

Патраков А. В.

# ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА

*В статье рассматриваются проблемы обеспечения информационной безопасности системы электронного правительства. Автор считает актуальным сегодня подготовку системы нормативных правовых актов, регламентирующих вопросы информационного взаимодействия государства, граждан и бизнеса, а также предусматривающих использование информационно-коммуникационных технологий в новых административных процессах. Совершенствование нормативно-правовой базы позволит устранить отставание законодательства в этой области от потребностей общества и характера общественных отношений, а также создать целостную правовую систему регулирования государственных услуг, оказываемых через информационно-телекоммуникационные сети.*

**Ключевые слова:** электронное правительство, кибербезопасность, информационная безопасность, служебная тайна.

Patrakov A. V.

# PROBLEMS OF INFORMATION SECURITY SYSTEMS E-GOVERNMENT

*This article discusses the information security system of e-government. The author considers relevant today training system of normative legal acts regulating the issues of information cooperation between the state, citizens and businesses, as well as incorporating the use of information and communication technologies in the new administrative processes. Improving the regulatory framework will eliminate the backlog of legislation in this area on the needs of society and the nature of social relations, and create a coherent legal system of regulation of public services provided through information and telecommunications networks.*

**Keywords:** e-government, cyber security, information security, official secrecy.

Одним из ключевых проблем в сфере информационной безопасности в целом, а также кибербезопасности в частности, является вопрос обеспечения информационной безопасности системы электронного правительства. Угрозы безопасности инфраструктуры электронного правительства, как крупнейшей в

России государственной информационной системы, имеют широчайший спектр. Это могут быть внутренние угрозы (со стороны людей, имеющих доступ к инфраструктуре электронного правительства), внешние (со стороны внешних по отношению к системе пользователей, киберпреступников, киберспецслужб), а

также угрозы объективного характера (потеря информации вследствие техногенных катастроф, природных катаклизмов). Поэтому при проектировании системы обеспечения информационной безопасности для инфраструктуры электронного правительства упор был сделан на комплексный подход. Система интегрирует разнородные средства защиты информации, необходимые для нейтрализации угроз безопасности для всех ее компонент, в единую взаимосвязанную среду, обеспечивающую выполнение целевых задач по информационной безопасности, вытекающих из моделей угроз и моделей нарушений, общесистемной политики безопасности и частных разделов политики безопасности.

Информационная безопасность является одной из важных компонент предоставления государственных услуг в электронном виде. При создании единого портала государственных услуг проводилась работа по анализу возможных угроз, на основе которых сформированы требования по защите информации при использовании портала государственных услуг. В системе безопасности портала используется обширный набор механизмов безопасности: межсетевые экраны, средства анализа содержимого, средства предотвращения вторжений, антивирусные средства защиты информации, средства мониторинга и контроля защищенности.

Программное обеспечение портала государственных услуг проходит сертификацию по требованиям информационной безопасности и отсутствию недеklarированных возможностей. Вместе с этим портал государственных услуг аттестован по требованиям ФСТЭК на обработку конфиденциальной информации и персональных данных по требованиям класса К1.

Для доступа на портал используется система аутентификации на основе электронной подписи, реализованная с помощью решений, прошедших сертификацию в ФСБ. Также для обеспечения защищенного межсетевого взаимодействия органов исполнительной власти и организаций, оказывающих государственные услуги, используется система защищенного документооборота. На уровне субъектов РФ утверждаются требования к информационной безопасности электронного правительства, регламентирующие принципы обеспечения информационной безопасности, требования к подсистемам защиты информации.

Основную платформу системы электронного правительства составляет телекоммуникационная инфраструктура ОАО «Ростелеком» – защищенная, сертифицированная корпоративная сеть передачи данных. Все внутренние каналы связи в рамках инфраструктуры электронного правительства защищены средствами криптографической защиты.

В соответствии со своим назначением и политикой информационной безопасности электронного правительства система не накапливает данных, связанных с персональной информацией граждан. Система призвана синхронизировать использование многочисленных учетных данных, которые ведутся различными ведомствами в соответствии с их полномочиями.

Обеспечение необходимого уровня информационной безопасности, в первую очередь персональных данных граждан, является одной из первоочередных проблем реализации программы электронного правительства, которая вызывает обоснованные опасения. И, несмотря на все преимущества электронного правительства, к вопросу информационной безопасности стоит подходить очень серьезно.

Несмотря на масштабы и темпы внедрения инфраструктуры электронного правительства существует ряд проблем, которые необходимо решить для успешного функционирования данной системы.

Во-первых, необходимо отметить, что наряду с переводом государственных услуг в электронный вид в настоящее время в отдельных федеральных законах имеются положения, ограничивающие предоставление государственных и муниципальных услуг в многофункциональных центрах и через портал государственных услуг. К таким положениям относятся нормы федеральных законов, прямо или косвенно ограничивающие и (или) создающие предпосылки для ограничения предоставления государственных и муниципальных услуг по принципу «одного окна», включающие обязательность предоставления заявителем документов, необходимых для получения государственных услуг, исключительно в орган, предоставляющий государственные услуги; наличие в федеральном законе требования получения результата государственной услуги заявителем исключительно в органе, предоставляющем государственные услуги; необходимость осу-

ществления личного взаимодействия заявителя уполномоченными представителями органов, предоставляющих государственные услуги, в целях совершения отдельных действий и процедур.

Во-вторых, выступая в качестве посредника между федеральными органами исполнительной власти, органами власти субъектов РФ, организациями, предоставляющими государственные услуги, и получателями государственных услуг, многофункциональные центры напрямую могут повлиять на результат оказания услуг, что может привести к негативным последствиям как для получателя услуги, так и для органа, ее предоставляющего. В свою очередь, законодательно не закреплена ответственность многофункциональных центров за ненадлежащее исполнение возложенных на них обязанностей в соответствии с нормативными правовыми актами и соглашением о взаимодействии.

Федеральный закон «Об организации предоставления государственных и муниципальных услуг»<sup>1</sup> лишь ссылается на то, что соглашения о взаимодействии, заключаемые между многофункциональными центрами и федеральными органами исполнительной власти, органами государственных внебюджетных фондов, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, должны включать ответственность сторон за неисполнение или ненадлежащее исполнение возложенных на них обязанностей.

Решением вышеупомянутых проблем может стать принятие законопроекта, внесенного в Государственную Думу 7 марта 2012 г. – проект федерального закона № 33022-6 «О внесении изменений в отдельные законодательные акты Российской Федерации в целях устранения ограничений для предоставления государственных и муниципальных услуг по принципу «одного окна»<sup>2</sup>. Цель – устранить ограничения для предоставления государственных и муниципальных услуг по принципу «одного окна». Проектом вносятся изменения в 23 закона в следующих сферах общественных отношений: образование и наука, здравоохранение, соцзащита, содействие занятости населения, имущественные отношения, предпринимательская деятельность, подтверждение гражданско-правового статуса и др.

Очевидной проблемой внедрения системы электронного правительства мы видим в

недостаточности и недоработанности нормативно-правовой базы в области регулирования электронного документооборота, в области использования электронной подписи.

Предоставление государственных услуг в электронной форме включает в себя не только организацию межведомственного электронного взаимодействия, но и электронную подачу заявления на предоставление услуги, отслеживание хода ее предоставления. Однако здесь имеется противоречие с Указом Президента № 351 от 17.03.2008<sup>3</sup>, согласно которому запрещается подключение к сети Интернет государственных информационных систем, содержащих сведения, составляющие служебную тайну (к числу которой относятся результаты предоставления государственных услуг). Таким образом, складывается парадоксальная ситуация: законом о предоставлении государственных услуг и другими подзаконными актами предусматривается предоставление государственных услуг в электронной форме, а техническая возможность такого предоставления, по сути, запрещена указом Президента.

На наш взгляд, указанные проблемы могут быть решены путем принятия Федерального закона «О служебной тайне» и согласования нормативных правовых документов, учитывая особенности правоотношений, возникающих в процессе предоставления государственных услуг. Категорирование на законодательном уровне информации, обрабатываемой органами власти в процессе предоставления государственных услуг, позволит определить принципы и правила ее использования в целях удовлетворения потребностей заказчиков государственных услуг и выполнения возложенных на органы власти обязанностей по их предоставлению.

Правительством Российской Федерации устанавливаются Правила использования простых электронных подписей при оказании государственных и муниципальных услуг, в том числе правила создания и выдачи ключей простых электронных подписей, а также перечень органов и организаций, имеющих право на создание и выдачу ключей простых электронных подписей в целях оказания государственных и муниципальных услуг. Также должны быть определены виды электронных подписей, использование которых допускается при обращении за получением государственных и муниципальных услуг. На сегодняшний день Правительством установлены

лишь правила использования усиленной квалифицированной электронной подписи органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой и требования к обеспечению совместимости средств электронной подписи при организации электронного взаимодействия органов исполнительной власти и органов местного самоуправления между собой. Вопрос использования электронной подписи получателями услуг пока нормативно не урегулирован.

Остро стоит проблема обеспечения информационной безопасности инфраструктуры электронного правительства. В процессе предоставления государственных услуг происходит накопление большого объема как персональных данных, так и служебной информации органов государственной власти. На данном этапе вопрос информационной безопасности рассматривается лишь поверхностно и упоминается в качестве одного из показателей системы электронного правительства. Не разработаны документы, регламентирующие порядок обработки персональных данных и служебной информации на уровне федеральных и региональных органов власти. Без должного уровня информационной безопасности технологические и социальные последствия компьютеризации и информатизации различных сфер общественной жизни весьма плачевны как для бизнеса и государства, так и для человека, учитывая то, что большая часть персональных данных о потребителях услуг будет сконцентрирована в рамках единой системы электронного правительства. Наблюдается несоответствие типовых форм документов по государственным услугам требованиям Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации<sup>4</sup>.

В целях обеспечения безопасности информации, обрабатываемой в системе электронного правительства, необходимо в первую очередь привести законодательство в соответствие с требованиями времени и развитием информационных технологий, провести единую политику защиты информации, разработать единую методику оценки угроз для объектов информатизации, входящих в электронное правительство. Необходимо также уточнить сферы компетенции федеральных органов исполнительной власти в

области информационной безопасности. Для обеспечения приемлемого уровня защиты информационных ресурсов электронного правительства необходимо создание комплексной системы обеспечения информационной безопасности. Система обеспечения информационной безопасности должна консолидировать правовые, технологические, организационные, технические и физические меры и способы защиты. Она должна иметь продуманную долгосрочную политику, обеспечивающую повышение уровня информационной безопасности в соответствии с появлением новых источников и средств реализации угроз.

Наряду с проблемами в области права, существуют технологические и социальные проблемы, препятствующие оказанию государственных услуг в электронном виде. А. А. Тедеев выделяет следующие проблемы развития и внедрения концепции электронного правительства:

- низкий уровень развития телекоммуникаций;
- низкий уровень компьютерной культуры населения и должностных лиц государственных органов власти и органов местного самоуправления;
- психологическая неготовность общества<sup>5</sup>.

Многие граждане до сих пор не имеют представления о системе электронного правительства, не говоря уже о посещении портала государственных услуг и многофункциональных центров. Граждане по-прежнему сами предоставляют в государственные органы полный комплект документов, необходимый для получения государственной услуги. Причина такой ситуации кроется в том, что ведомства, возможно, не донесли до граждан информацию о том, что теперь нет необходимости предоставления документов в бумажном виде, но также не исключено, что граждане не имеют доверия к электронным документам.

Еще одной проблемой, препятствующей эффективному развитию системы электронного правительства, является «информационное неравенство» – понятие, которое отражает социальную дифференциацию населения по принципу возможностей доступа к информационно-коммуникационным технологиям и выступает одной из серьезных угроз реализации информационных прав человека в условиях глобализации информационной среды.

Для осуществления качественного прорыва в данной сфере, о котором сегодня так много говорится, необходимым представляется подготовка системы нормативных правовых актов, регламентирующих вопросы информационного взаимодействия государства, граждан и бизнеса, а также предусматривающих использование информационно-коммуникационных технологий в новых

административных процессах. Совершенствование нормативно-правовой базы позволит устранить отставание законодательства в этой области от потребностей общества и характера общественных отношений, а также создать целостную правовую систему регулирования государственных услуг, оказываемых через информационно-телекоммуникационные сети.

---

### Литература

<sup>1</sup> См.: ФЗ «Об организации предоставления государственных и муниципальных услуг» от 27.07.2010 № 210-ФЗ // Российская газета. 2010. 30 июля.

<sup>2</sup> Проект федерального закона № 33022-6 «О внесении изменений в отдельные законодательные акты Российской Федерации в целях устранения ограничений для предоставления государственных и муниципальных услуг по принципу “одного окна” // <http://www.garantkey.ru/monitoring/buhgalter/1703/index.php>.

<sup>3</sup> Указ Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03. 2008 № 351 // СЗ РФ. 2008. № 12. Ст. 1110.

<sup>4</sup> Постановление Правительства РФ «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 № 687 // СЗ РФ. 2008. № 38. Ст. 4320.

<sup>5</sup> Тедеев А. А. Информационное право: учебник. М.: Изд-во Эксмо, 2005. С. 75.

### References

<sup>1</sup> Federal Law «On provision of state and municipal services» as of 27.07.2010 No. 210-FZ // Rossiiskaya gazeta. July 30, 2010.

<sup>2</sup> Draft Federal Law No.33022-6 «On amendments in certain statutory acts of the Russian Federation for the purposes of removal of constraints for provision of state and municipal services on one-stop» // <http://www.garantkey.ru/monitoring/buhgalter/1703/index.php>.

<sup>3</sup> Presidential Decree of the Russian Federation «On information security measures in the process of use of information and telecommunication networks of international informational exchange» as of 17.03. 2008 No. 351 // Sobranie Zakonodatel'stva Rossiiskoi Federatsii. 2008. No. 12. Art. 1110.

<sup>4</sup> Decision of the Government of the Russian Federation «On affirmation of the Resolution on peculiar features of processing of personal data performed without the use of automation means» as of 15.09.2008 No.687 // Sobranie Zakonodatel'stva Rossiiskoi Federatsii. 2008. No.38. Art. 4320.

<sup>5</sup> Tedeev A. A. Informatsionnoe pravo: uchebnik [Informational law: Course book]. Moscow: Izd-vo Eksmo, 2005. p. 75.

---

**Патраков Алексей Владимирович**, студент магистратуры кафедры конституционного и административного права ЮУрГУ. E-mail: avpatrakov@gmail.com.

**Patrakov Alexey**, graduate student of constitutional and administrative law SUSU. E-mail: avpatrakov@gmail.com.