УДК 346.9

СМОЛЕНСКИЙ МИХАИЛ БОРИСОВИЧ,
ЛЕВШИН НИКОЛАЙ СЕРГЕЕВИЧ

УЖЕСТОЧЕНИЕ ГОСУДАРСТВЕННОГО КОНТРОЛЯ ЭЛЕКТРОННЫХ КОММУНИКАЦИЙ КАК ПРИОРИТЕТНОЕ НАПРАВЛЕНИЕ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ГОСУДАРСТВА И ЕГО ГРАЖДАН

АННОТАЦИЯ

В статье представлен обзор ключевых угроз, порождаемых бесконтрольным развитием электронных коммуникаций. Авторы выделяют различные группы угроз и характеризуют степень их опасности для государства и его граждан. Помимо этого, авторы оценивают роль государственного контроля в перспективе минимизации рассматриваемых угроз и выносят предложения в части повышения его результативности.

Ключевые слова: государственная безопасность; государственный контроль; информационная безопасность; национальная безопасность; экономическая безопасность.

SMOLENSKIY M.B.,
LEVSHIN N.S.,

THE STRENGTHENING OF STATE ELECTRONIC COMMUNICATIONS CONTROL AS A PRIORITY DIRECTION AT PROVIDING THE SECURITY OF THE STATE AND ITS CITIZENS

ABSTRACT

This article provides an overview of the key threats posed by the uncontrolled development of electronic communications. The authors identify different groups of threats and characterize the degree of their danger to the state and its citizens. In addition, the authors assess the role of state control from the perspective of minimizing the threats under consideration and make proposals for improving its effectiveness.

Keywords: state security; state control; information security; national security; economic security.

Основные принципы концепции развития сети Интернет, известной нам под названием «Веб 2.0», были описаны еще в далёком, по меркам развития информационных технологий, 2005 году. В числе прочих принципов тогда фигурировал тезис, согласно которому информационные системы становятся тем лучше, чем больше людей вовлечено в их эксплуатацию [1].

На наш взгляд, прошедшее десятилетие уже более чем наглядно продемонстрировало несостоятельность данного тезиса, подтвердив справедливость куда более древнего тезиса о том, что количественный рост далеко не всегда способствует качественному.

Тем не менее, информационное пространство сети Интернет продолжает расширять свои границы. Развитие концепции «Веб 2.0» привело к экстенсивному росту числа информационных ресурсов, позволяющих пользователям размещать информацию без предварительной проверки, и, как следствие, к колоссальному росту объемов недостоверной, лишенной смысла, мошеннической и несущей угрозу для здоровья граждан и стабильности государств информации.

На сегодняшний день любой пользователь сети Интернет способен тиражировать любую информацию в пределах всего земного шара. И, как показывает практика, степень вреда, наносимого им при этом социуму, ограничивается только уровнем правовой культуры и морально-этических ограничений этого пользователя.

Специфика ущерба, наносимого посредством электронных коммуникаций заключается в том, что этот ущерб далеко не всегда очевиден. Даже регулярно наблюдая в сводках новостей и сюжетах фильмов реализацию большинства возможных угроз, происходящих из-за низкой степени контроля электронных коммуникаций, пользователи сети Интернет способны осознать реальность указанных угроз лишь на собственном опыте. Но, даже в этом случае, пострадавшие

далеко не всегда утруждают себя мыслями о том, почему с ними произошло то, что произошло, и какие их действия или меры государственного контроля помогли бы им этого избежать.

Рассматривая сеть Интернет в качестве потенциального источника угроз (как для отдельного гражданина, так и для всего государства в целом) можно выделить несколько групп угроз по направлению основного наносимого ими ущерба: ущерб здоровью, ущерб репутации, финансовый ущерб. Разумеется, некоторые угрозы могут давать комбинированный эффект. Например, беспрепятственное использование электронных коммуникаций террористическими группами для организации терактов может не только нанести ущерб здоровью и финансовому благополучию граждан, но и отразиться на репутации государства.

Говоря об ущербе здоровью граждан важно сказать, что деяния пользователей сети Интернет, несущие потенциальную угрозу здоровью, могут принимать довольно разнообразные формы, например:

- доведение до самоубийства или угнетение психического состояния [2];
- распространение несущих вред здоровью методов лечения (в том числе под видом рецептов так называемой «народной медицины») или несертифицированных «лекарственных» препаратов;
- распространение инструкций, позволяющих изготавливать оружие и взрывные устройства в домашних условиях (в том числе, распространение чертежей для печати оружия на 3D-принтере);
- упрощение подготовки преступлений (например, похититель или педофил может создать анкету с данными ровесника ребенка, чтобы от его лица пригласить ребенка в гости или на прогулку и, таким образом, подвести к ситуации, когда ему будет проще осуществить свои преступные намерения).

Говоря об ущербе репутации, который может быть нанесен с использованием каналов электронных коммуникаций, важно отметить, что он не характеризуется фиксированностью и может достигать колоссальных масштабов, что обусловлено стихийностью распространения информации. При этом, в отличие от ситуации с печатными СМИ, публикации опровержения на электронном ресурсе, послужившем первоисточником, может быть недостаточно для равноценной компенсации ущерба, поскольку нет никаких гарантий, что опровержение будет растиражировано и другими информационными посредниками, поспешившими распространить порочащую или дискредитирующую информацию. Проще говоря: аудитория, получившая опровержение, может существенно уступать по численности аудитории, получившей наносящую ущерб репутации информацию.

Говоря о финансовом ущербе, наносимом посредством каналов электронных коммуникаций, чаще всего подразумевают последствия действий Интернет-мошенников [3]. Финансовый ущерб, наносимый мошенниками благодаря свободе распространения информации в сети Интернет может достигать по-настоящему грандиозных масштабов. Наибольшее распространение получили мошеннические схемы, опирающиеся на принцип «салями» (названный так по аналогии с технологией производства одноименной колбасы – когда из непрезентабельных остатков разнообразных мясных продуктов получается аппетитный деликатес). В переложении на область финансовых махинаций данный принцип подразумевает, что обманув несколько миллионов человек на кажущиеся незначительными суммы, мошенник может безнаказанно стать обладателем нескольких миллионов, поскольку пострадавшие не будут тратить ресурсы на расследование потери незначительных денежных сумм.

Справедливости ради следует заметить, что реализация мошеннических схем посредством электронных коммуникаций популярна не только благодаря свободе распространения информации, но и благодаря отсутствию эффективных механизмов расследования правонарушений в сети Интернет.

Например, человеку, потерявшему стараниями мошенников сумму до 500 рублей, в большинстве случаев, просто не выгодно заявлять об этом в полицию. Дорога к полицейскому участку, поиск нужного следователя, ожидание

очереди и составление заявления могут занять весь рабочий день, за который «пострадавший» может заработать многим большую сумму. В то время как показатели раскрываемости преступлений этого типа еще далеки от идеала. Таким образом, обратившись в правоохранительные органы, пострадавший, в большинстве случаев, лишь максимизирует ущерб, нанесенный ему мошенниками.

Однако далеко не все угрозы исходящие от возможности бесконтрольного распространения информации характеризуются малозначительностью. Некоторые из таких угроз вполне способны дестабилизировать ситуацию в масштабах целого государства. Далее мы рассмотрим несколько примеров, наиболее наглядно иллюстрирующих данный тезис.

Начиная с 2008 года, в России реализуется Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года. Данная Концепция была разработана в соответствии с поручением Президента РФ, по итогам заседания Государственного совета, состоявшегося 21 июля 2006 г., и утверждена распоряжением Правительства от 17 ноября 2008 г. № 1662-р [4].

Главной целью вышеуказанной Концепции является обеспечение устойчивого повышения благосостояния российских граждан, национальной безопасности, динамичного развития экономики и укрепления позиций России в мировом сообществе. И, в рамках достижения этой цели, российскому государству необходимо обеспечить повышение эффективности и качества обслуживания граждан в государственных и коммерческих организациях. В свою очередь, один из ключевых путей решения данной задачи, кроется в упрощении процессов идентификации граждан для получения доступа к услугам различных организаций.

Поскольку современное общество переживает эпоху тотальной информатизации, решение задачи по упрощению идентификации граждан неизбежно свелось к идее внедрения универсального электронного носителя персональных данных. Внедрение такого носителя открывает возможность автоматического считывания паспортных данных, обеспечивая сокращение временных и ресурсных затрат на заполнение различных квитанций и прочих документов, и позволяя, тем самым, минимизировать проблему очередей.

27 июля 2010 года, был принят Федеральный закон № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг». В шестой главе указан закона был представлен новый инструмент идентификации граждан – универсальная электронная карта (далее – УЭК). Там же были прописаны и основные направления применения УЭК, включая возможность осуществления электронных платежей.

Здесь нужно отметить, что, ранее, внедрение государством каждого нового средства идентификации (например, идентификационного номера налогоплательщика – ИНН) сопровождалось волнениями среди представителей христианского вероучения. Эти волнения были обусловлены превратным толкованием текстов Откровений святого Иоанна Богослова, в которых можно найти строки о некоем числе, обладатели начертания которого получают возможность покупать и продавать:

«И он (зверь из земли, т.е. лжепророк Антихриста) сделает то, что всем, малым и великим, богатым и нищим, свободным и рабам, положено будет начертание на правую руку их, или на чело их, и что никому нельзя будет ни покупать, ни продавать, кроме того, кто имеет это начертание, или имя зверя, или число имени его. Здесь мудрость. Кто имеет ум, тот сочти число зверя; ибо это число человеческое. Число его 666» [5].

Очевидный логический аргумент, основанный на том, что в священных текстах идет речь о нанесении знаков на лоб и правую руку, отметается верующими под предлогом того, что указанные обстоятельства могут иметь метафорический характер: правая рука – деятельная жизнь по заповедям Божиим, чело – познание истины Божией.

Но в этой противоречивой ситуации на помощь обществу пришла Русская Православная Церковь (далее – РПЦ), иерархи которой своевременно выступили с разъяснениями об исторической традиции идентификации граждан государства, приводя в подтверждение своих доводов отрывок из Евангелия от Луки:

«В те дни вышло от кесаря Августа повеление сделать перепись по всей земле. Эта перепись была первая в правление Квириния Сириею. И пошли все записываться, каждый в свой город. Пошел также и Иосиф из Галилеи, из города Назарета, в Иудею, в город Давидов, называемый Вифлеем, потому что он был из дома и рода Давидова, записаться с Мариею, обрученною ему женою, которая была беременна» [6].

4 февраля 2013 года Архиерейским Собором Русской Православной Церкви был принят документ под названием «Позиция Церкви в связи с развитием технологий учета и обработки персональных данных», в котором утверждалось следующее: «Православная Церковь не отрицает необходимости учета граждан государством. Пречистая Дева Мария и святой Иосиф Обручник, послушав повеление кесарево, чтобы «пошли все записываться, каждый в свой город» (Лк. 2:3), направились в Вифлеем, где и был рожден Спаситель мира. С давних времен власть проводила переписи населения, выдавала документы, удостоверяющие личность. Эти меры нужны для охраны правопорядка и общественной безопасности, выполнения экономических и социальных функций».

Там же упоминается и о том, что еще 7 марта 2000 года Священный Синод Русской Православной Церкви подчеркивал в официальном заявлении, что «никакой внешний знак не нарушает духовного здоровья человека, если не становится следствием сознательной измены Христу и поругания веры» [7].

Однако нельзя сказать, чтобы вышеперечисленные разъяснения существенно способствовали уменьшению массовых волнений, поскольку число христиан, знакомых с официальной позицией РПЦ, существенно уступает числу сторонников некорректной трактовки.

Указанное положение вещей обусловлено тем обстоятельством, что для тиражирования некорректных трактовок священных текстов активно применяется такая методика массового распространения информации, как «спам». Суть данной методики сводится к размещению шаблонных информационных сообщений на страницах всех дискуссий в сети Интернет, участие в которых доступно распространителям [8].

Интересно, что тексту тиражируемой трактовки Откровений святого Иоанна Богослова традиционно сопутствует критика представителей действующей власти (уличающая их в стремлении манипулировать гражданами, посредством вживления управляющих чипов) или реклама услуг «православных юристов» (как они сами себя называют), готовых за умеренную плату «помочь братьям по вере» с оформлением отказа от получения универсальной электронной карты.

Таким образом, можно наблюдать, как псевдохристианские идеи используются представителями оппозиционных политических сил с целью провокации недовольства действующей властью, а предприимчивыми юристами – с целью расширения клиентской базы [9]. Но, важно понимать, что вне зависимости от частных целей преследуемых распространителями, тиражируемые тексты могут послужить причиной возникновения неконтролируемой массовой паники.

Массовая паника способна подорвать любую, даже самую стабильную, систему – будь то финансовая система (если граждане бросятся в банки за своими деньгами), система снабжения продовольствием (массовая скупка продуктов «про запас» может привести к реальному дефициту товара даже при отсутствии предпосылок к этому) или политическая система (например, запугивание населения предполагаемыми действиями политических оппонентов) [10].

Наглядным подтверждением того, что неконтролируемое распространение ложных слухов может спровоцировать массовую панику, служат массовые волнения российских граждан, наблюдавшиеся весной 2011 года, когда анонимный пользователь разместил в социальной сети «Вконтакте» объявление о том, что российское Правительство готовится утвердить закон о платном начальном образовании, и бесплатными останутся только несколько дисциплин. При этом номер законопроекта в сообщении не упоминался.

Спустя несколько суток на различных ресурсах в сети Интернет насчитывались миллионы копий этого анонимного объявления, ряд телевизионных каналов подготовили на эту тему нейтральные или даже подтверждающие

сюжеты, а оппозиционные партии умудрились собрать несколько митингов протеста. При этом никто из митингующих не мог объяснить против какого законопроекта они выступают. Что и неудивительно, поскольку законопроекты с подобными положениями никогда не выносились на рассмотрение. И убедиться в этом всего за несколько минут мог каждый член «современного информационного общества», посетив государственные электронные ресурсы, на которых размещаются тексты законопроектов.

Данный пример не является художественным вымыслом или преувеличением авторов. Это реальные события, нашедшие свое отражение в материалах Российской Газеты: «Мифология средней школы» [11] и «Страшилки о «платной» школе снова будоражат Интернет» [12]. Всё это говорит о том, что мы имеем дело с успешными прецедентами поднятия массовой паники, путем распространения слухов по каналам электронных коммуникаций.

Таким образом, резюмируя вышесказанное, можно констатировать, что на данном этапе развития российского общества очень важно своевременно отслеживать динамику ситуации с распространением провокационной информации в сфере компьютерных коммуникаций и препятствовать ее дальнейшему развитию.

При этом, в целях превентивной минимизации рисков распространения массовой паники, могут применяться, как традиционные мероприятия по борьбе со спамом, так и различные законодательные ограничения на распространение информации посредством компьютерных сетей.

В свете вышеприведенных угроз может казаться непонятным, почему любые попытки государственного регулирования сферы электронных коммуникаций вызывают у русскоязычных пользователей сети Интернет широкий резонанс. Анализируя природу описанного социального явления, можно выделить две наиболее вероятных причины такого резкого неприятия государственного вмешательства в регулирование электронных коммуникаций.

Первая причина выражается в том, что, на сегодняшний день, практически любой пользователь сети Интернет в той или иной степени может считаться правонарушителем. Большая часть правонарушений связана с нарушением авторских прав (например, использование чужих художественных произведений в качестве так называемых «аватарок» и «обоев», безвозмездное использование чужих текстов и т.п.). Совершать эти правонарушения пользователям нравится, поскольку при этом они удовлетворяют собственные желания, экономят денежные средства или даже обогащаются.

При этом пользователи сети Интернет далеко не всегда осознают, что совершают нечто противоправное. Соответственно, возникает аберрация восприятия, при которой любые попытки изменить текущее положение вещей будут восприниматься такими пользователями как ущемление их свобод [13]. На этом могут играть другие правонарушители, для которых ограничение свобод может обернуться разрушением источника доходов или порицаемых обществом развлечений. В качестве заинтересованных лиц они могут инициировать акции протеста, вызывающие широкий общественный резонанс, маскируя свои истинные мотивы под «борьбу с тоталитарным государственным строем». Что в свою очередь не упустят и представители оппозиционных сил.

Здесь следует отметить вторую по важности причину отрицания общественностью необходимости государственного регулирования в сфере электронных коммуникаций. Она заключается в том, что в обществе отсутствует четкое понимание угроз, порождаемых неконтролируемым развитием электронных коммуникаций.

Для любого представителя современного информационного общества компьютерные сети стали столь же необходимым в обиходе инструментом, как кухонный нож. Однако, в отличие от компьютерных сетей, необходимость законодательных ограничений использования, хранения и транспортировки ножей для любого члена социума более очевидна, ввиду наличия у ножей определенных элементов конструкции, способных в любой момент нанести ущерб человеческому организму.

Представляется очевидным, что в такой ситуации государство должно предпринимать превентивные меры по защите населения от возможных угроз. И если уровень правовой

культуры и этических норм в обществе слабо подвержен коррекции путем законодательных изменений, то остаются еще как минимум три рычага, которыми можно манипулировать за счет изменения действующего законодательства:

- ограничение возможности анонимного распространение информации посредством электронных коммуникаций [14];
- популяризация правил использования электронных коммуникаций;
- увеличение стоимости размещения информации в сети Интернет.

На первый взгляд наиболее перспективным из перечисленных направлений воздействия может показаться последнее, построенное на предположении, что рентабельность большинства мошеннических схем происходит из низкой стоимости «старта бизнеса».

Если в реальном мире мошенникам, для успешной имитации деятельности крупной компании, требуется, как минимум, арендовать офис, то сейчас любой школьник может анонимно получить адрес в сети Интернет и сымитировать на бесплатном сервере сайт крупной фирмы или даже государственного учреждения. Причем, при должной сноровке этого школьника, доказать его причастность к мошенничеству будет невозможно.

Государство, конечно, может установить высокую ценовую планку на используемые при разработке сайтов сервисы, но это, во-первых, приведет лишь к тому, что мошенники начнут использовать зарубежные сервисы, находящиеся в юрисдикции других государств, а, во-вторых, будет несправедливо по отношению к добропорядочным пользователям, стремящимся размещать объективно полезную для общества информацию.

Другое направление превентивного решения проблемы – научить каждого пользователя сети Интернет принципам её безопасного использования. Однако, учитывая ситуацию с обучением правилам дорожного движения, свидетельства которой мы ежедневно наблюдаем на улицах нашей страны, а также специфику IT-отрасли, эту идею можно смело отнести к утопическим.

Способы мошенничества посредством электронных коммуникаций развиваются быстрее информационных технологий и нет никакой возможности подготовить всё население страны, от мала до велика, до уровня опытного пользователя персонального компьютера, научить отличать правду от лжи, и совершенствовать их навыки по мере появления новых способов мошенничества.

Справедливости ради, следует отметить, что, несмотря на прогнозируемую малоэффективность работ в этом направлении, различными организациями предпринимаются разнообразные попытки популяризации правил безопасного поведения в среде компьютерных коммуникаций. Так в столичных школах уже распространяются брошюры «Безопасный интернет – детям» и «Безопасный интернет – рекомендации экспертов родителям», а так же проводятся родительские собрания и специальные уроки, посвященные вопросам обеспечения безопасности детей и подростков в сети Интернет [15].

Однако самым перспективным направлением для вмешательства государства является ограничение возможности анонимного распространения информации. Что произойдет, если все действия пользователя в сети Интернет будут привязаны к его персоне в реальном мире? Добропорядочные пользователи продолжат беспрепятственно общаться и делиться друг с другом достоверной информацией, как это происходит и в реальном мире. В то время как мошенники, похитители, террористы, педофилы и другие лица, представляющие общественную опасность, больше не смогут скрываться за масками и будут вынуждены либо прекратить вредоносную деятельность посредством электронных коммуникаций, либо продолжать её, но уже от своего настоящего лица, рискуя в любой момент ответить за слова и поступки по всей строгости закона.

Теоретически не сложно разработать комплекс из программ и идентификационных устройств, способный обеспечить однозначную привязку каждого слова, размещенного в сети Интернет, к идентификатору разместившего его гражданина государства, а затем законодательно обязать всех желающих размещать информацию в сети Интернет делать это исключительно посредством разработанной системы. Техно-

логии необходимые для реализации подобной системы уже изобретены и активно повсеместно российскими гражданами.

Так уже несколько лет успешно функционирует Единая Система Идентификации и Аутентификации – российская государственная информационная система, обеспечивающая доступ (регистрацию и аутентификацию) к сайтам государственных структур и некоторых коммерческих организаций, а так же доступ пользователей к сети Интернет в некоторых публичных местах.

Разумеется, разработка программного обеспечения (в том числе и систем управления информационным наполнением электронных ресурсов разных типов), рассчитанного на новые принципы авторизации и размещения информации, потребует дополнительного выделения крупных сумм из государственного бюджета. Но следует помнить о том, что на другой стороне весов находятся не только материальные средства и интересы граждан, но и их жизни.

К тому же, нет необходимости идентифицировать пользователей, использующих компьютерные сети исключительно для получения информации. Для превентивного устранения угроз достаточно требовать подтверждения личности лишь от тех пользователей, которые планируют размещать информацию или контактировать с другими пользователями. Таким образом, борьба с анонимностью не должна повлечь за собой каких-либо существенных трат со стороны законопослушных граждан и стать препятствием в получении информации.

К сожалению, в случае ограничения перечисленных мероприятий рамками одного государства, при существующем уровне технического развития, его граждане просто переключатся на ресурсы других государств, поэтому успешная реализация вышеприведенного решения возможна лишь в альянсе с другими крупными государствами, либо при условии ограничения доступа к электронным коммуникациям по модели КНР.

Однако, на данный момент, представители власти придерживаются мнения, что существующих в РФ ограничений вполне достаточно [16] и в переходе на ограничение электронных коммуникаций рамками государства по китайской модели нет особой необходимости [17]. Да и, взвешивая гипотетические перспективы включения крупных государств в подобный проект, можно прийти к выводу, что, в ближайшее годы, согласованные мероприятия по превентивному предотвращению угроз, порождаемых бесконтрольными электронными коммуникациями, не представляются осуществимыми.

Таким образом, государству остаются лишь малоэффективные меры защиты интересов граждан. Такие как сравнительно недавно внедренные в российское законодательство положения о локализации персональных данных [18] и механизме досудебных блокировок электронных ресурсов. Безусловно, указанные меры не способны нейтрализовать весь перечень угроз, возникающих в бесконтрольном пространстве компьютерных сетей. Поэтому было бы логично дополнить отечественное законодательство нормами, предписывающими блокировку ресурсов содержащих: мошенническую информацию, чертежи оружия и любую информацию, несущую угрозу здоровью граждан.

Для повышения скорости устранения угроз, можно сделать процесс блокировки электронных ресурсов общенародным. Такой механизм можно реализовать на базе действующего портала Госуслуги. Например: пользователь указывает в специальной форме заявки ссылку на информацию, которую считает вредоносной и обосновывает в сопроводительном комментарии необходимость ее блокировки, эта ссылка и сопроводительный комментарий пользователя появляются перед несколькими сотнями других граждан (выбранных случайно), которые за нее голосуют, если ссылка набирает определенный процент голосов за удаление, то она отправляется на проверку специалисту сервиса Госуслуги, выбранному так же в случайном порядке из числа прочих специалистов, тот проверяет ссылку и, если соглашается с решением пользователей о необходимости блокировки, то вносит ссылку в реестр запрещенных ресурсов.

Вышеприведенные рекомендации завершают данный обзор угроз, порождаемых бесконтрольным развитием электронных коммуникаций, и путей борьбы с ними. Оправдаются ли сделан-

ные нами прогнозы и найдут ли своё применение предложенные нами рекомендации, покажет время. Но, по мнению авторов, здоровым информационным обществом сможет стать только то общество, в котором каждый его участник будет нести персональную ответственность за распространяемую информацию, и на данном этапе российское государство делает лишь первые шаги на пути к его становлению.

Список литературы

1. *O'Reilly T.* What Is Web 2.0 [Электронный ресурс] – Режим доступа: http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=2 (дата обращения 28.04.2017).
2. *Волкова Е., Лебедева Н.* В контакте со смертью // Российская Газета, № 109 (6977), С.13.
3. *Комаров А. А.* Мошенничество в глобальной сети Интернет как одна из основных угроз становлению информационного общества в России // Право и безопасность. – 2008. – № 3. – С. 23-26.
4. Распоряжение Правительства РФ от 17.11.2008 N 1662-р (ред. от 08.08.2009) «О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 г.» // Собрание законодательства РФ, 24.11.2008, N 47, ст. 5489.
5. Откровение святого Иоанна Богослова // Библия. Книги Ветхого и Нового Завета, канонические. – М.: Российское Библейское общество, 2001.
6. Евангелие от Луки // Библия. Книги Ветхого и Нового Завета, канонические. – М.: Российское Библейское общество, 2001.
7. Позиция Церкви в связи с развитием технологий учета и обработки персональных данных. Официальный сайт Московского Патриархата. [Электронный ресурс] – Режим доступа: http://www.patriarchia.ru/db/text/2775107 (дата обращения 28.04.2017).
8. *Еляков А. Д.* Спам как общественная опасность // Вестник Самарского государственного экономического университета. – 2007. – № 8. – С.139-142.
9. *Levshin N.* Modern pseudo-christian ideas as an obstacle on the way of social and economic development of Russia // Научный альманах стран Причерноморья. – 2016. – № 3 (7). – С. 35-37.
10. *Чуев С. В.* Коммуникативные технологии политического менеджмента: учебное пособие. – Ростов н/Д: Издательский центр ДГТУ, 2016, С.124-125.
11. Мифология средней школы. «Российская Газета» от 03.06.2011. [Электронный ресурс] – Режим доступа: http://www.rg.ru/2011/06/03/platobrazovanie-site.html (дата обращения 28.04.2017).
12. Страшилки о «платной» школе снова будоражат Интернет: «Российская Газета» от 07.02.2013. [Электронный ресурс] – Режим доступа: http://www.rg.ru/2013/02/07/shkola-site.html (дата обращения 28.04.2017).
13. *Смоленский М. Б., Левшин Н. С.* Правовая культура и безопасность. – Ростов н/Д: Российская таможенная академия, Ростовский филиал, 2016. – 96 с.
14. *Линьков А. В., Гордеева М. Е.* Анализ проблемы анонимности в Интернете: пользователь, государство, злоумышленник // Перспективные информационные технологии (ПИТ 2015): труды Международной научно-технической конференции. – Самара: СГАУ, 2015. – С. 272-279.
15. Московские власти подчистят интернет для детей. Известия. [Электронный ресурс] – Режим доступа: http://izvestia.ru/news/672668
16. Путин посчитал «пока достаточными» существующие в РФ ограничения интернета. Интерфакс. [Электронный ресурс] – Режим доступа: http://www.interfax.ru/russia/556568 (дата обращения 28.04.2017).
17. Глава СПЧ выступил против ограничения интернета по модели КНР в России. Интерфакс. [Электронный ресурс] – Режим доступа: http://www.interfax.ru/russia/547176 (дата обращения 28.04.2017).
18. *Смоленский М. Б., Левшин Н. С.* Локализация персональных данных граждан РФ как составляющая экономической и национальной безопасности России // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2016. – № 2 (69). – С. 111-114.