национальной уголовно-правовой политики с целью обеспечения минимизации ущерба от криминального воздействия на область избирательных правоотношений.

2. Криминализация национального избирательного процесса способствует утрате доверия населения страны к формируемым на основе проведенных выборов органам государственной власти и местного самоуправления и, как следствие, нарастанию в обществе элементов социальной аномии и нарушению правопорядка.

3. Фактор противоправного воздействия на избирательные права граждан предопределяет нарастание угроз национальной безопасности государства, сопровождаемой утратой авторитета учреждений власти, а также снижением в государстве уровня демократии и размытием его правовой конструкции.

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) // Собрание законодательства РФ, 04 августа 2014 г. – № 31. – Ст. 4398.
2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства РФ, 17 июня 1996 г. – № 25. – Ст. 2954.
3. Федеральный закон от 12 июня 2002 г. № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» // Собрание законодательства РФ, 17 июня 2002 г. – № 24. – Ст. 2253.
4. Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации до 2020 года» // Собрание законодательства РФ, 04 января 2016 г. – № 1 (часть II). – Ст. 212.
5. Гилинский Я.И. Криминология: теория, история, эмпирическая база, социальный контроль. – СПб: Алеф-Пресс, 2014. – 574 с.
6. Иванов А.А., Шагиева Р.В. Основной вопрос криминологии: взгляд сквозь призму истории // Вестник Московского государственного областного университета. – 2017. – № 4. – С. 139-155.
7. Клейменов М.П. Криминологическое законодательство и криминологическое право в России // Lex Russia. – 2018. – № 2 (135). – С. 148-159.
8. Шестаков Д.А. Криминологическое законодательство и право противодействия преступности // Криминология вчера, сегодня и завтра. – 2013. – № 1 (28). – С. 48-49.

Чимаров С.Ю., Алексеев А.А.

Актуальные вопросы правового регулирования организационной защиты персональных данных сотрудников ОВД в сети «Интернет»

*Санкт-Петербургский университет МВД России
(Россия, Санкт-Петербург)*

doi: 10.18411/lj-05-2020-236

idsp: ljjournal-05-2020-236

Аннотация

В статье представлен анализ области правового регулирования защиты персональных данных сотрудников органов внутренних дел при их обращении к новым технологиям цифрового обмена. Авторы акцентируют внимание на особой значимости демонстрации сотрудниками правил цифровой бдительности, направленной на нейтрализацию новых угроз и вызовов современной киберпреступности.

Ключевые слова: правовое регулирование, персональные данные, органы внутренних дел, цифровой след, цифровая тень, цифровая бдительность, онлайн-коммуникация, киберпреступность, сетевой обмен, угроза безопасности.

Abstract

The article presents an analysis of the area of legal regulation of the protection of personal data of employees of internal affairs bodies when they turn to new digital exchange technologies. The authors emphasize the special importance of employees demonstrating the rules of digital vigilance aimed at neutralizing new threats and challenges of modern cybercrime.

Keywords: legal regulation, personal data, internal affairs agencies, digital footprint, digital shadow, digital vigilance, online communication, cybercrime, network sharing, security risk.

Современная парадигма информационного общества актуализирует область функционирования базового набора прав человека и в первую очередь закреплённое в ст. 34 Конституции РФ право на неприкосновенность частной жизни. Фактор реальной угрозы конституционным правам и свободам граждан в условиях экспоненциального воздействия на личность информационно-коммуникативных технологий и возникновения новых изолированных киберпреступных способов воздействия на человека зафиксирован в тексте Доктрины информационной безопасности, введенной в действие Указом Президента РФ от 5 декабря 2016 г. № 646 [4]. Не менее значимым для эпохи тотальной дигитализации общественных отношений является соблюдение цифровых прав. Указанная разновидность прав впервые была закреплена в марте 2019 г. в ст. 141.1 части первой ГК РФ. Согласно положениям данной статьи, «цифровыми правами признаются названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам» [3]. Специфика служебной деятельности сотрудников органов внутренних дел и особенности их правового статуса предъявляют повышенные требования к анонимизации личности каждого, кто проходит службу в системе МВД России и соблюдению сотрудниками органов внутренних дел канонов цифровой бдительности. Проблема анонимизации личности сотрудника неотделима от проблемы защиты его персональных данных, под которыми понимаются сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность [1]. Исходя из положений ст. 8 Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции», деятельность полиции должна быть открытой для общества. Вместе с тем, отмеченному принципу транспарентности согласно указанной ст. 8 не противоречит действие принципа необходимой защиты государственной и иной охраняемой законом тайны [2]. С учетом особенностей прохождения службы, сотрудники органов внутренних дел наиболее часто могут быть подвержены злоумышленным действиям в виде дискредитации личности, персональных угроз как в их адрес, так и по отношению к их родственникам. Нередко конечной целью психологического давления на сотрудников может стать манипулирование собранными сведениями об их частной жизни в интересах запланированного (желаемого) исхода рассмотрения конкретного дела нарушителя закона. В этой связи сотрудникам следует осознанно подходить к особенностям цифровой противоправной инженерии, формирующей область угроз безопасности, сопровождающихся похищением разноплановой информации. Эффект коммодификации, сопровождающейся стремлением некоторых сотрудников поделиться при сетевом обмене информацией о своей жизни или желанием получить одобрение своей персоны, создает предпосылки для имиджа органов внутренних дел и репутационным потерям для самого сотрудника.

Исходя из отмеченного, в интересах предотвращения утечек конфиденциальной информации и содействия укреплению авторитета органов внутренних дел ГУ МВД России отдельных субъектов РФ введен запрет на передачу служебной и иной некорректной информации по мессенджером и социальным сетям Viber, WhatsApp, Skype, Instagram, Twitter, Facebook, «ВКонтакте» и «Одноклассники», а также на использование для передачи электронных ящиков на Gmail.com, Mail.ru, Rambler.ru. Обязательным условием использования для передачи служебной информации социальных сетей является наличие у соответствующих технических устройств необходимого уровня защиты. Кроме того, любой выход в сетевое пространство

должен осуществляться исключительно со специальных сертифицированных устройств, с использованием паролей и аккаунтов ведомственной сети.

Идеология и общие контуры формата онлайн-обмена с участием сотрудников органов внутренних дел в сети «Интернет» определены в Приказе МВД России от 16 июня 2011 г. № 683 [5] и ряде иных ведомственных приказов. В соответствии с отмеченным Приказом, в системе МВД России общая координация взаимодействия с институтами гражданского общества и СМИ возложена на Управление общественных связей МВД России (далее-УОС МВД России). Проводя круглосуточный мониторинг и анализ материалов СМИ, информационно-коммуникационной сети «Интернет» о деятельности органов, организаций, подразделений системы МВД России и их должностных лиц, УОС МВД России выявляет, оценивает и прогнозирует угрозы информационному обеспечению государственной политики РФ в сфере внутренних дел, а также готовит предложения по противодействию этим угрозам. Аналитическая работа УОС МВД России составляет основу разрабатываемых учебных программ и рабочих учебных планов для подготовки и повышения квалификации сотрудников пресс-служб, подразделений информации и общественных связей по специализациям соответствующей направленности. Строгая регламентация системы сетевого обмена служащих полиции подтверждается на примере зарубежного опыта. В частности служащие полиции территориальной полиции Уилтшира (англ. «Wiltshire Police»), отвечающей за охрану правопорядка в округе Уилтшир на юго-западе Англии обязаны соблюдать правило семи «П» (англ. «Р»), напоминающее особенности онлайн-коммуникации и предостерегающее о наличии возможных опасностей свободного выхода в сеть «Интернет»: 1. Цель (англ. «Purpose»); 2. Профессионализм (англ. «Professionalism»); 3. Производительность (англ. «Productivity»); 4. Упреждение (англ. «Proactive»); 5. Личная ответственность (англ. «Personal Responsibility»); 6. Оформление (англ. «Preparation»); 7. Конфиденциальность (англ. «Privacy») [8, с. 4].

С учетом изложенного следует согласиться с позицией П.У. Кузнецова, считающего что существующие к настоящему времени сущностные классические юридические концепты общего выступают в качестве характера чрезвычайно устаревшего правового инструмента, не способного адекватному разрешению возникающих вызовов и угроз информационной действительности для различных субъектов онлайн-коммуникации [6, с. 39-40]. Отмеченное в полной мере относится и к указанным выше нормативно-правовым актам, которыми сотрудники органов внутренних дел руководствуются при своем обращении к сети «Интернет». Представляется, что данное обстоятельство послужило причиной издания Методических рекомендаций МВД России от 13 марта 2020 г. № 1/2704, в которых уточнены современные угрозы безопасности персональным данным сотрудникам органов внутренних дел и их близким, а также сформулированы способы противодействия отмеченным угрозам [7]. Уточняя определение терминов «цифровой след» (данные, самостоятельно передаваемые субъектом в цифровую среду) и «цифровая тень» (информация, создаваемая о людях автоматически посредством деятельности и устройств третьих лиц), Методические рекомендации МВД России способствуют оптимизации модели цифрового присутствия сотрудников органов внутренних дел в сетевом пространстве, правила безопасности для которого также важны, наряду с их соблюдением соответствующих правил для обычной (нецифровой среды). Конечный результат каждого выхода сотрудника в сеть «Интернет» и сообщения участникам онлайн-обмена своих цифровых следов должен обеспечивать минимизацию оставления сотрудником цифровых теней.

Резюмируя изложенное, следует заметить следующее: во-первых, фактор участия сотрудников органов внутренних дел в процессе сетевого обмена корреспондирует осознанию ими особой значимости демонстрации заповедей цифровой бдительности; во-вторых, неосмотрительное пользование сотрудниками

потенциалом сети «Интернет» подрывает имидж системы МВД России и наносит ущерб репутации сотрудникам; в-третьих, адекватность реагирования на угрозы и вызовы внедрения в практику современной коммуникации новых технологий предопределяется своевременным применением соответствующих норм правового регулирования области защиты персональных данных сотрудников органов внутренних дел.

1. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Собрание законодательства РФ, 10 марта 1997 г. – № 10. – Ст. 1127.
2. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» // Собрание законодательства РФ, 14 февраля 2011 г. – № 7. – Ст. 900.
3. Федеральный закон от 18 марта 2019 г. № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» // Собрание законодательства РФ, 25 марта 2019 г. – № 12. – Ст. 1224.
4. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 // Собрание законодательства РФ, 12 декабря 2016 г. – № 55. – Ст. 7074.
5. Приказ МВД России от 16 июня 2011 г. № 683 «Об утверждении Положения об Управлении по взаимодействию с институтами гражданского общества и средствами массовой информации Министерства внутренних дел Российской Федерации» // СПС КонсультантПлюс
6. Кузнецов П.У. 2012. Административная реформа в контексте формирования электронного правительства: терминологические проблемы // Российский юридический журнал. – 2012. – № 3. – С. 37-47.
7. Методические рекомендации МВД России от 13 марта 2020 г. № 1/2704 «О правилах поведения и организованной защите персональных данных сотрудников органов внутренних дел Российской Федерации и их близких в сети «Интернет» (документ официально не опубликован)
8. Social Media Guidance. A guide for police officers and police staff. January 2014. – 24 p. [Электронный ресурс]. – Режим доступа: <http://istmat.info/node/27762> (дата обращения: 12.04.2020)

Шелкоплясова Н.И., Конивец А.Д.

Защита авторских прав в сети Интернет

*Финансовый университет при Правительстве Российской Федерации
(Россия, Тула)*

doi: 10.18411/lj-05-2020-237

ids: lj-05-2020-237

Аннотация

В статье рассмотрена проблема авторского права в сети Интернет. Также были описаны способы защиты продукта интеллектуального труда. Приведена статистика интернет пользователей по всему миру, а также статистика стран, где посещение пиратских сайтов больше всего.

Ключевые слова: авторское право, права на интеллектуальную собственность, защита авторских прав в сети Интернет, способы защиты авторского права.

Abstract

The article considers the problem of copyright on the Internet. Ways to protect the product of intellectual work have also been described. The statistics of Internet users around the world and statistics of countries where visiting pirated sites the most.

Keywords: copyright, intellectual property rights, copyright protection on the Internet, ways to protect copyright.

На сегодняшний день Интернет является неотъемлемой частью нашей жизни. Благодаря ему мы можем найти любую, необходимую нам информацию, общаться с