

В. Г. Романовский

ассистент

кафедры уголовного права

Пензенский государственный университет, г. Пенза, Российская Федерация

ПРАВА ЧЕЛОВЕКА, «ГЛОБАЛЬНАЯ СЛЕЖКА» И ПРОТИВОДЕЙСТВИЕ ТЕРРОРИЗМУ¹

Аннотация. В статье рассматривается влияние информационных технологий на систему противодействия терроризму. Анализируются особенности американской модели «глобальной слежки», введенной Патриотическим актом в ответ на террористические атаки 11 сентября 2001 г. Следствием вступления в силу данного документа стало внедрение программы «Carnivore», вскрывающей и анализирующей информацию с интернет-страниц и серверов электронной почты. Данная программа осуществляет систематизацию вскрытой информации по определенным критериям с ее архивированием и хранением на жестких дисках. Данные не уничтожаются и могут быть извлечены по мере необходимости. Подобные цифровые технологии покушаются на традиционную модель защиты прав человека, предполагающую ограничения только в отношении конкретного человека при наличии конкретных оснований подозревать в совершении противоправных действий.

Ключевые слова: права человека, терроризм, цифровые технологии, противодействие, ограничения.

V. G. Romanovsky

Assistant

Department of Criminal Law

Penza State University, Penza, the Russian Federation

HUMAN RIGHTS, «GLOBAL SURVEILLANCE» AND COUNTERING TERRORISM

Abstract. The article discusses the impact of information technology on the system of countering terrorism. The features of the “global surveillance” model introduced by the Patriot Act in response to the terrorist attacks of September 11, 2001 are analyzed. The effect of the entry into force of this document was the introduction of the Carnivore program, which reveals and analyzes information from web pages and email servers. This program systematizes the opened information according to certain criteria with its archiving and storage on hard disks. Data is not deleted and can be retrieved as needed. Such digital technologies encroach on the traditional model of human rights protection, which implies restrictions only in relation to a specific person if there are specific grounds for suspecting to commit illegal acts.

Key words: human rights, terrorism, digital technologies, counteraction, restrictions.

Распространение информационных технологий выстраивает новую реальность, когда человек становится зависимым от технических средств, призванных облегчить его жизнь. Почти каждый россиянин, владея современным смартфоном, постоянно общаясь в различных мессенджерах, не догадывается, что тем самым он вносит информацию в цифровое пространство. Сведения могут быть зафиксированы, а значит, могут накапливаться, храниться, систематизироваться и распространяться. В связи с этим у многих государственных органов (и не только у них) появляется желание получить доступ к личной информации. Цели ознакомления

¹ Публикация подготовлена в рамках поддержанного РФФИ научного проекта № 17-03-00071-ОГОН.

могут быть различными: от правоохранительных до сугубо меркантильных (например, банковские организации тем самым могут получить доступ к информации, влияющей на оценку платежеспособности заемщика).

В рамках заявленной темы укажем, что противодействие терроризму в современном мире благодаря цифровым технологиям, с одной стороны, имеет некоторые преимущества (фиксация большинства действий человека в цифровом пространстве, вплоть до геопозиции), с другой – наталкивается на новые трудности. Благодаря распространению телефонов и появлению мессенджеров с надежной кодировкой граждане, готовящие совершение преступления, получили возможности постоянного общения при сохранении содержания разговоров в тайне.

Первым нормативным актом, поставившим перед собой цель разрушить «стены» цифрового общения, стал Акт о патриотизме, принятый в США в 2001 г. после известной атаки на Всемирный торговый центр 11 сентября. К этому времени ФБР осознало необходимость осуществления разведывательных действий в киберпространстве. Последним аргументом стал тот факт, что террористы, направившие самолеты на гражданские объекты, вели переговоры с помощью мессенджеров [18].

К 2001 г. в США была разработана программа глобальной слежки с помощью автоматической системы шпионажа «Carnivore» (переводится как «Хищник»), вскрывающей и анализирующей информацию с интернет-страниц и серверов электронной почты. По сути данная программа осуществляет систематизацию вскрытой информации по определенным критериям с ее архивированием и хранением на жестких дисках. Данные не уничтожаются и могут быть извлечены по мере необходимости: «Пакеты могут выбираться на основании IP-адреса или, в случае электронной почты, по имени пользователя в полях TO и FROM, а в отдельных случаях – на основании их содержания. Перехваченные пакеты могут быть зарегистрированы полностью (полнотекстовый режим). Регистрация также может ограничиться только адресной частью (режим по ключевым словам), включающей IP-адрес и имя пользователя» [15]. Кстати, существуют и иные аналогичные программы: Omnivore и Etherpeek.

Подобные программы есть и в европейских странах, и в Российской Федерации. В нашей стране автоматическая система имеет сокращенное название СОРМ [16]. Правила (ч. I) применения оборудования систем коммутации, включая программное обеспечение, обеспечивающие выполнение установленных действий при проведении оперативно-розыскных мероприятий, утверждены Приказом Минкомсвязи России от 12 декабря 2016 г. № 645. Часть II утверждена Приказом Минкомсвязи России от 19 ноября 2012 г. № 268, ч. III – Приказом Минкомсвязи России от 16 апреля 2014 г. № 83, а ч. IV – Приказом Минкомсвязи России от 26 февраля 2018 г. № 86.

Постановлением Правительства РФ от 27 августа 2005 г. № 538 утверждены Правила взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность. Совместным Приказом Минкомсвязи России № 391, ФСБ России № 437 от 1 августа 2017 г. утверждены также Типовые Требования к плану мероприятий по внедрению технических средств для проведения оперативно-розыскных мероприятий. Правительственные Правила закрепляют обязательность соблюдения определенных технических параметров ввода в эксплуатацию технических средств в сети связи оператора связи. В соответствии с поправками в ряд федеральных законов, обозначенными средствами массовой информации как «пакет Яровой» (Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»; Федеральный закон от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и

Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»), операторы связи обязаны хранить информацию, полученную в процессе электронного общения.

Благодаря принудительной установке указанных программы изменяется концепция ограничений права на неприкосновенность частной жизни, на что указывают как российские, так и зарубежные ученые. Изначально развитие законодательства, предусматривающего скрытое наблюдение за человеком, выстраивалось на основе введения специальных формальных требований к санкциям, которая выдается правоохранительным органам. В течение нескольких десятилетий американская модель оттачивала, какие именно сведения должны указываться в ордере, чтобы не допустить нарушение конституционных прав. Так, например, определялась цель получаемой информации, что означало недопустимость прослушивания разговоров, не имеющих прямого отношения к расследованию.

Борьба с терроризмом показала, что ее эффективность зависит от глубины отслеживания всех потенциальных связей лиц, подозреваемых в причастности к террористической деятельности. Это означает, что при осуществлении электронного наблюдения нельзя достоверно определить, кто именно может вступать в подозрительные контакты, какие преступления планируются при осуществлении разговоров. Кроме того, сама формулировка – причастность к террористической организации – не отвечала критериям точности, ясности. С другой стороны, построение террористических организаций на основе сетевого общения не позволяло эффективно использовать старую модель, когда есть потребность в раскрытии конкретного преступления [14].

Американская программа «Carnivore» автоматически архивирует электронные данные всех проводимых коммуникаций. Иными словами, все электронные сообщения всех граждан сохраняются и могут в последующем быть истребованными (технология «невода» [17, с. 39]). Возможности осуществления контроля (как судебного, так и общественного) сужаются значительным образом: факт истребования информации (тем более скрытая манипуляция) отследить невозможно. При этом подобная система архивирования всей информации позволяет спецслужбам вести разведывательную оперативную деятельность по выявлению террористических угроз [19]. Ради справедливости следует отметить, что заявляемые столь всеобъемлющие возможности подобных программ вызывают у многих специалистов серьезный скепсис [11].

Время идет – технологии меняются. В настоящее время спецслужбами (российскими и зарубежными) активно используется хакерская атака сайтов, посещаемых потенциальными террористами для внедрения вирусных программ, которые, в свою очередь, распространяются на компьютеры посетителей сайтов. При внедрении вирусной программы (по типу «троянской») информация с компьютера отправляется на сервер спецслужб [12]. По такой же схеме возможна слежка за гражданином через электронное устройство (ноутбук, компьютер, телефон), оборудованное видеокамерой (в связи с этим и выпускаются рекомендации о заклеивке камер на ноутбуках). Подобные схемы не урегулированы законодательным образом в большинстве стран мира, поскольку их судебное санкционирование достаточно сложно описать [1, с. 29]. Сама операция больше похожа на провокацию и способствует совершению злоупотреблений. Кстати, в ноябре 2015 г. были преданы гласности факты использования данных технологий шотландской полицией для осуществления скрытого сбора информации о СМИ и их поставщиках конфиденциальной информации [2].

На возможность злоупотреблений наталкивает и та основа, которая подается при введении ограничений. Многими исследователями отмечается, что террор как раз служит благодатной причиной введения специальных ограничений [8, с. 449]. Э. Гросс указывает: «Когда, с одной стороны, мы являемся свидетелями конкретных

злодеяний, сцен улиц и торговых центров, превращенных в арены смерти, а с другой стороны, мы сталкиваемся с абстрактным правом (автор пишет о праве на неприкосновенность частной жизни – прим. В.Р.), наша интуиция однозначно меняет баланс в пользу национальной безопасности» [6, с. 36]. Одновременно автор задает справедливые вопросы: «Как мы можем поймать террориста, несущего взрывной пояс, без просвечивания тел всех пассажиров в самолете? Как мы можем раскрыть террористическую ячейку, члены которой общаются с помощью электронных средств коммуникации, не раскрывая содержания своих сообщений и в то же время сканируя сообщения миллионов людей? И как мы должны идентифицировать террористов, собирающих разведданные о процедурах безопасности на туристической площадке или в торговом центре, не устанавливая камеры наблюдения, которые снимают не только подозрительные действия, но и действия невинных людей?» [6, с. 36].

Д. Коми, будучи Директором ФБР, в своем официальном заявлении в 2016 г. указывал: «Благодаря широкому распространению социальных сетей террористы могут выявлять, оценивать, вербовать и радикализировать уязвимых лиц всех возрастов в Соединенных Штатах. Благодаря этому совершаются поездки для осуществления нападений на нашу Родину. В результате иностранные террористические организации теперь имеют прямой доступ в Соединенные Штаты, как никогда раньше. Преступные коммуникации происходят на общедоступных сайтах социальных сетей, некоторые из них – через частные платформы обмена сообщениями. Эти зашифрованные платформы прямого обмена сообщениями чрезвычайно проблематичны для нас при их использовании террористами» [4].

Осуществление тотального контроля проникает во все сферы жизни, чему способствуют технические достижения: установка сканеров личных вещей и одежды человека; размещение открытых видеокамер и скрытого наблюдения в общественных местах; личный досмотр при посещении публичных мероприятий. Человек все больше ощущает постоянный контроль в своей повседневной жизни. Возникает порочный круг. С одной стороны, каждый гражданин постоянно сталкивается с постоянным вторжением в свою частную жизнь, с другой – государственные органы все больше настаивают на расширении своих полномочий. Снижается общий объем конфиденциальности информации, это приводит к понижению требований к самому режиму конфиденциальности и защиты персональной информации: «Такая нисходящая спираль может затронуть само чувство самоидентичности, которое есть у людей – чувство пространства для самовыражения и экспериментов, чувство достоинства и самообладания, чувство легкости и полета при публичном представлении» [5].

Американские конституционалисты выделяют еще одну проблему при осуществлении «глобальной слежки» в целях противодействия терроризму. Необходимость выявления террористов обуславливает их типизацию. В связи с этим формулирование признаков, которые отвечают выработанным критериям, приводит к тому, что спецслужбы занимаются не поиском террористов, а поиском граждан, которые отвечают выявленным признакам [13]. Р. Хардин проводит аналогию с практикой выявления рака: граждане США сдают некоторые тестовые анализы. При получении положительного результата происходит дальнейшая работа с пациентом. На этом построена система массовой диспансеризации. Точно так же при осуществлении тотального контроля можно выявить потенциальных террористов, которых можно в дальнейшем отслеживать и привлекать к ответственности, в случае выявления признаков преступного поведения. Р. Хардин выделяет два критерия, которые несут в себе риски: членство в экстремистской группе и «арабское или исламское происхождение». Первый признак напоминает «охоту на ведьм» времен «маккартизма», когда сам факт принадлежности к коммунистической организации являлся основой для дискриминации гражданина. Второй признак реанимирует «темные призраки» дискриминационного законодательства США в

отношении афроамериканцев. Р. Хардин приводит еще одну аналогию – с расследованием убийств: «Пул возможных подозреваемых при расследовании убийств обычно намного меньше, чем пул потенциальных террористов, прежде чем они совершат нападение. Тем не менее, уровень ложных срабатываний при аресте и даже при осуждении предполагаемых убийц, по-видимому, очень высок» [7, с. 82]. Нечто подобное будет наблюдаться и при преследовании потенциальных террористов [9, с. 327]. Установление тотального контроля за частной жизнью граждан обуславливает обвинение в том, что государство подозревает каждого человека в преступной деятельности. Данный тезис выдвигался и при критике «пакета Яровой», предопределяющего виновность каждого гражданина, поскольку предусматривается хранение информации о частной жизни гражданина против его воли и вне связанных подозрений в преступной деятельности. Однако в США придерживаются концепции «разумного ожидания конфиденциальности», разработанной Р. Макатуром, указавшим на знание каждого пользователя Интернета о возможности отслеживания переданной во Всемирной паутине информации [10, с. 124]. Данная концепция имеет значительное число сторонников, придерживающихся этатистских взглядов [3, с. 21]. Благодаря ей сторонники «глобальной слежки» указывают на необходимость всеобщего контроля, обусловленного желанием каждого чувствовать себя в безопасности.

Таким образом, технические возможности позволяют спецслужбам осуществлять всесторонний контроль за многими сторонами частной жизни человека. Этому способствует использование каждым из нас различных гаджетов и телефонов, совмещающих в себе многочисленные функции отслеживания любого внешнего действия (звонок, отправка сообщения, перемещение в пространстве и т.д.). «Глобальная слежка», как это часто формулируется в зарубежной юридической печати, с одной стороны, имеет своих сторонников, указывающих на усиление террористических угроз, с другой – противников, обращающих внимание на разрушение традиционной концепции прав человека. По-видимому, необходим поиск «золотой середины», позволяющей осуществлять эффективную борьбу с различными угрозами безопасности личности, обществу, государству, и при этом исключающей излишнее вторжение в область личной свободы, не позволяющей необоснованные ограничения прав человека.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Безрукова О.В. Терроризм и современное право: актуальные вопросы противодействия: монография / О.В. Безрукова, Е.А. Капитонова, Г.П. Кулешова, Н.А. Подольный, О.В. Романовская, В.Г. Романовский, Г.Б. Романовский, Е.В. Ширманов. — М. : Проспект, 2018. — 176 с.
2. Безрукова О.В. и др. Терроризм, права человека и демократические ценности в России и за рубежом / О.В. Безрукова, М.В. Демидов, Е.А. Капитонова, Г.П. Кулешова, Н.А. Подольный, О.В. Романовская, В.Г. Романовский, Г.Б. Романовский, Д.М. Торкунов, М.А. Торкунов. — М. : Юрлитинформ, 2019. — 232 с.
3. Власихин В.А. «Патриотический акт»: юридический анализ / В.А. Власихин // Сайт Agentura.Ru [Электронный ресурс]. — Режим доступа: <http://www.agentura.ru/dossier/usa/zakon-antiterror/> (дата обращения: 28.04.2019).
4. Гольдштейн Б.С. Законный перехват сообщений: подходы ETSI, CALEA и COPM / Б.С. Гольдштейн, В.С. Елагин // Вестник связи. — 2007. — № 3. — С. 66–72.
5. Каримов В.Х. Возможности реализации государством комплекса мер по предотвращению террористических угроз // Российский следователь. — 2016. — № 16. — С. 38–41.
6. Романовская О.В. Акт о патриотизме: ограничения права на неприкосновенность частной жизни в США в целях противодействия терроризму / О.В. Романовская // Электронный научный журнал «Наука. Общество. Государство». — 2017. — Т. 5, № 2. — С. 10–16 [Электронный ресурс]. — Режим доступа: https://esj.pnzgu.ru/files/esj.pnzgu.ru/romanovskaya_ov_17_2_02.pdf (дата обращения: 11.04.2019).

7. Романовская О.В. Акт о свободе: ограничения прав человека в США в целях противодействия терроризму / О.В. Романовская // Электронный научный журнал «Наука. Общество. Государство». — 2017 — Т. 5. № 3. — С. 65–71 [Электронный ресурс]. — Режим доступа: https://esj.pnzgu.ru/files/esj.pnzgu.ru/romanovskaya_ov_17_3_10.pdf/(дата обращения: 14.04.2019).

8. Anyanwu Ch. Fear of communicating fear versus fear of terrorism: A human rights violation or a sign of our time? [Electronic resource] / Ch. Anyanwu // International Journal of Speech-Language Pathology — 2018. — Vol. 20. — no. 1. — P. 26–33. Mode of access: <https://www.tandfonline.com/doi/citedby/10.1080/17549507.2018.1419281?scroll=top&needAccess=true> (accessed 14.04.2019).

9. Brooks L. Police Scotland criticised for breaching law to spy on journalists' sources [Electronic resource] / L. Brooks // The Guardian — 2015, 25 Nov. Mode of access: <https://www.theguardian.com/uk-news/2015/nov/25/police-scotland-criticised-for-breaching-law-to-spy-on-journalists-sources> (accessed 14.04.2019).

10. Coleman S. E-mail, terrorism, and the right to privacy [Electronic resource] / S. Coleman // Ethics and Information Technology — 2006. — Vol. 8. — no. 1. — P. 17–27. Mode of access: <https://link.springer.com/article/10.1007%2Fs10676-006-9103-5> (accessed 14.04.2019).

11. Comey James B. Encryption Tightrope: Balancing Americans' Security and Privacy / B. Comey James // [Electronic resource] — Mode of access: <https://www.fbi.gov/news/testimony/encryption-tightrope-balancing-americans-security-and-privacy> (accessed 14.04.2019).

12. Galison P. Minow M.; Wilson R. A.(ed.) Our Privacy, Ourselves in the Age of Technological Intrusions. Human Rights in the «War on Terror». [Electronic resource] / P. Galison, M. Minow // Cambridge, Cambridge University Press 2001. — 347 p. Mode of access: <https://www.cambridge.org/core/books/human-rights-in-the-war-on-terror/36ED22AC0F1CFBBD8CF5CF05CB8B8E5> (accessed 14.04.2019).

13. Gross E. The Struggle of a Democracy against Terrorism – Protection of Human Rights: The Right to Privacy versus the National Interest – the Proper Balance / E. Gross // Cornell International Law Journal. — 2004. — Vol. 37. — no. 1. — Article 2. — P. 36.

14. Hardin R. Civil Liberties in the Era of mass Terrorism [Electronic resource] / R. Hardin // The Journal of Ethics. — 2004. — no. 8. — P. 77–95. Mode of access: <http://www.nyu.edu/gsas/dept/politics/faculty/hardin/research/CivLiberties.pdf> (accessed 14.04.2019).

15. Heymann P. Civil Liberties and Human Rights in the Aftermath of September 11 [Electronic resource] / P. Heymann // Harvard Journal of Law and Public Policy. — 2002. — Vol. 25. — no. 2. — P. 441–456. Mode of access: <http://www.harvard-jlpp.com/vols-25-29/#253> (accessed 14.04.2019).

16. Kam C. D., Kinder, D. R. Terror and ethnocentrism: Foundations of American support for the war on terrorism [Electronic resource] / C.D. Kam, D.R. Kinder // The Journal of Politics. — 2007. — Vol. 69. — no. 2. — P. 320–338. Mode of access: <http://pscourses.ucsd.edu/ps100da/Kam%20and%20Kinder%20Terror%20and%20Ethnocentrism.pdf> (accessed 14.04.2019).

17. McArthur R. L. Reasonable Expectations of Privacy [Electronic resource] / R. L. McArthur // Ethics and Information Technology. — 2001. — Vol. 3. — no. 2. P. 123–128. Mode of access: <https://link.springer.com/article/10.1023%2FA%3A1011898010298> (accessed 14.04.2019).

18. Poulsen K. FBI retires Carnivore. Looks to commercial surveillance tools / K. Poulsen // [Electronic resource] — Mode of access: https://www.theregister.co.uk/2005/01/15/fbi_retires_carnivore/ (accessed 14.04.2019)

19. Zetter K. Everything we know about how the FBI Hacks People / K. Zetter // [Electronic resource] — Mode of access: <https://www.wired.com/2016/05/history-fbis-hacking/> (accessed 14.04.2019).

REFERENCES

1. Bezrukova O. V., Kapitonova E. A., Kuleshova G. P., Podol'nyi N. A., Romanovskaia O. V., Romanovskii V. G., Romanovskii G. B., Shirmanov E. V. *Terrorizm i sovremennoe pravo: aktual'nye voprosy protivodei-stviia: monografiia* [Terrorism and modern law: topical counteraction issues: monograph]. Moscow, Prospekt Publ., 2018, 176 p.

2. Bezrukova O. V., Demidov M. V., Kapitonova E. A., Kuleshova G. P., Podol'nyi N. A., Romanovskaia O. V., Romanovskii V. G., Romanovskii G. B., Torkunov D. M., Torkunov M. A. *Terrorizm, prava cheloveka i demokraticheskie tsennosti v Rossii i za rubezhom* [Terrorism, human rights and democratic values in Russia and abroad]. Moscow, Iurlitinform Publ., 2019, 232 p.
3. Vlasikhin V. A. «Patrioticheskiy akt»: iuridicheskii analiz («Patriotic Act»: Legal Analysis). Available at: <http://www.agentura.ru/dossier/usa/zakon-antiterror/> (accessed 28.04.2019).
4. Gol'dshtein B. S., Elagin V. S. Zakonnyi perekhvat soobshchenii: podkhody ETSI, CALEA i SORM (Legitimate message interception: ETSI, CALEA and SORM approaches). *Vestnik svyazi = Journal of Connection*, 2007, no. 3, pp. 66-72 (in Russian).
5. Karimov V. Kh. Possibilities of implementation by the state of a set of measures for protection from terrorist threats. *Rossiiskii sledovatel' = Russian Investigator*, 2016, no. 16, pp 38-41 (in Russian).
6. Romanovskaya O. V. The patriot act: restrictions on the right to privacy in the US in order to counter terrorism. *Elektronnyi nauchnyi zhurnal «Nauka. Obshchestvo. Gosudarstvo» = Electronic scientific journal «Science. Society. State»*, 2017, vol. 5, no. 2, pp. 10-16 (in Russian). Available at: https://esj.pnzgu.ru/files/esj.pnzgu.ru/romanovskaya_ov_17_2_02.pdf (accessed 15.04.2019).
7. Romanovskaya O. V. The Freedom Act: restrictions of human rights in the US for countering terrorism. *Elektronnyi nauchnyi zhurnal «Nauka. Obshchestvo. Gosudarstvo» = Electronic scientific journal «Science. Society. State»*, 2017, vol. 5, no. 3, pp. 65-71 (in Russian). Available at: https://esj.pnzgu.ru/files/esj.pnzgu.ru/romanovskaya_ov_17_3_10.pdf (accessed 18.04.2019).
8. Anyanwu Ch. Fear of communicating fear versus fear of terrorism: A human rights violation or a sign of our time? *International Journal of Speech-Language Pathology*, 2018, vol. 20, no. 1, p. 26-33. Available at: <https://www.tandfonline.com/doi/citedby/10.1080/17549507.2018.1419281?scroll=top&needAccess=true> (accessed 14.04.2019).
9. Brooks L. Police Scotland criticised for breaching law to spy on journalists' sources. *The Guardian*, 2015, 25 Nov. Available at: <https://www.theguardian.com/uk-news/2015/nov/25/police-scotland-criticised-for-breaching-law-to-spy-on-journalists-sources> (accessed 14.04.2019).
10. Coleman S. E-mail, terrorism, and the right to privacy. *Ethics and Information Technology*, 2006, vol.8, no. 1, p. 17-27. Available at: <https://link.springer.com/article/10.1007%2Fs10676-006-9103-5> (accessed 14.04.2019).
11. Comey James B. *Encryption Tightrope: Balancing Americans' Security and Privacy*. Available at: <https://www.fbi.gov/news/testimony/encryption-tightrope-balancing-americans-security-and-privacy> (accessed 14.04.2019).
12. Galison P. Minow M.; Wilson R.A.(ed.) *Our Privacy, Ourselves in the Age of Technological Intrusions. Human Rights in the «War on Terror»*. Cambridge, Cambridge University Press, 2001, 347 p. Available at: <https://www.cambridge.org/core/books/human-rights-in-the-war-on-terror/36ED22AC0F1CFBBD8CF5CF05CB8B8E5> (accessed 14.04.2019).
13. Gross E. The Struggle of a Democracy against Terrorism – Protection of Human Rights: The Right to Privacy versus the National Interest – the Proper Balance. *Cornell International Law*, 2004, vol. 37, no. 1, Art. 2, p. 36.
14. Hardin R. Civil Liberties in the Era of mass Terrorism. *The Journal of Ethics*, 2004, no. 8, p. 77-95. Available at: <http://www.nyu.edu/gsas/dept/politics/faculty/hardin/research/CivLiberties.pdf> (accessed 14.04.2019).
15. Heymann P. Civil Liberties and Human Rights in the Aftermath of September 11. *Harvard Journal of Law and Public Policy*, 2002, vol. 25, no. 2, p. 441-456. Available at: <http://www.harvard-jlpp.com/vols-25-29/#253> (accessed 14.04.2019).
16. Kam C. D., Kinder, D. R. Terror and ethnocentrism: Foundations of American support for the war on terrorism. *The Journal of Politics*, 2007, vol. 69, no. 2, p. 320-338. Available at: <http://pscourses.ucsd.edu/ps100da/Kam%20and%20Kinder%20Terror%20and%20Ethnocentrism.pdf> (accessed 14.04.2019).
17. McArthur R. L. Reasonable Expectations of Privacy. *Ethics and Information Technology*, 2001, vol. 3, no. 2, p. 123-128. Available at: <https://link.springer.com/article/10.1023%2FA%3A1011898010298> (accessed 14.04.2019).
18. Poulsen K. *FBI retires Carnivore. Looks to commercial surveillance tools*. Available at: https://www.theregister.co.uk/2005/01/15/fbi_retires_carnivore/ (accessed 14.04.2019).

19. Zetter K. *Everything we know about how the FBI Hacks People*. Available at: <https://www.wired.com/2016/05/history-fbis-hacking/> (accessed 14.04.2019).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Романовский Владислав Георгиевич — ассистент, кафедра уголовного права, Пензенский государственный университет, 440026, г. Пенза, ул. Красная 40, Российская Федерация, e-mail: up406@mail.ru.

AUTHOR

Romanovsky Vladislav Georgievich — Assistant, department of Criminal Law, Penza State University, 40 Krasnaya Street, Penza, 440026, the Russian Federation, e-mail: up406@mail.ru.

БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ СТАТЬИ

Романовский В.Г. Права человека, «глобальная слежка» и противодействие терроризму / В.Г. Романовский // Электронный научный журнал «Наука. Общество. Государство». — 2019. — Т. 7, № 2 [Электронный ресурс]. — Режим доступа: <http://esj.pnzgu.ru>.

BIBLIOGRAPHIC DESCRIPTION

Romanovsky V. G. Human rights, «global surveillance» and countering terrorism. *Electronic scientific journal «Science. Society. State»*, 2019, vol. 7, no. 2, available at: <http://esj.pnzgu.ru> (In Russian).