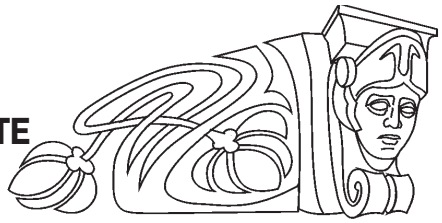
УДК 34.01

ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ И ПОЛИТИКО-ПРАВОВЫЕ МЕХАНИЗМЫ ЗАЩИТЫ ЛИЧНОСТИ В РОССИЙСКОМ ИНТЕРНЕТЕ



Ф. А. Вестов, Е. О. Глухова

Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского
E-mail: vestovfa@mail.ru, Kuzminaeo@list.ru

О. Ф. Фаст

Саратовская государственная юридическая академия
E-mail: Fastolga@mail.ru

В статье анализируются проблемы защиты прав и свобод личности и информации о человеке в сети Интернет. Определяются признаки безопасности и ее обеспечения силовыми структурами правоохранительных органов России.
Ключевые слова: безопасность, личность, права и свободы, силовые структуры, сеть Интернет, информация правоохранительные органы.

Law Enforcement and the Political and Legal Mechanisms for the Protection of the Person in Russian Internet

F. A. Vestov, O. E. Glukhova, O. F. Fast

The article analyzes the problems of protection of the rights and freedoms of an individual, and information about an individual on the Internet. The author defines the security characteristics and its provision by the law enforcement bodies of Russia.
Key words: security, individual rights and freedoms, law enforcement agencies, Internet, information law enforcement.

DOI: 10.18500/1818-9601-2017-17-3-337-340

Актуальность данной темы состоит в том что в современных условиях развития правового государства России Интернет стал неотъемлемой частью общества и человека. Люди, выставляя информацию о себе в социальных сетях, подвергаются опасности, сами того не подозревая. Этим пользуются мошенники. Поэтому в данное время очень актуальной является защита прав и свобод личности и информации о ней в Интернете силовыми структурами правоохранительных органов правового государства[1]. В этой связи возникает ряд вопросов: 1) регулирование сетей – это регулирование частной сферы или публичной сферы?; 2) должно ли государство защищать присутствие гражданина в Интернете как его частную жизнь или как его публичную деятельность?; 3) кто должен отвечать за то, что обеспечивает ребенку до 14 лет свободный доступ в публичную сферу коммуникаций?; 4) в какой мере политически оправданно вмешательство правоохранительных органов в деятельность соответствующих коммуникационных систем в целях обеспечения информационной безопасности человека?

Говоря об информационной безопасности, мы имеем в виду защиту информации от случайных или злонамеренных действий, которые могут привести к нанесению ущерба как информации так и ее владельцам.

Стандартная модель безопасности характеризуется тремя категориями:

– конфиденциальность – это состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на это право[2];

– целостность – это такое размещение информации, когда исключается несанкционированная модификация информации;

– доступность – избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа к ней.

Информация в Сети охватывает все стороны жизнедеятельности человека и общества. Пользователи доверяют данной форме коммуникаций себя и свою деятельность. Однако опыт работы в области компьютерных технологий полон примеров недобросовестного использования ресурсов Интернета.

Одними из условий проникновения злоумышленников в компьютерные сети является беспечность и неподготовленность пользователей сетей. Яркими примерами этого являются: вовлечение через Интернет террористами новых членов, которые переезжают в самопровозглашенное Исламское государство (запрещенное в России), а также создание сетей в Интернете по вовлечению школьников, студентов (под благовидными предлогами) для совершения самоубийств. В этой связи возникает необходимость еще в детском саду, обязательно в школе обучать пользователей Интернета обеспечению личной безопасности.

Беспечность характерна не только для рядовых пользователей, но и для части специалистов в области компьютерной безопасности. Вместе с тем причина не только в халатности, но и в сравнительно небольшом опыте специалистов по обеспечению безопасности в сфере информационных технологий. Связано это со стремительным ростом рынка сетевых технологий и самой сети Интернет в условиях глобального развития политических и иных процессов во всемирном пространстве. Неподготовленность специальных служб стран приводит к политическим катаклизмам, свержению суще-

ствующих режимов вне рамок конституционного поля этих государств, возможности вмешательства во внутриполитические процессы извне, в том числе осуществлению «цветных» революций (Ирак, Ливия и др.) с использованием возможностей Интернета.

С учетом зарубежного опыта в России предприняты меры институционального характера по недопущению незаконных политических преобразований с использованием возможностей Глобальной сети. Так, согласно Указу Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», запрещено подключение информационных систем информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, или информации, владельцами которой являются госорганы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, которые могут использоваться для передачи информации через государственную границу РФ, в том числе Интернет[3].

Одной из основных политических проблем в этой сфере является, на наш взгляд, безопасность персональных данных. Каждый имеет право на неприкосновенность его частной жизни, на тайну переписки, телефонных переговоров, телеграфных и иных сообщений.

Надо отметить, что информация о гражданах (персональные данные в настоящее время находятся в многочисленных базах государственных и частных учреждений: здравоохранения по месту жительства, банковских системах, пенсионных фондах, избирательных списках, данных правайдеров о пользователях Интернета. Эти базы данных, как правило, недостаточно защищены. К ним имеет доступ множество людей, контроль над которыми не установлен. В данном случае личность, т. е. ее персональные данные, не защищены от различных злоупотреблений. Для современных хакеров не является преградой даже хорошая защита системы, не говоря уже о конфиденциальности персональных данных в «бытовых» системах.

Вместе с тем такая информация неизбежно появляется при электронных денежных расчетах по кредитным карточкам и в особенности при онлайновой торговле. При этом интернет-сайт выполняет функцию прилавка обычного магазина, а с 1994 г., когда были изобретены cookies (специальные файлы, которые позволяют идентифицировать посетителя того или иного интернет-сайта), «продавцы» этого магазина стали различать покупателей, ранее бывших анонимными.

На начальной стадии находится в России реальная защита авторских прав на интеллектуальную собственность. Российское законодательство в сфере национальной безопасности, а в частности Закон РФ от 5 марта 1992 г. № 2446-I «О безопасности», под безопасностью понимает состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. В связи с этим важное политическое значение имеет правовое урегулирование защищенности указанных интересов при обмене данными в сети Интернет[4]. Это подтверждается практикой выборов в США, где в результате политического противостояния избранный президент и через сто дней не имет возможности нормально исполнять свои обязанности.

В Интернете право на жизнь, свободу и безопасность включает в себя следующее:

– защиту от преступлений в любых формах. Каждый должен быть защищен от всех форм преступлений, в том числе и совершенных с помощью Интернета, включая преследования и злоупотребления своей цифровой идентификацией и неправомерное использование персональных данных;

– безопасность в Интернете. Каждый человек имеет право на обеспечение безопасного соединения с Интернетом и безопасную деятельность в Сети. Право на безопасное использование Интернета также следует из права на свободу выражения своего видения развития тех или иных процессов в обществе, так как полная актуализация права на выражение невозможна при небезопасном характере соединения. Такие угрозы, как распространение вирусов, кража личных данных и виртуальной идентификации и 42 другие угрозы, таким образом, должны предотвращаться правоохранительными органами[5].

В Интернете право на неприкосновенность частной жизни включает следующее:

– национальное законодательство о неприкосновенности частной жизни;

– политика конфиденциальности в Интернете. Политика конфиденциальности и настройки всех услуг должны быть изложены четко и ясно, находиться в легкодоступном месте на ресурсах, а управление настройками конфиденциальности должно быть комплексным и удобным в использовании[6].

Право на частную жизнь должно защищаться по стандартам конфиденциальности IT-системы, обеспечивая защиту всех элементов систем от несанкционированного доступа к IT-системам без согласия:

– право на виртуальную личность. Каждый человек имеет право на виртуальную личность: виртуальная человеческая личность неприкосновенна. Цифровые подписи, имена пользователей, пароли, PIN-коды не должны использоваться или изменяться другими лицам без согласия владельца.

– право на анонимность и использование шифрования. Каждый человек имеет право общаться анонимно в Интернете; право на использование технологии шифрования для обеспечения безопасного частного и анонимного общения;

– свобода от слежки. Каждый имеет право свободно общаться без произвольного наблюдения или перехвата информации или угрозы наблюдения или перехвата информации;

– свобода от клеветы. Интерпретируется данное ограничение следующим образом: никто не должен подвергаться незаконным посягательствам на его честь и репутацию в Интернете. Каждый человек имеет право на защиту от таких посягательств. Право на защиту частной жизни непосредственно связано с правом на защиту репутации, чести и достоинства.

Электронно-цифровая подпись обеспечивает защиту аутентификации и целостности электронных документов. Она может использоваться при необходимости контроля с целью удостоверения личности подписавшего электронный документ, а также при проверке, было ли содержание подписанного документа изменено. 10 января 2002 г. Президентом РФ был подписан Закон «Об электронной цифровой подписи». Исходя из вышеизложенного, сложно сделать вывод о том, где ответственность за сохранность сведений о частной жизни возлагается на государство в лице ответственных за это органов, а где гражданин, пользуясь сетью Интернет, становится участником публичной сферы деятельности и определяется его мера ответственности. Эти вопрсы требуют теоретико-политического осмысления и правового разрешения.

Одна из самых острых и актуальных тем – защита детей от информации, могущей нанести им вред, особенно когда она распространяется по Интернету. Наиболее наглядно тема защиты детей может быть проиллюстрирована на примере порнографии. Если до интернет-эпохи порнографические материалы можно было получить только в специальных магазинах, по почте и из рук в руки, то в настоящее время эти сведения стали значительно доступнее. Характерно, что качественное увеличение степени доступности изменило характер самой порноиндустрии – она диверсифицировалась, колоссально выросла ее спецификация. Государственный контроль оборота порнографических материалов в новых условиях стал намного более сложной задачей. Однако самым неприятным феноменом стал не рост порноиндустрии как отрасли, а легкость доступности материалов для несовершеннолетних. Феномен порнографии онлайн является распространенным аргументом сторонников введения способов и процедур ограничения доступа к интернет-контенту и к самому Интернету[7].

Эти способы включают:

1) добровольную инсталляцию самими пользователями на собственных машинах программ контент-фильтрации;

2) юридическое принуждение интернет-провайдеров инсталлировать программы или специальное оборудование («железо») для фильтрации на различных узлах обработки данных;

3) классическую меру воздействия – административное и/или уголовное преследование хозяев порнопорталов, открытых в нарушение закона, регулирующего оборот порнографической продукции;

4) юридически закрепленную процедуру верификации возраста пользователя в публичных местах, интернет-кафе и публичных Wi-Fi-зонах) с целью выбора профиля фильтрации;

5) создание и пропаганду общественной системы жалоб на порнографические сайты с целью их добавления в «черные списки»;

6) глубокую фильтрацию порнографического контента на узлах сопряжения национального Интернета и Глобальной сети с целью изоляции национальной сети от зарубежного антиморального контента на основании нормативно-правовых актов различного уровня.

Использование методов (2) и (6) сопряжено с негативными эффектами, связанными с несовершенством систем фильтрации, вследствие которых неизбежны технические ошибки, из-за которых в «черные списки» попадают сайты, не содержащие порнографии. В связи с этим особое значение имеет профессиональная подготовка сотрудников специальных подразделений правоохранительных органов, которые контролируют безопасность сети Интернет, выявляют наличие в выложенной информации оснований для привлечения к уголовной[8] или административной ответственности лиц, осуществивших несанкционированный доступ к информации. Вместе с тем значение имеет установление степени виновности собственников телекоммуникационных сетей связи, которые используются преступными сообществами, запрещенными организациями (Исламское государство и др.) в целях осуществления террористических актов (Россия, Франция, Англия и др.), склонения несовершеннолетних к самоубийству и других опасных преступлений. В данной ситуации важной становится проблема ответственности родителей или лиц, их заменяющих, которые должны осуществлять контроль за пользование возможностями Интернета детьми. В этом направлении помочь родителям может повышение их компетентности в данной сфере по ограничению доступа детей к Интернету. Помимо установления повышенной правовой ответственности взрослых за поведение детей, глубокой проработке подлежит проблема политической корректности вмешательства правоохранительных органов в сферу реализации по-

литических свобод подрастающего поколения и формирования из них ответственных граждан за свою страну.

Примечания

1 См.: *Вестов Ф. А., Фаст О. Ф.* Правовое государство : теоретическое проектирование и современная политическая практика / под ред. Н. И. Шестова. М. : Проспект, 2016.

2 См.: *Партыка Т. Л., Попов И. И.* Информационная безопасность : учеб. пособие. 3-е изд. М. : Форум, 2008.

3 См.: О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена : указ Президента РФ от 17 марта 2008 г. № 351 (с изм. и доп. от 21.10.2008, 14.01.2011, 25.07.2014, 22.05.2015. Доступ из справ.-правовой системы «Гарант» ; Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных : утв. постановлением Правительства РФ от 17 ноября 2007 г. // Рос. газ. 2007. 21 нояб.

4 См.: Доктрина информационной безопасности Российской Федерации : утв. указом Президента РФ от 5 декабря 2016 г. № 646. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html) (дата обращения: 25.05.2017).

5 См.: *Левова И., Шуклин Г., Винник Д.* Права интернет-пользователей : Россия и мир, теория и практика / Ассоциация интернет-издателей. М. : Кабинетный ученый, 2013.

6 См.: *Безбогов А. А.* Методы и средства защиты компьютерной информации : учеб. пособие. Тамбов : Изд-во Тамб. гос. техн. ун-та, 2008.

7 См.: Детская порнография : модель законодательства и всемирный обзор. 2010. URL: http://sartraccc.ru/Pub_inter/ kindporno.pdf (дата обращения: 25.05.2017).

8 См.: *Вестов Ф. А., Глухова Е. О.* Российское уголовное право : учеб. пособие (Общая часть, тема 1–9). Саратов : Саратовский источник, 2016.

Образец для цитирования:

Вестов Ф. А., Глухова Е. О., Фаст О. Ф. Правоохранительные органы и политико-правовые механизмы защиты личности в российском Интернете // Изв. Сарат. ун-та. Нов. сер. Сер. Социология. Политология. 2017. Т. 17, вып. 3. С. 337–340. DOI: 10.18500/1818-9601-2017-17-3-337-340.

Cite this article as:

Vestov F. A., Glukhova O. E., Fast O. F. Law Enforcement and the Political and Legal Mechanisms for the Protection of the Person in Russian Internet. *Izv. Saratov Univ. (N. S.), Ser. Sociology. Politology,* 2017, vol. 17, iss. 3, pp. 337–340 (in Russian). DOI: 10.18500/1818-9601-2017-17-3-337-340.