УДК 332

Епифанцева Ксения Сергеевна
кандидат социологических наук,
главный специалист-эксперт департамента
развития законодательства Министерства юстиций РФ
ksenia44@yandex.ru
Казакова Елизавета Игоревна
стажер Совета Федерации Федерального Собрания РФ,
студентка 4 курса
Российской академии народного хозяйства и государственной службы
при Президенте Российской Федерации,
ksenia44@yandex.ru
Самыгин Сергей Иванович
доктор социологических наук, профессор кафедры
управления персоналом и социологии
Ростовского государственного экономического университета
darya.maksimovich@gmail.com
Ksenia S. Epifantseva
candidate of sociological Sciences,
chief specialist-expert of Department of development of legislation of the Ministry of justice of the Russian Federation
ksenia44@yandex.ru
Elizaveta I. Kazakova
Intern of the Federation Council of the Federal Assembly
of the Russian Federation 4-th year student Russian Academy of National Economy and Public Administration
when the President of the Russian Federation,
ksenia44@yandex.ru
Sergei I. Samygin
doctor of sociological sciences, professor of department of personnel management and sociology of the Rostov state economic university
darya.maksimovich@gmail.com

Ресурсы Интернет в государственном управлении: проблемы обеспечения национальной безопасности

Web Resources in Public Administration: problems of national security

Аннотация. *Статья посвящена проблеме обеспечения национальной безопасности в сфере взаимодействия электронного правительства с гражданами. В статье рассматриваются основные моменты, несущие риски и угрозы оказания государственных услуг при использовании ресурсов Интернет. Авторы приходят к выводу о том, что проблема обеспечения национальной безопасности российского государства входит в число*

ключевых социально-информационных проблем и условий постоянного взаимодействия при формировании системы государственных услуг посредством ресурсов Интернет.

Ключевые слова: *ресурсы Интернет, государственное управление, электронное правительство, национальная безопасность, сетевое взаимодействие.*

Abstract. *The article deals with the problem of national security in the field of e-government interaction with citizens. This article discusses highlights of carrying the risks and threats for public services by using Internet resources. The authors conclude that the problem of ensuring the national security of the Russian state is one of the key social issues of information and conditions of constant interaction in the formation of public service system through Internet resources.*

Keywords: *resources of Internet, public administration, e-government, national security, networking.*

Глобальная сеть Интернет и новые информационные технологии открывают широкие горизонты и небывалые возможности во многих сферах человеческой деятельности, и сектор государственного управления не является исключением, поскольку информационная открытость государственного управления – это один из важных признаков демократизации современного российского государства. Еще в 2000 г. Россия в числе ведущих мировых держав приняла Глобальную хартию Информационного общества (ИО). При этом, ИО рассматривается как образ жизни, образование, работа, взаимодействие правительства и гражданского общества. В настоящее время можно отметить, что электронные государственные услуги, онлайн-медицина, образование, финансовые и транспортные услуги, а так же электронная библиотека и многое другое, связанное с Интернет, стали привычной частью жизни все большего числа россиян. По данным различных экспертных групп, включая фонд «Общественное мнение», в России в 2015-2016 г. г. было 83-84 млн. постоянных интернет-пользователей, а суточная интернет-аудитория достигала 66 млн. человек. В связи с этим, в последние годы были уточнены задачи электронного правительства. Из них приоритетными стали: предоставление единой точки непрерывного доступа граждан и организаций к электронным услугам; преодоление информационного неравенства; возможность непрерывного обучения; развитие цифровой экономики и т. д. Причём, под цифровой экономикой подразумевается деятельность, в которой ключевыми факторами производства являются данные, а технологии анализа больших объемов данных – главными способами повышения её эффективности. Как тут не вспомнить крылатую фразу: кто владеет информацией, тот владеет миром!

Однако при этом неисчерпаемые ресурсы Интернет порождают новые серьезные проблемы, связанные не только с информационной безопасностью простых граждан, но и с национальной безопасностью российского общества и государства. К сожалению, сегодня и в других государствах даже самые

серьезные спецслужбы не в состоянии полностью защитить государственные структуры от утечки государственной информации. В этом контексте стоит вспомнить события 2011г., когда на сайте «Викиликс» появилась секретная информация из правительственных учреждений США. Утечка конфиденциальной информации из правительственных структур России, как указывает С.А. Овчинников, также имела место [1]. По сообщению «Ведомостей» от 31 марта 2012 года, в результате утечки данных пострадало до 10 млн. держателей пластиковых карт Visa и MasterCard: «крупнейшие платежные системы – Visa и MasterCard заявили о том, что информация о держателях платежных пластиковых карт может оказаться под угрозой по вине третьей стороны» [2].

По данным Совета Безопасности РФ в 2016 г. на российские информационные ресурсы было совершено более 70 миллионов компьютерных атак или почти втрое больше, чем в 2015 г. Более 60 процентов атак совершалось из-за рубежа. При этом удалось пресечь работу 1300 источников атакующего воздействия внутри страны и почти 500 за рубежом, а так же отразить атаки на 5 крупнейших российских банков (Российская Газета 15.02.2017 г.).

Очевидно, что доверие российских граждан к государственным услугам, предоставляемым электронным правительством, напрямую зависит от уровня обеспечения безопасности его инфраструктуры, ибо в процессе оказания государственных услуг осуществляется не только передача и обработка персональных данных граждан, но и иная конфиденциальная информация: политического, экономического, социально-психологического, медицинского, юридического и иного характера. При этом, все субъекты информационного сетевого взаимодействия должны отчетливо понимать: каким образом, и насколько надежно и серьезно будут защищены их персональные данные в процессе интерактивного взаимодействия правительства с обществом.

В этой связи сегодня перед российским государством остро стоит важная задача по обеспечению национальной безопасности, которая продиктована наличием реально существующих угроз на разных уровнях, а именно: угрозы на уровне личности – ее правам и свободам; угрозы на уровне социума – его демократическим социально-политическим институтам и на государственном уровне – угрозы независимости, целостности государства.

В нормативно-правовых документах отражены и законодательно закреплены основные понятия и определения, связанные с безопасностью личности, общества и государства. Так, в соответствии со Стратегией национальной безопасности РФ до 2020 года дано следующее определение: «Национальная безопасность – состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства»[3].

Заметим, что приведенное определение охватывает широкий спектр проблем обеспечения безопасности, в том числе распространяется и на ресурсы Интернет-коммуникации в системе государственного управления [4]. В частности, понятийный аппарат Стратегии национальной безопасности, среди прочих важных компонентов, содержит компонент «средства обеспечения национальной безопасности» – Интернет, программные, телекоммуникационные технологии, включая информационные средства, применяемые в процессе обеспечения национальной безопасности с целью сбора, формирования, обработки, передачи или приема информации о состоянии национальной безопасности и мерах по ее укреплению. Т.е., обеспечение национальной безопасности в сфере деятельности электронного правительства представляет собой такой способ функционирования системы электронного правительства, которое сможет обеспечивать сохранение конфиденциальности информации в процессе сетевого взаимодействия[5].

В феврале 2015 года в Москве на 17-ом Национальном форуме информационной безопасности подробно рассматривались вопросы обеспечения национальной безопасности в области внедрения Интернет-технологий в государственное управление, которые, по мнению выступившего на форуме первого заместителя председателя комитета Государственной Думы по безопасности и противодействию коррупции Магомеда Вахаева, обрели всеобщий характер.

Особое внимание в рамках форума было уделено проблемам организации, внедрения и защите электронного документооборота не только на федеральном, но и на региональном уровне. Отмечалось, что особую важность приобретает проблема обеспечения безопасности при обработке документов и личных персональных данных граждан; предоставлении гражданам информации о начислении налогов на имущество и доходы, получении адресной социальной помощи; постановке на регистрационный учет или снятии с учета транспортных средств и др. Как только во взаимодействии государственного управления и гражданина появляется электронный документооборот с возможными правовыми последствиями, возникает необходимость в обеспечении сервисов безопасности.

Подробно обсуждались также и актуальные проблемы идентификации и аутентификации при реализации сетевого интерактивного взаимодействия российских граждан с электронным правительством. К сожалению, по свидетельству многих участников форума, российская нормативная база пока существенно отстает от нормативной базы некоторых других стран, поэтому сегодня настоятельно необходимы доработки как на уровне законов, так и на уровне требований обеспечения безопасности и достоверности электронной идентификации участников электронного взаимодействия.

По сути дела, вышеназванный форум дал старт широкому обсуждению стратегических направлений развития российского информационного общества. В декабре 2016 г. Совет Безопасности РФ опубликовал на своем сайте проект «Стратегии развития информационного общества в Российской

Федерации на 2017-2030 года» (далее – Стратегия). В проекте Стратегии среди национальных приоритетов выделено – свободное, устойчивое и безопасное взаимодействие между гражданами, органами государственной власти, органами местного самоуправления и организациями. А среди задач – обеспечение поэтапного перехода государственных органов власти и органов местного самоуправления к использованию единой инфраструктуры электронного правительства, входящей в информационную структуру Российской Федерации, комплексная защита которой, в свою очередь, должна обеспечивать обнаружение, предупреждение и ликвидацию последствий компьютерных атак.

Как справедливо отметил еще в 2012 г. С.А. Овчинников, в современных условиях внедрения ресурсов Интернет в деятельность электронного правительства и перевода оказания государственных услуг гражданам в электронный вид потребуется постоянное наращивание мощности государственных центров обработки данных, внедрение систем, действующих на принципе «облачных технологий», концентрации в них значительной по объему критически важной информации как на уровне государства, так и на уровне граждан. «В этих условиях с целью защиты информационных ресурсов и предотвращения нанесения ущерба интересам граждан и государства необходимо использовать комплекс мер по обеспечению информационной национальной безопасности»[7, с. 179].

Безусловно, обеспечение национальной безопасности в государственном управлении, использующем ресурсы Интернет, должно сочетаться с информационной открытостью демократического управления. Информационная открытость включает в себя две составляющие. Первая составляющая информационной открытости – право граждан на информацию и обязанности электронного правительства ее предоставлять. Согласно ч.4 ст. 29 Конституции РФ каждый имеет право свободно искать, получать, воспроизводить и распространять информацию всякими законными способами. Исключением является информация, ограниченная в обороте законодательно. Вторая составляющая – обязанность предоставить информацию. Таким образом, информационная открытость связана с обеспечением доступа к информации и предоставлением последней для удовлетворения различного рода потребностей граждан, при условии, что информация не ограничена и не запрещена в обороте законом. При этом важно заметить, что действующее законодательство устанавливает и ограничивает информационную открытость для обеспечения национальной безопасности российского государственного управления, а также жизни и здоровья граждан [8]. Данные ограничения, как указывает современный исследователь применения интернет-технологий в государственном управлении РФ Е.А. Филиппов, должны быть зафиксированы в законе. На сегодняшний день, по мнению Е.А. Филиппова, информационная открытость ограничена в двух областях: а) области, затрагивающей государственную тайну и б) области, затрагивающей иную охраняемую законом информацию:

профессиональную (служебную) тайну, налоговую тайну, сведения персональных данных, постановки медицинского диагноза и т.д.[9].

По свидетельству С.А. Овчинникова и Е.В. Ковалевой, каждого российского гражданина «посчитали» минимум 17 раз: при выдаче свидетельства о рождении, выдаче паспорта, военного билета, при постановке на учет в пенсионном фонде, налоговой службе, фонде социального страхования, а также при посещении поликлиники и стационара и пр. «Насколько надежно защищены реестры, регистры и кадастры, знают только их владельцы и об этом можно судить только по косвенным признакам, хотя факты утечки конфиденциальных сведений на последнее время все более часто становятся достоянием гласности» [10, с. 207].

Итак, проблема обеспечения национальной безопасности российского государства входит в число ключевых социально-информационных проблем и условий постоянного взаимодействия при формировании системы государственных услуг посредством ресурсов Интернет не только в целях повышения эффективности системы государственного управления, но и в целях улучшения качества жизни российских граждан[11].

Интеграция ресурсов Интернет в сферу государственного управления, интенсивность развития электронного правительства по причине активного принятия различных федеральных и региональных программ построения информационного российского социума должны увеличиться. Поэтому решение проблемы обеспечения национальной безопасности в электронном правительстве России, с одной стороны, должно повысить социальное доверие российских граждан к реализации государственных услуг, предоставляемым государственным управлением посредством ресурсов Интернет; с другой, – обеспечить защиту государственного электронного управления от угроз национальной безопасности России.

Литература:

1. *Овчинников С.А. Организационно-кадровый аспект безопасности: проблема инсайдеровский угрозы электронному правительству // Вестник Саратовского государственного социально-экономического университета. 2012. №4 (43).С.178-181.*
2. *[Электронныйресурс]. - URL:http://money.ru.msn.com/news/232803 (дата обращения: 08.02.2016).*
3. *Официальный сайт Совета безопасности Российской Федерации // Стратегия национальной безопасности Российской Федерации до 2020 года [Электронный ресурс]. - URL: http://www.scrf.gov.ru/documents/1/99.html.*
4. *Гафиатулина Н.Х., Самыгин С.И. Социальная коммуникация в профилактике конфликтов: учебно-методическое пособие. М.: РУСАЙНС, 2016. 164 С.*
5. *Верещагина А.В., Самыгин С.И. Гафиатулина Н.Х. и др. Социология безопасности. М.: ИНФРА-М, 2017. 264 с.*

6. *[Электронный ресурс]. - URL: http://www.fa.ru/dep/press/about-us/Pages/Informatsionnaya-bezopasnost-–-neotemlemaya-chast-n.aspx (дата обращения: 11.02.2016).*

7. *Овчинников С.А. Указ. Соч.*

8. *MShakhbanova M.M., Gafiatulina N.Kh., Vereshchagina A.V., Samygin S.I., Imgrunt S.I.Social and economic consequences of regional ethnic migration for national security and social health of the Russian youth // Social Science (Pakistan). 2016. T.11. № 16. C. 3886-3893.*

9. *Филиппов Е.А. Особенности использования интернет-технологий в государственном управлении Российской Федерации // Пробелы в российском законодательстве. Юридический журнал. 2011. №5. С. 270-273.*

10. *Овчинников С.А., Ковалева Е.В. Вопросы защиты информации при переходе на оказание государственных услуг в электронном виде // Вестник Саратовского социально-экономического университета. 2012. №5 (44). С. 205-207.*

11. *Гафиатулина Н.Х., Олишевский Д.П. Социально-политические процессы: вопросы прогнозирования // Хроники объединенного фонда электронных ресурсов Наука и образование. М., 2015. №11 (78). С. 110.*

Literature:

1. *Ovchinnikov S.A. Organizational and human resources aspect of security: the problem of insider threats e-Government // Bulletin of Saratov State Socio-Economic University. 2012. №4 (43). 178-181.*

2. *[Electronic resource]. - URL: http: //money.ru.msn.com/news/232803 (reference date: 02.08.2016).*

3. *The official website of the Russian Federation Security Council // Russian National Security Strategy until 2020 [electronic resource]. - URL: http://www.scrf.gov.ru/docu-ments/1/99.html.*

4. *Gafiatulina N.K, Samygin S.I. Social communication in the prevention of conflicts: a teaching aid. M.: RUSAYNS, 2016. 164 p.*

5. *Vereschagina A.V., Gafiatulina N.K., Samygin S.I. Sociology of security. M .: INFRA-M, 2017. 264 p.*

6. *[Электронный ресурс]. - URL: http://www.fa.ru/dep/press/about-us/Pages/Informatsionnaya-bezopasnost-–-neotemlemaya-chast-n.aspx (дата обращения: 11.02.2016).*

7. *Ovchinnikov S.A. Decree. Vol.*

8. *Shakhbanova M.M., Gafiatulina N.Kh., Vereshchagina A.V., Samygin S.I., Imgrunt S.I.Social and economic consequences of regional ethnic migration for national security and social health of the Russian youth // Social Science (Pakistan). 2016. T.11. № 16. Pp. 3886-3893.*

9. *Filippov E.A. Features of the use of Internet technologies in the public administration of the Russian Federation // Gaps in Russian legislation. Legal Journal. 2011. №5. Pp. 270-273.*

10. Ovchinnikov S.A.,Kovalev E.V. The protection of information during the transition to the provision of public services in electronic form // Saratov Journal of Socio-Economic University. 2012. №5 (44). Pp. 205-207.

11. Gafiatulina N.K., Olishevsky D.P. Socio-political processes: forecasting questions // the combined fund of electronic resources Chronicle Science and Education. M., 2015. №11 (78). P. 110.