Информация для цитирования:
Пастухов П. С., Лосавио М. Использование информационных технологий для обеспечения безопасности личности, общества и государства // Вестник Пермского университета. Юридические науки. 2017. Вып. 36. С. 231–236. DOI: 10.17072/1995-4190-2017-36-231-236.
Pastukhov P. S., Losavio M. Ispol'zovanie informatsionnykh tekhnologiy dlya obespecheniya bezopasnosti lichnosti, obshchestva i gosudarstva [Use of Information Technology to Ensure Security of the Individual, Society and State]. *Vestnik Permskogo Universiteta. Juridicheskie Nauki* – Perm University Herald. Juridical Sciences. 2017. Issue 36. Pp. 231–236. (In Russ.). DOI: 10.17072/1995-4190-2017-36-231-236.

УДК 342
DOI: 10.17072/1995-4190-2017-36-231-236

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЛИЧНОСТИ, ОБЩЕСТВА И ГОСУДАРСТВА

П. С. Пастухов

Доктор юридических наук, доцент кафедры уголовного процесса и криминалистики
Пермский государственный национальный исследовательский университет
614990, Россия, г. Пермь, ул. Букирева, 15
ORCID: 0000-0003-0391-5540
ResearcherID: B-5451-2017
e-mail: pps64@mail.ru

М. Лосавио

Профессор
Университет Луисвилля (США)
40292, США, штат Кентукки
ORCID: 0000-0003-4542-8599
ResearcherID: E-3528-2017
e-mail: michael.losavio@louisville.edu

Введение: *в статье анализируются угрозы современного общества для личности, общества и государства, исследуются основные направления использования современных информационных технологий для обеспечения безопасности и повышения эффективности государственной деятельности и правоприменительной практики.* ***Цель:*** *на основе изучения технических характеристик компьютерных технологий, программного обеспечения выявить сферы применения информационных технологий, определить правовое регулирование применения технологий для обеспечения эффективности государственной и управленческой деятельности в правоприменительной практике с целью создания безопасной среды проживания.* ***Методы:*** *методологическую основу данного исследования составляет совокупность методов научного познания. В статье использованы общенаучные и частнонаучные методы исследования, в частности формально-юридический, сравнительно-правовой, технико-юридический.* ***Результаты:*** *авторы утверждают, что технические, организационные, управленческие, правовые аспекты внедрения информационных технологий оптимизируют деятельность по обеспечению безопасности, но в условиях повсеместной информатизации возникают новые риски для частной жизни граждан. В статье исследуются гарантии от тотального контроля для предотвращения вмешательства в частную жизнь человека. Анализируются отдельные аспекты, связанные с необходимостью достижения разумного баланса между внедрением информационных технологий и обеспечением конституционных гарантий неприкосновенности частной жизни.* ***Выводы:*** *в современном информационном обществе, в условиях повсеместного распространения искусственного интеллекта, количественного роста компь-*

ютерных преступлений, применение информационных технологий во всех сферах правоохранительной, экономической, регулятивной деятельности является необходимым, неизбежным и самым перспективным направлением развития для обеспечения безопасности личности, общества и государства.

Ключевые слова: информационные угрозы; информационные технологии; геоинформационные технологии; правоохранительная деятельность; расследование преступлений; безопасность личности, общества и государства

USE OF INFORMATION TECHNOLOGY TO ENSURE SECURITY OF THE INDIVIDUAL, SOCIETY AND STATE

P. S. Pastukhov

Perm State University
15, Bukireva st., Perm, 614990, Russia
ORCID: 0000-0003-0391-5540
ResearcherID: B-5451-2017
e-mail: pps64@mail.ru

M. Losavio

University of Louisville
Louisville, Kentucky, 40292, USA
ORCID: 0000-0003-0391-5540
ResearcherID: B-5451-2017
e-mail: michael.losavio@louisville.edu

Introduction: *the article analyzes threats to the individual, society and state present in the modern society, and considers the principal directions in the use of modern information technology for ensuring security and increasing efficiency of the state activities and law enforcement.* ***Purpose:*** *based on the study of technical characteristics of computer technologies and software, to identify spheres of the information technology application, to determine the legal regulation of the technology application for providing the efficiency of the state and administrative activities in law enforcement with the aim of creating a safe living environment.* ***Methods:*** *the methodological framework of the research is based on a set of methods of scientific cognition, including general scientific and specific scientific ones, in particular the formal-legal, comparative law, technical-legal methods.* ***Results:*** *the authors state that technical, organizational, administrative and legal aspects of the information technology implementation optimize the activities on ensuring security, but the conditions of the global computerization create new risks for privacy. The article explores the guarantees against the total control to prevent the invasion of privacy. Some specific aspects are analyzed necessary to reach a reasonable balance between the information technology implementation and observance of the constitutional guarantees of privacy.* ***Conclusions:*** *in the modern information society, with the widespread use of the artificial intellect and the increasing number of cybercrimes, the application of information technology in all the spheres of law enforcement, economic and regulatory activities is a necessary, inevitable and the most promising way of development to ensure security of the individual, society and state.*

Keywords: information threats; information technology; geo-information technology; law enforcement; crime investigation; security of the individual; society and state

Введение

Современное развитие общества порождает множество угроз природного, техногенного, экологического, конфликтного характера, а также в части распространения внутреннего и международного терроризма, ухудшения транспортной безопасности, управленческих рисков. Особое место из этого перечня отводится угрозам информационной безопасности, к которым относятся:

– нарушение информационного обеспечения деятельности органов государственной власти, муниципальных предприятий и служб;

– перехват трансляций телерадиовещания, систем оповещения и информирования населения;

– несанкционированный доступ к информации о деятельности органов государственной власти, муниципальных предприятий и служб;

– несанкционированный доступ к управлению информационными ресурсами;

– оказание целенаправленного негативного информационного воздействия на население через средства массовой информации и информационно-телекоммуникационную сеть Интернет;

– неполная реализация прав граждан в области получения и обмена достоверной информацией, в том числе манипулирование массовым сознанием с использованием информационно-психологического воздействия;

– провоцирование социальной, межнациональной и религиозной напряженности через деятельность отдельных (в том числе электронных) средств массовой информации;

– распространение злоупотреблений в кредитно-финансовой сфере, связанных с проникновением в компьютерные системы и сети[1] [3].

В условиях таких угроз и рисков граждане нуждаются в повышении общего уровня общественной безопасности, правопорядка и безопасности среды обитания за счет существенного улучшения координации деятельности сил и служб, ответственных за решение этих задач.

Основное содержание

Задачи по нейтрализации угроз, минимизации рисков, предотвращению ущерба в условиях информационного общества необходимо решать путем внедрения комплексной информационной системы, обеспечивающей прогнозирование, мониторинг, предупреждение и ликвидацию возможных угроз. Информационные технологии необходимы для контроля и устранения последствий чрезвычайных ситуаций и правонарушений с интеграцией под ее управлением действий информационно-управляющих подсистем дежурных, диспетчерских, муниципальных служб для их оперативного взаимодействия в интересах муниципального образования.

Одной из основных неотложных причин внедрения информационных технологий в управленческую и правоохранительную деятельность является информационно-технический характер современной преступности. Правоприменительная практика свидетельствует о том, что с каждым годом растет число преступлений как в сфере компьютерной информации, так и преступлений с использованием компьютерных технологий, в результате чего формируются цифровые следы преступлений. Из этого следует, что раскрывать и расследовать преступления с использованием информационных технологий возможно только с использованием правоохранительными органами информационных технологий.

Необходимость развития и внедрения информационных технологий связана со скоростью принятия решений. В условиях динамичной экономики, деятельности всех человеческой деятельности [3], основанной на информационных технологиях, в критических ситуациях необходимо принимать грамотные управленческие решения в кратчайшие сроки. Принятие выверенных решений требует мгновенного получения и анализа всей информации, причем из всех возможных источников, что невозможно без развитых автоматизированных информационных поисковых систем, автоматизированных банков данных, систем анализа и оповещения.

К названным причинам внедрения информационных технологий следует добавить экономическую целесообразность, необходимость сокращения бюрократического аппарата, более качественного предоставления государственных услуг, повышения качества и уровня жизни.

Названные и неназванные причины внедрения информационных технологий ставят перед правоохранительными органами и органами государственной, муниципальной власти задачи формирования коммуникационной платформы с целью предотвращения и устранения рисков общественной безопасности, правопорядка и создания безопасной среды обитания на базе межведомственного взаимодействия. Для этого необходимо определить потенциальные точки уязвимости, своевременно реагировать на возникающие угрозы в чрезвычайных ситуациях.

Существующие информационные угрозы и необходимость принятия антитеррористических мер побудили российского законодателя в июле 2016 года внести изменения в законодательство, обязывающее операторов связи и организаторов распространения информации в сети Интернет хранить информацию пользователей и передавать ее уполномоченным органам. Указанные изменения вызвали бурные

[1] *Об утверждении* Концепции построения и развития аппаратно-программного комплекса «Безопасный город»: распоряжение Правительства Рос. Федерации от 3 дек. 2014 г. № 2446-р // Собр. законодательства Рос. Федерации. 2014. № 50, ст. 7220.

дискуссии в обществе. Сторонники нововведений аргументировали свою поддержку необходимостью борьбы с терроризмом. Противники считали, что это приведет к вторжению в частную жизнь граждан.

Измененные нормы российского законодательства о противодействии терроризму[2], об органах безопасности[3], о связи[4], об информации и информационных технологиях[5] и другие обязывают операторов связи хранить на территории РФ информацию о фактах приема, передачи, доставки и/или обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи в течение 3 лет с момента окончания осуществления таких действий.

Операторы связи и организаторы распространения информации в сети Интернет в настоящее время обязаны предоставлять эту информацию государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации. Для беспрепятственного получения такой информации в законодательство об оперативно-розыскной деятельности включено новое оперативно-розыскное мероприятие – получение компьютерной информации[6].

В сфере правоохранительной деятельности планируется более интенсивно развивать информационно-управляющие системы, системы обработки и идентификации дактилоскопической, генной, баллистической и иной криминалистически значимой информации, программное и информационное обеспечение перспективных и современных автоматизированных систем управления, информационно-справочную работу в интересах подразделений МВД России[7].

Среди действующих эффективных информационных технологий, обеспечивающих безопасность, следует назвать видеонаблюдение и видеофиксацию, в том числе снятие, обработку и передачу видеопотока с камер видеонаблюдения о правонарушениях и ситуациях чрезвычайного характера, в том числе повреждения коммуникаций, инфраструктуры и имущества. В этом случае проводится анализ видео- и аудиопотоков, включая: автоматическую регистрацию событий на базе системы видеоанализа потока; видеоанализ событий; аналитику видеопотока в режиме реального времени; идентификацию и распознавание лиц.

Уникальные возможности использования информационных технологий в правоприменительной деятельности содержатся в позиционировании подвижных объектов (геолокация). Геолокация – это обнаружение координат реального географического положения любого объекта[8]. Определение местоположения (широты и долготы места) пользователя сети Интернет осуществляется по радиосигналам глобальной навигационной спутниковой системы ГЛОНАСС/GPS, по уровню сигналов точек доступа WiFi, по номеру соты CellID в сети сотовой связи, по IP-адресу компьютера. Геоинформационные системы представляют собой сложные информационные системы создаваемые благодаря интеграции массивов обычной (чаще фактографической) информации относительно объектов учета, с массивами географической (топографических карт, планов и др.). Геоинформационные системы МВД – это сложные информационные системы, создаваемые благодаря интеграции баз данных обычных информационных систем, функционирующих в подразделениях МВД на определенном уровне с базами данных соответствующей картографической информации, с целью представления информации об определенных объектах наглядно в пространственном их расположении на картах или планах.

В целях развития геолокации и технологической инфраструктуры системы в интересах государственных и иных информационных систем, осуществляющих сбор и обработку навигационной информации, поступающей от транспортных средств, оснащенных аппаратурой спутниковой навигации государством предпринимаются меры по реализации этих техно-

---

[2] *О противодействии* терроризму: Федер. закон Рос. Федерации от 6 марта 2006 г. № 35-ФЗ (в ред. от 06.07.2016) // Собр. законодательства Рос. Федерации. 2006. № 11, ст. 1146.

[3] *О Федеральной* службе безопасности: Федер. закон Рос. Федерации от 3 апр. 1995 г. № 40-ФЗ (в ред. от 06.07.2016) // Там же. 1995. № 46, ст. 1269.

[4] *О связи:* Федер. закон Рос. Федерации от 7 июля 2003 г. № 126-ФЗ (в ред. от 06.07.2016) // Там же. 2003. № 52, ст. 2895.

[5] *Об информации*, информационных технологиях и о защите информации: Федер. закон Рос. Федерации от 27 июля 2006 г. № 149-ФЗ (ред. от 06.07.2016) // Там же. 2006. № 31, ч. 1, ст. 3448.

[6] *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: Федер. закон Рос. Федерации от 6 июля 2016 г. № 374-ФЗ // Рос. газета. 2016. 8 июля.

[7] *Об организации* научного обеспечения и применении положительного опыта в органах внутренних дел Российской Федерации и внутренних войсках МВД России [Электронный ресурс]: приказ МВД России от 18 марта 2013 г. № 150. Доступ из справ.-правовой системы «КонсультантПлюс».

[8] *Об утверждении* Концепции построения и развития аппаратно-программного комплекса «Безопасный город»: распоряжение Правительства Рос. Федерации от 3 дек. 2014 г. № 2446-р.

логий[9]. Для этого должна быть создана коммуникационная платформа или единое информационное пространство с учетом разграничения прав доступа к информации разного характера позволит обеспечить информационный обмен между участниками всех федеральных и муниципальных органов исполнительной власти в области обеспечения безопасности[10].

В современных условиях информационные технологии играют ключевую роль в информационном обеспечении расследования преступлений. С информационных позиций информационное обеспечение – это совокупность единой системы сбора и получения информации из внешних и внутренних источников, схем информационных потоков, циркулирующих в ходе раскрытия и расследования преступлений, а также методология использования имеющихся баз данных и построения новых баз данных.

Информационное обеспечение представляет собой процесс с определенными, последовательно сменяющими друг друга стадиями, в котором субъекты воздействуют на объекты (информацию) для достижения конкретных результатов (целей). Процесс информационного обеспечения начинается с получения криминалистически значимой информации от ее источника или потенциального носителя.

Все потенциальные носители и источники получения информации о преступлении и преступнике можно подразделить на три группы: гомологические, предметные и документальные. К группе гомологических источников и носителей информации относятся: живые лица, трупы, останки трупов, биологический материал живых лиц (кровь, слюна, сперма и т. д.). В группу предметных носителей информации входят: оружие, боеприпасы и взрывчатые вещества, транспортные средства, различные технические устройства, одежда, обувь, бытовые предметы и т. д. К группе документальных носителей информации можно отнести: письменные документы, фото-, кино- и видеоизображения, фонограммы, графические изображения, машинные документы и др. Та информация, которую несут эти источники, является объектом информационного обеспечения. В своем большинстве она становится основой для ведения криминалистических и розыскных учетов, а сами предметы (боеприпасы, взрывчатые вещества и т. д.) могут служить для пополнения натурных коллекций экспертно-криминалистических подразделений.

Новые информационные технологии расширили не только следовую картину преступлений, но и перечень предметов и документов – вещественных доказательств, подлежащих криминалистической регистрации. Регистрация и долговременное хранение интернет-трафика, всех телефонных соединений, наличие жесткой взаимосвязи абонента и базовой станции, а также технические возможности современных компьютерных средств и систем управления базами данных позволяют весьма оперативно обработать колоссальные объемы биллинговой и коммуникационной информации и получить сведения, облегчающие расследование преступлений.

Современные информационные технологии и автоматизированные базы данных позволяют изучить личности всех субъектов преступной деятельности, быстро проверить все выдвигаемые версии, принять законное решение в кратчайшие сроки.

При этом надо учитывать, что на пути внедрения информационных технологий возникают несколько основных проблем [4]. Первая проблема связана с возможностью тотального контроля за поведением личности. Поэтому законодателю следует учитывать этот вид новых угроз и не допустить ухудшения конституционных гарантий неприкосновенности личности. Вторая проблема связана с информационной безопасностью, возможностью раскрытия персональных данных, кражи коммерческой, профессиональной, служебной и государственной тайны. В российском уголовно-процессуальном законодательстве существует проблема использования электронной информации в качестве доказательств по уголовным делам. Эта проблема существует из-за уголовно-процессуальной формы, не отвечающей вызовам и требованиям информационного общества. Существующая уголовно-процессуальная форма требует письменного оформления доказательственной информации в протоколах следственных действий, но которая, при настоящих объемах цифровой информации, вынуждает следователя выполнять трудоемкую работу по собиранию доказательств. Только в июле 2016 г. за-

[9] *Об утверждении* плана мероприятий («дорожной карты») по созданию открытого акционерного общества «ГЛОНАСС», развитию государственной автоматизированной информационной системы «ЭРА-ГЛОНАСС» и ее использованию в интересах других информационно-навигационных комплексов и систем, создаваемых федеральными органами исполнительной власти и организациями: распоряжение Правительства Рос. Федерации от 9 авг. 2014 г. № 1498-р // Собр. законодательства Рос. Федерации. 2014. № 49, ст. 4693.

[10] *Об инфраструктуре*, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме: постановление Правительства Рос. Федерации от 8 июня 2011 г. № 451 (ред. от 05.12.2014) // Там же. 2011. № 1, ст. 3503.

конодатель предпринял, да и то, на наш взгляд, недостаточные усилия по модернизации уголовно-процессуального доказывания[11]. Учитывая бурное развитие информационных технологий и устаревшую уголовно-процессуальную форму, мы неоднократно говорили о необходимости модернизации совершенствовании уголовно-процессуального доказывания в диссертационном [1, с. 454] и монографических исследованиях [2, с. 352].

Помимо этого, существуют проблемы ведомственной разобщенности, недостаточности финансирования для закупки и внедрения информационных технологий. Названные проблемы необходимо учитывать всем заинтересованным субъектам информационных технологий и в этой связи формировать новые информационные правоотношения.

Выводы

Обобщая вышеизложенное, можно заключить, что в современном информационном обществе, в условиях возрастания общих и информационных угроз, роста компьютерной преступности, повсеместного распространения искусственного интеллекта, применение информационных технологий во всех сферах правоохранительной, экономической, регулятивной деятельности является необходимым, неизбежным и самым перспективным направлением деятельности для обеспечения безопасности личности, общества и государства.

Для этого требуется создание единой информационной среды, обеспечивающей эффективное и незамедлительное взаимодействие всех сил и служб, ответственных за общественную безопасность и правопорядок. Для повышения эффективности деятельности по раскрытию и расследованию преступлений необходимо создать интегрированные банки данных криминалистически значимой информации, достичь более высокого уровня информатизации правоохранительных органов. Степень технической оснащенности всех органов предварительного расследования телекоммуникационной инфраструктурой и информационными ресурсами должна отвечать современным вызовам и техническим требованиям. При внедрении информационных технологий во все сферы государственной и правоохранительной деятельности в погоне за обеспечением безопасности общества и государства нельзя допустить перегибов, пренебрежения конституционными гарантиями прав личности в сфере частной жизни.

В новой структуре информационных правоотношений необходимо учитывать существующие информационные угрозы и риски, обеспечивать гарантии права личности на частную жизнь, безопасность общества и государства.

[11] *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: Федер. закон Рос. Федерации от 6 июля 2016 г. № 374-ФЗ // Рос. газета. 2016. 8 июля.

Библиографический список

1. *Пастухов П. С.* Модернизация уголовно-процессуального доказывания в условиях информационного общества: дис. … д-ра юрид. наук. М., 2015. 454 с.
2. *Пастухов П. С.* Доктринальная модель совершенствования уголовно-процессуального доказывания в условиях информационного общества: монография. М.: Юрлитинформ, 2015. 352 с.
3. *Losavio M., Pastukhov P., Polyakova S.* Cyber Black Box/Event Data Recorder: Legal and Ethical Perspectives and Challenges with Digital Forensics // Journal of Digital Forensics, Security and Law. 2016. Vol. 10, № 4. P. 43–57.
4. *Losavio M., Pastukhov P., Polyakova S.* Regulatory aspects of cloud computing in business environments // Cloud Technology: Concepts, Methodologies, Tools and Applications. 2014. № 1. P. 1373–1386.

References

1. *Pastukhov P. S. Modernizatsiya ugolovno-protsessual'nogo dokazyvaniya v usloviyakh informatsionnogo obshchestva: dis. ... d-ra. yurid. nauk* [Modernization of Criminal Procedure Evidence in the Information Society: Dr. jurid. sci. diss.]. Moscow, 2015. 454 p. (In Russ.).
2. *Pastukhov P. S. Doktrinal'naya model' sovershenstvovaniya ugolovno-protsessual'nogo dokazyvaniya v usloviyakh informatsionnogo obshchestva: monografiya* [Doctrinal Model of Improvement of Criminal Procedure Evidence in the Information Society: monograph; ed. by P. S. Pastukhov]. Moscow, 2015. 352 p. (In Russ.).
3. *Losavio M., Pastukov P. and Polyakova S.* Cyber Black Box/Event Data Recorder: Legal and Ethical Perspectives and Challenges with Digital Forensics. *Journal of Digital Forensics, Security and Law.* 2016. Vol. 10. No. 4. Pp. 43–57. (In Eng.).
4. *Losavio M., Pastukhov P., Polyakova S.* Regulatory Aspects of Cloud Computing in Business Environments. In book: Cloud Technology: Concepts, Methodologies, Tools, and Applications. 2014. No. 1. Pp. 1373–1386. (In Eng.).