непонятна позиция самого автора по этому вопросу.

Выводы, интерес читательской аудитории. Несмотря на актуальность темы, статья "Организация деятельности органов внутренних дел в условиях появления новых вызовов кибербезопасности России" не может быть рекомендована к опубликованию, т.к. не отвечает требованиям, предъявляемым к научным работам.

Результаты процедуры повторного рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться здесь.

РЕЦЕНЗИЯ на статью на тему «Организация деятельности органов внутренних дел в условиях появления новых вызовов кибербезопасности России».

Предмет исследования. Предложенная на рецензирование статья посвящена организации «…деятельности органов внутренних дел в условиях появления новых вызовов кибербезопасности России». Автором выбран особый предмет исследования: предложенные вопросы исследуются с точки зрения конституционного, административного и информационного права, при этом автором отмечено, что «… ученые, программисты и энтузиасты придумывают и создают революционные технические решения в цифровой среде, некоторые из которых упрощают нам жизнь, другие могут стать серьезной проблемой, поскольку используются для кибермошенничества». Изучаются НПА, имеющие отношение к цели исследования. Также изучается и обобщается определенный, не очень большой (4 наименования), объем российской научной литературы по заявленной проблематике, анализ и дискуссия с данными авторами-оппонентами присутствует. Литература более современная имеется в наличии в интернете и СПС. Но автор остановился на периоде 2006 - 2017г.г. При этом автор отмечает: «Киберпреступность с каждым годом приобретает все большую популярность и тем самым все большее значение ей придается со стороны правоохранительных органов».

Методология исследования. Цель исследования определена названием и содержанием работы: «…главенствующую роль в борьбе с киберпреступностью занимают органы

внутренних дел, что объясняется, во-первых, установленными законом полномочиями. Во-вторых, их главенствующей ролью в качестве органа, уполномоченного обеспечивать национальную безопасность Российской Федерации…», «…статистика, показывающая негативную тенденцию увеличения киберпреступности, связана с цифровизацией общественных отношений, открытостью и доступностью информации в сети Интернет, в котором к тому же легко оставаться анонимным». Они могут быть обозначены в качестве рассмотрения и разрешения отдельных проблемных аспектов, связанных с вышеназванными вопросами и использованием определенного опыта. Исходя из поставленных цели и задач, автором выбрана определенная методологическая основа исследования. Автором используется совокупность частнонаучных, специально-юридических методов познания. В частности, методы анализа и синтеза позволили обобщить некоторые подходы к предложенной тематике и повлияли на выводы автора. Наибольшую роль сыграли специально-юридические методы. В частности, автором применялись формально-юридический и сравнительно-правовой методы, которые позволили провести анализ и осуществить толкование норм актов российского законодательства и сопоставить различные документы. В частности, делаются такие выводы: «С учетом главенствующей роли МВД России в обеспечении кибербезопасности особое внимание должно быть уделено организации деятельности названного органа, что позволить повысить эффективность и оперативность в выявлении, пресечении и раскрытии киберпреступлений» и др. Таким образом, выбранная автором методология в полной мере адекватна цели статьи, позволяет изучить многие аспекты темы.

Актуальность заявленной проблематики не вызывает сомнений. Данная тема является важной в России, с правовой точки зрения предлагаемая автором работа может считаться актуальной, а именно он отмечает «…при кажущейся правовой определенности деятельности Управления и появления Положения, все же некоторые вопросы не раскрыты законодателем и до сих пор остаются нерешенными. В частности, вопросы организации взаимодействия Управления с другими органами государственной власти, которые так же специализируются на обеспечении кибербезопасности». И на самом деле здесь должен следовать анализ работ оппонентов, и он следует, но в ограниченном количестве, и автор показывает определенное умение владеть материалом. Тем самым, научные изыскания в предложенной области стоит только приветствовать.

Научная новизна. Научная новизна предложенной статьи не вызывает сомнения. Она выражается в конкретных научных выводах автора. Среди них, например, такой: «Представляется необходимым позволить Управлению самостоятельно принимать решения в части ограничения доступа к информационным ресурсам в сети Интернет, на которых размещена информация, создающая угрозу причинения вреда жизни, здоровью и имуществу граждан, и которую Управление выявило посредством мониторинга информационных ресурсов на предмет соблюдения законодательства». Как видно, указанный и иные «теоретические» выводы могут быть в определенной мере использованы в дальнейших исследованиях. Таким образом, материалы статьи в представленном виде могут иметь некоторый интерес для научного сообщества.

Стиль, структура, содержание. Тематика статьи соответствует специализации журнала «Административное право и практика администрирования», так как посвящена организации «…деятельности органов внутренних дел в условиях появления новых вызовов кибербезопасности России». В статье присутствует аналитика по научным работам оппонентов, поэтому автор отмечает, что уже ставился вопрос, близкий к данной теме и автор использует их материалы, дискутирует с оппонентами. Содержание статьи соответствует названию, так как автор рассмотрел заявленные проблемы, достиг цели своего исследования. Качество представления исследования и его результатов

следует признать доработанным. Из текста статьи прямо следуют предмет, задачи, методология, результаты исследования, научная новизна. Оформление работы соответствует требованиям, предъявляемым к подобного рода работам. Существенные нарушения данных требований не обнаружены, кроме отсутствия современной литературы и описки «относится к ведомости Управления» (наверное «ведению»?).

Библиография не очень полная, содержит публикации в период 2006 - 2017г.г., НПА, к которым автор обращается. Это позволяет автору правильно определить проблемы и поставить их на обсуждение. Следует не очень высоко оценить качество представленной и использованной литературы. Присутствие современной научной литературы показало бы большую обоснованность выводов автора и повлияло бы на выводы автора. Труды приведенных авторов соответствуют теме исследования, обладают определенным признаком достаточности, способствуют раскрытию некоторых аспектов темы.

Апелляция к оппонентам. Автор провел анализ текущего состояния исследуемой проблемы по материалам в основном НПА. Автор описывает некоторые точки зрения оппонентов на проблему, аргументирует более правильную по его мнению позицию, опираясь в некоторых случаях на работы оппонентов, предлагает варианты решения проблем.

Выводы, интерес читательской аудитории. Выводы являются логичными, конкретными «… в результате изучения законодательства было выяснено, что МВД России не имеет возможности принимать решения по ограничению доступа к противоправной информации, за распространением и размещением в сети Интернет которой МВД России не только следит, но и в отношении которой расследует преступления» и др. Статья в данном виде может быть интересна читательской аудитории в плане наличия в ней систематизированных позиций автора применительно к заявленным в статье вопросам.

На основании изложенного, суммируя все положительные и отрицательные стороны статьи «рекомендую опубликовать» с учетом замечаний.