

ЭКСПЕРТНО-КРИМИНАЛИСТИЧЕСКАЯ ДЕЯТЕЛЬНОСТЬ ПОЛИЦИИ

Шаповалова Г.М.

ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ (CLOUD COMPUTING) И ПРОБЛЕМЫ СБОРА ДОКАЗАТЕЛЬСТВ

Аннотация: Автором в статье рассматриваются вопросы, посвященные готовности правоохранительных органов к обнаружению, фиксации и расследованию новых общественно опасных деяний в облачных сервисах глобальной сети Интернет. В условиях информационного общества доминирующую роль играют информационные технологии, информационные системы и телекоммуникационные сети, в том числе сеть Интернет, позволяющие создавать, хранить, обрабатывать и обмениваться информацией в корпоративных, государственных и международных масштабах благодаря облачным, сервисам (cloud computing). Автор уделяет внимание на то, что облачные провайдеры взаимодействующие с облачными клиентами полностью получают права над управлением данных своих клиентов, а также учитывая сложность технологических процессов и географическое расположение облачных провайдеров и их клиентов могут осложнять работу правоохранительных органов по обнаружению, выемки, сохранению (информационных следов) в рамках процессуальных действий. Во времена сверх динамических изменений, государство нуждается в повышении качественного скачка научных исследований, что возможно при переходе к новой концепции научных исследований, эмпирическая модель и рационалистическая доктрина теории познания должны иметь достаточно высокую динамику обновления. В заключении автором были обозначены самые слабые места в противостоянии к новым, ранее не рассматриваемым, общественно опасным деяниям в жизни нашего общества. Предполагается, что в связи с тем, что облачные вычисления становятся все более востребованные на рынке информационных услуг, преступная деятельность будет, вероятно, расти. Автор убежден, что результаты научных исследований криминалистической сути общественно опасных деяний и их апробация в практике с применением современных технико-криминалистических средств и методов будут способствовать предотвращению и эффективному расследованию преступлений в среде облачных сервисов.

Ключевые слова: Криминалистика, облачные вычисления, облачный сервис, Интернет, доказательства, дефиниции, право, информационный след, расследование, стандарт.

Review: The author of the article considers the problems of law-enforcement agencies' readiness to reveal, fix, and investigate new socially dangerous acts in the Internet cloud services. In the conditions of information society, IT play special role, along

with information systems and telecommunication networks, including the Internet. They give the opportunity to create, store, process, and share the information on corporative, state, and international scale using cloud computing. The author emphasizes that cloud providers, interacting with cloud clients, get access to all the data of their clients, and, taking into account the complexity of technological processes and geographical position of cloud providers, can complicate the work of law-enforcement agencies, directed at detection, seizure, and preservation of information traces within procedural actions. In times of dynamic changes, the state needs increasing the quantum leap in scientific research, which is possible in terms of a new concept of scientific research; empirical model and rationalist doctrine of epistemology should be dynamically renewed. In the conclusion the author outlines the weakest points in fighting against new socially dangerous acts. It is supposed that, due to the spread of cloud computing, criminal activity will intensify. The author is convinced that the results of scientific research of criminal essence of socially dangerous acts and their testing in practice, using the modern technical and criminalistic means, will promote the prevention and effective investigation of crimes in the sphere of cloud computing.

Keywords: Law, definitions, evidence, Internet, cloud service, cloud computing, criminalistics, information trace, investigation, standard.

Во времена сверх динамических изменений, государство нуждается в повышении качественного скачка научных исследований, что возможно при переходе к новой концепции научных исследований, эмпирическая модель и рационалистическая концепция теории познания должны иметь достаточно высокую динамику обновления. При возрастающей роли науки, превращении ее в непосредственную производительную силу, перед ней ставятся сложные задачи. Одна из них – это борьба с современной преступностью на основе достижений криминалистики, которая обеспечивает поисково-познавательную деятельность в раскрытии преступлений. За долгие годы своего существования, криминалистика создала научные разработки в общей теории, научные методы исследования и опирающуюся на них систему частных криминалистических теорий и методов. Частные криминалистические теории относятся ко всем

разделам криминалистики: технике, тактике и методике. На этой общей и частной теоретической и методической основе разрабатываются технико-криминалистические средства, тактические приемы и методики расследования и предупреждения преступлений.

При обобщении научных методик расследования разных видов преступлений, криминалистика сталкивается, на основе использования данных отдельных естественных, технических и гуманитарных наук, в необходимости применении новых средств, приемов и методов раскрытия, расследования и предупреждения преступлений. Одно из ранних научных трудов посвященное использованию научно-технических средств в раскрытии и расследовании преступлений описано в практическом руководстве « Основы уголовной техники» С.Н. Трегубовым (1915 г.) [7].

Сегодня мы имеем дело с новой парадигмой информационных технологий, которая формирует уникальную

информационную среду (виртуальную) нашего общества – cloud computing «облачные вычисления». Национальный институт стандартизации и технологий (NIST) – подготовил унифицированное определение: облачные вычисления – это модель, позволяющая осуществлять повсеместный и удобный доступ по требованию к общему пулу конфигурируемых вычислительных ресурсов (например, совокупность сетей, серверов, хранилищ данных, приложений и услуг), который может быть оперативно предоставлен сервисным провайдером [10]. На рынке появился новый вид информационных услуг – облачные вычисления, предоставляемый провайдером облачных услуг «поставщиком услуг» юридическим или физическим лицам «потребителям услуг».

Что же с практической точки зрения представляют облачные вычисления.

На основании стандартизации и технической регламентации специалистов IT облачные вычисления имеет **5 основных характеристик**: 1) *по требованию самообслуживания*. Потребитель услуги в одностороннем порядке управляет и контролирует, например, серверное время, сетевые хранилища без участия поставщика услуг и др.; 2) *широкий спектр доступа*. Разнообразие использования сервиса за счет неоднородных тонких или толстых клиентских платформ (например, мобильных телефонов, планшетов, ноутбуков и рабочих станций); 3) *пул ресурсов*. Вычислительные ресурсы провайдера объединяются для обслуживания нескольких потребителей через мульти-арендные модели, назначаются и переназначаются динамически в соответствии с потребителем спросом. Заказчик ни только не контролирует,

но и не знает точное местоположение предоставляемых ресурсов, конечно, при желании он может получить интересующую его информацию, но она будет представлена на более высоком уровне абстракции, например, страна, штат или центр обработки данных. Так, ресурсы по хранению, обработке, ресурсы памяти, пропускной способности сети и др.; 4) *быстрая эластичность*. Возможность масштабирования вычислительной системы уменьшая или увеличивая ее в соответствии со спросом заказчика; 5) *сервис измерений (контроля)*. Облачные системы автоматически контролируют и оптимизируют использование ресурсов, например, хранение данных, обработку данных, пропускную способность и учетные записи пользователей, обеспечивая прозрачность как для поставщика сервиса, так и для потребителя.

3 базовые модели сервиса: 1) **SaaS** (Программное обеспечение как сервис). Предоставляемые потребителю приложения на сервере провайдера с различных клиентских устройств через интерфейс тонкого клиента, такой как браузер (например, web-почта, или интерфейс программы Office365). Всем процессом управляет провайдер; 2) **PaaS** (Платформа как сервис). Потребитель имеет возможность установки на облачной инфраструктуре провайдера приобретенные или созданные, с помощью языков программирования, библиотек, служб и средств, приложения; 3) **IaaS** (Инфраструктура как услуга).

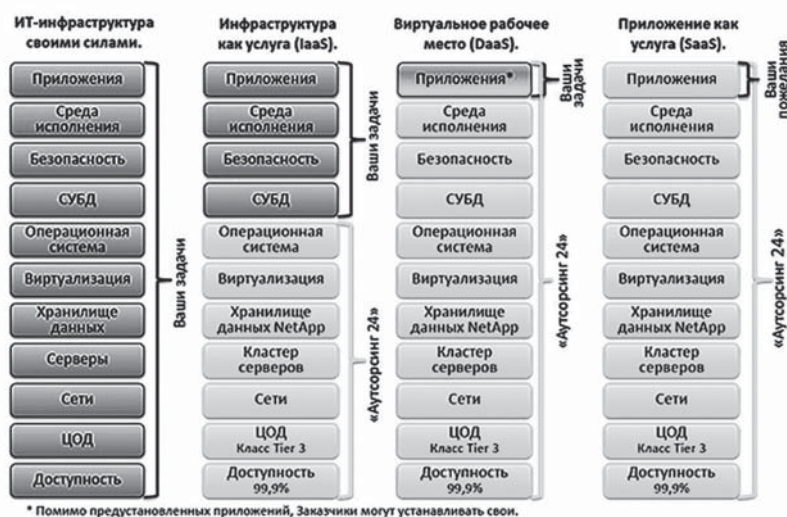
У потребителя появляются дополнительные возможности использования вычислительных ресурсов, сетей облачного провайдера, на которых он может развертывать и выполнять любое программное обеспечение, например,

(операционные системы и приложения и др.) для обработки, хранения данных.

4 способа реализации предоставленной услуги: 1) *частное облако*. Провайдер предлагает облачную инфраструктуру, исключительного, для использования одной организацией. Существовать облачная инфраструктура может как у провайдера так на сетевых и вычислительных ресурсах предприятия. Право управления и эксплуатации остается за организацией; 2) *публичное облако*. Облачная инфраструктура для открытого общественного пользования. Например, в бизнесе, академической или образовательной среде, государственной среде, других организаций или их объединений. Она существует на территории облачного провайдера; 3) *гибридное облако*. Облачная инфраструктура состоит из композиции различных облачных инфраструктур (частных, публичных, сообществ), остающихся уникальными сущностями, но связаны друг с другом через стандартные или собственные технологии, что обеспечивает совместимость данных и приложений (например, для получения дополнительных ресурсов, которых не хватает в частном облаке); 4) *облако сообществ*. Облачная инфраструктура создана для исключительного использования конкретным сообществом потребителей из организаций, имеющих общие задачи (например, бизнес-сообщества, IT-сообщества и др.). Управлять и эксплуатировать имеет право одна и более организаций в сообществе или третья сто-

рона, а также их комбинации. Облачная инфраструктура может существовать как на предприятии, так и вне [10].

Строятся облачные сервисы на фундаменте таких технологий, как распределённые вычисления, включающие в себя кластеризацию, серверную виртуализацию и динамическое предоставление ресурсов, а также сервисы общего пользования SOA (service-oriented architecture) – сервис-ориентированную архитектуру и широкомасштабную автоматизацию управления. При этом основная нагрузка приходится на поставщика облачных услуг: установку оборудования и программного обеспечения, резервное копирование, техническое обслуживание, модернизацию и обеспечение безопасности данных. Графически это представлено на рисунке 1.



* Помимо предустановленных приложений, Заказчики могут устанавливать свои.

Рис. 1. Концептуальная эталонная модель облачных сервисов.

Для потребителя из всех вопросов, решаемых провайдером облачных вычислений, является – обеспечение безопасности данных. В рамках данного исследования особый интерес представляет практическая готовность следственных органов и криминали-

стов к обнаружению, фиксации, сохранению доказательств (информационных следов). Насколько сегодня правоохранительные органы готовы к предотвращению, реагированию и расследованию преступлений в облачных сервисах?

Безусловно, данные исследования на сегодня являются актуальными, что подтверждается научными публикациями. Например, в статье «Анализ проблем доверия в облачных технологиях» авторы указывают на то, что всех волнует доверие провайдеру облачных услуг. Эта тема обсуждается во многих странах, но оптимальное решение до сих пор не найдено [2]. «Недоверие – ключевое слово, описывающее российский рынок облаков. У него много аргументов: недостаточное знание о возможностях облака, ощущение неразвитости платформ (хотя это не так), нестабильность и «закручивание гаек» в интернете, отставание в выработке стандартов качества», – комментирует генеральный директор компании «Облакотек» Максим Захаренко [18]. В другой статье «Безопасность облачных вычислений» автор прямо указывает, что найти универсальное решение по безопасности невозможно, так как существует множество вариантов построения облачных инфраструктур [5]. С этим нельзя не согласиться, судя по описанию концептуальной эталонной модели облачных сервисов, описанной выше. Но при этом спорить о том, работать с облачными сервисами или нет бессмысленно, так как они уже прочно вошли в нашу жизнь уточняют О.Ю. Пескова и К.Е. Степовая [4]. Нельзя обойти и проблему законодательного регулирования отрасли информационных технологий. Облачному сервису необ-

ходимо формирование единых унифицированных правовых дефиниций закрепленных в национальных стандартах или утвержденных по стандартам международных организаций. Специалисты в области законодательства в странах Евросоюза и США обращают внимание на то, что этот процесс у них уже завершился [11]. Чего нельзя сказать про российское законодательство.

Из-за многовариантности построения облачных инфраструктур, предлагаемых на нашем рынке в качестве информационных услуг – это явление имеет скрытый для общества характер преступлений. Количественные и качественные изменения преступного общества уже давно, как только появились компьютеры и компьютерные сети общего пользования, поменяли свой вектор в пользу интеллекта и изобретательности. Криминалистический портрет современного преступника – профессионально подготовленный специалист криминального IT бизнеса. Об этом должны помнить правоохранительные органы и повышать свой профессиональный уровень на опережение.

Очевидно, что без фундаментальных научных исследований в этой предметной области деятельность правоохранительных органов будет оставаться неэффективной. Анализ и оценка криминалистических характеристик новых видов преступлений, а также их квалификация позволит ускорить процесс их теоретического закрепления тактических приемов, разработке специализированных технико-криминалистических средств, обогатить систему частных криминалистических теорий и методов и практического применения при расследовании преступлений, а также высказать рекомендации по их совершенствованию.

На основании анализа научной литературы в формат актуальности вошли следующие вопросы: 1. Полнота доверия; 2. Обнаружение следов; 3. Целостность данных; 4. Сегрегация потенциальных доказательств в многопользовательской системе; 5. Восстановление удаленных данных в общей и распределенной виртуальной среде; 6. Сбор доказательств у нескольких облачных провайдеров; 7. Сохранение доказательств. Решение их, на наш взгляд, будет способствовать положительным результатам борьбы с преступностью в среде облачных сервисов.

Необходимо отметить, что для решения задач по предупреждению и расследованию существуют в первую очередь объективные причины. Как пример, облачные сервисы технологически расширяют границы часовых поясов и межгосударственные границы, что усугубляет расследование уголовных преступлений в рамках государства, но еще хуже обстоят дела за его пределами. Безусловно, наработанные методики расследования преступления в сфере компьютерной информации, глава 28 УК РФ [8], мошенничество в сфере компьютерной информации ст. 159.6. УК РФ [8], имеют положительный эффект, но это не освобождает от изучения криминалистических особенностей преступной деятельности в сфере облачных сервисов с учетом их закономерностей взаимосвязей и дополнительных знаний, которые будут способствовать раскрытию преступлений.

Все сказанное выше должно проецироваться в качественные показатели по проведению первоначальных неотложных следственных действий и проверочных мероприятий, своевременное и грамотное назначение необ-

ходимых судебных экспертиз. Такими профессиональными компетенциями должен обладать современный сотрудник правоохранительных органов. Что происходит на практике в реальной жизни? Рассмотрим ряд примеров из реальных расследований.

Пример №1. При рассмотрении одного из востребованных сервисов SaaS, можно назвать объективные причины, ограничивающие эффективное расследование: 1. Огромное количество потенциальных доказательств: десятки тысяч файлов; 2. Потеря данных: перезагрузка системы может удалить жизненно важные следы и улики; 3. Квалификационные признаки преступления: преступление может оставаться незамеченным в течение нескольких месяцев или лет (например, мошенничество) [17].

Субъективные причины, ограничивающие эффективное расследование. Для собирания этих доказательств требуются специальные знания и соответствующая подготовка. Необходимого объема знаний в вопросах облачных сервисов сегодня не хватает и самим специалистам IT, что уж говорить о сотрудниках правоохранительных органов. Чтобы лучше понять программно-технические процессы, необходимо больше научного и методического материала посвященного этой теме. На сегодня есть следующие источники полезной информации: научно-практическое пособие Е.Р. Россинской, А.И. Усова «Судебная компьютерно-техническая экспертиза», в котором изложены общетеоретические, процессуальные, методические и практические аспекты судебно-экспертной деятельности при раскрытии и расследовании преступлений, сопряженных с использовани-

ем компьютерных средств и технологий [6]. Практическое пособие Н.Н. Федотова «Компьютерная форензика» посвященное методам раскрытия и расследования компьютерных преступлений, правилам сбора, закрепления и представления доказательств по ним применительно к российскому законодательству [9], электронный ресурс Ю.М Баркалова «Подготовка экспертов по производству компьютерных судебных экспертиз» [1], интернет-ресурс <http://www.oxygen-forensic.com/en/> (прим. нет поддержки русского языка) [12] и др. Российских изданий такого содержания и качества недостаточно, а названные нуждаются в дополнениях. Но это не уменьшает их значимость, так как основополагающие теоретические догмы как система основных положений криминалистического научно-направленного составляют их основу. Следовательно, изложенный материал будет способствовать повышению квалификации традиционными практическими занятиями для получения навыков работы. Новые профессиональные компетенции, в свою очередь, будут способствовать повышению результатов при расследовании и проведении компьютерно-технических экспертиз.

На опережение работают частные компании, предлагая свои услуги, например, «Лаборатория Цифровой Форензики» – российская компания, предоставляющая качественные услуги в области информационной безопасности для бизнеса [13], или **Group-IB** – международная компания по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий [14].

Пример №2. Можно назвать объективные причины ограничивающие эф-

фективное расследование: все чаще следователи сталкиваются с тем, что доступ к данным в облачных системах невозможен, или, по крайней мере, очень затруднен. Процесс распределения данных приводит к ситуации, когда информация может распространяться через огромное количество вычислительных устройств, часть из которых находится вне национальной или даже международной юрисдикции. Данные о клиенте могут храниться на нескольких серверах в разных национальных географических зонах (что может привести к “трансграничности потоков данных”). Например, глобальная система бронирования «Amadeus» работает в 215 странах мира, своим клиентам дает возможность в режиме реального времени бронировать: билеты на рейсы более 420 авиакомпаний и просматривать расписание рейсов свыше 710 авиакомпаний мира; гостиничные номера 110 000 гостиниц [15].

На основании конвенции «О защите физических лиц при автоматизированной обработке персональных данных» [3], каждое физического лица, независимо от его гражданства или местожительства имеет права на неприкосновенность частной жизни, в отношении автоматизированной обработки касающихся его персональных данных («защита данных»). Что осложняет решать вопросы по получению необходимых данных о субъектах.

В заключении можно выделить самые слабые места в противостоянии к новым, ранее не рассматриваемым, общественно опасным деяниям в жизни нашего общества. В связи с тем, что облачные вычисления становятся все более востребованные на рынке информационных услуг, преступная деятельность

будет, вероятно, расти. Перечисленные проблемы охватывают теоретические и практические аспекты обнаружения, выемки, сохранения, и обязательной оценки, анализа доказательств (информационных следов). Несомненно, требуется комплексный подход к вопросам законодательства с учетом различных отраслей права. Соблюдение законности процессуальных решений по уголовным делам, снижение сроков предваритель-

ного расследования, неукоснительное соблюдение прав и законных интересов участников уголовного судопроизводства, а также государственного контроля и правового регулирования Интернета. В формировании позиции Российской Федерации в рамках международного права, тесной связи по расследованию трансграничных преступлений с международной полицией (Interpol) в сфере киберпространства.

Библиография:

1. Баркалов, Ю.М., Подготовка экспертов по производству компьютерных судебных экспертиз [Электронный ресурс] : методические рекомендации / Юрий Михайлович Баркалов . – Воронеж : Воронежский институт МВД России (ВорЮИ МВД России), 2013 . – 65 с.
2. Белова, Т.Г., Побеженко И.И., Побеженко В.В. Анализ проблем доверия в облачных технологиях. Восточно-Европейский журнал передовых технологий. Украинская Государственная Академия железнодорожного транспорта. УКРАИНА. Харьков. № 2 (62) том 2. 2013. С. – 59-61.
3. О защите физических лиц при автоматизированной обработке персональных данных: Конвенция (ETS N 108) [рус., англ.] (Заключена в г. Страсбурге 28.01.1981); // Собрание законодательства РФ. 3 февраля 2014 г. N 5. Ст. 419; О ратификации конвенции совета европы о защите физических лиц при автоматизированной обработке персональных данных: Федеральный закон от 19 декабря 2005 г. N 160-ФЗ // Собрание законодательства РФ, 26.12.2005, N 52 (часть I) ст. 5573.
4. Пескова О.Ю., Степовая К.Е. Особенности анализа информационной безопасности облачных систем. Известия Южного федерального университета. Технические науки. Выпуск № 12 (149). 2013. С. – 39-47.
5. Прудникова А.А. Безопасность облачных вычислений. Журнал Мир Телекома. Облачные технологии. №1. 2013. С. 50-55; <http://mirtelecoma.ru/magazine/pechatnaya-versiya/>.
6. Россинская, Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. – М.: Право и закон, (Серия «Практическая юриспруденция. Судебная экспертиза») 2001. – 416 с.
7. Трегубов С.Н. Основы уголовной техники. Научно-технические приемы расследования преступлений. Петроград, издание юридического книжного склада. Право, 1915. – 334 с.
8. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 13.07.2015, с изм. от 16.07.2015) (с изм. и доп., вступ. в силу с 25.07.2015) // Собрание законодательства РФ, 17.06.1996, N 25, ст. 2954.
9. Федотов, Н.Н., Форензика-компьютерная криминалистика-М.: Юридический Мир, 2007. – 432 с.
10. Peter Mel I, Timothy Grance. NIST Special Publication 800-145. The NIST Definition of cloud computing. 2011. 3 p.; The National Institute of Standards and Technology, NIST. DateViews 10.10.2015 <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.
11. http://www.cnews.ru/reviews/cloud_2014/articles/rossijskie_oblaka_ne_razmenivayutsya_po_melocham (дата доступа 10.10.2015).
12. <http://www.oxygen-forensic.com/en/> (дата доступа 10.10.2015).
13. <http://forensicservices.ru/>, (дата доступа 10.10.2015).
14. <http://www.group-ib.ru/>, (дата доступа 10.10.2015).

15. <http://www.slideshare.net/AmazonWebServices/modern-it-governance-through-transparency-and-automation> (дата доступа 10.10.2015).
16. <http://www.amadeus.ru/about/index.htm> (дата доступа 10.10.2015).
17. http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ForumVIII/Agenda/3-1-0950-overview-CC_Wksp2015_Overview_Herman.pdf.
18. <http://expert.ru/northwest/2014/06/delovyie-oblaka/> (дата доступа 10.10.2015).
19. А. В. Царегородцев Критичные вопросы оперативного и организационно-технического управления информационной безопасностью облачных вычислений // Национальная безопасность / nota bene. – 2011. – 6. – С. 11 – 17.
20. Царегородцев А.В., Ермошкин Г.Н. Базовые принципы построения дерева целей информационной безопасности среды облачных вычислений // Национальная безопасность / nota bene. – 2013. – 5. – С. 69 – 79. DOI: 10.7256/2073-8560.2013.5.9583.
21. Царегородцев А.В. Построение деревьев целей для идентификации требований безопасности среды облачных вычислений // Национальная безопасность / nota bene. – 2013. – 5. – С. 51 – 68. DOI: 10.7256/2073-8560.2013.5.9587.
22. А.В. Царегородцев, А.К. Качко Один из подходов к моделированию маршрута распределения обработки критичных данных в гибридной среде облачных вычислений // Национальная безопасность / nota bene. – 2012. – 5. – С. 43 – 49.
23. Е. П. Ищенко Российская криминалистика первой четверти XXI века: главные направления развития // Союз криминалистов и криминологов. – 2013. – 1. – С. 154 – 159.
24. Царегородцев А.В., Ермошкин Г.Н. Модель оценки рисков информационной безопасности информационных систем на основе облачных вычислений // Национальная безопасность / nota bene. – 2013. – 6. – С. 46 – 54. DOI: 10.7256/2073-8560.2013.6.9585.
25. Яровенко В.В., Полещук О.В. Справочники как составная часть обеспечения криминалистической информацией следственной деятельности // Право и политика. – 2014. – 12. – С. 1865 – 1870. DOI: 10.7256/1811-9018.2014.12.13689.

References (transliterated):

1. Barkalov, Yu.M., Podgotovka ekspertov po proizvodstvu komp'yuternykh sudebnykh ekspertiz [Elektronnyi resurs] : metodicheskie rekomendatsii / Yurii Mikhailovich Barkalov . – Voronezh : Voronezhskii institut MVD Rossii (VorYul MVD Rossii), 2013 . – 65 s.
2. Belova, T.G., Pobezhenko I.I., Pobezhenko V.V. Analiz problem doveriya v oblachnykh tekhnologiyakh. Vostochno-Evropeiskii zhurnal peredovykh tekhnologii. Ukrainskaya Gosudarstvennaya Akademiya zheleznodorozhnogo transporta. UKRAINA. Khar'kov. № 2 (62) tom 2. 2013. S. – 59-61.
3. Peskova O.Yu., Stepovaya K.E. Osobennosti analiza informatsionnoi bezopasnosti oblachnykh sistem. Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskie nauki. Vypusk № 12 (149). 2013. S. – 39-47.
4. Prudnikova A.A. Bezopasnost' oblachnykh vychislenii. Zhurnal Mir Telekom. Oblachnye tekhnologii. №1. 2013. S. 50-55; <http://mirtelecoma.ru/magazine/pechatnaya-versiya/>.
5. Rossinskaya, E.R., Usov A.I. Sudebnaya komp'yuterno-tekhnicheskaya ekspertiza. – M.: Pravo i zakon, (Seriya «Prakticheskaya yurisprudentsiya. Sudebnaya ekspertiza») 2001. – 416 s.
6. Tregubov S.N. Osnovy ugolovnoi tekhniki. Nauchno-tekhnicheskie priemy rassledovaniya prestuplenii. Petrograd, izdanie yuridicheskogo knizhnogo sklada. Pravo, 1915. – 334 s.
7. Fedotov, N.N., Forenzika-komp'yuternaya kriminalistika-M.: Yuridicheskii Mir, 2007. – 432 s.
8. Peter Mel I, Timothy Grance. NIST Special Publication 800-145. The NIST Definition of cloud computing. 2011. 3 p.; The National Institute of Standards and Technology, NIST. DateViews 10.10.2015 <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.
9. А. В. Царегородцев Критичные вопросы оперативного и организационно-технического управления информационной безопасностью облачных вычислений // Национальная безопасность / nota bene. – 2011. – 6. – С. 11 – 17.

10. Tsaregorodtsev A.V., Ermoshkin G.N. Bazovye printsipy postroeniya dereva tselei informatsionnoi bezopasnosti sredi oblachnykh vychislenii // Natsional'naya bezopasnost' / nota bene. – 2013. – 5. – С. 69 – 79. DOI: 10.7256/2073-8560.2013.5.9583.
11. Tsaregorodtsev A.V. Postroenie derev'ev tselei dlya identifikatsii trebovaniy bezopasnosti sredi oblachnykh vychislenii // Natsional'naya bezopasnost' / nota bene. – 2013. – 5. – С. 51 – 68. DOI: 10.7256/2073-8560.2013.5.9587.
12. A.V. Tsaregorodtsev, A.K. Kachko Odin iz podkhodov k modelirovaniyu marshruta raspredeleniya obrabotki kritichnykh dannyykh v gibridnoi srede oblachnykh vychislenii // Natsional'naya bezopasnost' / nota bene. – 2012. – 5. – С. 43 – 49.
13. 23. E. P. Ishchenko Rossiiskaya kriminalistika pervoi chetverti XXI veka: glavnye napravleniya razvitiya // Soyuz kriminalistov i kriminologov. – 2013. – 1. – С. 154 – 159.
14. Tsaregorodtsev A.V., Ermoshkin G.N. Model' otsenki riskov informatsionnoi bezopasnosti informatsionnykh sistem na osnove oblachnykh vychislenii // Natsional'naya bezopasnost' / nota bene. – 2013. – 6. – С. 46 – 54. DOI: 10.7256/2073-8560.2013.6.9585.
15. Yarovenko V.V., Poleshchuk O.V. Spravochniki kak sostavnaya chast' obespecheniya kriminalisticheskoi informatsiei sledstvennoi deyatelnosti // Pravo i politika. – 2014. – 12. – С. 1865 – 1870. DOI: 10.7256/1811-9018.2014.12.13689.