Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Забайкальский государственный университет»

На правах рукописи

Кухарский Артем Николаевич

Информационная безопасность политического процесса как элемент государственного и муниципального управления России

Специальность 23.00.02 – Политические институты, процессы и технологии

Диссертация на соискание ученой степени
кандидата политических наук

Научный руководитель:
д-р полит. наук, профессор
Бейдина Татьяна Евгеньевна

Чита – 2019

Оглавление

ВВЕДЕНИЕ

Актуальность темы исследования. Интерес научного сообщества к исследованию проблемы информационной безопасности политического процесса, ее предпосылок и факторов обеспечения возник из-за тенденций глобализации, появления новых центров силы и политических акторов. Один из наиболее влиятельных мировых политических трендов современного периода проявляется в росте взаимозависимости стран и народов. Это служит внешней предпосылкой для развития информационной безопасности политического процесса. Информационная безопасность характеризуется как позитивными факторами, так и возрастанием международных информационных угроз в экономической, военной и политической сферах жизнедеятельности государства, что ослабляет стабильность и сотрудничество стран на мировой арене.

Данные информационные угрозы реализуются через определенных внешнеполитических акторов, для которых характерно стремление к главенствованию в информационном пространстве путем информационного воздействия на политические объединения, личность, социальные группы. Помимо внешнеполитической составляющей угрозы реализуются посредством применения современных технологий в сфере информатизации, направленных на развал политической системы, дестабилизацию традиционных ценностей, размывание личности, нарушение территориальной целостности и суверенитета государств. Это характеризует внутриполитическую составляющую информационной безопасности.

Очевидно, что исследователи ставят в центр внимания проблемы, связанные с разработкой принципов и новых технологий информационного манипулирования в политической сфере, а также определение источников борьбы

с возникающими угрозами и реализацией информационной безопасности на глобальном, региональном и национальном уровнях. Теоретический аспект темы исследования в целом связан с показом значимости внешнеполитических и внутриполитических составляющих информационной безопасности. Теоретическую и практическую актуальность имеет научное осмысление вопроса, ориентированное на определение понятия «информационная безопасность», рассматриваемая некоторыми исследователями как безопасность сетей и информационных систем, трактуемых как кибербезопасность. Другая часть разработчиков рассматривают информационную безопасность как манипулирование сведениями, воздействие информацией на сознание общества, пропаганда в сети интернет.

Не менее актуальным и важным в исследовании информационной безопасности является изучение угроз безопасности с применением информационно-компьютерных технологий при осуществлении и реализации общественно-опасных преступлений, совершение террористических актов, вмешательство в дела суверенных государств, развязывание межгосударственных конфликтов, разжигание межэтнической розни.

Информационная безопасность в концептуальных и ключевых нормативно-правовых документах многих государств рассматривается как важнейшая составляющая национальной безопасности. Таким образом, изучение целей, задач, сравнительный анализ подходов и ключевых проблем обеспечения безопасности политического процесса, оценка результативности и продуктивности этих подходов представляются весьма актуальной проблемой.

В ходе реализации социально-политических преобразований в современный период общество в России трансформировалось в качественно новое состояние, которое характеризуется, в частности, сращиванием органов государственной и муниципальной власти с бизнес-структурами, что обуславливает пересмотр целей и задач государственных и муниципальных органов, органов обеспечения национальной, региональной и муниципальной безопасности.

Переход в новое состояние государства связан с возникновением совершенно новых угроз как национальной безопасности в целом, так и ее основных составляющих – социально-экономической, общественной и информационной безопасности. Как отмечал М.Ю. Величко: «Возникновение данных угроз на фоне медленного и недостаточного развития российской законодательной базы связано, прежде всего, с бурным развитием рыночных отношений, интеграцией России в глобальные мировые социально-политические отношения. Все это требует переосмысления и разработки новых механизмов организации противодействия национальной и транснациональной преступности, а также нейтрализации внутренних и внешних угроз»[1].

Одним из важных условий социально-политического развития России является обеспечение низкого уровня криминальности. В настоящее время рычаги и методы борьбы с преступностью не в полной мере соответствуют состоянию и динамике развития организованной преступности, уменьшению оборота наркотических средств, торговле людьми, экстремизму, терроризму.

Революция в сфере информатизации способствует созданию и внедрению в социально-политическую систему инноваций, которые достаточны для эффективного решения современных государственных и региональных проблем, для обеспечения рационального использования природных ресурсов, политического, социального, духовного и культурного развития общества, а также его безопасности. Этими же достижениями в сфере информатизации пользуется преступность, которая имеет неограниченные возможности по доступу к информационно-техническим и экономическим ресурсам, их увеличению и приспособлению в своей деятельности. Эти обстоятельства требуют переосмысления взглядов и разработку новых концептуальных подходов к вопросам информационной безопасности, решения проблем с такими явлениями как кибертерроризм и киберпреступность для обеспечения как информационной

[1] Величко, М. Ю. Информационная безопасность в деятельности органов внутренних дел: теоретико-правовой аспект [Электронный ресурс]. – Режим доступа: http://lawtheses.com/informatsionnaya-bezopasnost-v-deyatelnosti-organov-vnutrennih-del-teoretiko-pravovoy-aspekt#ixzz5IfdhgH2A.

безопасности, так и в целом национальной. Актуальность информационной безопасности в условиях интеграции информационных систем и изучение разнообразных рычагов ее управления вызвано тем, что проблематику информационной безопасности исследуют традиционно, в первую очередь, с технических позиций.

Степень исследованности проблемы. С технической точки зрения оценка информационной безопасности началась с 1816 г. с анализа возникающих средств информационной коммуникации. В тот период основной задачей стояла защита основных информационных баз данных государства и общества. После 1816 г. с появлением средств электро и радиосвязи начали применять помехоустойчивое кодирование сигнала. С 1935 г. зафиксировано направление на сочетание технических и организационных мер для повышения защищённости радиолокационных и гидроакустических средств. С 1946 г. начинается внедрение в деятельность общества и государства электронно-вычислительной техники, что ориентировало информационную безопасность на ограничение доступа к оборудованию. 1965 г. характеризуется созданием информационно-коммуникационных сетей. В тот период перед информационной безопасностью стояла задача переработки и передачи администратору управления сетевыми ресурсами. С 1973 г. обеспечение информационной безопасности связано с разработкой новых критериев безопасности, сгруппировалось новое сообщество «хакеров», целью которых было нанести ущерб информационным каналам отдельных пользователей, организациям и целым странам. Информация стала важнейшим ресурсом государства, а обеспечение её безопасности − важнейшей составляющей национальной безопасности. В этот период сформировалась новая отрасль международного права − информационное право. 1985 г. обусловлен созданием мировых информационно-коммуникационных сетей с применением космических технологий обеспечения.

В исследовании политического процесса активно участвовали классики политической мысли Д. Истон, Г. Алмонд, Б. Пауэлл. Для исследования

информационной безопасности подходит информационно-коммуникативная модель политической системы Карла Дойча и его характеристика, напрямую связанная с особенностями информационно-коммуникативного действия. Оценка политического процесса дана Н.А. Барановым[2], М.Ю. Зеленковым[34], А.В. Новиковой[5], которая характеризует внешнеполитические и внутриполитические процессы и дает характеристику многоаспектности политического процесса. Очевидно, что политический процесс включает: «субъекты и участники процесса; объект процесса; средства, методы, ресурсы, которые связывают субъект и объект–цель»[6]. Субъектами политического процесса являются «политические системы, политические институты (государство, гражданское общество, политические партии и т. д.), организованные и неорганизованные группы людей, индивиды»[7]. Наш авторский подход учитывает данные характеристики политического процесса, но выделяет в качестве важного актора политического процесса информационную составляющую и ее ресурсное обеспечение в лице информационной безопасности политического процесса.

Развитие информационной безопасности рассматривают как одну из основных частей национальной безопасности, системы политического процесса, управления и реализации государственной и муниципальной службы, такие исследователи как: А.Ю. Азаров[8], М.Д. Березинская, Г.Е. Веселов, Н.А. Лызь, А.Е. Лызь[9], К.О. Полыхань[10], В.П. Талимончик[11], П.Ю. Филяк, В.М. Шварев[12],

---

[2] Баранов, Н.А. Политические отношения и политических процесс в современной России. – СПб.: БГТУ, 2004. – 30 п.л.

[3] Зеленков, М.Ю. Политология. – М.: Юрид. ин-т МИИТа, 2009. – 302с.

[4] Зеленков, М.Ю. Политология [Электронный ресурс]. – Режим доступа: https://psyera.ru/politicheskiy-process-ponyatie-sushchnost-i-soderzhanie_8232.htm.

[5] Новикова, А.В. Регионы РФ в политическом процессе модернизирующейся России, и их влияние на обеспечение национальной безопасности /А.В. Новикова. – Забайкальский гос. ун-т. – Чита: ЗабГУ, 2016.-230с.

[6] Зеленков, М.Ю. Политология [Электронный ресурс]. – Режим доступа: https://psyera.ru/politicheskiy-process-ponyatie-sushchnost-i-soderzhanie_8232.htm.

[7] Там же.

[8] Березинская, М.Д., Азаров, А.Ю. Информационная безопасность современного общества // В сборнике: Информационное общество: состояние, проблемы, перспективы, 2017. – С. 45-52.

[9] Лызь, Н.А., Веселов, Г.Е., Лызь, А.Е. Информационно-психологическая безопасность в системах безопасности человека и информационной безопасности государства // Известия ЮФУ. Технические науки. 2014. – № 8 (157). – С. 58-66.

J. Andress[13], L. Gordon[14], R. Moore[15], T. Schlienger[16], J. Wiley[17]. Информационную безопасность в системе национальной безопасности изучали такие авторы как: Е.В. Алексеева[18], А.А. Галушкин[19], Е.А. Проценко[20], М.А. Сизьмин[21], В.П. Шерстюк[22], M.T. Ahles[23], D.M.J. Fiddner[24], D.C. Gompert[25], J.F. Stickman[26].

Можно отметить работы по информационной безопасности политического процесса: Я.В. Катуева[27], К.И. Кузнецова[28], Н.И. Стуженко, А.А. Чеботаревой[29],[30],

---

[10] Полыхань, К.О. Проблемы и особенности состояния информационной безопасности в соответствии с доктриной информационной безопасности Российской Федерации // Устойчивое развитие науки и образования. 2019. – № 5. – С. 154-160.

[11] Талимончик, В.П. Информационная безопасность в контексте всеобъемлющей системы международной безопасности // Известия высших учебных заведений. Правоведение. 2008. – № 2 (277). – С. 103-111.

[12] Филяк, П.Ю., Шварев В.М. Обеспечение информационной безопасности организации на основе системы менеджмента информационной безопасности // Информация и безопасность. 2015. – Т.18. – № 4. – С. 580-583.

[13] Andress, J The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice // — Syngress, 2014. − 240 p.

[14] Gordon, L. The Economics of Information Security Investment : / Lawrence Gordon, Martin Loeb // ACM Transactions on Information and System Security. – 2002. – Vol. 5, no. 4 (November).

[15] Moore, R. Investigating High Technology Computer Crime: − 2nd ed.− Boston : Anderson Publ., 2011. − 318 p.

[16] Schlienger, T. Information security culture: From analysis to change / Thomas Schlienger, Stephanie Teufel // South African Computer Journal. – Pretoria, South Africa, 2003. – Vol. 31.

[17] Wiley, J. Security and Preservation Considerations // Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management / Bidgoli, H. – John Wiley & Sons, 2006. – Vol. 3.

[18] Алексеева, Е.В. Доктрина информационной безопасности Российской Федерации как ключевой аспект правового обеспечения национальной безопасности в информационной сфере // Ленинградский юридический журнал. 2016. – № 4 (46). – С. 97-103.

[19] Галушкин, А.А. К Вопросу о значении понятий «национальная безопасность», «информационная безопасность», «национальная информационная безопасность» // Правозащитник. 2015. –№ 2. –С. 8.

[20] Проценко, Е.А. Информационная безопасность субъектов Российской Федерации как составная часть национальной безопасности России // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2006. –№ 25. –С. 111-115.

[21] Сизьмин, М.А. Информационная (информационно-психологическая) безопасность в структуре национальной безопасности (на примере США и России) // Известия Иркутской государственной экономической академии (Байкальский государственный университет экономики и права). 2014. –№ 3. –С. 28.

[22] Шерстюк, В.П. Информационная безопасность в системе обеспечения национальной безопасности России, федеральные и региональные аспекты обеспечения информационной безопасности // Информационное общество. 1999. – № 5. – С. 3-5.

[23] Ahles, M.T. Information systems impact on national security execution: a model for the security assistance training program execution in security assistance offices // thesis, degree: Ph.D., degreeYear: 2002, Institute: Union Institute and University, adviser: Cherie Lohr.

[24] Fiddner, D.M.J. Hhe information infrastructure system as a national security risk and united states information infrastructure system national security policy, 1990—2000 // thesis, 2004, Degree: Ph.D. DegreeYear: 2003, Institute: University of Pittsburgh, Adviser: Phil Williams.

[25] Gompert, D.C. National security in the information age // Naval War College Review. 1998. – Т.51. – № 4. – С. 22-40.

[26] Stickman, J.F. Assessing United States information assurance policy response to computer-based threats to national security // thesis, degree: D.P.A., degreeYear: 2001, Institute: University of Southern California, adviser: Chester A. Newland.

[27] Катуева, Я.В. Характеристики информационного пространства в задаче управления безопасностью субъекта федерации // Труды международного симпозиума Надежность и качество. 2010. – Т.1. –С. 23-24.

[28] Кузнецова, К.И. Информационная безопасность и проблема информационного неравенства в системе безопасности современного общества // В сборнике: ИНТЕЛЛЕКТУАЛЬНЫЙ ПОТЕНЦИАЛ XXI ВЕКА сборник статей международной научно-практической конференции: в 2 частях. 2018. – С. 192-195.

А.И. Шеметова[31], L. Freeman, S. Gartner[32], J. Hughes[33], M. Jessica[34], R. Lynne, A. Merwe[35], C. Pettey, G. Peace[36]. Отметим авторов, изучавших информационную безопасность в системе муниципального и государственного управления, среди которых: А.В. Баскаков, С.Е. Зайцев[37], А.Н. Ищенко, Р. Кулян, А.В. Нестеров[38], А.Г. Остапенко, А.Н. Прокопенко, Г.Л. Рогальский[39], А.А. Страхов[40],

---

[29] Чеботарева, А.А. Человек и электронное государство. Право на информационную безопасность // монография / А. А. Чеботарева; М-во образования и науки Российской Федерации, гос. образовательное учреждение высш. проф. образования «Читинский гос. ун-т» (ЧитГУ). Чита, 2011.

[30] Чеботарева, А.А. Обеспечение информационной безопасности личности: роль международной информационной безопасности и стратегического партнерства // Вестник Академии права и управления. 2016. – № 1 (42). – С. 48-51.

[31] Стуженко, Н.И., Шеметов, А.И. Информационное обеспечение управления безопасностью региона // Научный альманах. 2015. – № 10-3 (12). – С. 251-254.

[32] Pettey, C. Gartner Says Digital Disruptors Are Impacting All Industries; Digital KPIs Are Crucial to Measuring Success: – Gartner, Inc., 2017.

[33] Hughes, J. Quantitative Metrics and Risk Assessment : The Three Tenets Model of Cybersecurity : / J. Hughes, G. Cybenko // Technology Innovation Management Review. – Ottawa, Canada : Talent First Network (Carleton University), 2013. – August. – P. 15–24.

[34] Lynne, R. Jessica Moyer Cyber-security, cyber-attack, and the development of governmental response: the librarian's view // New Library World. 2004. –Т.105. – № 7-8. – С. 248-255.

[35] Merwe, V. Characteristics and Responsibilities involved in a Phishing Attack : / Loock, Marianne, Dabrowski, Marek // WISICT '05 Proceedings of the 4th international symposium on Information and communication technologies. — Cape Town, South Africa, 2005. – 3 January. – P. 249–254.

[36] Freeman, L. Peace G. Information Ethics: Privacy and Intellectual Property. – Hersey: Information Science Publishing, 2005.

[37] Зайцев, С.Е. Политики информационной безопасности в системах информационной безопасности // Научный вестник Московского государственного технического университета гражданской авиации. 2008. – № 137. –С. 37-44.

[38] Нестеров, А.В. Существует ли информационная безопасность, или некоторые аспекты законопроекта технического регламента «О безопасности информационных технологий» // Правовые вопросы связи. 2007. – № 1. – С. 31-35.

[39] Кулян, Р., Кулян, Р. Рогальский, Г.Л. Информационное обеспечение управления экономической безопасностью муниципального образования: временной аспект // Экономические науки. 2009. –№ 56. –С. 233-237.

[40] Ищенко, А.Н., Прокопенко, А.Н., Страхов, А.А Новая доктрина информационной безопасности Российской Федерации как основа противодействия угрозам безопасности России в информационной сфере // Проблемы правоохранительной деятельности. 2017. – № 2. – С. 55-62.

В.Б. Щербаков[41], Y. Cherdantseva[42], C. Gray[43], A. McCullagh[44], A.J. Ramirez[45], S. Samonas[46].

Теоретико-методологической основой исследования являются работы зарубежных и отечественных исследователей по защите информации и информационной безопасности, среди которых труды: М.В. Арсентьева[47], Ю.М. Батурина[48], Н.И. Ветрова[49], В.Б. Вехова[50], Б.В. Здравомыслова[51], А. Крутских[52], Ю.И. Ляпунова[53], В.В. Панферовой[54], Н.Н. Потрубач[55], О. Г. Сивакова[56], Л. Черняк[57].

Многие ученые ограничивают информационную безопасность исключительно до проблемы защищенности компьютерной информации. Как утверждает О.В. Генне: «Для реализации результативных подходов

---

[41] Баскаков, А.В., Остапенко, А.Г., Щербаков, В.Б. Политика информационной безопасности как основной документ организации в создании системы информационной безопасности // Информация и безопасность. 2006. – Т.9. –№ 2. –С. 43-47.

[42] Cherdantseva, Y. Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals // Organizational, Legal, and Technological Dimensions of Information System Administrator / Y. Cherdantseva, J. Hilton. — IGI Global Publishing, 2013.

[43] Gray, C. Review: information security policies, procedures and standards: guidelines for effective information security management // ITNOW. 2003. – Т.45. –№ 2. –С. 30-b.

[44] McCullagh, A. Non-Repudiation in the Digital Environment : / Adrian McCullagh, William Caelli // Technology Innovation Management Review. – Chicago, USA : First Monday, 2000. – Vol. 8, no. 8 (August).

[45] Ramirez, A.J. Globalizacion y derecho social en Mexico. El entorno latinoamericano y las politicas sociales // thesis, degree: Dr., degreeYear: 2005, Institute: Universidad de Navarra (Spain).

[46] Samonas, S. The CIA Strikes Back : Redefining Confidentiality, Integrity and Availability in Security : [англ.] / Samonas, S., Coss, D. // Journal of Information System Security. – Washington DC, USA: Information Institute Publishing, 2014. – Vol. 10, no. 3.

[47] Арсентьев, М.В. Состояние информационной безопасности в России / М.В. Арсентьев // Информационные ресурсы России. 2003. – №2. – С. 19-21.

[48] Батурин, Ю. М., Жодзишскнй, А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юрид. лит., 1991. – 160 с.

[49] Ветров, П.И. Уголовное право. – М., 1999. – С. 183-184.

[50] Вехов, В.Б., Попова, В.В., Илюшин, Д.А. Тактические особенности расследования преступлений в сфере компьютерной информации: Науч.-практ, пособие. Изд. 2-е, доп. и испр. – М.: «ЛэксЭст», 2004. – 160 с.

[51] Здравомыслов, Б.В. Уголовное право Российской Федерации. Особенная часть / Под ред. Б.В. Здравомыслова. М., 1996. – С. 356.

[52] Крутских, А., Крамаренко, Г. Дипломатия и информационно-коммуникационная революция / А. Крутских, Г. Крамаренко // Международная жизнь. 2003. – №7. – С.102-113.

[53] Ляпунов, Ю.И., Пушкин, А.В. Преступления в сфере компьютерной информации // Уголовное право. Особенная часть / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. – М., 1998.

[54] Панферова, В. В. Информационная политика в современной России / В. В. Панферова // Социально-гуманитарные знания. 2005. – № 5. – С. 53-68.

[55] Потрубач, Н.Н. Проблемы информационной безопасности / Н.Н. Потрубач // Социально-гуманитарные знания. 1999. – №2. – С.264-273.

[56] Сиваков, О. Г. Актуальные проблемы информационной безопасности в научно-технической сфере / О.Г. Сиваков // Информационные ресурсы России. 2003. – № 4. – С. 25-28.

[57] Черняк, Л. Новые задачи информационной безопасности / Л. Черняк // Открытые системы. СУБД. 2005. – № 5/6. – С. 16-18.

целесообразно взаимоувязанное исследование множество факторов информационной безопасности»[58].

Становление и развитие информационной безопасности – интегральная проблема, в которой выделяются несколько уровней: процедурный, административный, законодательный и программно-технический. С точки зрения данных уровней существует потребность формирования теоретико-методологических принципов и положений информационной безопасности органов государственной и муниципальной власти.

Проблему информационной безопасности и ее государственное регулирование начали изучать во второй половине XX в. параллельно с развитием мирового обмена научно-техническими достижениями. Бесценный вклад в данную сферу внесли: А.Б. Антопольский[59], Г.Т. Артамонов[60], М.Д. Березинская, А.Ю.Азаров[61], И.Л. Бачило[62], А.Б. Венгеров[63], А.А.Галушкин[64], Я.Г. Дорфман[65], Г.В. Емельянов[66], В.А.Копылов[67], С.С. Куликов[68], В.Н. Лопатин, Г.Г. Почепцов[69], М.М. Рассолов[70], А.А. Чеботарева

---

[58] Генне, О.В. Основные положения стеганографии // Защита информации Конфидент. – 2001. – №3. – С.20-25.

[59] Антопольский, А.Б. Актуальные проблемы учета и регистрации информационных ресурсов // Проблемы информатизации. – 2001. – № 2.

[60] Артамонов, Г.Т. О противоречиях перехода к информационному обществу/ Г.Т.Артамонов//Вестник ВОИВТ. – 1998. – №3. – С.42–44.

[61] Березинская, М.Д., Азаров, А.Ю. Информационная безопасность современного общества // Информационное общество: состояние, проблемы, перспективы 2017. –С. 45-52.

[62] Бачило, И.Л., Лопатин, В.Н., Федотов, М.А. Информационное право. / Под ред. академика РАН Б. Н. Топорнина. СПб.: Издательство Р. Асланова «Юридический центр Пресс», 2005.

[63] Венгеров, А.Б. Право и информационное обеспечение АСУ / А.Б. Венгеров // Советское государство и право. – 1972. – № 8. – С. 28-36.

[64] Галушкин, А.А. К вопросу о значении понятий «национальная безопасность», «информационную безопасность», «национальная информационная безопасность» // Правозащитник. 2015. – № 2. – С. 8.

[65] Дорфман, Я.Г. Рецензия на книгу А.И. Михайлова, А.И. Черного, Р.С. Гиляревского «Основы научной информации» / Я.Г. Дорфман// Научно-техническая информация. – 1996. - № 7. – С. 46-47.

[66] Емельянов, Г.В., Стрельцов, А.А. Информационная безопасность России. Учебное пособие / Под ред. А.А. Прохожева. −М.: Всероссийский научно-технический информационный центр. 2000. – С. 34

[67] Копылов, В.А. Информационное право. – 2-е изд., перераб. и доп. - М.: Юристь, 2002. – 512с.

[68] Куликов, С.С. Управление информационной безопасностью информационно-телекоммуникационных систем, подвергающихся атакам типа «сетевой шторм» // Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем Остапенко А.Г. Сборник научных трудов. под ред. чл.-корр. РАН В.И. Борисова. Воронеж, 2013. – С. 032-047.

[69] Почепцов, Г.Г. Информационные войны, Серия: Образовательная библиотека. Издательство: Рефл-бук, 2001г. – 576 с.

[70] Рассолов, И.М. Информационное право / Рассолов И.М. - М.: Норма, Инфра: –М.: 2010. – 352 с.

и др. Среди зарубежных ученых можно отметить работы: J. Beniger[71], M. Castels[72], P. Ferdinand[73], B. Novick[74], J. Rondfeldt[75], N. Wiener[76], S. Wilbur[77], R. Wright[78].

Единственным политологом, рассматривающим информационную безопасность с позиции внешнего политического процесса, был доктор политических наук П.А. Махмадов[79]. С позиции внутреннего политического процесса информационная безопасность рассматривалась в Краснодаре[80], Ставрополе[81], а политологический анализ был осуществлен в Санкт-Петербурге[82]. Таким образом, как показывает степень научной разработанности проблемы, изучение информационной безопасности политического процесса на региональном и муниципальном уровнях проводилось недостаточно, а муниципальный уровень не затронут никем.

Объектом диссертационного исследования является информационная безопасность политического процесса в системе государственного, муниципального управления. Комплексность исследования информационной безопасности политического процесса связана с тем, что данное явление охватывает различные сферы жизнедеятельности государства.

---

[71] Beniger, J. The Control Revolution: Technological and Economic Origins of the Information Society, Cambridge, Mass., Harvard University Press, 1986.

[72] Castells, M. The Power of Identity. Maiden (Ma.) Oxford, Blackwell Publishers, 1997. Цит.по: Новая постиндустриальная волна на Западе: Антология. −Москва: Academia, 1999. –С. 494.

[73] Peter Ferdinand. The Internet, Democracy and Democratization. In Democratization, –Vol.7, –No.1, Spring 2000. – P.6.

[74] Noveck, B. Paradoxical Partners: Electronic Communication and electronic Democracy. In Democratization, – Vol.7, – No.1, Spring 2000. – P.32.

[75] Arquilla, J, and Ronfeldt D. eds., In Athena's Camp: Preparing for Conflict in the Information Age, Santa Monica, Calif.: RAND, MR-880-OSD/RC, 1997. –P.460.

[76] Винер, Н. Кибернетика. −М.: 1968.

[77] Shawn, P. Wilbur. «An Archaeology of Cyberspace. Virtuality, Community, Identity». In David Bell and Barbara Kennedy (Eds.) Cybercultures Reader. Routledge, 2000, – P.45.

[78] Wright, R. Three Scientists and Their Gods: Looking for Meaning in an Age of Information. −New York: Harper and Row, 1989. – P.5.

[79] Махмадов, П. А. Информационная безопасность в системе политической коммуникации: состояние и приоритеты обеспечения (на материалах государств Центральной Азии): дис. … д-ра полит. наук: 23.00.04 / Махмадов Парвиз Абдурахмонович, Душанбе, 2018. 323 с.

[80] Чайка, И. Г. Политические технологии обеспечения информационной безопасности региона: на примере Краснодарского края: дис. … к-та полит. наук: 23.00.02 / Чайка Иван Геннадьевич, Краснодар, 2010. 210 с.

[81] Проценко, Е. В. Информационная безопасность политической коммуникации в современной России: дис. … к-та полит. наук: 23.00.02 / Проценко Евгений Васильевич. Ставрополь, 2009. 199 с.

[82] Бородин, А. С. Информационная безопасность в современной России: политологический анализ: дис. … к-та полит. наук: 23.00.02 / Бородин Алексей Сергеевич. Санкт-Петербург, 2009. 211 с.

Предметом исследования является комплексный анализ обеспечения информационной безопасности политического процесса, в том числе в региональном аспекте.

Цель диссертационного исследования – определить эффективные направления и механизмы обеспечения информационной безопасности политического процесса государственного, муниципального управления России.

В исследовании были поставлены следующие **задачи**:

1. Осуществить анализ теоретических подходов к исследованию политического процесса, информационной безопасности и информационной интеграции как этапа развития государственного и муниципального управления России.

2. Создать модель информационной открытости и выявить направления информационных угроз для государственных и муниципальных органов власти.

3. Дать авторскую характеристику информационной безопасности органов власти на примере Забайкальского края и определить пути совершенствования информационной безопасности Забайкалья.

4. Выявить роль организационных механизмов защищенности информации в органах муниципальной власти и разработать предложения по улучшению информационной безопасности органов власти субъектов РФ.

Научной новизной исследования являются результаты комплексного анализа организационно-правовых механизмов и методов обеспечения информационной безопасности политического процесса государственного и муниципального управления России, к которым относятся:

1. Авторское обоснование информационной безопасности политического процесса с позиции защиты носителя власти, ресурсов, методов, исполнителей процесса.

2. Создание модели информационной открытости на основе оценки государственного и муниципального регулирования информационной

безопасности политического процесса с учетом угроз для государственных и муниципальных органов власти России.

3. Нахождение путей совершенствования защиты информационной безопасности Забайкальского края.

4. Разработка предложений по улучшению обеспечения информационной безопасности политического процесса.

Теоретическая и практическая значимость диссертации. Исследование проблемы информационной безопасности политического процесса показывает значимость информационной составляющей. Получение полной информации о функционировании политического процесса органов власти целесообразно с точки зрения важности информации для государства. Существует теоретическая необходимость регулирования организационно-правовых основ информационной безопасности как регионов, так и муниципалитетов. Результаты исследования могут быть применены при подготовке бакалавров, магистров, обучающихся на политических и социологических специальностях, а также могут быть полезны преподавателям на лекциях по политологии, национальной безопасности, геополитике, государственному, муниципальному управлению, аспирантам и специалистам. Практическая значимость работы заключается в возможности использования сформулированных положений, выводов в качестве инструментов и положений для государственной политики в сфере информационной безопасности. Результаты исследования могут содействовать дальнейшему анализу актуальных проблем информационной безопасности управления, исследованиям в сфере политологии и социологии. Практическая значимость результатов работы состоит в их направленности на решение проблем, стоящих перед государственными и муниципальными образованиями по обеспечению безопасности личности, общества и государства.

Методологические основы исследования. Методологию исследования составляют структурно-функциональный, институциональный, системный, информационно-коммуникативный подходы. Решение задач диссертационного

исследования осуществлялось с применением следующих методов: индукции, дедукции, компаративистского сравнения для сопоставления практик зарубежных стран по информационной безопасности и открытости власти. Применены также системный, структурно-функциональный и социологические методы. Указанные методы позволили охарактеризовать значимость информационной безопасности политического процесса и подробно изучить общественно-политическое мнение населения Забайкальского края по улучшению информационной безопасности органов власти посредством проведенного социологического опроса. Было опрошено 9 муниципальных районов Забайкальского края и более 300 чиновников. С применением метода контент-анализа был осуществлен анализ упоминаемости информационной открытости и интеграции в крае. Метод политического прогнозирования позволил сделать вывод о перспективах развития информационной составляющей политического процесса.

Положения, выносимые на защиту:

1. Существует многообразная трактовка понятия «информационная безопасность»: с позиции управления, организационного развития и политического процесса. Определение информационной безопасности как состояния защищенности, безусловно, целесообразно с позиции управления. С точки зрения организационного развития информационная безопасность политического процесса – это система мероприятий, направленных на административно-техническую защиту, прежде всего, конфиденциальных данных субъектов политического процесса и программно-системные механизмы реализации управленческих решений. Если рассматривать информационную безопасность политического процесса, нужно учесть специфику политического процесса и его элементов: акторов, государства как носителя власти, многообразных ресурсов институтов политического процесса. Мы даем синтезированное, авторское определение информационной безопасности политического процесса, которое объединяет все три трактовки с позиции управления, организационного развития и политического процесса. Поэтому,

информационная безопасность политического процесса – это защищенность субъектов политического процесса как системы административно-технических мероприятий, ориентированных на защиту носителей власти в лице государства, партий, общественных организаций, многообразных ресурсов и методов противодействия информационным угрозам. И в этом научная значимость работы.

2. Создана модель информационной открытости с целью совершенствования информационной безопасности и внедрения информационных технологий, сети «интернет» для обеспечения открытости органов власти Забайкальского края для населения. Информационная открытость органов муниципальной власти предполагает равный доступ граждан к информационным системам города Читы и муниципальных районов, в том числе «Газимуро-Заводского района», где расположено знаменитое Быстринское месторождение золота, меди и железа, разрабатываемое Норникелем. Информационная открытость служит основой информационной безопасности органов власти и способствует оптимизации внутренних процессов и улучшению управленческого потенциала властных структур. Модель создана на основе авторского подхода, предполагающего совершенствование организационных основ информационной безопасности и ориентированного на четыре направления. Первое направление соблюдение прав и свобод человека и гражданина в области получения информации и пользования ею требует повысить эффективность использования информационной инфраструктуры в интересах общественного развития. Второе направление информационное обеспечение государственной политики РФ путем государственных открытых информационных ресурсов, укрепления СМИ, расширения их возможностей по своевременному доведению достоверной информации. Третье направление – развитие современных информационных технологий, отечественной индустрии информации (в том числе индустрии средств информатизации, телекоммуникации и связи), обеспечение потребностей внутреннего рынка продукцией и выход этой продукции на мировой рынок, а

также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. Четвертое направление защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности телекоммуникационных систем. С этой целью необходимо повышать безопасность, в первую очередь, первичных сетей связи, федеральных органов власти, органов власти субъектов РФ и местного самоуправления. Особое внимание при защите информационных ресурсов надо обратить на финансово-кредитную сферу, на административно-хозяйственную деятельность, на вооружение, военную технику, инфраструктуру всех органов власти и их ресурсное обеспечение.

3. Авторская оценка состояния информационной безопасности дотационного и приграничного региона – Забайкальского края определена на основе социологического опроса муниципальных служащих края. Было обосновано удовлетворительное состояние информационной среды Забайкальского края и готовности муниципалитетов и их служащих к реализации информационной безопасности политического процесса на местах. В исследовании приняли участие девять муниципальных районов Забайкальского края, а именно Агинский, Газимуро-Заводский, Карымский, Могойтуйский, Могочинский, Хилокский, Чернышевский, Читинский, Шилкинский и 326 муниципальных служащих. Был сделан вывод, что в будущем информационная безопасность Забайкальского края – один из основных приоритетов с учетом электронного документооборота и информатизации органов власти.

4. Предложения по обеспечению информационной безопасности включают в себя следующее: необходимость проведения мероприятий по совершенствованию информационной безопасности политического процесса с целью административной, организационно-технической защиты информации. Первый уровень защиты информации – административный. Для обеспечения деятельности по информационной безопасности на административном уровне необходима реализация политики информационной безопасности. При

осуществлении политика безопасности не должна противоречить принятым нормативно-правовым документам государства и чем надежнее система реализации, тем эффективней должна быть политика информационной безопасности. В зависимости от выбранной политики безопасности необходимо применять индивидуальные методы защиты информации. Второй уровень по обеспечению защиты информации – это организационно-технический уровень.

Степень достоверности исследования подтверждается использованием работ как отечественных, так и зарубежных ученых по исследуемой проблеме, данных двух социологических исследований, обоснованием выводов и рекомендаций. Достоверность подтверждается развитой источниковой базой кандидатской диссертации, среди которой:

1. Нормы международного права, правовая база Российской Федерации по защите информации. В диссертационном исследовании мы опирали на следующие нормативно-правовые документы:

− Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10.12.1948)[83], в ст. 30 закреплено ключевое положение о свободе информации.

− Конвенция о защите прав человека и основных свобод ETS N 005 (Рим, 4 ноября 1950 г.)[84], ст. 10 закреплено право человека свободно выражать свое мнение. Это означает свободу получать и распространять информацию, в ч. 2 статьи содержится важная информация о том, что «осуществление этих свобод, налагающее обязанности и ответственность, может быть сопряжено с определенными формальностями, условиями, ограничениями или санкциями, которые предусмотрены законом и необходимы в демократическом обществе в интересах национальной безопасности…»

[83] Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10.12.1948) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_120805/.

[84] Конвенция о защите прав человека и основных свобод ETS N 005 (Рим, 4 ноября 1950 г.) (с изменениями и дополнениями) [Электронный ресурс]. – Режим доступа: https://base.garant.ru/2540800/.

− Международный пакт о гражданских и политических правах (Нью-Йорк, 16 декабря 1966 г.)[85].

− Конвенция Содружества Независимых Государств о правах и основных свободах человека (заключена в Минске 26.05.1995) (вместе с «Положением о Комиссии по правам человека Содружества Независимых Государств», утв. 24.09.1993)[86].

− Окинавская хартия глобального информационного общества 21 июля 2000 года[87], акцентирует внимание на высокие темпы развития информационных технологий современного мира и закрепляет базовые подходы к развитию глобального информационного пространства.

− Конвенция о защите физических лиц при автоматизированной обработке персональных данных (г. Страсбург 28.01.1981) (вместе с поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ N 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999).[88] Здесь также определены основные понятия, такие как «персональные данные», «автоматизированные базы данных», «автоматическая обработка персональных данных». Эта первый документ, вводящий обязывающие международные нормы, защищающие человека от злоупотреблений при сборе и обработке персональных данных.

---

[85] Международный пакт о гражданских и политических правах (Нью-Йорк, 16 декабря 1966 г.) [Электронный ресурс]. – Ррежим доступа: https://base.garant.ru/2540295/.

[86] Конвенция Содружества Независимых Государств о правах и основных свободах человека (заключена в Минске 26.05.1995) (вместе с «Положением о Комиссии по правам человека Содружества Независимых Государств», утв. 24.09.1993) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_6966/.

[87] Окинавская хартия глобального информационного общества 21 июля 2000 года [Электронный ресурс]. – Режим доступа: https://base.garant.ru/2560931/.

[88] Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) (вместе с поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ N 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_121499/.

− Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.)[89], включает в себя не только национальное уголовное законодательство устанавливающее ответственность за нарушения компьютерной информации, но и декларирующее международное сотрудничество по преодолению нарушений.

− Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ)[90].

− Закон Российской Федерации от 21.07.1993 N 5485-1 (ред. от 08.03.2015) «О государственной тайне»[91].

− Федеральный закон от 28 декабря 2010 г. N 390-ФЗ «О безопасности»[92].

− Федеральный закон от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности [93].

− Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»[94].

− Федеральный закон от 7 июля 2003 г. N 126-ФЗ «О связи»[95].

− Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне»[96].

---

[89] Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.) [Электронный ресурс]. – Режим доступа: https://base.garant.ru/4089723/.

[90] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_28399/.

[91] Закон Российской Федерации от 21.07.1993 N 5485-1 (ред. от 08.03.2015) «О государственной тайне» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/.

[92] Федеральный закон от 28 декабря 2010 г. N 390-ФЗ «О безопасности» [Электронный ресурс]. – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=187049.

[93] Федеральный закон от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности» [Электронный ресурс]. – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=113-658.

[94] Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/-Cons_doc_LAW_61798/.

[95] Федеральный закон от 7 июля 2003 г. N 126-ФЗ «О связи» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/Cons_doc_law_43224/.

[96] Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне». [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/.

− Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»[97].

− Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ[98].

− Федеральный закон от 27.07.2010 N 224-ФЗ (ред. от 27.12.2018) «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»[99].

− Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы»[100].

− Указ Президента РФ от 17.03.2008 N 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»[101].

− Указ Президента РФ от 22.05.2015 N 260 «О некоторых вопросах информационной безопасности Российской Федерации» (вместе с «Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» и размещения (публикации) в ней информации через российский

---

[97] Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи». [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_112701/.

[98] Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_220885/.

[99] Федеральный закон от 27.07.2010 N 224-ФЗ (ред. от 27.12.2018) «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?from=103037-0&rnd=F4D1A53C9769ABE7588C801F7519379F&req=doc&base=LAW&n=310162&REFDOC=103037&REFBASE=LAW#28d967a5p5s.

[100] Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» [Электронный ресурс]. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71570570/.

[101] Указ Президента РФ от 17.03.2008 N 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_75586/#dst0.

государственный сегмент информационно-телекоммуникационной сети «Интернет»»)[102].

− Распоряжение Правительства РФ от 10.07.2013 N 1187-р (ред. от 24.03.2018) «О Перечнях информации о деятельности государственных органов, органов местного самоуправления, размещаемой в сети «Интернет» в форме открытых данных».[103]

− Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646)[104].

− «Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 N 7)[105].

2. Статистические материалы (данные о электронном документообороте, информационной открытости и уровне информационного развития России в мире).

− Индекс развития электронного правительства (E-Government Development Index, EGDI). Индекс развития электронного правительства (E-Government Development Index, EGDI) составляется раз в два года Департаментом экономического и социального развития ООН (UN DESA, the United Nations Department of Economic and Social Affairs) Индекс состоит из трех подиндексов,

---

[102] Указ Президента РФ от 22.05.2015 N 260 «О некоторых вопросах информационной безопасности Российской Федерации» (вместе с «Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети «Интернет») [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_179963/.

[103] Распоряжение Правительства РФ от 10.07.2013 N 1187-р (ред. от 24.03.2018) «О Перечнях информации о деятельности государственных органов, органов местного самоуправления, размещаемой в сети «Интернет» в форме открытых данных» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_149441/.

[104] Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) [Электронный ресурс]. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71456224/.

[105] Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 N 7) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_328854/.

характеризующих состояние ИКТ-инфраструктуры, человеческого капитала и онлайновых государственных услуг[106].

− Индекс развития информационно-коммуникационных технологий (ICT Development Index). Индекс развития информационных и коммуникационных технологий (ИКТ) (ICT Development Index, IDI) ежегодно измеряется Международным союзом электросвязи — специализированным подразделением ООН. Индекс состоит из 11 статистических показателей, отражающих доступность и использование ИКТ, а также практические навыки применения ИКТ населением 190 стран мира[107].

− Индекс готовности стран к сетевому обществу (Networked Readiness Index). Индекс готовности стран к сетевому обществу (Networked Readiness Index, NRI) ежегодно рассчитывается международной организацией «Всемирный экономический форум» совместно с Международной школой бизнеса «INSEAD». Индекс отражает уровень готовности стран к повсеместному использованию ИКТ для целей социально-экономического развития[108].

− Динамика повышения открытости министерств и ведомств при «Концепции открытости федеральных органов исполнительной власти» (утвержденная распоряжением Правительства Российской Федерации от 30 января 2014 г.)[109].

3. Периодика и данные информационных агентств, базы которых были использованы в процессе исследования:

− Отчет: актуальные киберугрозы – 2018г. Тренды и прогнозы компании Positive Technologies (дата опубликования 12 марта 2019 г.)[110].

− Отчёт Центра мониторинга за первое полугодие 2018 г. компании «Перспективный мониторинг», занимающейся исследованиями состояния

---

[106] Сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. [Электронный ресурс]. – Режим доступа: https://digital.gov.ru/ru/activity/statistic/rating/mezhdunarodnye-rejtingi/.

[107] Сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. [Электронный ресурс]. – Режим доступа: https://digital.gov.ru/ru/activity/statistic/rating/mezhdunarodnye-rejtingi/.

[108] Там же.

[109] Сайт «Стандарт открытости» [Электронный ресурс]. – Режим доступа: https://openstandard.ru/.

[110] Актуальные киберугрозы – 2018. Тренды и прогнозы (дата опубликования 12 марта 2019 г.) компании Positive Technologies. [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/.

безопасности информационных систем и программных продуктов, мониторингом и предотвращением атак, расследованиями инцидентов, разрабатывает решения по информационной безопасности[111].

− Доклад о результатах деятельности федеральной службы государственной статистики в 2018 году и основных направлениях на 2019 год и плановый период 2020 и 2021 годов[112].

Апробация результатов исследования. Основные идеи и теоретические положения диссертации апробированы и получили положительную оценку научной общественности и педагогических работников учебных заведений Читы, Красноярска, Новосибирска, Ростова-на-Дону, Барнаула, Биробиджана, Иркутска, Благовещенска, Душанбе, Курска и Москвы. Они излагались автором: в научных докладах и материалах 15 международной научной конференции, г. Новосибирск 12-18 апреля 2013г.; материалах научно-практической конференции с международным участием, 07-08 апреля 2015г. «Проблемы повышения эффективности местного самоуправления в условиях современных реформ и политических процессов в России», г. Ростов-на-Дону; материалах IV международной научно-практической конференции «Местное самоуправление на современном этапе: теория и практика», г. Чита; материалах всероссийской научно-практической конференции «Российский политический процесс в региональном измерении: история, теория, практика», г. Барнаул; материалах «Десятые Байкальские социально-гуманитарные чтения», г. Иркутск; материалах международной научно-практической конференции: «Современные проблемы развития экономики России и Китая», г. Благовещенск; материалах всероссийской научно-практической конференции с международным участием 14-15 апреля 2017г. «Защита окружающей среды как фактор социально-экономического развития территорий муниципальных образований: опыт и проблемы», г. Ростов-

[111] Отчёт Центра мониторинга за первое полугодие 2018 г. компании «Перспективный мониторинг». [Электронный ресурс]. – Режим доступа: https://amonitoring.ru/service/security-operation-center1/mssp/quarterly-reports/2018-1_amonitoring_halfyear_report.pdf.

[112] Федеральная служба государственной статистики (РОССТАТ). [Электронный ресурс]. – Режим доступа: http://www.gks.ru/free_doc/new_site/rosstat/os/doclad-2019%20.pdf .

на-Дону; материалах XIV международной научно-практической конференции: Фундаментальные и прикладные науки сегодня. 20-21 февраля 2018г. North Charleston, USA; в сборниках: материалах IX Всероссийской (с международным участием) научно-практическая конференции «Евразийство: теоретический потенциал и практические приложения», г. Барнаул; материалах VIII всероссийского конгресса политологов «Политика развития, государство и мировой порядок», г. Москва; материалах Третьего всероссийского элитологического конгресса с международным участием «Российская элитология: инновационные ответы на вызовы современного мира»; материалах X международной научно-практической конференции «Регионы России: стратегии и механизмы модернизации, инновационного и технологического развития». 6-7 июня 2019 г., Курск.

Основные выводы и положения диссертации были опубликованы автором в 31 работах, в том числе в 7 статьях в реферируемых изданиях, а также в сборниках международных и всероссийских научно-практических конференций.

Отдельные этапы исследования и его результаты обсуждались на заседаниях кафедры государственного, муниципального управления и политики федерального государственного бюджетного образовательного учреждения высшего образования «Забайкальский государственный университет», диссертация рекомендована к защите.

Структура исследования. Диссертация состоит из введения, трех глав, включающих семь параграфов, заключения, списка литературы, содержащего 176 название. В работе представлены 33 рисунка и 9 таблиц.

Общий объем работы – 199 стр.

ГЛАВА 1 ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ПОЛИТИЧЕСКОГО ПРОЦЕССА

1.1 Взаимосвязь понятий «политический процесс», «информационная безопасность», «национальная безопасность», «информационная открытость»

Одной из основных категорий политической науки является политический процесс, отражающий трансформацию общественно-политической жизни государства, в первую очередь, органов государственной и муниципальной власти, а также государственных институтов. В современный период информационная безопасность политического процесса с учетом информатизации государства играет значимую роль в стабильности его развития в целом. По этому поводу французский философ О. Конт утверждал, что общество существует в двух состояниях: статическое и динамическое. Политика как общественное явление обладает единством статики и динамики. Категории: «устойчивость», «стабильность» принадлежат статике, а «изменение», «развитие» – динамике.

Политический процесс в состоянии динамики подразумевает движение политических систем и их мобильность, а также активное воздействие общественных объединений, учреждений и социальных групп на системы. В данном контексте происходит накопление новых признаков и свойств. В тенденциях XIXв. наблюдается динамика политического процесса, направленная на технологический прорыв (ноу-хау) и информатизацию общества, а также органов государственного и муниципального управления. Благодаря реализации данной динамики перед государством возникают вопросы формирования концепции информационной безопасности политического процесса и защиты всех ресурсов государства от внутренних и внешних угроз. Политический процесс в состоянии статики означает устойчивое развитие и взаимоотношения внутри и

вне политических систем, выстраивание политических акторов и их политических ролей. Характеристикой политического процесса является динамичная сторона политики в виде интегральных преобразований, основой которых является деятельность общества, осуществляющего реализацию своих интересов и потребностей в данных процессах. В большинстве определений динамика отражает сложность политических процессов. При этом понятие «политический процесс» в узком смысле рассматривается как функционирование политической системы, а в широком смысле – политическая жизнь в целом.

Согласно структурно-функциональному подходу политический процесс рассматривается как механизм самоструктурирования системы, как политическая социализация граждан путем их участия в принятии решений политической жизни. Политический процесс в концепции системного подхода считается целостной системой. Системный подход оценивает стабильность его элементов, вследствие иерархичного расположения его компонентов и наличия базовых элементов. Таким базовым элементом является государство, которому общество предоставляет полномочия для управления взаимоотношениями и которое обладает для выполнения данных полномочий всеми ресурсами.

Зарубежные исследователи Г. Алмонд и Б. Пауэлл установили внутренние взаимодействия в политической системе, а Д. Истон определил большинство внешних взаимодействий. Данные утверждения о политическом процессе дали основание аргументировать его как функционирование политических систем, обеспечивающее их активный баланс с обществом. Г. Алмонд и Б. Пауэлл функции политического процесса рассматривали как функции политических систем: выработка политического курса, вынесение судебных решений. Д. Истон исследовал политический процесс с точки зрения Г. Алмонда и Б. Пауэлла, но выделял трансформацию поступающей информации из управляемой среды. В данных обстоятельствах обеспечивается взаимосвязь внешней среды с политической системой, происходит регулирование действий политических акторов, изъятие и распределение ресурсов из среды, их адаптивность на сигналы

из внешней среды, что осуществляется путем воздействия государственной и муниципальной власти. Принимая доступные ресурсы, соответствующие требования, решения, исходящие из внешней среды, государственные и муниципальные органы власти способствуют эффективному функционированию деятельности политической системы, ее стабилизации.

С точки зрения коммуникативного подхода политический процесс рассматривается как процесс управления, а также достижения определенных целей и задач по координации человеческих усилий. Социолог и политолог К. Ганс характеризовал политический процесс как оперативный и достоверный обмен сведениями между всеми акторами политической жизни, обеспечение политически значимых сведений как внутри политической системы, так и между системами. СМИ гарантирует данный процесс технологично, ориентируясь на деятельность политических партий, общественных движений, встречи политических лидеров.

Институциональный подход рассматривает политический процесс как формирование и деятельность политических институтов, в процессе которых политический процесс приобретает неконституционный и конституциональный, неконтролируемый и контролируемый характер. Американский исследователь Д. Норт характеризует институты, как правило, ориентирующиеся на соблюдение императивных обязываний, которые мобилизуют общество. Данные принципы закрепляются в организациях, которые показываются у Д. Норта в виде игроков, придерживающих определенных целей. Существуют неформальные и формальные институты. Примерами формального института являются: соглашения между партийными лидерами, партийные фракции или их совместные действия в парламенте. К неофициальным институтам относятся политические объединения, основывающиеся на согласованном содействии и обмене ресурсами. Не оформлены организационно, но обладают устойчивостью объединения депутатов, которые также относятся к неофициальным институтам.

Информационная безопасность политического процесса предполагает характеристику политического процесса и его региональных особенностей. Для исследования информационной безопасности подходит информационно-коммуникативная модель политической системы американского теоретика Карла Дойча и его характеристика, напрямую связанная с особенностями информационно-коммуникативного действия. К. Дойч в своей работе «Нервы управления: модели политической коммуникации и контроля» считал, что, используя информационно-коммуникативную модель, можно охарактеризовать передачу политической информации от управляющих к управляемым. Подчеркивая важность информационной составляющей в политическом процессе К. Дойч утверждал, что информационная нагрузка определяется масштабом правительственных программ и влияет на участников политического процесса.

Политический процесс включает: «субъекты и участники процесса; объект процесса; средства, методы, ресурсы, которые связывают субъект и объект–цель»[113]. Субъектами политического процесса являются «политические системы, политические институты (государство, гражданское общество, политические партии и т. д.), организованные и неорганизованные группы людей, индивиды»[114]. По нашему мнению, к субъектам политического процесса можно отнести информационную составляющую с учетом значимости информации для органов власти.

В XX в. влияние деструктивных факторов на различные сферы общества стало значительно проявляться. Началась дезинтеграция политических структур и традиционных систем, которые в предшествующие этапы истории развития государства стали обладать более или менее стабильным характером. Устойчивостью стал характеризоваться и политический процесс. На данные оценки обращал внимание отечественный исследователь А.С. Панарин и исследователи философии постмодернизма. Будучи общественным явлением,

[113] Зеленков, М.Ю. Политология [Электронный ресурс]. – Режим доступа: https://psyera.ru/politicheskiy-process-ponyatie-sushchnost-i-soderzhanie_8232.htm.

[114] Там же.

политический процесс подчиняется культурным, общественным, религиозным, финансовым воздействиям. Политический процесс, имеющий определенный характер, формируется в пространстве и во времени. Представляя собой политические изменения, политические процессы обладают конкретными ритмами, темпами, последовательностью своей реализации. Сигналы, идущие из внешней среды, в виде условий, степени удовлетворения, многообразны в разных государствах. На разных ступенях их развития формируется напряженность процесса, разрешение которого возможно путем повышения эффективности давления на органы власти, а также смены властных акторов или изменения типа управления.

В нашем представлении «политический процесс» содержит пространственно-временные трансформации, происходящие в политической системе государства. Их взаимодействие и функционирование, возможности движения и обновления, взаимодействие вне и внутри политических систем, формирование, деятельность политических институтов, динамика общепризнанных ценностей, распределение ролей политических акторов характеризуют динамику политических субъектов.

Политический процесс, результатом которого становится формирование и развитие политической системы, подразумевает собой движение внутри системы и ее взаимосвязь с внешней средой, деятельность компонентов системы. В этом случае на разных стадиях формирования в него включаются неинституциональные, а также внесистемные политические явления.

Нами исследованы региональные политические процессы. Как отмечено Ю.С. Дульщиковым: «Регионы Российской Федерации отличаются друг от друга по территории, численности, этническому составу, уровню экономического развития и т.д., что в значительной мере объясняет различия в региональных политических процессах».[115] Осуществление механизмов региональных

[115] Дульщиков, Ю.С. Региональная политика и управление. - М.: Изд-во РАГС, 2001.- 257 с.

политических процессов в России изучалось А.В. Новиковой[116],[117], где она отмечала их зависимость от следующих институтов:

1) федеральной власти и ее территориальных институтов;

2) системы разделения властей в регионах (законодательной, исполнительной и судебной);

3) организации местного самоуправления;

4) разнообразных политических сил (общественных движений, корпоративных образований, партий, СМИ), способных оказывать воздействие на принятие управленческих решений.

А. В. Новиковой было отмечено: «Соотношение этих сил во многом определяет структуру власти, ее конфигурацию в регионах и тенденции изменений, поэтому проблема особенностей формирования региональных политических процессов в современной России имеет большое значение»[118].

По нашему мнению, основными акторами регионального политического процесса являются:

– система органов государственной власти, муниципалитеты, партии, иные политические организации;

– деятели, реализующие информационную безопасность как необходимое условие функционирования органов власти любого уровня;

– население регионов и муниципалитетов;

– система международных отношений.

Под акторами информационной безопасности мы имеем ввиду, прежде всего, деятелей, реализующих информационную безопасность. Здесь мы акцентируем внимание на том, что информационная безопасность – это составляющая политического процесса ориентированная на защищенность органов власти от манипулирования информации.

---

[116] Новикова, А.В. Региональные особенности политических процессов субъектов Российской Федерации в условиях внешней и внутренней модернизации (монография). М.: МАКС Пресс, 2015. – 166 с.

[117] Новикова, А.В. Регионы РФ в политическом процессе модернизирующейся России и их влияние на обеспечение национальной безопасности (монография). Чита: ЗабГУ, 2016. – 200 с.

[118] Новикова, А.В. Тенденции региональных политических процессов в Сибирском федеральном округе // Материалы «Десятые Байкальские социально-гуманитарные чтения» в двух томах, Иркутск, 2017г. С19-23

Экономические изменения главным образом определяют политическое структурирование регионов и политическую жизнь, а непосредственно политика региона находится в зависимости от уровня жизни и социальных условий населения, организации власти. По свидетельству А.В. Новиковой: «Субъекты регионального политического процесса используют социально-экономические и административные ресурсы в борьбе за удержание власти в конкретном регионе... В основе типологизации российских регионов и организации моделей власти лежат различные признаки и социальные основания, среди которых можно выделить: несовершенство федеративных отношений с непропорциональным финансированием из федерального бюджета, различные социальные статусы местной политической, административной элиты, роль губернатора»[119].

Степень финансовой независимости является наиболее принципиальным фактором при политической типологизации регионов, которая является экономическим индикатором политики. Политику можно оценить с позиции ее социальной и финансовой эффективности. По оценке А.В. Абрамова: «Уровень экономической свободы определяет и степень политической свободы, который является одним из важнейших факторов, дающих возможность проанализировать особенности региональных политических процессов»[120].

Отношение субъектов регионального политического процесса оказывает влияние на авторитет региональной политической элиты, так как монопольная позиция одного из субъектов регионального политического процесса дает ему возможность манипулировать сознанием общества, концентрировать в одних руках административные и экономические ресурсы. Данная характеристика субъектов регионального процесса дает преимущество осуществления практически безальтернативных выборов, нивелирующих политическую борьбу.

---

[119] Новикова, А.В. Регионы РФ в политическом процессе модернизирующейся России и их влияние на обеспечение национальной безопасности (монография). Чита: ЗабГУ, 2016. – С72-73.

[120] Абрамов, А.В. Политический институт и политическая институционализация: определение понятия // Власть, май. 2010. -С. 55;

К изучению региональных политических процессов можно подходить с разных сторон, что отмечено А.В. Новиковой. Нами на основе ее опыта были выделены следующие подходы:

1. Институциональный и формально-правовой подходы, в центре внимания, которых находятся политические институты, функционирующие в регионе, в том числе органы власти, составляющие формально-правовой каркас политической ситуации. Рассматриваются органы исполнительной, законодательной, судебной власти и местного самоуправления, политические партии, которые действуют на территории региона.

2. Элитистский подход, главное внимание здесь уделяется личностям лидеров и элитным группам, формирующим «реальное» поле взаимодействия на территории региона. Нами было отмечено, что распространены исследования такого феномена, как региональное политическое лидерство.

3. Конфликтологический подход, главный акцент делается на конфликтах, которые определяют политическую ситуацию и политический процесс.

4. Информационный подход, где выделены реально действующие информационные акторы.

Такой анализ подходов к региональным политическим процессам позволяет лучше и точнее выявлять группы влияния, действующие в субъектах Российской Федерации.

Характеризуя теоретические основы информационной безопасности, необходимо отметить, что важное место приобретает информационная безопасность. В XXI в. информационное воздействие неуклонно становится главным механизмом управления людьми. Данное воздействие в новой эре информатизации вытесняет физическое воздействие, веками считавшееся единственным рычагом управления.

Это стало одной из причин, почему информационная безопасность считается одной из ключевых элементов политического процесса и национальной безопасности. Обеспечение защиты прав и свобод гражданина, общества и

государства призвана осуществлять деятельность в сфере информационной безопасности. Под информационной безопасностью в структурах государственного и муниципального управления понимают согласно «Доктрине информационной безопасности Российской Федерации» (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) – «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства»[121]. Данное определение универсально и используется всеми структурами власти, оно содержит общее определение защиты информации, как государства, так и его гражданина. Как утверждает О.А. Степанова: «Предельно допустимый учет и удовлетворение интересов личности, общества и государства можно рассматривать в качестве одного из основных принципов, на основе которого должно строиться обеспечение информационной безопасности, в том числе и в сфере государственного управления»[122]. Информационная безопасность становится жизненно важным механизмом достижения интересов человека, общества и государства, а также стержневым и важнейшим элементом всей системы национальной безопасности.

05 декабря 2016г. Президент России В.В. Путин утвердил своим указом №646 новую Доктрину информационной безопасности России, где определены новые национальные интересы и направления обеспечения информационной безопасности (см. приложение А).

В современный период текущие и стратегические задачи внешней и внутренней политики государства по обеспечению информационной безопасности основываются на «Стратегии национальной безопасности РФ до

[121] Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) [Электронный ресурс]. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71456224/.

[122] Степанов, О. А. Ключевые аспекты правового регулирования использования и развития информационно-электронных технологий // Государство и право. 2004, – N 4. – С. 70.

2020 г.»[123] (утверждена Указом Президента РФ 12 мая 2009 г. № 537). В данной стратегии в число внешних угроз национальной безопасности Российской Федерации отнесены угрозы развития ближайших государств, их информационно-коммуникативные средства борьбы с целью достижения верховенства в военной сфере. В «Доктрине информационной безопасности» отмечено: для «обеспечения информационной безопасности Российской Федерации нужно преодолеть технологическое отставание в важнейших областях информатизации, телекоммуникаций и связи, определяющие состояние национальной безопасности, разработать и внедрить технологии информационной безопасности в системах государственного и военного управления, системах управления экологически опасными производствами и критически важными объектами, а также обеспечить условия для гармонизации национальной информационной инфраструктуры с глобальными информационными сетями и системами»[124]. Угрозы информационной безопасности необходимо анализировать в перспективе улучшения основ телекоммуникационных и информационных систем, объектов элементов инфраструктуры и степени опасности.

В информационно-коммуникативных процессах возрос масштаб манипулятивного воздействия на различные массы людей, что может стать угрозой здоровью и психическому состоянию россиян и, как следствие, национальным интересам России. Результатом слабой информационной политики и дезинформации населения стала потеря значительной частью населения базовых мировоззренческих установок. Из этого часть россиян открывают счета в зарубежных банках и готовы иммигрировать из страны. Главная цель информационного воздействия в современный период – культивирование эгоцентризма, навязывание западных стандартов и дезинформация населения. Эти тенденции лидируют в информационных системах и, как следствие, проявляются

[123] Указ Президента Российской Федерации от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года» // Российская газета. - № 4912. – 12.05.2009.

[124] Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // Российская газета. – № 187. – 28.09.2000.

в реальной жизни россиян, начиная с 90-х гг. XX в. С учетом данных тенденций возрастает значимость информации в политическом процессе.

В атмосфере всеохватывающего обмана, демагогии, навязывания извращенных жизненных ценностей происходит духовно-нравственная дезориентация людей, рушатся их внутренние устои. В данном контексте россияне были разделены на три группы (рисунок 1) [125].

Рисунок 1 – Модели выделения групп по Петрову В. П., Петрову С. В.

Первая группа реализовывала все свои деяния под прикрытием изощренной дезинформации. Во второй группе – расцвет психических расстройств, наркомании, суицидов, это так же в значительной мере результат информационного давления на людей. Удел третьей группы – манипулируемое воздействие структур на сознание людей.

Подобное типологизация людей еще раз определяет важность информационной безопасности и показывает, как отражается травмированная психика людей на состоянии сознания в целом по стране, и в какой мере россияне

[125] Петров, В. П., Петров С. В. Информационная безопасность человека и общества / В. П. Петров, С. В. Петров. – М.: ЭНАС, 2007. – 336 с.

готовы стать опорой ее национальной безопасности. Однако, все большая часть управленцев стала на путь понимания того факта, что информация является одной из фундаментальных факторов, детерминирующих динамику развития общества, его будущее.

Таким образом, «для стабильного развития общества становится все более необходимой последовательная государственная политика в области обеспечения информационной безопасности, которая должна предъявить каждому субъекту информационных отношений определенные обязательные требования».[126]

Следовательно, нынешнее кризисное состояние страны обусловлено не только материально-экономическими факторами, но, прежде всего, имеет психологические и духовно-нравственные корни. Для анализа этого состояния нужны новые методы, базирующиеся на осознании роли личности и важности информационных факторов в жизни современного государства. Новые методы должны быть ориентированы на фактическое очищение информационного пространства России от недостоверной и искаженной информации.

Формирование информационного пространства, использовавшего современные методы и средства воздействия, является велением времени. Российское информационное пространство призвано играть фундаментальную роль в жизни российского государства. Условием эффективного функционирования информационного пространства считается наличие стабильной обратной связи в его информационных каналах, которое позволяет учитывать и знать мнение граждан при определении приоритетов духовно-нравственного, экономического, политического развития общества.

В.В. Гафнер отмечает: «Но для того, чтобы в интересах национальной безопасности избежать негативных последствий перехода к информационному обществу, необходима хорошо продуманная стратегически и четко выверенная под конкретные условия текущей жизни государственная политика в этой

---

[126] Кузнецова, Н., Кульбы, В. Информационная безопасность систем организационного управления: Теоретические основы // Под редакцией Н. Кузнецова и В. Кульбы. – М.: Наука, 2006. – С. 23.

области»[127]. Нами предлагается решить фундаментальную задачу установления роли государства в формировании информационного общества и проследить его функционирование по отношению не только к телекоммуникационным и информационным ресурсам, но и к СМИ. Эта задача высокого уровня. Ее решение выводит на уровень обобщения стратегии становления России по формированию информационного пространства страны.

Основные приоритеты развития информационно-коммуникационных технологий в ракурсе регионального политического процесса отражены в «Концепции региональной информатизации»[128], разработанной Мининформсвязи РФ. Концепция содержит задачи, приоритеты использования информационно-коммуникационных технологий в органах государственной власти субъектов РФ и местного самоуправления, а также «электронного правительства». Благодаря реализации «Концепции…», разработаны программы информатизации региона и развития информационных технологий, а также определены модели финансирования информатизации из средств федерального бюджета.

Согласно концепции, информатизация региона направлена на повышение эффективности решения социально–экономических задач развития регионов, обеспечение функционирования и взаимодействия федеральных органов государственной власти, органов государственной власти субъектов РФ, органов местного самоуправления и учреждений. Кроме того, информатизация региона ориентирована на обеспечение прозрачности и информационной открытости органов управления, а также на формирование доступа гражданам к информационным ресурсам. Реализация целей и задач информатизации региона осуществляется на основе интегрированной территориальной информационной системы, которая существует в совокупности информационных систем всех уровней государственной власти, объединенных защитой информационно-

[127] Гафнер, В.В. Информационная безопасность / В.В. Гафнер. – Рн/Д: Феникс, 2015. – 324с.

[128] Распоряжение Правительства РФ от 29.12.2014 N 2769-р (ред. от 18.10.2018) «Об утверждении Концепции региональной информатизации» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_173678/.

телекоммуникационной инфраструктуры и ресурсов, обеспечивающих их взаимодействие.

Важным ресурсом является кадровый ресурс. Для реализации концепций информатизации государственных и муниципальных органов власти необходима подготовка специалистов по кибербезопасности, которых мало как во власти, так и в коммерческой среде. В лаборатории «Касперского» существуют 134 вакансии на специалистов по кибербезопасности. 01 ноября 2019г. Минобрнауки объявили о том, что нужны учебно-научные центры по информационной безопасности, чтобы избежать риска снижения уровня образования специалистов по кибербезопасности из-за разницы в условиях подготовки в разных учреждениях, а также чтобы обеспечить «единое многомерное образовательное пространство»[129]. Минобрнауки России совместно с федеральными властями необходимо обеспечить создание учебно-научных центров по информационной безопасности в федеральных округах страны, ибо проблема обеспечения информационной безопасности, гарантирующей защиту интересов личности, бизнеса и государства, определена как одна из национальных целей развития РФ до 2024 г. Отметим, что в августе-сентябре 2019 г. Минобрнауки РФ провело анкетирование вузов по вопросам подготовки кадров в области информационной безопасности. Результаты показали, что есть сложности с тем, что ресурсное обеспечение у разных вузов существенно варьируется, что создает различные условия подготовки специалистов по информационной безопасности. Также был рост числа студентов направления «Информационная безопасность», который из-за разницы в условиях обучения может привести к повышению рисков снижения качества подготовки специалистов. Одной из мер по минимизации возможных рисков может быть создание центров, которые обеспечат построение единого многомерного образовательного пространства в области информационной безопасности.

[129] Риа новости. В Минобрнауки рассказали, для чего нужны центры по кибербезопасности. [Электронный ресурс]. – Режим доступа: https://ria.ru/20191101/1560464194.html.

Центры должны осуществлять подготовку, переподготовку, повышение квалификации и прохождение практик (стажировок) специалистов по информационной безопасности, а также способствовать реализации научных исследований и производственных задач в интересах образовательных учреждений федеральных округов. Кроме того, к функционалу центров относится распространение технологий организации образовательного процесса по информационной безопасности, учебно-методическая поддержка и консультирование, обеспечение тесного взаимодействия с основными работодателями специалистов по кибербезопасности, мониторинг и своевременная диагностика имеющихся проблем. Центры предлагается создавать на конкурсной основе на базе ведущих образовательных организаций, где имеется достаточный кадровый, научный и технологический задел. Центры могут стать сосредоточением передовых решений в области информационной безопасности, точками роста и концентрации новейшего оборудования необходимого для реализации государственных и муниципальных решений.

В современных условиях важную роль играет муниципальная информационная система. По утверждению В.Г. Систера: «Муниципальная информационная система (далее МИС) представляет собой целостную технологическую, программную и информационную среду создания, хранения, анализа и распространения информации в интересах муниципальных органов власти, предприятий и граждан. МИС является средством информационной поддержки муниципального управления, и ее необходимо рассматривать как объединение всех принятых в организации технологий обработки информации»[130].

Существуют следующие направления современных информационных технологий в деятельности органов муниципального управления:

1. Хранение и обработка сведений путем безбумажных методов.

[130] Систер, В.Г. Информационные технологии на службе города// Информационное общество, 2003. – №1. – С.143

2. Взаимодействие субъектов муниципального управления в информационной сфере.

3. Реализация управленческих решений через информационно–аналитическую поддержку.

Создание условий для принятия эффективных решений муниципального управления как целостной социально–экономической системы есть цель информатизации. В современный период повышается значимость управления информационной безопасности, что требует теоретического анализа системы организационно-правового обеспечения данной сферы.

Нужно отметить информационную открытость, как один из элементов информационной безопасности политического процесса. Мы солидарны с О.В. Малаховой, что информационная открытость органов государственного управления – «целостный комплекс совместных мер системы государственного управления и общественного контроля, направленных на предоставление сведений о деятельности государственных органов, предусмотренных законодательством, обществу в целом или конкретным лицам в целях обеспечения прозрачности и подотчетности государственных органов в рамках установленного порядка на началах равенства доступа к информации»[131]. «Главными составляющими открытости власти называют прозрачность, нахождение под публичным контролем, доступность всем и в любое время, и чувствительность к новым идеям и требованиям, готовность оперативно реагировать»[132].

Сущность понятия «информационная открытость» в научной литературе А.Е. Каменской определяется как «организационно-правовой режим деятельности каждого актора социального взаимодействия, гарантирующий участникам этого взаимодействия возможность извлекать достаточный и необходимый объем

---

[131] Малахова, О.В. Информационная открытость деятельности органов государственной власти: региональные практики/О.В. Малахова, В.А. Суханова//Среднерусский вестник общественных наук. – 2015. – № 2 (38). – С. 83

[132] Михеева, Т.А. Информационная прозрачность и открытость органов государственной власти/Т.А. Михеева//Государственное и муниципальное управление в XXI веке: теория, методология, практика. – 2013. – № 9. – С. 98

сведений о задачах, структуре, целях, финансовых и иных условиях деятельности»[133].

По мнению И.А. Бегининой: открытость власти – это «минимизация рисков, связанных с подготовкой управленческих решений большого социального масштаба, возможность достаточно точно спрогнозировать вероятные последствия их принятия:

– предоставление гражданам возможности успешно подготовиться к ожидаемым подвижкам в экономической и социальной ситуации;

– предотвращение или как минимум снижение угрозы отчуждения;

– не чрезвычайная и не конфронтационная, а инициативная мобилизация общественных сил на решение проблем самого общества;

– прибавление социального, политического, экономического, психологического потенциала федерализма;

– синхронизация процессов, протекающих в центре и на местах;

– оповещение региональных и местных властей об оптимальном курсе федеральной власти»[134].

В связи с вышесказанным, по нашему мнению, к общим функциональным задачам информационной политики следует отнести:

– «предоставление на базе формирования массовых коммуникаций и информационного обмена открытого информационного обслуживания общества;

– информационное обеспечение деятельности органов государственного и муниципального управления;

– реализация открытого информационного взаимодействия гражданского общества и власти;

– совершенствование информационных систем и телекоммуникационной инфраструктуры;

---

[133] Каменская, Е.А. Сущность и особенности информационной открытости органов власти в современной России/Е.А. Каменская //Общество: политика, экономика, право. – 2011. – № 2. – С. 19

[134] Там же.

– эффективное развитие и формирование национальных информационных ресурсов и реализация свободного доступа к ним;

– формирование необходимой нормативно-правовой базы организации информационного общества»[135].

Целесообразно выделить, что информационная открытость и ее обеспечение не является односторонним процессом. Стремление гражданского общества к получению полных и достоверных сведений о деятельности органов государственной и муниципальной власти, контроль и активная позиция общественности и их институтов по отношению к власти соотносятся с желанием власти проинформировать о своей деятельности общество. Прозрачность опередеяется как освещение деятельности власти, содержания и механизма реализации, разъяснение целей публичной политики, а «открытость – как создание публичными органами власти условий для беспрепятственного доступа граждан к информации о его деятельности и к процессу принятия решений на всех этапах их приготовления»[136].

Согласно определению, открытые государственные данные – «это информация, созданная в пределах своих полномочий государственными органами, либо поступившая в указанные органы и организации, а также информационно-аналитические организации, участвующие в публикации собственных открытых данных на территории РФ, которая подлежит размещению в сети Интернет в формате, обеспечивающем ее автоматическую обработку в целях повторного использования без предварительного изменения человеком, и может свободно использоваться в любых соответствующих закону целях любыми лицами независимо от формы ее размещения»[137]. Открытые данные – это

---

[135] Каменская, Е.А. Сущность и особенности информационной открытости органов власти в современной России/Е.А. Каменская //Общество: политика, экономика, право. – 2011. – № 2. – С. 19

[136] Михеева, Т.А. Информационная прозрачность и открытость органов государственной власти/Т.А. Михеева//Государственное и муниципальное управление в XXI веке: теория, методология, практика. – 2013. – № 9. – С. 98

[137] Временный регламент подготовки и размещения общедоступной информации Росстата в формате открытых данных / Утвержденного Заместитель руководителя Федеральной службы государственной статистики Г.К.Оксенойт 21.02.2017 [Электронный ресурс]. – Режим доступа: https://rulaws.ru/acts/Vremennyy-reglament-podgotovki-i-razmescheniya-obschedostupnoy-informatsii-Rosstata-v-formate-otkrytyh-dan/.

сведения, формируемые государственными органами в виде машиночитаемых форматов. Примеры подобных форматов: ODS, XML, CSV, JSON. Задача раскрытия сведений, а также их публикации в машиночитаемых форматах упрощает доступ граждан, которые могут для себя переработать приложения, аналитику. Поэтому, «информационная открытость» – это организационно-правовой режим деятельности любого актора политического процесса, обеспечивающий возможность получения необходимых объемов сведений о целях, задачах деятельности государственного органа.

Информационная открытость органов власти различных структур является залогом развития демократических процессов в государстве, способствует формированию гражданской позиции, является одной из форм контроля за деятельностью органов власти. Кроме того, выполнение требований к развитию и осуществлению политики информационной открытости органов государственной власти дает возможность предугадать направления формирования информационного пространства общества, отслеживать взаимоотношения акторов и ее среды, грамотно осуществлять анализ и ранжировать виды деятельности, акцентируя интерес на актуальных вопросах, реализуя в стратегической перспективе сбалансированное развитие общества. Деятельность органов государственной и муниципальной власти как открытого и демократического механизма политического управления, обеспечение ею постоянного сбалансированного диалога с обществом считается важным обстоятельством формирования наиболее обширных возможностей для адекватного восприятия обществом функционирования государственных структур и, следовательно, обеспечения поддержки принимаемых общественно-политических решений.

Таким образом, различные трактовки политического процесса показывают значимость информационной составляющей в обеспечении информационной безопасности. Очевидно, что место информационной безопасности в системе политического процесса очень значимое. Получение полной информации о

функционировании политического процесса органов власти целесообразно с точки зрения важности информации для населения субъектов РФ и государства. Существует необходимость обоснования организационно-правовых основ информационной безопасности региона и его информационной открытости.

1.2 Теоретико-методологический анализ системы управления информационной безопасностью: организационно-правовые характеристики

Анализ системы управления информационной безопасностью предполагает характеристику следующих теоретических конструктов: регион, политическая власть, обеспечение информационной безопасности.

Понятие регион существует многозначно:

1. Как международный регион – страны, государства мира, объединения государств.
2. Как любое место развития, в том числе муниципальные образования.
3. Как субъект Российской Федерации.

В теоретическом плане нами даны региональные характеристики информационной безопасности с оценки муниципальных образований и субъектов Российской Федерации.

Каждый субъект федерации имеет свой уровень социально-экономического развития, природно-ресурсный потенциал, производственную специализацию. Поэтому направление региональной политики не может быть стандартным для всех регионов, ее необходимо координировать, опираясь на конкретные данные.

Региональная политика призвана сглаживать различные диспропорции и кризисы в аспекте социального и экономического развития регионов.

В России сейчас можно выделить различные группы проблемных регионов[138]:

1. Слаборазвитые. Население этих регионов в своем большинстве можно назвать бедным, так как более 80% граждан находятся ниже черты бедности.

[138] Региональная политика [Электронный ресурс]. – Режим доступа: http://uchebnik.online/regionalnaya-ekonomika_738/regionalnaya-ekonomika-regionalnaya-25532.html.

Здесь можно выделить следующие субъекты федерации: Алтай, Тува, Марий Эл и др.

2. Депрессивные. К такому типу относятся регионы, производственные мощности которых не используются из-за сокращения государственного заказа и разрыва кооперационных связей. В советские времена было построено большое количество небольших городов, население которых в своем большинстве работало на одном крупном градообразующем предприятии. После того, как государственные заказы прекратились, предприятия оказались в кризисной ситуации. Следствием этого стали задержка или невыплата заработной платы, снижение уровня жизни населения. К таким районам можно отнести отдельные области Западной и Восточной Сибири, Урала, в том числе и Забайкальский край характеризующийся резким падением промышленного производства, высоким уровнем безработицей и низким прожиточным минимумом.

3. Регионы с экологическими проблемами. Характеризуются наличием вредного производства, либо переживают последствия различных катастроф (Поволжье, Урал, Кузбасс и др.). Существует и другие классификации регионов, но по теоретическим соображениям мы их затрагивать не будем.

Важным для нашего исследования является характеристика власти. По утверждению А.Н. Новиковой: «Понятие власти многозначно, имеет публичный характер и оценивается как доминирование воли субъекта над объектом. Власть носит не только волевой, но и социальный, коллективный и политический характер. Являясь объектом политологического анализа, сильная централизованная политическая власть призвана способствовать целостности государства. Проблема политической власти неразрывно связана с федеративным устройством Российской Федерации и с единством системы государственной власти... Можно определить политическую власть как способность определенного индивида, группы, класса осуществлять свою волю в политике и нормах права»[139].

[139] Новикова, А.В. Политическая власть и политическое управление в субъектах Российской Федерации: монография / А.В. Новикова; Забайкал гос. ун-т. – Чита: ЗабГУ, 2014. – С. 35-36.

Как отмечено в Философской энциклопедии: «Политическая власть обладает рядом особенностей:

1) верховенство, обязательность решений политической власти для всякой иной власти;

2) право на легальное использование насилия;

3) публичность (всеобщность и безличность);

4) наличие единого центра принятия решений;

5) выполнение роли арбитра в конфликтах между представителями различных социальных групп;

6) многообразие используемых ресурсов;

7) обеспечение максимальной стабильности общества как целого в рамках существующих отношений собственности, действующих законов и конституции»[140].

Политическая власть интересует политологов. Она является базисом политической системы и оказывает влияние на развитие духовной, общественной, социальной, экономической систем. Как утверждает А.В. Новикова: Политическая власть – термин, «обозначающий реальную возможность и способность определенного класса, социальной группы или части общества, а также представляющих их организаций и индивидов распространять свою волю относительно других групп, отдельных индивидов, осуществлять общие интересы и цели насильственными и ненасильственными средствами. Политическую власть можно определить как способ реализации групповых интересов и достижения общих целей. Таким образом, в целом власть есть способность и возможность воздействовать на деятельность, поведение людей с позиции воли, авторитета, права, силы, знания. Каждый вид власти заслуживает

[140] Философская энциклопедия. Словари и энциклопедии на Академике [Электронный ресурс]. - Режим доступа: http://dic.academic.ru/dic.nsf/enc_philosophy/211/%D0%92%D0%9B%D0%90%D0%A1%D0%A2-%D0%AC.

внимания. Политическая власть, как и любой другой вид власти, означает право, и способность одних проводить свою волю по отношению к другим»[141].

Поскольку нами рассматривается информационная составляющая политической власти, то требуется применение определенных технологий, прежде всего информационных. Воздействие на национальную безопасность страны, предполагающее политическую стабильность и консенсус, влияет на взаимодействие федеральных и региональных органов власти. Об этом не раз упоминал исследователь О.Ф. Шабров: «При анализе эффективности управления учитывают два аспекта: системная стабильность и уровень результативности достижения целей»[142]. О.Ф. Шабров в подобной концепции утверждает, что неэффективная власть не способна на протяжении продолжительного периода быть стабильной. При этом легитимность власти соотноситься с ее эффективностью. Согласно суждению автора, данные две характеристики взаимосвязаны диалектически – «легитимность власти обуславливается ее эффективностью, а эффективность находится в зависимости от ее легитимности, так как по мере потери легитимности воздействия власти встречаются все наиболее интенсивное сопротивление общества»[143]. Таким образом, описываемый О.Ф. Шабровым процесс укрепления устойчивости политической системы базируется на взаимообусловленности двух отдельных детерминант – легитимности и эффективности.

Организационно-правовое обеспечение информационной безопасности предполагает реализацию комплекса законов, нормативов, управленческих решений, регламентирующих как единую деятельность по обеспечению информационной безопасности, так и формирование, функционирование специализированных систем защиты сведений и информации. Главными

---

[141] Новикова, А.В. Политическая власть и политическое управление в субъектах Российской Федерации: монография / А.В. Новикова; Забайкал гос. ун-т. – Чита: ЗабГУ, 2014. – С. 37-38.

[142] Шабров, О.Ф. Политико-административное управление в Российской Федерации: состояние и актуальные проблемы // Власть.-2004.-№11

[143] Шабров, О.Ф. Политическая власть, ее эффективность и легитимность / О.Ф. Шабров // Политология. – М.: Изд-во РАГС, 2002. – С. 135-136.

функциями организационно-правового обеспечения информационной безопасности являются:

− «развитие основных методов и принципов отнесения сведений к защищаемой информации конфиденциального характера;

− регулирование системы органов власти и должностных лиц, имеющих ответственность за реализацию защиты информации;

− формирование системы различных видов документов, регулирующих механизмы по реализации системы защиты информации;

− детализация мер ответственности за нарушения норм защиты информации;

− закрепление регламента по решению конфликтных ситуаций по вопросам обеспечения защиты информации;

− становление экономических, налоговых взаимоотношений с целью эффективной борьбы с киберпреступностью и защиты информации в информационной сфере;

– улучшение компонентов экономического и налогового мотивирования научно-технологического прогресса в сфере информатизации и защиты информации»[144].

С.Г. Аксенов по данному вопросу отмечал: «Основными принципами становления организационно-правового обеспечения информационной безопасности являются:

− строгость соблюдения общепризнанных норм и правил защиты баз данных лицами, обладающими доступом к конфиденциальной и защищаемой информации;

− нормативно-правовое фиксирование норм ответственности за несоблюдение режима и порядка защиты информации;

− технико-математические решения придания юридической силы в области организационно-правового обеспечения защиты информации;

---

[144] Аксенов, С.Г. Организационно-правовые основы обеспечения информационной безопасности органов государственной власти // Налоги – 2008, – N 3(2).

– процессуальное формирование процедур решения ситуаций, реализующихся при защите информации и обеспечения информационной безопасности системы» [145].

Необходимо выделить, что нормативно-правовые базы государства в сфере информационной безопасности считаются необходимой мерой, которая удовлетворяет главную потребность в защите информации и сведений при формировании военных, политических, социально-экономических направлений деятельности государства. Особый интерес со стороны западных государств к реализации и становлению такой базы обусловлен возрастающими расходами на противоборство с угрозами в информационной сфере. Все это без исключения вынуждает западные государства всерьез работать над целями и задачами нормативно-правовой базы в области защиты информации. В данном контексте С.Г. Аксенов утверждал: «В Соединенных штатах первый нормативно-правовой акт в области информационной безопасности и защиты информации был принят в 1906 г., а к современному периоду принято более 500 нормативных актов ответственности за разглашение информации, киберпреступность»[146]. Развитие нормативно-правовой базы в информационной сфере и защиты информации предполагает, что государство оберегает свои информационные ресурсы. Информационные ресурсы подразделяют на три группы (см. рисунок 2)[147].

[145] Аксенов, С.Г. Организационно-правовые основы обеспечения информационной безопасности органов государственной власти // Налоги – 2008, – N 3(2).

[146] Там же.

[147] Беззубцев, О.А. Ковалев, А.Н. О лицензировании и сертификации в области защиты информации [Электронный ресурс]. – Режим доступа: http://www.cryptopro.ru/sites/default/-files/docs/licen.pdf.

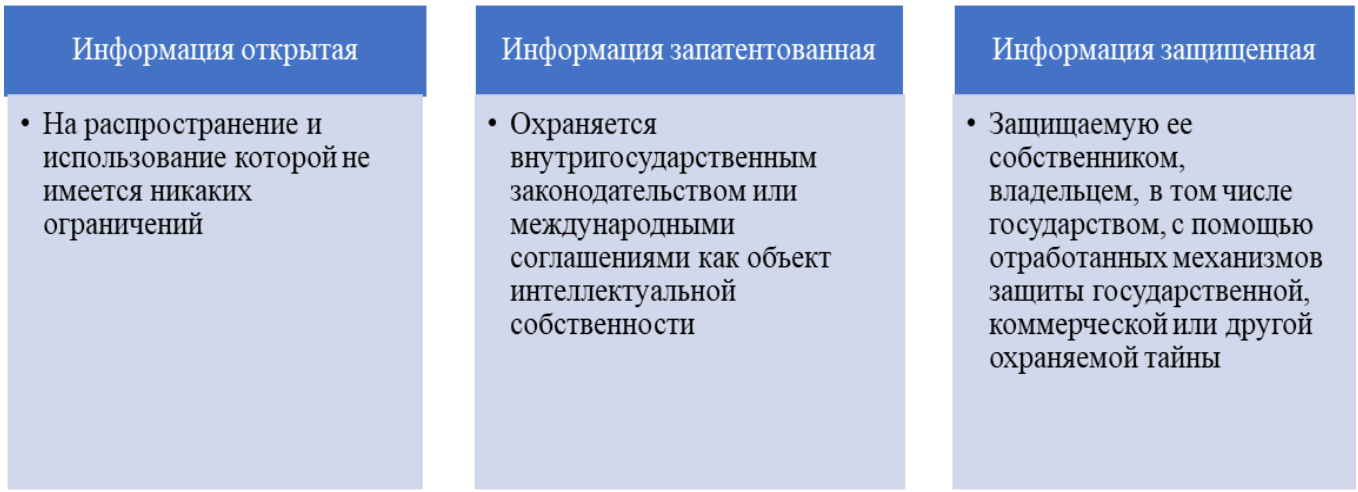


Рисунок 2 – Виды информационного ресурса государства по О.А. Беззубцеву, А.Н. Ковалеву.

Защита направлена на важные сведения для пользователя. Запрет на передаваемую информацию, предоставляющую выгоду, дает возможность выделять следующие характеристики:

1. Информация относящаяся к категории защищенной, которая составляет государственную тайну.

2. Сведения, составляющие коммерческую тайну, относят к конфиденциальной информации.

Важной характеристикой информационной безопасности является государственная тайна. Главным компонентом информационной безопасности в системе органов государственного и муниципального управления является государственная тайна. Основным нормативно-правовым документом в сфере информационной безопасности о государственной тайне, является Закон РФ «О государственной тайне», где понятие «государственная тайна» трактуется как: «защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации»[148].

[148] Закон Российской Федерации от 21.07.1993 N 5485-1 (ред. от 08.03.2015) «О государственной тайне» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/.

Основными объектами и компонентами отнесения сведений, составляющих государственную тайну, являются:

– предметы, явления, события, составляющие государственную тайну;

– правонарушитель, от которого осуществляется защита государственной тайны;

– закрепление в законодательных базах информации, которая включает государственную тайну;

– наносимый ущерб экономике, внешней политике, обороне в случаях разглашения сведений, составляющих государственную тайну.

В Указе Президента РФ от 30 ноября 1995 г. N 1203 закреплены сведения, относящиеся к государственной тайне.

Сведениям не присваивается гриф секретности в следующих случаях:

– рассекречивание данных не влечет угрозы нарушения законодательства и национальной безопасности государства;

– скрытие сведений способно нарушать права и свободы человека и гражданина;

– сведения, наносящие вред здоровью и жизни граждан.

В ст. 7 Закона РФ «О государственной тайне» содержатся все условия и факторы, запрещающие засекречивать сведения. Порядок сведений, которые отнесены к государственной тайне, определен «Правилами отнесения сведений, составляющих государственную тайну, к различным степеням секретности»[149]. В законе РФ «О государственной тайне» определено, что степень ущерба зависит и от степени секретности вследствии их разглашения.

В России формирование методов информационной безопасности реализуется по трем направлениям:

– государственные интересы;

– права граждан на частную жизнь;

[149] Постановление Правительства РФ от 4 сентября 1995 г. N 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_7686/.

– экономическая и финансовая деятельность.

Организационно-правовые характеристики информационной безопасности предполагают анализ нормативно-правовой базы, которая включает:

– Конституцию РФ.

– Федеральные законы и законы РФ.

– Кодексы РФ.

– Постановления Правительства РФ.

– Ведомственные нормативные акты.

Целесообразно выделить федеральные законы РФ, регулирующие взаимоотношения в информационной сфере, касающиеся различных органов власти:

– «Об электронной цифровой подписи»[150];

– «О лицензировании отдельных видов деятельности»[151];

– «О государственной тайне»[152];

– «Об информации, информационных технологиях и о защите информации»[153];

– «О связи»[154];

– «О безопасности»[155];

– «О коммерческой тайне»[156].

Защита прав собственности считается значимым элементов информационной безопасности и сведения воспринимаются как объект

---

[150] Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_112701/.

[151] Федеральный закон от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности». / [Электронный ресурс]. – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=113-658.

[152] Закон Российской Федерации от 21.07.1993 N 5485-1 (ред. от 08.03.2015) «О государственной тайне» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/.

[153] Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/-Cons_doc_LAW_61798/.

[154] Федеральный закон от 7 июля 2003 г. N 126-ФЗ «О связи» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/Cons_doc_law_43224/.

[155] Федеральный закон от 28 декабря 2010 г. N 390-ФЗ «О безопасности» [Электронный ресурс]. – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=187049.

[156] Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/.

собственности. В ст. 128[157] Гражданского кодекса РФ впервые в истории права РФ информация поставлена в качестве объекта права. Вся информация в правовом отношении делится на следующие основные элементы[158]:

1) «Информация без ограничения права доступа:

– информация для общего пользования;

– информация о состоянии и мониторинге окружающей среды;

– сведения о состоянии здоровья граждан в районах размещения объектов по хранению химического оружия и объектов по уничтожению химического оружия;

– информация, содержащая сведения о фактах и обстоятельствах, имеющих угрозу здоровью, жизни граждан» [159].

2) Информация с ограниченным доступом:

– коммерческая тайна;

– профессиональная тайна;

– служебная тайна;

– персональные данные;

– банковская тайна;

– государственная тайна.

3) Информация, запрещенная для распространения:

– ложная реклама;

– пропаганда к войне;

– информация, разжигающая национальную рознь.

4) Объекты интеллектуальной собственности, к которым информация не может быть отнесена с «грифом ограниченного доступа» и защиты интеллектуальной собственности:

– патентное право;

---

[157] Гражданский кодекс Российской Федерации часть первая от 30 ноября 1994 г. N 51-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/Cons_doc_LAW_5142/.

[158] Семененко, В.А. Информационная безопасность. В.А. Семененко. – М.: МГИУ, 2010. – 277 с.

[159] Федеральный закон от 02.05.1997 N 76-ФЗ (ред. от 23.05.2015) «Об уничтожении химического оружия» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_14292/.

- авторское право;
- средства индивидуализации.

Ноу-хау составляют исключения, так как они охраняются в режиме коммерческой тайны.

Нами выделена разноаспектность защиты информации в органах государственной и муниципальной власти. Политический анализ предполагает характеристику функционирования органов региональной и муниципальной власти и оценку позиций населения Забайкальского края. Кроме того, политическими акторами, безусловно, является население Газимуро-Заводского района, ибо Быстринское месторождение находится в 16 км к востоку от поселка Газимурский Завод. В 2015–2016 гг. была проведена доразведка в целях прироста подготовленных к освоению запасов на флангах и глубоких горизонтах. По результатам работ получен прирост запасов полезных ископаемых, который составил 51,8 млн. т. руды. Значимый для Забайкальского края «Норникель» также имеет лицензии на геологоразведку прилегающих к месторождению площадей: Быстринско-Ширинского месторождения, Западно-Шахтаминской и Центрально-Шахтаминской площади. Месторождение «Быстринское» разрабатывается открытым способом. Отработка ведется на двух карьерах — «Верхне-Ильдиканском», «Быстринском-2». Еще два карьера — «Медный чайник» и «Южно-Родственный» — будут введены в 2030 г. Поэтому так важно просветить население района для решения обозначенных стратегических проблем. Очевидно, что целый спектр государственных и муниципальных мероприятий зависит от числа опасностей и возможностей органов власти регулировать данные угрозы, используя надлежащие контрмеры. Одной из имеющихся угроз защиты информации, служит потеря сведений по техническим каналам. Объектами допуска являются элементы информатизации органов государственной и муниципальной власти, в том числе технологическое оборудование, архивы, специализированные библиотеки, те объекты, в которых имеется информация ограниченного допуска. Для преодоления большей части

технических каналов утечки сведений органы власти осуществляют технологически сложные методы защиты информации. Для предотвращения потерь информации по технологическим каналам в органах власти на разном уровне реализуется комплекс мероприятий. В.И. Ярочкиным выделены основные мероприятия по уменьшению информационных потерь:

– «увеличение защищенности информационных систем;

– реализация защиты сведений составляющих государственную тайну;

– мероприятия, нацеленные на устранение запрещенного проникновения в данные органов МВД и утечки информации;

– усовершенствование системы подготовки кадров по использованию технических средств защиты информации» [160].

Зачастую уязвимыми местами в области информационной безопасности считается деятельность пользователей систем и технического персонала, приводящая к утечке сведений. В данном случае открытые информационные системы обязаны корректировать на предмет конфиденциальной информации и исключения поступления сведений под грифом секретности. Государство в условиях интеграции информационных, инновационных технологий ужесточает нормативно-регламентированные требования к организации безопасности баз данных и обновлению сведений с грифом секретности. Данная тенденция связана с циркуляцией больших масс информации, составляющей государственную тайну в телекоммуникационных системах государства. Безусловно, этому уделяется большое внимание. В каждом органе власти, как на региональном, так и муниципальном уровне, действует собственная специализированная связь, которая настроена на специальной аппаратуре засекреченным кодом.

Политический анализ проблем предполагает анализ рисков и характеристик противодействия в случае неблагоприятного политического исхода. Нами составлена следующая таблица 1 по оценке информационных рисков в Забайкалье.

[160] Ярочкин, В.И. Информационная безопасность. В.И. Ярочкин. – М.: Акад. Проект, 2008. – 544 с.

Таблица 1 – Информационные риски и их политическое решение в Забайкалье.

Риски	Политические решения
Вероятность неблагоприятного исхода в связи с высоким уровнем социально-политической напряженности, с неудовлетворённостью граждан ситуацией в регионе, протестным голосованием.	Управлять риском на основе конструктивного взаимодействия и создания обратной связи с населением.
Не прохождение предложений по обеспечению информационной безопасности политического процесса.	С учетом значимости предложений пропустить их организаторам и реализовать.
Недостаточность информационно-коммуникативного обеспечения, невысокая информационная открытость.	Развитие информационных технологий как среди граждан, так и государственных, муниципальных служащих.
Слабая представленность в социальных сетях.	Анонсирование мероприятий в СМИ как важного актора политического процесса.
Действия органов государственного и муниципального управления.	Информирование целевой аудитории о 44ФЗ и противодействии коррупции.

Таким образом, данные таблицы 1 свидетельствуют о высоких социально-политических рисках по определению эффективных направлений информационной безопасности политического процесса в Забайкальском крае.

Затрудненность развития нормативно-правовых и организационных методов усовершенствования безопасности информации органов власти актуально на современном этапе. В условиях глобализации и прогресса информационных средств и достижений данная проблема находится в приоритетных направлениях политики РФ.

21-23 октября на Московском международном форуме инновационного развития глава ФСБ А. В. Бортников подчеркивает, что в 2019 г. было двести информационных вмешательств в деятельность органов власти. 16 октября, в Сочи на международном совещании руководителей спецслужб, органов безопасности и правоохранительных органов была обозначена серьезная проблема нежелания IT-компаний сотрудничать со спецслужбами.

Как утверждает Александр Васильевич Бортников: «Интернет с его глобальным охватом аудитории становится основной площадкой для продвижения идеологии терроризма, вербовки и распространения информации о

способах проведения терактов. Основным инструментом коммуникации между бандитами по-прежнему являются интернет-мессенджеры, обладающие высокой криптозащитой»[161]. Очевидно, что нежелание ряда ведущих мировых IT-компаний сотрудничать со спецслужбами ухудшает сферу информационной безопасности.

В настоящее время назревает и угроза использования при совершении терактов технологий беспроводной связи, независимой от услуг сотовых операторов и наличия доступа в интернет. А.В. Бортников подчеркнул: «Невозможно эффективно противостоять террористическим угрозам до тех пор, пока террористы будут беспрепятственно пользоваться закрытыми каналами коммуникации в глобальной сети. В этой связи приглашаем всех наших партнеров присоединиться к реализации российской инициативы, выдвинутой на прошлогоднем совещании в Москве, относительно депонирования ключей шифрования для мобильных устройств»[162]. Внедрение этого механизма обеспечит правоохранительным органам на законодательном уровне контроль за информационным обменом между преступниками и гарантирует право граждан на тайну переписки, исключив доступ к ней третьих лиц. Совершенно очевидно, что необходимо объединить усилия национальных спецслужб по выявлению и блокированию в интернете материалов экстремистского и террористического содержания и наладить в этих целях сотрудничество с IT-компаниями.

Кроме того, необходимо противопоставить массированной пропаганде террористов эффективное партнерское взаимодействие спецслужб и выработку конкретных мер по защите мирового информационного пространства от идеологии терроризма. Хакерские атаки, совершаемые террористами, могут привести к межгосударственным конфликтам. Международные террористические организации развивают собственные киберподразделения. Растет угроза внедрения террористами вредоносных программ на объекты критической инфраструктуры с целью провоцирования масштабных аварий. Возможность при

[161] Информационное агентство ТАСС. Глава ФСБ видит серьезную проблему в нежелании IT-компаний сотрудничать со спецслужбами. [Электронный ресурс]. – Режим доступа: https://tass.ru/obschestvo/7006012.

[162] Там же.

этом подконтрольных террористам хакерских сообществ маскировать свои атаки под целенаправленные враждебные действия, совершаемые каким-либо государством, чревата возникновением реальных политических и военных конфликтов. Проблема осложняется распространением в интернете хакерских программ, адаптированных для непрофессиональных пользователей. При этом необходимо развивать информационную открытость для безопасного и достоверного доступа граждан ко всей информации, необходимой для государственных и муниципальных органов власти.

Начало процесса информационной открытости было зафиксировано в Постановлении Правительства РФ от 24.11.2009 N 953 (ред. от 20.04.2017) «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти»[163].

Суть его состоит в нормативно-правовом закреплении обязанностей органов исполнительной власти в том числе: обеспечивать доступ граждан к сведениям о деятельности посредством развития информативных ресурсов с особым перечнем, утвержденным этим же Постановлением. В этих условиях ставится задача размещения информации в системах общего пользования, т.е. в сети интернет. Но здесь возникают проблемы, отмеченные Ю.Г. Просвирниным: «Из приблизительно 50-ти имеющихся органов исполнительной власти, в первый период реализации Постановления №953, его требованиям целиком отвечали сайты шести органов: Минобразования, МНС, Госатомнадзора, ФКЦБ, Минприроды, Минобороны»[164].

Для регулирования нормативно-правовых положений в сфере информатизации во второй половине 2006 г. вступил в силу новый закон от 27

[163] Постановление Правительства РФ от 24 ноября 2009 г. N 953 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти» (с изменениями и дополнениями) [Электронный ресурс]. – Режим доступа: http://base.garant.ru/196682/#ixzz3pGRuZncQ.

[164] Просвирнин, Ю.Г. Проблемы информационной открытости органов власти / Ю.Г. Просвирнин // Правовая наука и реформа юридического образования. – 2011. – № 1. – С. 112.

июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации».[165]

В статье 8 п.5 149-ФЗ органы власти должны гарантировать доступ, в том числе с применением информационных технологий и телекоммуникационных сетей, а также сети интернет, к сведениям о деятельности органа на государственном языке соответствующей республики и на русском языке в соответствии с нормативно-правовой базой субъектов РФ[166].

Также в статье 8 149-ФЗ сказано, что не может быть ограничен доступ к:

1) «нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами».[167]

Следовательно, нормативно-правовыми актами были закреплены принцип открытости информации о деятельности органов власти, а также открытый допуск к таким сведениям, помимо случаев, определенных законом. Действительно, практическое обеспечение данных норм открывает множество коллизий и недостатков, не дающих вероятность извлечь требуемую информацию с целью

[165] Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/.

[166] Там же.

[167] Там же.

реализации эффективных методов принятия политических решений, в том числе с целью защиты своих прав.

«Стратегия развития информационного общества» от 7 февраля 2008 г. № Пр-212[168] стала новым этапом информационной открытости государственных и муниципальных органов с целью повышения информационной открытости функционирования органов власти.

09 мая 2017 г. Указом Президента №203 была принята новая Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы[169], где отмечается, что электронные СМИ, информационные системы, социальные сети стали частью повседневной жизни россиян. Пользователями российского сегмента сети «Интернет» в 2016 г. стали более 80 млн человек. Целью стратегии является создание условий для формирования в России общества знаний.

Среди приоритетов Стратегии – формирование информационного пространства с учетом потребностей в получении качественных и достоверных сведений; создание и применение российских информационных и коммуникационных технологий, обеспечение их конкурентоспособности на международном уровне. В стратегии отмечены:

- Необходимость обеспечивать национальные интересы в области цифровой экономики.
- На международном уровне необходимо создать новые механизмы партнерства, призванные выработать систему доверия в Интернете, гарантирующую конфиденциальность и личную безопасность пользователей и исключающую анонимность, безответственность пользователей и безнаказанность правонарушителей.

---

[168] Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 07.02.2008 N Пр-212) [Электронный ресурс]. – Режим доступа: http://base.garant.ru/192762/.

[169] Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» [Электронный ресурс]. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71570570/.

− Следует обеспечить экспорт российских информационных и коммуникационных технологий, регулировать импорт иностранных технологий, создать условия для технологического преимущества бизнес-моделей российских организаций в глобальной цифровой экономике.

− Приводится приоритетный сценарий развития информационного общества в России. Правительство РФ должно утвердить показатели и этапы реализации стратегии.

В 2019 г. утверждена национальная программа «Цифровая экономика Российской Федерации» [170] в которой поставлены следующие цели:

− Увеличение внутренних затрат на развитие цифровой экономики за счет всех источников (по доле в валовом внутреннем продукте страны) не менее чем в три раза по сравнению с 2017 годом.

− Создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступных для всех организаций и домохозяйств.

− Использование преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями.

Поставлены следующие задачи национального проекта:

1. Федеральный проект «Нормативное регулирование цифровой среды». Создать систему правового регулирования цифровой экономики, основанной на гибком подходе к каждой сфере, а также внедрению гражданского оборота на базе цифровых технологий.

2. Федеральный проект «Информационная инфраструктура». Создание глобальной конкурентоспособной инфраструктуры передачи, обработки и хранения данных преимущественно на основе отечественных разработок.

---

[170] Паспорт национальной «Программы «Цифровая экономика Российской Федерации». Федеральный проект «Нормативное регулирование цифровой среды» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 N 7) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_328854/.

3. Федеральный проект «Кадры для цифровой экономики». Обеспечение подготовки высококвалифицированных кадров для цифровой экономики.

4. Федеральный проект «Информационная безопасность». Обеспечение информационной безопасности на основе отечественных разработок при передаче, обработке и хранении данных, гарантирующей защиту интересов личности, бизнеса и государства.

5. Федеральный проект «Цифровые технологии». Создание «сквозных» цифровых технологий преимущественно на основе отечественных разработок.

6. Федеральный проект «Цифровое государственное управление». Внедрение цифровых технологий и платформенных решений в сферах государственного управления и оказания государственных услуг, в том числе в интересах населения и субъектов малого и среднего предпринимательства, включая индивидуальных предпринимателей.

Проект «Открытый регион»[171] с точки зрения реализации повышает эффективность работы органов государственной и муниципальной власти. Для этого в рамках проекта формируются принципы открытого управления с учетом специфики конкретного субъекта РФ или муниципалитетов.

«В современный период в рамках проекта «Открытый регион» внедрение механизмов информационной открытости управления осуществляется в 31 субъекте РФ, в их числе: Волгоградская область, Вологодская область, Воронежская область, Ивановская область, Кабардино-Балкарская Республика, Калужская область, Кировская область, Краснодарский край, Красноярский край, Ленинградская область, Москва, Мурманская область, Новгородская область, Новосибирская область, Пермский край, Приморский край, Республика Башкортостан, Республика Ингушетия, Республика Татарстан, Самарская область, Санкт-Петербург, Свердловская область, Ставропольский край, Томская область, Тульская область, Тюменская область, Ульяновская область, Хабаровский край,

[171] Открытый регион [Электронный ресурс]. – Режим доступа: http://open.gov.ru/openregion/.

Чувашская республика, Ярославская область»[172]. Исходя из перечня субъектов, очевидно, что Забайкальский край не входит в проект «Открытый регион», что, безусловно, актуализирует проблему обеспечения информационной безопасности депрессивного и приграничного субъекта РФ, каковым является Забайкалье.

При осуществлении проектов в субъектах РФ для повышения открытости государственного управления в регионе требуется принятие комплексной нормативно-правовой базы. В целом, политика информационной открытости государственного управления выразилась в теории «Электронного правительства», которая предполагает обеспечение эффективного взаимодействия, базирующегося на увеличении открытости информационных ресурсов и объема информации, которую органы власти должны размещать в информационной системе и телекоммуникационных сетях (сети интернет).

Теоретический анализ организационно-правовых характеристик информационной безопасности предполагает оценку функций, приемов, ресурсов, методов обеспечения информационной безопасности.

Таким образом, специфической является информационная безопасность в органах государственной власти и муниципального управления. Для предотвращения утечки информации в данных органах формируются целый комплекс мероприятий в том числе регулирование на предмет государственной тайны и конфиденциальной информации. Возникает вопрос о сущности данных мероприятий, создании высокотехнологичного общества и реализации программ «Электронное Правительство» и «Электронный муниципалитет».

Реализация мероприятий по информационной безопасности политического процесса наиболее отвечает интересам устойчивого развития регионов, муниципалитетов, населения Забайкалья. Однако, потребуется расширение полномочий контрольных органов, увеличение их численности, разработка нормативно-правовой базы по вопросам защиты информации как конфиденциальной, так и составляющей тайну.

---

[172] Открытый регион [Электронный ресурс]. – Режим доступа: http://open.gov.ru/openregion/.

Можно утверждать, что по результатам диссертационной работы защиту информации в подразделениях администраций муниципалитетов можно осуществить при интенсивной работе по внедрению систем электронного документооборота. В электронном документообороте возможно, настроить режим ограничения доступа. В отличие от бумажного документооборота для папок электронного архива рекомендуется предоставлять права доступа для редактирования ответственным пользователям. Другие пользователи обладают возможностью только на чтение данных документов. В подобном случае информация будут защищена не только от распространения, но и от несанкционированного копирования. Защита бумажных носителей способна поддерживаться мерой обязательного прописывания в инструкции специалистов государственного и муниципального управления персональной ответственности за распространение, либо передачу сторонним лицам информации. Такова позитивная динамика системы управления информационной безопасностью.

1.3 Информационная интеграция и инновация как этап развития государственного и муниципального управления России

Президент РФ В.В. Путин ориентировал на создание информационно−высокотехнологичного общества Российской Федерации. Результатом установки стала федеральная целевая программа – «Информационное общество», которая охватывает все сферы жизнедеятельности России. Для реализации данной задачи в 2008 г. был сформирован Совет при Президенте РФ по развитию информационного общества, касающийся реализации программы «Электронного правительства» (2009).

В современный период продолжается развитие инновационных технологий. 23 октября 2019г. в инновационном центре «Сколково» завершился VIII международный Форум «Открытые инновации», который посетили более 20 000 человек. За три дня на площадках Форума состоялось свыше 150 деловых сессий. «Открытые инновации 2019» прошли в формате трех тематических дней – «Цифровой человек», «Интеллектуальная экономика», «Технологии будущего». 22 октября состоялась пленарная сессия с участием Председателя Правительства России Д. А. Медведева, посвященная главным вызовам цифровизации и информатизации общества, бизнеса и государственной власти.

Спикерами «Открытых инноваций» стали 655 представителей бизнеса, науки, органов власти, топ-менеджеров российских и международных корпораций, экспертов в сфере высоких технологий, образования, инвестиций. География участников Форума включала 102 страны, в том числе Германию, Корею, США, Японию, Францию, Великобританию, Австралию, Тунис. Работу Форума освещали около 1000 представителей российских и зарубежных СМИ, состоялось более 40 пресс-мероприятий. В выставочном пространстве Форума

Startup Expo были представлены свыше 160 инновационных решений. Для многих стартапов «Открытые инновации» стали первой площадкой для презентации идей и разработок. Программа «Открытых инноваций» в этом 2019 г. включала в себя Телемедфорум, практический бизнес-форум по системам искусственного интеллекта RAIF, технологическую конференцию Bloomberg Sooner Than You Think, презентацию Московского инновационного кластера, международный конкурс East Bound, финал федерального Конкурса инноваций в образовании.

За три дня на полях Форума было подписано 29 соглашений между российскими и международными компаниями, фондами и институтами развития. Среди них: партнерское соглашение об открытии в «Сколково» корпоративного стартап-акселератора Orange Fab; подписание основных условий создания Японо-Российского фонда «Новые рубежи»; меморандум о сотрудничестве Фонда «Сколково» и Минздрава России в области цифровой медицины; соглашение Фонда содействия инновациям и Фонда «Росконгресс» о сотрудничестве в рамках проекта «Бизнес Приорити».

Соорганизаторами Форума «Открытые инновации» выступили Министерство экономического развития РФ, Правительство Москвы, Фонд «Сколково», РВК, Фонд инфраструктурных и образовательных программ, Фонд содействия инновациям, Государственная корпорация развития «ВЭБ.РФ». Стратегические партнеры «Открытых инноваций» – RAIF (The Russian Artificial Intelligence Forum) и Почта России. Генеральные партнеры Форума – Японская ассоциация по торговле с Россией и новыми независимыми государствами (РОТОБО) и Госкорпорация «Росатом». Официальные партнеры – ОАО «РЖД», SberCloud и Ассоциация IPChain. Интеллектуальный партнер Форума – Группа Всемирного банка. Партнер биржи деловых контактов – EY. Образовательный партнер – Московская школа управления СКОЛКОВО. FoodTech Partner – Группа компаний «ЭФКО». Marine Information Technology Partner – «Морские Инновации». Digital&Transformation Partner – КПМГ. Официальный автомобиль Форума –Porsche.

На форуме были представлены не только инновации во всех областей жизнедеятельности человека, но и новые решения и механизмы развития информационного поля РФ. Большой акцент был сделан на инновации в сфере органов власти и информационных систем, с подписанием контрактов с крупными компаниями по развитию IT-технологий[173].

Значимой инновацией последних лет в сфере информационной интеграции и безопасности является программа «Электронный муниципалитет» (далее «ЭМ»). Одной из причин создания программы «ЭМ» является то, что около 80% взаимодействий между властью и обществом происходит на местном уровне.

Информационная система «ЭМ» – программный комплекс, предназначенный для автоматизации функций органов местного самоуправления (далее ОМСУ)[174].

Цели системы «ЭМ»:

– Унификация информации, обрабатываемой ОМСУ, с целью:

А) консолидации данных на уровне муниципального района для оценки социально-экономического развития региона в целом;

Б) организации регламентированного обмена информацией с государственными органами власти и учреждениями.

– Сокращение количества обработки данных хозяйственного и других видов учета, справок и выписок для населения и других видов отчетов администрацией ОМСУ.

– Сокращение времени получения государственных и муниципальных услуг гражданами[175].

Обозначим концепцию «ЭМ» в ракурсе муниципальной службы. Под сущностью муниципальной службы понимаем выполнение муниципальными

---

[173] Официальный сайт форума «Открытые инновации». [Электронный ресурс]. – Режим доступа: https://openinnovations.ru/press-center/news.

[174] Информационная система (ИС) «Электронный муниципалитет» [Электронный ресурс]. – Режим доступа: http://r62.center-inform.ru/download/products_and_solutions/presentation_municipality.pdf.

[175] Там же.

служащими полномочий и взаимодействий с внешней средой в деятельности ОМСУ.

Одна из проблем информационной безопасности на всех этапах становления информационного общества страны − это человеческий фактор. По свидетельству Председателя Правительства РФ Д.А. Медведева, некомпетентность чиновников связана с их неумением внедрять и использовать информационные технологии в деятельности органов местного самоуправления. Замечание справедливое, но проблема заключается в том, что информационные инновации предполагают модернизацию государственной и муниципальной служб и постановку информационных технологий в качестве универсальных инструментов чиновника.

В современный период существует двойственность в восприятии теории «электронное правительство», так как идет ассоциация только с государственными учреждениями, но «Электронное правительство» включает в себя и деятельность органов местного самоуправления.

Начало такого толкования «электронного правительства» заключается в следующем:

1. Термин «электронное правительство» заимствован с английского E-Government. Но термин government обозначает все уровни власти.

2. В статье 110 Конституции РФ Правительство оценивается как высший федеральный исполнительный орган государственной власти.

3. Ключевым моментом в концепции «электронного правительства» является то, что необходимо обозначить уровень информатизации муниципалитета. Но какой это уровень и как его достичь органы власти не имеют представления. Этот факт неблагоприятно влияет на роль, которая возложена на органы муниципальной власти по формированию «информационного общества».

Электронное взаимодействие в контексте «Электронного правительства» предполагает функционирование всех элементов как единой системы при их контактах. Поэтому самостоятельная ИС «Электронный муниципалитет» вполне

имеет право на существование и развитие. Как утверждает Ю.А. Михеев, ученик В.М. Глушкова, создателя государственной автоматизированной системы управления (ОГАС) СССР: «Субъекты РФ, муниципальные образования – это типично сетевые социально-экономические структуры. С точки зрения информационных технологий управленческие процессы в этих структурах базируются на принципах параллельности, адаптации, когерентности… При этом всегда существует необходимость сохранения целостности управления»[176].

Законодательная база, регламентирующая деятельность ОМСУ, закрепляет строгие требования, предъявляемые к качеству работы муниципалитетов, в том числе к срокам выполнения требований законодательства при оказании муниципальных услуг. Активно развиваются информационные системы федерального уровня, предназначенные, в том числе, для сокращения бюрократических барьеров и упрощения процессов получения гражданами муниципальных услуг.

При этом муниципалитеты часто оказываются в двойственном положении: с одной стороны – философия электронного правительства подводит ОМСУ к эффективному информационному обмену, с другой – отсутствие современных средств автоматизации на местах тормозит выполнение этих требований, и в целом эффективную работу местных администраций. Рассмотрим на рисунке 3 недостатки бумажного учета информационного обмена.

[176] Михеев, Ю.А. Типизация региональных ИТ-решений не панацея, а повод… // PC WEEK. 2006. – №16. – С. 42–43.

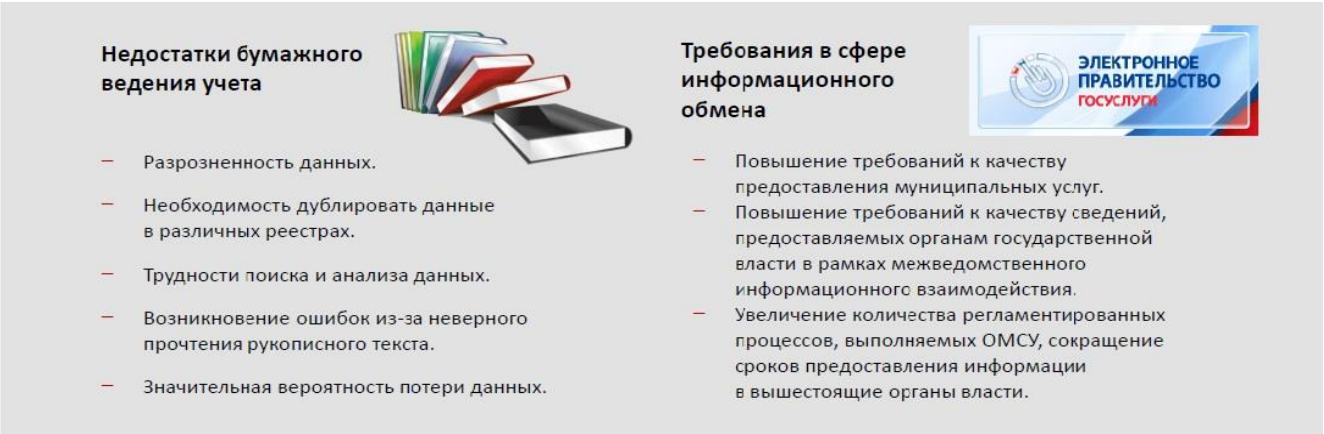


Рисунок 3 – Недостатки бумажного учета и требования к информационному обмену.[177]

Автоматизация функций ОМСУ на базе ИС «Электронный муниципалитет» решает проблемы с внедрением и позволяет:

1) провести комплексную автоматизацию функций ОМСУ с организацией единого хранилища данных;

2) обеспечить эффективный информационный обмен между ОМСУ и другими заинтересованными участниками в электронном виде.

Рассмотрим плюсы автоматизации и информационного обмена в электронном виде. Автоматизация дает возможности организовывать единый информационный контент для всех участников и единую базу данных; автоматизированные поиск и отчетность; точность перенесения данных в производные документы. Информационный обмен повышает качество предоставления муниципальных услуг населению и обеспечение должного качества сведений, предоставляемых органам государственной власти. Характеристики электронного муниципалитета с точки зрения органов исполнительной власти региона представлены на рисунке 4.

[177] Информационная система (ИС) «Электронный муниципалитет» [Электронный ресурс]. – Режим доступа: http://r62.center-inform.ru/download/products_and_solutions/presentation_municipality.pdf.

Рисунок 4 – ИС «Электронный муниципалитет».[178]

ИС «Электронный муниципалитет» решает задачу объединения нескольких видов учета, осуществляемого органами местного самоуправления, в единой информационной системе как указано в рисунке 5.

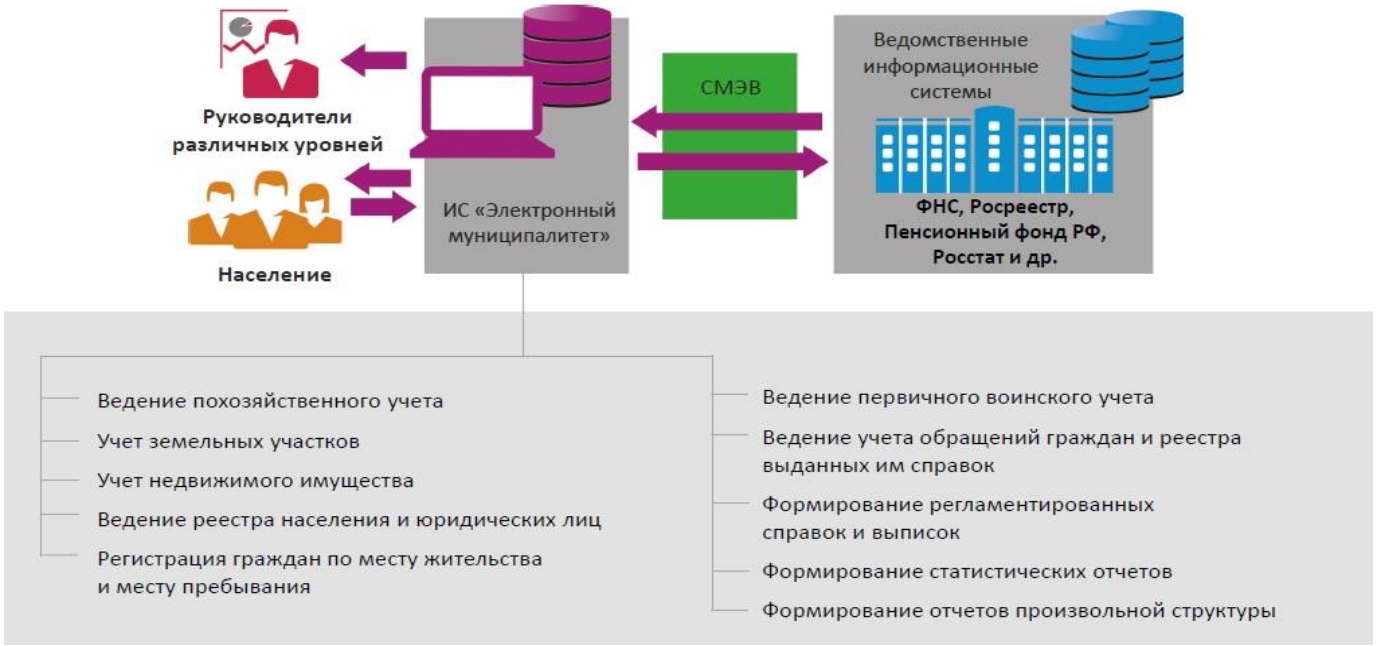


Рисунок 5 – Задачи решаемые ИС.[179]

[178] Информационная система (ИС) «Электронный муниципалитет» [Электронный ресурс]. – Режим доступа: http://r62.center-inform.ru/download/products_and_solutions/presentation_municipality.pdf.

ИС «Электронный муниципалитет» – современный программный комплекс, разработанный на основе передовых технологий с учетом тенденций развития информационных систем, предназначенных для автоматизации государственных учреждений и органов власти.

В современный период для эффективного использования электронного документооборота между гражданами и государственными органами начали использовать электронный документооборот «СБИС». «СБИС Электронный документооборот» - единая система для работы с отчетными данными и программный комплекс для автоматизации потока внутренних и внешних организационных документов. Данную систему в основном используют индивидуальные предприниматели и юридические лица при сдаче отчетности в такие государственные органы как:

1. Налоговая служба.
2. Пенсионный фонд.
3. Росприроднадзор.
4. Миграционная служба.
5. Фонд социального страхования.
6. Росстат.
7. Центробанк.
8. Росалкогольрегулирование

Многие государственные органы перешли на систему «СБИС» для мгновенной отправки документов и сдачи различной отчетности, как утверждает сама система: «Хранящиеся в СБИС электронные документы можно представить в суд, казначейство или любой другой госорган как в виде файлов-оригиналов, так и в виде бумажных копий со штампом. А в налоговую их удобно отправить через интернет: получив истребование, просто выберите нужные документы из

[179] Информационная система (ИС) «Электронный муниципалитет» [Электронный ресурс]. – Режим доступа: http://r62.center-inform.ru/download/products_and_solutions/presentation_municipality.pdf.

списка и нажмите «Отправить». Далее СБИС сам сделает опись, все отправит и уведомит вас о приеме документов инспектором»[180].

Основные функции электронного документооборота «СБИС»:

– Сдача налоговых, алкогольных, статистических отчетностей в электронном виде.

– Создание электронной подписи для подписания виртуальных документов.

– Принятие писем и уведомлений от государственных органов и наоборот. Это три основных функций программы взаимодействия с государственными органами. Также существуют другие полезные внутренние функции программы для работы организации, такие как: складской учет, кадровая работа, работа с кассами и финансами. «СБИС» является ведущей программой электронного взаимодействия с государственными органами.

Для формирования и развития информационной интеграции и инноваций необходимо стабильное региональное единое информационное пространство. Информационное пространство основывается на информационных ресурсах, к которым относятся:

− Ресурсы деятельности региональных органов власти.

− Ресурсы общественных организаций, действующих в политическом поле органов региональной власти.

Важную роль в информационном пространстве России занимают именно информационные ресурсы. Формирование информационных ресурсов государственных и региональных органов власти возложено на органы власти, являющиеся заказчиком информационных систем и отвечающие за обеспечение доступа к ним. Структуры региональных властей и управления с точки зрения заказчика информационных систем закреплены законодательно. Задачи по созданию информационных ресурсов для обеспечения деятельности структур власти определяют:

---

[180] Официальный сайт электронного документооборота «СБИС» [Электронный ресурс]. – Режим доступа: https://sbis.ru (дата обращения 10.09.2019).

− Президент РФ;

− Совет Федерации РФ;

− Государственная Дума РФ;

− Правительство РФ;

− Судебная система РФ;

− Исполнительные органы власти РФ;

− Государственная власть субъекта РФ.

Становление информационного пространства региона ориентировано на выполнение следующих задач:

− контроль со стороны граждан и негосударственных учреждений за деятельностью органов государственной власти и ОМСУ;

− увеличение общественной активности граждан посредством использования открытой социально-экономической, общественно-политической информации;

− обеспечение гражданских прав и свобод на информационный массив;

− поддержание стабильного уровня информационного потенциала;

− интеграционное единство с мировым информационным полем;

− обеспечение согласованности политических решений федеральных органов государственной власти, власти субъектов РФ и органов ОМСУ с точки зрения соблюдения прав и свобод как органов власти, так и граждан государства.

Под единым информационным пространством государства понимается совокупность информационных ресурсов и информационной инфраструктуры, позволяющая создавать защищенное информационное взаимодействие государства, организаций и граждан, а также максимально полная реализация информационных потребностей на всей территории государства при сохранении баланса интересов на вхождение в мировое информационное поле.

Базовыми характеристиками единого информационного пространства являются:

− создание единых принципов для всех акторов информационного взаимодействия при сочетании как самоуправления, так и государственного регулирования;

− реализация защищенных информационных контактов государства и граждан;

− полное удовлетворение всех информационных требований на всем пространстве государства;

− равенство акторов информационного взаимодействия и всех информационных ресурсов с точки зрения норм права;

Как утверждает В.Н. Лопатин: «Вновь формируемые информационные ресурсы, включаемые в единое информационное пространство, должны быть на законном основании доступны органам управления государственной власти, хозяйствующим субъектам и гражданам. Развитие информационного пространства в интересах органов государственной власти направлено на объединение и продвижение существующих информационно-аналитических ресурсов, предназначенных для обеспечения их эффективной управленческой деятельности»[181]. Очевидно, что развитие единого информационного поля предусматривает достижение оперативного доступа к имеющейся информации и расширение единого информационного пространства.

Как следует из приведенного материала, информационное пространство органов власти составляют информационно-телекоммуникационные системы, обеспечивающие информационную поддержку безопасности личности, общества, государства.

При недостатках информационных систем органы власти могут быть базой, обеспечивающей реализацию государственных информационных ресурсов. Ведение министерствами и ведомствами государственных информационных ресурсов с целью интеграционного взаимодействия предполагает решение

[181] Лопатин, В. Н. Теоретико-правовые проблемы защиты единого информационного пространства и их отражение в системах российского права и законодательства [Электронный ресурс]. – Режим доступа:http:/for-expert.ru/problemy_inform_prava/15.

сложных организационных моментов и технических вопросов, связанных с обеспечением скоординированного развития. Координация информации на всей территории России осуществляется органами государственного управления, которые имеют сложные территориальные инфраструктуры для достижения интересов федеральных и региональных органов власти, а также всех организаций и граждан РФ. Становление единого информационного пространства России позволит увеличить эффективность функционирования всех ветвей власти за счет улучшения степени информационной поддержки на основе использования информационного взаимодействия при решении комплексных задач государства.

На технических носителях, прежде всего – специализированные информационные массивы в виде автоматизированных баз данных (ЛБД), а также информационные ресурсы в сети интернет, распределенные по WEB-сайтам. К информационным ресурсам относятся отдельные документы и массивы документов в информационных системах. Информационные ресурсы выступают как объект правовых отношений государства, физических и юридических лиц. Информационные ресурсы могут быть государственными и негосударственными и как элемент состава имущества находятся в собственности граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений.

Важной проблемой является информационная интеграция как аспект государственного и муниципального управления России в условиях глобализации. Очевидно, интеграция в органах власти РФ – это процесс объединения деятельности политических акторов, информационных систем и программных обеспечений. Следует отметить следующие основные подходы к ведению интеграции информационных систем политического процесса:

1. «Стихийная» интеграция – интеграция систем при отсутствии единой инфраструктуры, приводящая к низкой стабильности потому что:

- не реализована единая среда исполнения процессов;
- не обоснованы конкретные базы данных и их источники.

2. На базе электронного документооборота формируется унифицированная информационная система для решения вопросов органов власти, что влечет за собой следующие проблемы:

- нестабильность работы инфраструктуры при высокой нагрузке;
- ограниченность процессов автоматизации;
- закрытый формат баз данных;
- отсутствие открытых протоколов взаимодействия с внешней средой;
- ограничения на реализацию информационной структуры по соблюдению в деятельности органов власти прав личности.

3. Рекомендуется в органах власти использовать единую интеграционную систему ESB, которая характеризуется следующими параметрами:

- высокий уровень стандартизации;
- развитость интегральной инфраструктуры;
- встроенные механизмы выполнения процессов;
- определенность оценки и моделирования ключевых параметров;
- поддержка версий различных процессов и возможность изменить работу его работы моментально без остановки функций исполнения.

Интеграция системы осуществляется при соблюдении технологических требований, включающих в себя следующие этапы:

1. Обоснование условий к интеграции систем.
2. Выполнение требований к эксплуатации систем.
3. Стандартизация взаимодействия открытых информационных систем.
4. Сквозной мониторинг к управлению.
5. Единые методы к становлению информационной инфраструктуры.
6. Набор механизмов технологической платформы для работы с интеграционными компонентами.

Приведем примеры технологических платформ, ориентированных на решение проблем информационной интеграции:

− IBM WebSphere MQ – платформа, осуществляющая обеспечение стабильной доставки сообщений.

− IBM WebSphere Service Registry and Repository – система регистрации сервисов систем.

− IBM Business Process Manager – методы автоматизации процессов интеграции.

− IBM WebSphere ILOG JRules – средство создания правил.

Процессы информационно-политических решений включают в себя осуществление таких подсистем, как:

− Подсистема автоматизации регламентов.

− Подсистема управления сервисами для регистрации новых информационных систем в интегральной системе собственными силами органов власти.

− Подсистема доставки сообщений для решения вопросов стабильной доставки сообщений в политическом процессе.

− Подсистема управления бизнес-правилами для создания множества трудных интеграционных процессов в условиях сложности управленческого выполнения решений.

Управление информационной безопасностью политического процесса представлено на рисунке 6.

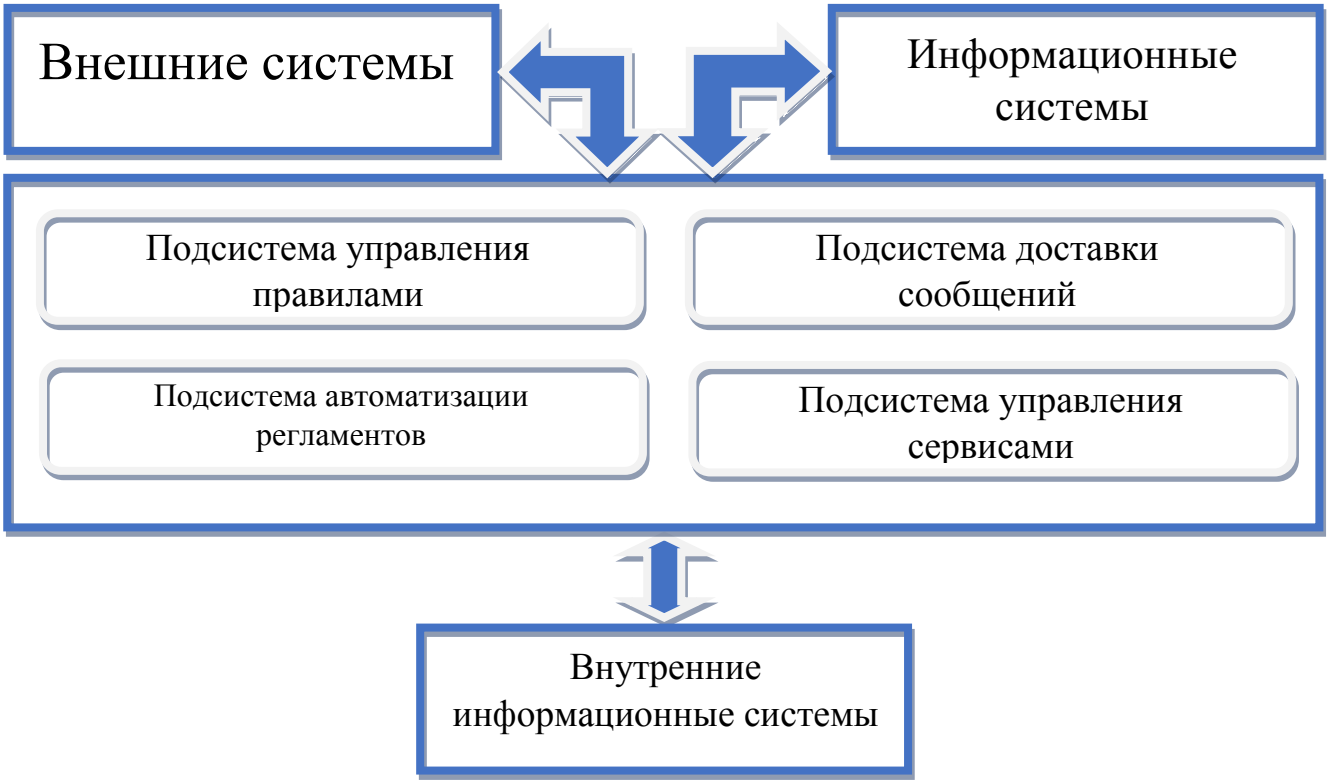


Рисунок 6 – Управление информационной безопасностью политического процесса.

Интеграция процессов предполагает задействование сквозных процессов, где на отдельных этапах используются приложения. При этом обработка информации на данных этапах производится в приложениях, а функции реализации процесса осуществляет специализированная подсистема. Для функционирования данного способа интеграции традиционно используют технологию WorkFlow.

Приложения промежуточного слоя объединяют интегральное программное обеспечение. Ведущие компании уже занимаются разработкой комплексных интегрирующих пакетов для корпоративных информационных систем. К ним, в частности, относятся Oracle 10g, Microsoft BizTalk Server, IBM WebSphere, SAP Netweaver. Так, в BizTalk Server реализованы функции подготовки и транспортировки информации в электронном документообороте.

Важной составляющей информационной безопасности политического процесса с точки зрения технологической реализации является языковый формат. К лингвистическому обеспечению интегральных информационных систем

относятся инвариантные языки программного обеспечения. Из стандартов STEP известным становится Express, язык разметки XML и формат EDIFACT. Для согласованности поддержки семантической баз данных пользуются языком метаданных RDFS и языки представления онтологий приложений OWL.

Подводя итоги, можно констатировать, что информационная безопасность политического процесса реализуется посредством унификации методов обмена, для чего используют транспортные протоколы. В Web-технологиях распространённым является протокол HTTP. С помощью протокола HTTP характеризуются взаимодействия «клиент-сервер». Для нахождения необходимого сервера и реализации связи в ориентированной среде пользуются протоколами WSDL, SOAP и UDDI. При этом протокол HTTP используют в качестве транспортного средства для сообщений SOAP.

Кроме того, в развитии информационной безопасности государственного и муниципального управления появились следующие инновации: программы «Электронное Правительство» и «Электронный муниципалитет». Включение всех уровней власти в систему электронного взаимодействия повышает качество информационной безопасности политического процесса как государственного, так и муниципального управления. Для развития информационной интеграции и инновации органов власти применяется новый информационный продукт «СБИС», который обеспечивает оперативный доступ к информационным ресурсам.

ГЛАВА 2 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ГОСУДАРСТВЕННОГО И МУНИЦИПАЛЬНОГО УПРАВЛЕНИЯ РОССИИ

2.1 Оценка информационных угроз органов государственного и муниципального управления

С развитием информационного общества, мировые тенденции диктуют условия полной информационной открытости органов государственной власти. В связи с этим формируются нормативы, регламентирующие доступ заинтересованных лиц к информационным ресурсам государства. При разработке управленческих решений власть также зависима от данных информационных ресурсов. Подобная зависимость особенно проявляется в местном самоуправлении, так как их деятельность напрямую связана со всеми сферами жизнедеятельности человека и накоплением оперативной информации. По утверждению Е.А. Горшкова: «Возрастание процессов информатизации в предоставление услуг органами федеральной и муниципальной власти при помощи электронного документооборота способствует усилению необходимости использования органами муниципалитета информации, своевременности, достоверности ее получения»[182].

Как отмечают специалисты, множество баз данных подвергаются угрозам несанкционированного доступа, что влечет за собой негативное воздействие на конфиденциальные сведения, вследствие чего нарушается режим достижения информационной безопасности. В различных источниках четко не определены факторы риска обеспечения безопасности конфиденциальной информации в органах местного самоуправления. В нашем исследовании мы определили

[182] Горшков, Е. А. Саганова, В. Н. Обзор и анализ инструментальных средств обеспечения кадровой деятельности // Современные тенденции технических наук (II): материалы междунар. заоч. науч. конф. (г. Уфа, май 2013г.). – Уфа: Лето, 2013. – С. 5–7.

факторы риска, изложенные в «Доктрине информационной безопасности» на рисунке 7[183]:

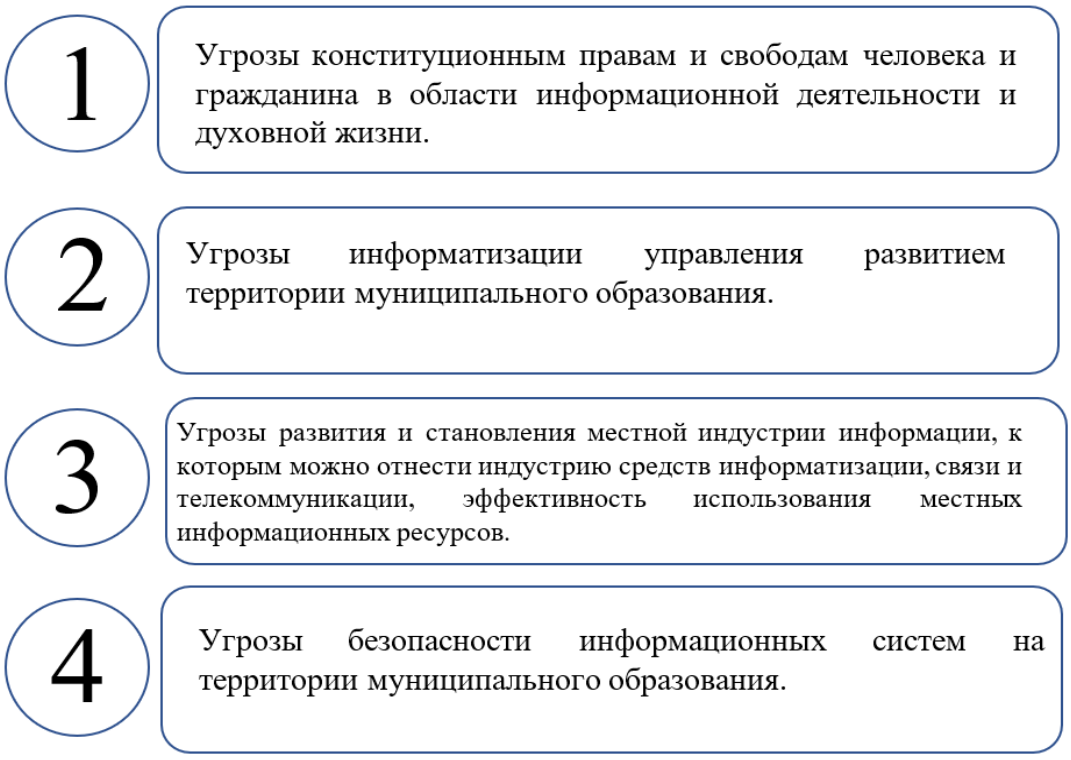


Рисунок 7 – Факторы риска безопасности конфиденциальной информации.

Информационные угрозы первой категории, как показано на рис. 7, подвергаются влиянию следующих факторов:

– принятие нормативно-правовые актов, ущемляющих права граждан в информационной деятельности;

– формирование монополии на распространение телекоммуникационных систем и информации в пределах территории;

– противодействие криминальным структурам и защита семейной и личной тайны, телефонных переговоров и переписки;

– ограничение доступа к общественно-необходимой информации;

– противоправная реализация средств воздействия на общественное сознание;

– неисполнение органами власти, обществом требований законодательства, регулирующего отношения в информационной сфере;

[183] Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // Российская газета. – № 187. – 28.09.2000.

– ограничение доступа населения к открытым информационным ресурсам, в том числе архивным материалам и социально-значимой информации;

– старение систем накопления культурных ценностей в муниципальном образовании;

– манипулятивное воздействие информацией;

– уменьшение человеческого ресурса, что способствует затруднению подготовки и переподготовки персонала для формирования и использования информационных и телекоммуникационных ноу-хау технологий;

– несоблюдение прав и свобод в сфере массовой коммуникации и информации.

Угрозами информационной безопасности социально-экономического развития муниципалитета являются:

– монополизация информационного пространства муниципалитета ограниченным числом информационных структур;

– вмешательство в деятельность СМИ по информированию граждан, в том числе на территории образования;

– низкое предоставление информационных средств муниципалитетам из-за дефицита квалифицированных кадров, неумения их осуществлять эффективно местную информационную политику.

Проанализируем наиболее частые факторы, стимулирующие угрозы информационной безопасности деятельности. Органы муниципальной власти отмечают незащищенность в технологическом плане информационных систем, создаваемых на территории муниципального образования. Угрозами муниципалитетов являются:

– «незаконное использование и сбор информации;

– несоблюдение технологий обработки информации;

– внедрение нелицензированных программных компонентов;

– реализация элементов, дестабилизирующих деятельность систем защиты информации;

– повреждение, средств обработки информационно-телекоммуникационных систем;

– активное вмешательство в ключевые системы защиты данных;

– взлом паролей и средств защиты информации;

– утечка информации по техническим каналам;

– внедрение средств-устройств перехвата информации по каналам связи;

– хищение, уничтожение носителей информации;

– перехват информации в сетях, дешифрование информации;

– использование нелицензионных и несертифицированных зарубежных и отечественных средств защиты данных;

– несанкционированный доступ к информации, находящейся в базах данных;

– нарушение нормативно-правовых актов ограничивающих распространение информации»[184].

Политологами источники угроз информационной безопасности политического процесса на разных уровнях власти разделяются на внешние и внутренние. Особенности муниципальных органов власти представляют возможность учитывать внутренние источники, а внешние сложно распределить, так как муниципальные информационные ресурсы тесно связаны с ресурсами государства. Проблематично определить конкретную границу отличия одних параметров от других. Возможно, предположить, что значительным является такой источник как уровень коррупции муниципалитета.

Коррупция непосредственно связана с информационной безопасностью политического процесса, так как существуют организованные экономические группировки и преступные структуры. Из-за введения допуска к конфиденциальным сведениям возрастает влияние криминальных структур на интересы граждан, происходит уменьшение безопасности местного сообщества, и в целом страны в информационной сфере. При повышении прозрачности

[184] Донская, Е. Н., Панько, Ю. В. Отдельные аспекты обеспечения информационной безопасности деятельности органов местного самоуправления // Молодой ученый. – 2014. – №8. – С. 453-457.

информационных систем органов муниципальной власти увеличивается вероятность значительного сокращения коррупции. Информация и сведения о деятельности органов власти могут быть ограниченными и подконтрольными. В данном случае сами предпосылки являются основанием возникновения и развития коррупции. Существует потребность в создании восприимчивых систем управления информационным обеспечением и ресурсами органов муниципальной власти, что ограничено финансовым и трудовым потенциалами муниципалитета. Небольшое субсидирование информационной безопасности муниципалитета, одной стороны, связано с традициями формирования районных бюджетов (субсидирование происходит либо при необходимости, либо в выполнении нормативных условий). Помимо этого, для формирования продуктивной системы безопасности необходимы технологические процессы, внедрение которых должно реализовывается на постоянной основе, что требует финансирования в крупном объеме. Зачастую бюджет муниципалитета осуществить не в состоянии безопасность, а нерегулярность финансирования не дает продуктивной информационной защиты. Данные предпосылки возникновения угроз информационной безопасности в муниципалитете связаны с эффективностью управления экономическим развитием территории. Низкая динамичность муниципалитетов по предоставлению данных окружению, малоразвитость концепций допуска к информационным ресурсам сообщества содействуют формированию альтернативных методов извлечения данных. В этом случае муниципальное управление взамен концепции информативной защищенности сдерживает допуск пользователей к данным, что уменьшает степень защищенности информативных данных. Источники опасностей защищенности в муниципалитетах трудно структурировать, что обуславливает сложности по их ликвидации. Данные обстоятельства актуализируют организацию защиты иинформации и сведений в муниципальных информационных системах.

Безопасность информационной системы можно оценить как качество, содержащееся в возможности системы гарантировать конфиденциальность и

целостность информации. Угрозы информационным системам целесообразно объединить в следующие группы:

1) угроза отказа от обслуживания – блокировка доступа к ресурсу вычислительной системы;

2) угроза нарушения целостности – умышленное или неумышленное изменение баз данных, хранящихся в вычислительной системе;

3) угроза раскрытия информации.

По природе возникновения угрозы можно разделить на:

1) естественные;

2) искусственные.

Естественные угрозы – это угрозы, связанные с влиянием на информационные системы объективных физических процессов или природных явлений. Искусственные угрозы – это угрозы информационной системе, обусловленные деятельностью человека. Пользователем могут быть осуществлены непреднамеренные и преднамеренные действия, представляющие угрозу безопасности информационной системы, схематично обозначенные в таблице 2:

Таблица 2 – Непреднамеренные и преднамеренные действия, представляющие угрозу безопасности информационной системы.

Непреднамеренные действия	Преднамеренные действия
1) доведение до состояния частичного или полного отказа системы, разрушения аппаратных, программных, информационных ресурсов системы	1) физическое разрушение системы или вывод из строя наиболее важных ее компонентов
2)неправомерное включение оборудования или изменение режимов работы устройств и программ	2) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем
3) нелегальное внедрение и использование неучтенных программ, не являющихся необходимыми для выполнения служебных обязанностей, с	3) дезорганизация функционирования системы

Продолжение таблицы 2.

последующим необоснованным расходованием ресурсов	
4) заражение компьютера вирусами	4) внедрение агентов в число персонала (в том числе и в службу безопасности), вербовка персонала или отдельных пользователей, имеющих определенные полномочия
5) разглашение конфиденциальной информации	5) применение подслушивающих устройств, видеосъемка
6) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования и тд.)	6) хищение носителей информации
7) игнорирование организационных ограничений	7) незаконное получение паролей и других реквизитов разграничения доступа
8) некомпетентное использование, неправомерное отключение средств защиты информации	8) вскрытие шифров криптозащиты информации
9) ввод ошибочных данных	9) внедрение аппаратных специальных вложений, «троянских коней»
10) повреждение каналов связи	10)несанкционированное копирование носителей информации

Действия, представляющие угрозу безопасности информационной системе, могут быть и преднамеренными, что предполагает:

1) дезорганизацию деятельности информационной системы;
2) кражу любых носителей информации;
3) разрушение информационной системы или ее компонентов;
4) видеосъемку, а также использование средств подслушивающих;
5) внедрение агентов в число кадров, вербовка персонала или отдельных пользователей, имеющих определенные доступ;
6) внедрение вирусных программ «троянских коней»;

7) отключение или разрушение подсистем обеспечения функционирования вычислительных систем;

8) незаконное копирование носителей информации;

9) противозаконное получение паролей;

10) вскрытие криптозащиты информации;

Так как предпосылки угроз безопасности информационных систем на уровне муниципалитета связаны с условиями, присущими всей системе власти, можно утверждать, что способности муниципальной власти по устранению угроз ограничены, именно по этой причине существует необходимость проведения общесистемных мероприятий на уровне страны. Взаимосвязь частных и общественных сетей и совместное применение информационных ресурсов усложняют управленческое руководство к их допуску.

Проведем анализ проблем информационного обеспечения муниципальных образований Забайкальского края, который можно применить в ракурсе нашего социологического исследования.

Сфера нормативно-правового регулирования информационного обеспечения муниципалитета должна охватывать весь жизненный цикл информационного обеспечения: «проектирование - создание - эксплуатация – замена». Последний этап замены характеризуется поддержанием информационного обеспечения в актуальном состоянии. Возможны стратегии замены систем по критерию интегральных эксплуатационных расходов или по принципу переоценки.

Существуют факторы, которые непосредственно влияют на реализацию информационной безопасности, сформированные по результатам социологического опроса муниципалитетов Забайкальского края (см. рисунок 8):

1. Неквалифицированный персонал, отвечающий за обеспечение информационного обеспечения. Это один из главных факторов в формировании и становлении этого вида деятельности.

2. Нехватка ресурсов, тоже значимый фактор, ведь именно он определяет закупку и модернизацию ИКТ и его программного обеспечения.

3. Отсутствие широкополосного интернета по всей территории Забайкальского края и обеспечение всех жителей качественной связью и интернетом.

4. Изношенность оборудования и его обеспечения и др.

Рисунок 8 – Степень воздействия факторов на проблему исследования.

По рисунку 8 можно сделать вывод, что на реализацию информационной безопасности муниципалитетов в значительной степени влияют такие факторы как нехватка экономических и информационных ресурсов, а так же неквалифицированный персонал – эти факторы набрали наибольшие проценты соответственно 30 и 35.

В результате проведенного анализа реализации обеспечения информационной безопасности в Забайкалье следует выделить такие аспекты, как:

– совершенствование нормативно-правовой базы информационной безопасности, а также формирования баз данных при взаимодействии муниципальных учреждений;

– модернизация организационно-управленческих методов управления информацией внутри администрации;

– развитие мероприятий по реализации методов защиты как бумажного документооборота, так и электронного;

– эффективное управление системами и мероприятиями персональной ответственности за возникновение информационных угроз в работе администрации.

Данные направления помогут сориентировать администрацию не только на формирование системной деятельности по обеспечению информационной безопасности, но и на развитие конкретных мер в данных направлениях, что увеличит уровень информационной безопасности муниципалитета.

Значимым направлением по повышению информационной безопасности считается рационализация бумажного документооборота. В современный период в условиях информатизации каналов связи и перехода на электронный документооборот количественно повышается обрабатываемая и передаваемая информация в электронном виде. Большие объемы информации, которые содержатся на бумажных носителях, стабильно хранятся и требуют архивного хранения в бумажном виде. Более того, в муниципальной власти используются организационно-распорядительные документы, которые следует оформлять в бумажном виде. Постановления или управленческие решения органов власти требуют защиты от несанкционированного доступа. В.В. Бордюже, А.В. Белозеров утверждали: «Необходимо уменьшить специалистов подразделений администрации, участвующих в принятии управленческих решений, а также гарантировать обезличенность запроса, сохранив персональные данные заявителя только в том подразделении, куда он обратился за разрешением»[185].

[185] Бордюже, В.В., Белозеров, А.В., Софьина, И.В. Информационная безопасность: Монография / В.В. Бордюже, А.В. Белозеров, И.В. Софьина. – Пермь: Пермский центр научно-технической информации, 2009.- С 276.

В данный момент времени подобные запросы принимает муниципальное учреждение «Многофункциональный центр» (далее МФЦ). Реализация полной защиты сведений средствами МФЦ не представляется возможной. Необходимо обеспечить заявителю выбор на подачу запроса через МФЦ или в администрацию с информированием о степени защиты его конфиденциальных данных. Если данные не связаны с конфиденциальными сведениями заявителя, и он оповещен об этом, в таком случае запросы может обрабатывать МФЦ. Если запрос с информацией, которую заявителю необходимо защитить, то действует следующий алгоритм: подается запрос о документации через МФЦ или в надлежащее подразделение администрации. Еще один вариант защиты – это отправление запроса в электронном варианте с надлежащей документацией потребует личного посещения специалистов администрации. В данном случае защита информации может быть решена при помощи технических средств безопасности. Можно утверждать, что результативные методы защиты информации в подразделениях администрации муниципалитета можно осуществить при интенсивной работе по внедрению систем электронного документооборота. В электронном документообороте возможно настроить режим ограничения доступа. В отличие от бумажного документооборота для папок электронного архива рекомендуется предоставлять права доступа для редактирования ответственным пользователям. Другие пользователи обладают возможностью только на чтение данных документов. В подобном случае информация будут защищена не только от распространения, но и от несанкционированного копирования. Защита бумажных носителей способна поддерживаться мерой обязательного прописывания в инструкции специалистов персональной ответственности за распространение, либо передачу сторонним лицам информации, относящейся к конфиденциальным сведениям или к государственной тайне.

В современный период такие меры имеются в должностных инструкциях специалистов отдела кадров, касающихся в основном сведений о

государственной и муниципальной тайне, конфиденциальной информации и сведений с ограниченным доступом. Данные ограничения связаны с отдельными видами информации, однако, не касаются других видов, что уменьшает уровень безопасности муниципалитета.

Можно сделать вывод, что перечисленные выше направления по обеспечению информационной безопасности в администрации муниципалитета, связаны с формированием ноу-хау и современных информационных технологий, обладающих новыми методами защиты автоматизированных систем и программного обеспечения с целью внедрения электронного документооборота. Необходимы формы персональной ответственности и контроля за использование, распространение и несанкционированное копирование сведений. Данный надзор гарантирует технические средства, но, на наш взгляд, результативным способом будет сочетание технических средств с административными мерами контроля. Ограничение функций, осуществляемых с документами, которые содержат конфиденциальные сведения, позволит снизить риск утечек информации во внешнюю среду. Оптимизация внутренних процессов и управление персоналом администраций муниципалитетов является первоочередными мерами улучшения защиты информации. Также для эффективной организации информационной безопасности должна учитываться информационная открытость муниципалитетов и органов власти как инновационный фактор развития информатизации управления. Такова авторская оценка информационных угроз органов государственного и муниципального управления.

2.2 Информационная открытость и основные направления политического процесса по реализации информационной безопасности

В XXI в. демократическими называются те государства, которые обеспечивают как нормативно, так фактически на своей территории режим «открытого правления». Это режим, где каждый гражданин государства имеет право узнать, как эффективно, разумно и законно действует тот или иной орган публичной власти. Без необходимого качества открытости социально-политических процессов их итог чаще всего коррупционный. Государство в данном случае теряет и отстает в развитии от более открытых и потому более развитых стран – соседей.

Государственное и муниципальное управление является специфической системой, где одним из основных принципов управления является открытость власти перед обществом. Этот принцип обязательный и предполагает открытость информации при принятии и реализации управленческих решений. Можно выделить авторов, изучавших аспекты информационной открытости как государственной так и муниципальной власти: М.С. Арканникова[186], И.М. Дзялошинский[187], А.С. Довлатов[188], А.В. Иванченко[189], М.В. Черноусов[190] и другие. Необходимо отметить, что характеристика открытости муниципалитетов характеризуется чаше постановкой проблемы, чем ее решением.

---

[186] Арканникова, М.С. Информационная открытость как ресурс конкурентоспособности регионов: концептуальные подходы. – М.: Полит. ин-т. 2008. – С. 49.

[187] Дзялошинский, И.М. Информационная открытость органов местного самоуправления как основа социального партнерства [Электронный документ]. – Режим доступа: www.dzyalosh.ru.

[188] Довлатов, А.С. Государственное регулирование информационной открытости как фактор повышения эффективности национальной экономики: диссертация ... канд. эконом. н. : 08.00.05. – М.: 2004. – С. 171.

[189] Иванченко, А.В. Обеспечение открытости органов власти для граждан и юридических лиц. – М.: 2007. – 178 с.

[190] Черноусов, М.В. Совершенствование механизмов информационной открытости в системе муниципального управления // Вестник Самарского муниципального института управления: теоретический и научно-методический журнал. 2010, – № 2 (13). – 132 с.

Анализу установления гражданского общества в России как необходимого фактора развития открытого государственного управления посвящены работы Э.Я. Баталова[191], Ю.В. Ирхина[192], Д. Кина[193], В.В. Лапкина[194], В.Н. Якимца[195]. Данные работы уделяют внимание политической трансформации гражданского общества и органов государственной и муниципальной власти при переходе от одного политического режима к другому. Так же политологом Л.А. Лепиховой рассматривается возможность и перспективы внедрения новейших информационных технологий и сети интернет в политической сфере. Осуществляется это политологических исследований для обеспечения открытости государственной и муниципальной власти[196].

В современный период коммуникативное общество, все его участники непрерывно взаимодействуют. Так, согласно мнению популярного социолога Э.Гидденса, «современный мир зависит от непрерывной коммуникации или взаимодействия между людьми, пространственно отдаленными друг от друга»[197]. Таким образом, обеспечение непрерывной коммуникации в социально-политической системе является стержнем ее функционирования. Поэтому источником взаимодействия с общественностью является коммуникация, которая становится главным элементом связей с общественностью.

Государственное и муниципальное управление также представляет особые системы, где одним из принципов управления является открытость власти перед обществом. Этот принцип является обязательным для соблюдения и предполагает «обеспечение открытости информации при выработке и принятии управленческих решений»[198].

---

[191] Баталов, Э.Я. Политическое - «слишком человеческое» 2000. – 136 с.

[192] Ирхин, Ю.В. Гражданское общество и власть: проблемы взаимодействия и контроля в современной России // Социально-гуманитарные знания. 2007, – № 5.

[193] Кин, Д. Демократия и гражданское общество. – СПб.: 2001. – 400 с.

[194] Лапкин, В.В. Сравнительные политические исследования России и зарубежных стран. –М.: 2008. – 292 с.

[195] Якимца, В.Н. Оценка состояния и развития гражданского общества России: проблемы, инструменты и региональная специфика / под. ред. В.Н. Якимца. Труды ИСА РАН. – Т.57. – М.: Красанд, 2010. – 200 с.

[196] Лепихова, Л. А. Открытость политической власти: технологический анализ: дис. ... канд. полит. наук: 23.00.02 / Лепихова Лидия Алексеевна, –Ростов-на-Дону, 2007. – 164 с.

[197] Гидденс, Э. Социология. – М.: 1999.

[198] Демин, В., Пак, Т. Организация работы пресс-служб – международные стандарты. –Алматы, 2005.

Важным правом гражданина, закрепленным в Конституции Российской Федерации, является право на информацию (ст. 24, 29 Конституции РФ). А как гласит пункт «б» части 1 ст. 72 Конституции Российской Федерации: «В совместном ведении Российской Федерации и ее субъектов находится защита прав и свобод человека и гражданина»[199].

Что касается совершенствования информационной открытости органов муниципальной власти, то необходимо разработать целый комплекс мероприятий. Так, например, эффективной может быть организация специализированных общественных мероприятий, которая сделала бы работу муниципалитета наиболее понятной для общественности[200]. Необходимо также регулярно организовывать депутатские приемы граждан, выездные заседания комитетов на значимых социальных объектах, депутатские рейды контроля исполнения нормативно-правовых актов как федерального, так и местного значения.

Многие граждане заблуждаются в том, что не могут повлиять на политику страны, и нести ответственность за судьбу России. Государство нуждается в эффективной и прозрачной власти. Именно общественные организации, профессиональные союзы и партии должны представлять интересы граждан, осуществлять гражданский контроль над властью.

Для повышения доверия населения к муниципалитетам необходимо добиваться максимальной общественной подотчетности депутатов, что в частности должно включать:

– внедрение общих показателей для оценки и мониторинга общественной отчетности депутатов;

– практики кампаний органами муниципалитетов, включающие такие элементы как: право избирателей на информацию о работе депутатов в думах и позицию депутатов при принятии решений;

---

[199] Конституция Российской Федерации от 12 декабря 1993 года. // Российская газета. – 25 декабря 1993 г.

[200] Муниципальная власть и гражданское общество: проблемы диалога и перспективы развития: материалы межрегион. научн.-практ. конф. (25 февраля 2010 г.) / отв. ред. В.Б. Прокопьев. – Улан-Удэ: Изд-во Бурятского госуниверситета, 2010. – С.76.

– создание условий для общедоступного получения информации о деятельности депутатов по системе «единого открытого информационного окна», где можно было бы узнать результаты голосования, включая стенограммы выступлений по различным вопросам;

– передачи радио, материалы публикаций, должны отвечать критериям открытости и прозрачности их работы (и содержать элементы общественного отчета);

– соответствие предвыборных программ деятельности депутатов;

– развитие института общественных экспертов, оценивающих результаты работы депутатов;

– развитие практики участия граждан в заседаниях Дум.

Органы муниципальной власти должны опираться на принципы прозрачности, честности и открытости в своей деятельности с целью, чтобы данный институт носил не декларативный характер, а имел устойчивое развитие в обществе. Существуют как количественные, так и качественные показатели информационной открытости, что отмечено нами в таблице 3.

Таблица 3 – Количественные и качественные показатели информационной открытости.

Количественные	Качественные
Провести мероприятия по информационным технологиям.	В качестве экономического эффекта ожидается привлечение инвестиций в муниципальные районы Забайкалья. Политический эффект – информационная открытость и анализ СМИ как актора политики.
Опросить наибольшее количество граждан и муниципальных служащих по проблеме информационной открытости, не менее 300 респондентов.	В результате реализации повысится мощность позиционирования региональных и муниципальных властей в СМИ и будет дана им положительная оценка.
Разработать три направления развития муниципальной системы.	Так как информационная открытость служит основой информационной безопасности органов власти, то наступит оптимизация внутренних процессов и улучшение управления персоналом администраций муниципалитетов.
Провести тренинги и лекции по безопасности информационных систем в социально-политических системах субъектах РФ	В результате реализации повысится информационная грамотность граждан и государственных, муниципальных служащих.

Анализ таблицы 3 показывает, что назрела необходимость перехода количественных показателей в качественные характеристики. Осуществление путей совершенствования информационной безопасности Забайкалья является качественным приоритетом информационного развития субъекта РФ.

В рамках обеспечения информационной открытости государственной и муниципальной власти 26 декабря 2013 г. Правительственной комиссии по координации деятельности открытого правительства утверждена Методика мониторинга и оценки открытости федеральных органов исполнительной власти[201]

Основными методами мониторинга открытости являются:

а) самообследование (самоанализ) федеральными органами исполнительной власти достигнутых результатов по внедрению и развитию механизмов (инструментов) открытости;

б) экспертная оценка эффективности внедрения федеральными органами исполнительной власти механизмов (инструментов) открытости и соответствия их деятельности принципам, целям и задачам открытости, утвержденными Концепцией открытости (далее – экспертная оценка);

в) социологические исследования по изучению уровня доверия и удовлетворенности граждан, общественных объединений и предпринимательского сообщества уровнем открытости федеральных органов исполнительной власти.[202]

Самообследование федеральные органы исполнительной власти проводят по каждому из механизмов (инструментов) открытости, предусмотренных Концепцией открытости:

1. Реализация принципа информационной открытости федерального органа исполнительной власти.

---

[201] Методика мониторинга и оценки открытости федеральных органов исполнительной власти утверждена протоколом заочного голосования Правительственной комиссии по координации деятельности открытого правительства от 26 декабря 2013 г. № АМ-П36-89пр [Электронный ресурс]. – Режим доступа: open.gov.ru/upload/iblock/f32/f32f65ebe06aa62bb1a9f247e5c85dda.doc.

[202] Там же.

2. Обеспечение работы с открытыми данными.

3. Обеспечение понятности нормативно-правового регулирования, государственных политик и программ, разрабатываемых (реализуемых) федеральными органами исполнительной власти.

4. Принятие планов деятельности федеральных органов исполнительной власти на период 2013 - 2018 гг. и годовой публичной декларации целей и задач; их общественному обсуждению и экспертному сопровождению.

5. Формирование отчетности федерального органа исполнительной власти.

6. Информирование о работе с обращениями граждан и организаций.

7. Организация работы с референтными группами федерального органа исполнительной власти.

8. Взаимодействие федерального органа исполнительной власти с общественным советом.

9. Работа пресс-службы федерального органа исполнительной власти.

10. Организация независимой антикоррупционной экспертизы и общественного мониторинга правоприменения.[203]

Внедрение каждого из механизмов (инструментов) открытости предполагает наличие 3 стадий развития механизма (инструмента) открытости в деятельности федеральных органов исполнительной власти (далее - стадия), которые отражают последовательное формирование и совершенствование конкретного механизма (инструмента) открытости.

Показатели развития механизмов (инструментов) открытости (далее - показатели развития), распределенные по трем стадиям, могут учитываться федеральными органами исполнительной власти при разработке и утверждении ведомственных планов (дорожных карт), реализации принципов открытости в своей деятельности.

---

[203] Методика мониторинга и оценки открытости федеральных органов исполнительной власти утверждена протоколом заочного голосования Правительственной комиссии по координации деятельности открытого правительства от «26» декабря 2013 г. № АМ-П36-89пр [Электронный ресурс]. – Режим доступа: open.gov.ru/upload/iblock/f32/f32f65ebe06aa62bb1a9f247e5c85dda.doc (дата обращения 08.09.2019).

Выполнение показателей развития первой стадии является обязательным для внедрения каждого механизма (инструмента) открытости, поскольку они устанавливаются на основе требований нормативно-правовых актов. Показатели развития второй стадии отражают динамику формирования и использования механизмов (инструментов) открытости в деятельности федеральных органов исполнительной власти. На третьей стадии показатели развития учитывают использование федеральным органом исполнительной власти для совершенствования работы механизмов (инструментов) открытости веб-технологий.

Все показатели развития на каждой из трех стадий для всех механизмов (инструментов) открытости оцениваются по номинальной шкале: по факту наличия или отсутствия значения и (или) по факту формального соответствия «есть» – «нет». Значение показателя развития принимается равным нулю в случае ответа при оценке внедрения «нет», равным единице – «частично да, частично нет», равным двум – «да».

Оценка внедрения рассчитывается федеральными органами исполнительной власти путем суммирования значений показателей развития по каждой из трех стадий отдельно. Первая стадия оценивается как 0,1 от суммы значений показателей, а результирующая оценка введения для каждого из инструментов открытости рассчитывается по формуле, показанной на рисунке 9:

$$OS_{1\div x} = S_1 + 0{,}1 \times S_1 \times (S_2 + S_3)$$

$OS_{1\div x}$ – результирующая оценка внедрения каждого из механизмов (инструментов) открытости

x – количество созданных федеральным органом исполнительной власти механизмов (инструментов) открытости

S_1 – сумма значений показателей развития на первой стадии

S_2 – сумма значений показателей развития на второй стадии

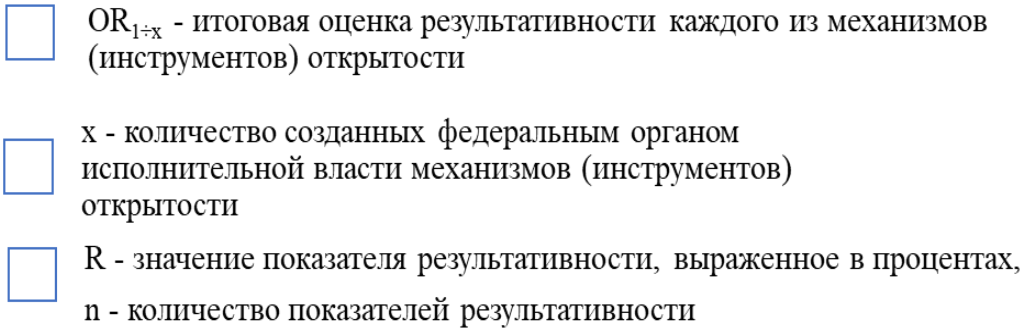
S_3 – сумма значений показателей развития на третьей стадии

Рисунок 9 – Формула расчета оценки внедрения.

Для анализа итогов и динамики введения инструментов открытости формируются характеристики результативности работы инструментов открытости (далее – показатели результативности). При достижении по инструменту открытости всеми федеральными органами власти суммы значений первой стадии равной 10, показатели развития упраздняются, и вместо них по решению правительственной комиссии добавляется новый показатель результативности. Аналогично правительственной комиссией принимается решение по упразднению показателей развития на второй и третьей стадиях соответственно.

Значения показателей результативности рассчитываются на основе статистических показателей федеральными органами исполнительной власти и выражаются в процентах. Таким образом, оценка результативности для каждого инструмента открытости рассчитывается по следующей формуле, представленной на рисунке 10:

$$OR_{1\div x} = 0{,}1 \times (R_1 + R_2 + R_n)$$



$OR_{1\div x}$ - итоговая оценка результативности каждого из механизмов (инструментов) открытости

x - количество созданных федеральным органом исполнительной власти механизмов (инструментов) открытости

R - значение показателя результативности, выраженное в процентах,

n - количество показателей результативности

Рисунок 10 – Формула расчета значений показателей результативности.

Значение интегрального показателя введения созданных федеральным органом исполнительной власти инструмента открытости рассчитывается по формуле: $OV_{1\div x} = OS_{1\div x} + OR_{1\div x}$, где:

$OV_{1\div x}$ - интегральный показатель внедрения каждого из механизмов (инструментов) открытости, $OS_{1\div x}$ - результирующая оценка внедрения каждого из механизмов (инструментов) открытости, $OR_{1\div x}$ - итоговая оценка результативности каждого из механизмов (инструментов) открытости/ x - количество созданных федеральным органом исполнительной власти механизмов (инструментов) открытости.

Результаты проведенного самообследования федеральные органы исполнительной власти представляют в правительственную комиссию для формирования общего рейтинга открытости федеральных органов исполнительной власти. Результаты самообследования также подлежат опубликованию на интернет-ресурсе системы «Открытое Правительство».

По результатам мониторинга открытости рассчитывается индекс открытости, который на основе единого подхода к оценке уровня открытости федеральных органов власти позволяет формировать общий рейтинг открытости федеральных органов исполнительной власти.

На начальном этапе проведения мониторинга открытости индекс открытости определяется путем суммирования значений показателей открытости, полученных для каждого федерального органа исполнительной власти, по формуле:

$$O = (OV_1 + OV_2 + OV_x) / 10 + (OQ_1 + OQ_2 + OQ_x) / 10 + 0{,}1 \times (M_1 + M_n),$$

где: O - индекс открытости, $OV_{1 \div x}$ - интегральный показатель внедрения каждого из механизмов (инструментов) открытости, $OQ_{1 \div x}$ - итоговая экспертная оценка эффективности работы каждого из механизмов (инструментов) открытости, x - количество созданных федеральным органом исполнительной власти механизмов (инструментов) открытости, M - результаты мониторинга экспертной оценки эффективности механизма (инструмента) открытости, выраженные в процентах в соответствии с установленной шкалой оценки, n - количество учитываемых мониторингов экспертной оценки эффективности механизма (инструмента) открытости.

При расчете рейтинга открытости федеральных органов исполнительной власти могут учитываться результаты социологических исследований по изучению доверия и удовлетворенности граждан, общественных объединений и предпринимательского сообщества уровнем открытости федеральных органов исполнительной власти. Таким образом, в рамках проекта «Открытый регион» для обеспечения информационной открытости государственной и муниципальной власти 26 декабря 2013 г. правительственной комиссии по координации деятельности открытого правительства утверждена Методика мониторинга и оценки открытости федеральных органов исполнительной власти, анализ которой приведен в нашей диссертационной работе.

Таким образом, постоянное совершенствование обеспечения открытости деятельности органов муниципальной власти является самым верным путем к максимизации доверия граждан к властным структурам, успешному осуществлению проводимых в стране преобразований.

Что касается основных направленний политического процесса по обеспечению информационной безопасности, то стабильное функционирование региональных социально-политических комплексов управления зависит от состояния информационной безопасности (далее ИБ) политического процесса. Под информационной безопасностью политического процесса понимается состояние защищенности информационной среды, обеспечивающее развитие в интересах граждан. Обеспечение ИБ связано с защитой прав личности, общества, государства на получение достоверной информации законными способами, на неприкосновенность частной жизни, на сохранение и приумножение духовно-нравственных и культурных ценностей, норм и традиций общественной жизни. Как отмечено А.А. Шелупановым: «Решение поставленных задач невозможно без участия в системе обеспечения ИБ РФ акторов политического процесса»[204].

К основным направлениям деятельности по обеспечению ИБ, сформулированным на основе анализа содержания Доктрины информационной безопасности Российской Федерации, относятся:

– формирование, и рациональное управление информационными ресурсами;

– выявление угроз ИБ и их источников;

– защита информационных прав личности, общества от негативных информационных воздействий;

– защита информации, составляющей государственную тайну, от угроз ее утечки, в том числе в результате несанкционированного доступа к информации;

– защита информации от несанкционированных и непреднамеренных воздействий.

Указанные направления реализуются конкретными видами деятельности, выполняемыми органам власти, предприятиями, учреждениями в соответствии с их компетенцией. Слаженность деятельности по обеспечению ИБ требует

[204] Шелупанов, А.А., Зайцев, А.П., Мещеряков, Р.В. Основы защиты информации. Изд. 5-е, перераб. И доп. – Томск: В-Спектр, 2011. – 244с.

скоординированных действий в условиях сложности возникающих проблем. К основным координируемым проблемам относятся:

1. Прогнозирование угроз ИБ и последствий их реализации. Для решения проблемы целесообразно создание моделей угроз применительно к направлениям обеспечения ИБ.

2. Разработка нормативно-правового обеспечения защиты информационных ресурсов, в том числе конфиденциальной информации.

3. Формирование единой политики учета и систематизация реализации доступа к информационным ресурсам.

4. Совершенствование информационно-телекоммуникационных средств и систем органов власти.

5. Локализация распространения недостоверной информации, информационно-психологических воздействий на граждан по различным каналам.

6. Развитие систем защиты технических каналов информации от разведок и утечек.

7. Проведение мероприятий по обеспечению важных объектов информационной инфраструктуры в условиях угрозы терроризма.

8. Повышение квалификации специалистов в области ИБ.

Каждая из проблем требует специфических методов решения. Общая координация решения данных проблем может осуществляться созданным специализированным советом, а решение конкретных организационно-технических вопросов целесообразно возложить на компетентные учреждения региона по каждой из проблем. Для этого могут быть созданы соответствующие координационные советы.

Рассмотрим варианты развития системы защиты информации (далее СЗИ). Первый вариант развития управления СЗИ:

– создание нормативно-правовых, научно-технических, организационных и информационных условий для управления СЗИ;

– организация эффективной системы управления деятельности в области защиты информации, приспособленной к изменениям внешней среды;

– обеспечение эффективного уровня защиты информации, составляющей государственную тайну, от несанкционированного доступа к такой информации.

При реализации данного варианта развития обеспечивается защита конфиденциальной информации от угроз несанкционированного доступа и непреднамеренных воздействий. Вопросы защиты коммерческой и профессиональной, а также персональных данных находятся вне компетенции деятельности СЗИ.

Второй вариант развития управления СЗИ может быть детализирован:

1. Сфера деятельности СЗИ должна быть ограничена защитой только информации, заключающей государственную тайну, здесь исключается защита служебной тайны. В этом случае ресурсы СЗИ сосредотачиваются на защите важной информации. Однако, возникает опасность неравномерной защиты одной и той же информации в органах муниципалитета и органах государственной власти, что впоследствии может нанести ущерб их деятельности. Также, непринятие мер по защите служебной информации, отнесенной к тайне, создает предпосылки к раскрытию информации при анализе массивов сведений.

2. СЗИ может расширить деятельность в результате возложения на себя дополнительной ответственности по защите персональных данных. Необходимость данной ответственности обусловлена тем, что персональные сведения накапливаются в больших объемах в органах муниципалитета и, по сути, являются информацией, относимой к служебной тайне. Деятельность негосударственных организаций, связанная с обработкой персональных данных подлежит государственному лицензированию в соответствии с ФЗ 149 «Об информации, информационных технологиях и о защите информации». Защита безопасности персональных данных нацелена на реализацию одной из функций государства, а именно на обеспечение прав и свобод граждан. Возложение на СЗИ

функции по защите персональных данных повлечет за собой необходимость выполнения дополнительных задач управления.

3. Сфера деятельности СЗИ содержит проблемы обеспечения защиты коммерческой тайны, в данном контексте необходимо отметить, что государственные органы не могут возложить на себя полную ответственность по защите данных видов информации, так как режим защиты устанавливается собственником такой информации. Функции СЗИ в данном случае ограничиваться правовыми условиями для развития инфраструктуры в области защиты различных видов информации.

4. Деятельность СЗИ может рассматривается широко и включает вопросы защиты информационных ресурсов по техническим каналам с ограниченным доступом от утечки информации и несанкционированного доступа.

Осуществление данного варианта развития наиболее соответствует увеличению степени безопасности и устойчивого развития региона, но понадобится интенсификация полномочий контрольных органов, увеличение их численности, разработка нормативно-правовой базы по вопросам защиты информации. Перечисленные выше варианты развития СЗИ не являются в полной мере альтернативными, их можно рассмотреть как отдельные этапы развития системы.

На первом этапе целью развития СЗИ является обеспечение требуемого уровня ИБ и защита информации от несанкционированного доступа и непредумышленного влияния по техническим каналам. На втором этапе усилия деятельности СЗИ сосредоточены на обеспечении эффективной реализации информационной безопасности по защите сведений, составляющих служебную тайну. Третий этап развития СЗИ нацелен на реализацию необходимого уровня безопасности персональных данных. На четвертом этапе развития СЗИ появляется защита информации, составляющая коммерческую и профессиональную тайну. На пятом этапе деятельности СЗИ обеспечивается требуемый уровень защиты

информационных ресурсов от утечки информации, включающей тайну. Таким образом, цель СЗИ состоит в достижении развития деятельности этой системы.

В настоящее время нецелесообразна реализация третьего варианта СЗИ. Принятый в настоящее время принцип управления СЗИ, основанный на децентрализованном управлении, наиболее полно соответствует основным принципам управления в современном государстве. Децентрализованное управление с межведомственной координацией органов исполнительной власти, функционирующих на коллективной базе, гарантирует равновесие различных ведомств, предприятий и организаций вневедомственной принадлежности в интересах регионов в целом.

Приоритетность и важность решения задач формирования СЗИ в современный период обуславливается потребностью, в первую очередь, сохранить и гарантировать развитие организационной структуры СЗИ как основы функционирования системы. В перспективе следует формировать концепцию мониторинга характеристик состояния и развития информационного обеспечения деятельности органов СЗИ. Очевидно, что взаимный обмен данными между органами СЗИ создает из совокупности изолированных органов систему, способную решать общие задачи. В конечном итоге, следует гарантировать усовершенствование системы документооборота в области СЗИ по упорядочиванию деятельности всех органов СЗИ по достижению информационной безопасности.

Таким образом, существуют следующие основные направления по обеспечению информационной безопасности политического процесса России:

1. Выявление угроз информационной безопасности.
2. Совершенствование информационных средств.
3. Реализация уровней защиты информации путем создания системы защиты информации, которая сводится к ответственности за защиту персональных данных, коммерческой и профессиональной тайны, к реагированию на

несанкционированное воздействие как на технические каналы, так и на информационные системы.

Следует отметить, что совершенствование механизмов реализации открытости государственного управления в субъектах Российской Федерации, направлено, в первую очередь, на:

1. «Снижение уровня коррупции, в том числе в процессе предоставления бюджетных услуг, а также их усиление результативности предоставления за счет формирования конкурентной среды в их исполнении и более полного применения возможностей общества в разработке управленческих решений и реализации отдельных государственных задач.

2. Совершенствование качества управленческих решений органов государственной и региональной власти.

3. Повышение профессиональных возможностей и кадрового потенциала государственной гражданской службы.

4. Подъем качества государственных и муниципальных услуг, а также уровня удовлетворенности населения данным качеством.

5. Своевременный и оптимальный ответ на социально-экономические вызовы, следствие чего осуществляется рост качества жизни».[205]

В методических рекомендациях по внедрению принципов и механизмов открытого государственного управления для субъектов РФ определены направления по улучшению и формированию информационной открытости (см. таблицу 4):

[205] Методические рекомендации по внедрению принципов и механизмов открытого государственного управления в субъектах Российской Федерации [Электронный ресурс]. – Режим доступа: http://open.gov.ru/upload/iblock/00f/00fe0e47c2b1d068ad07318689bb13c4.pdf.

Таблица 4 – Направления по улучшению и формированию информационной открытости.

Направление	***Задачи***
1. Повышение доступности и прозрачности информации о государственной деятельности:	− обеспечение государством качественного сбора и хранения информации, обеспечение доступности информации для граждан, оперативное реагирование на информационные запросы; − расширение доступной информации и раскрытие данных о деятельности разных уровней власти в формате, приспособленном для дальнейшего использования и создания востребованных обществом информационных продуктов; − публикация данных о государственных расходах и выполнении важных общественных услуг и работ; − анализ и учет требований общества к информации.
2. Стимулирование участия гражданского общества в процессе формирования и принятия решений:	− повышение прозрачности управленческих процессов; − создание и использование каналов обратной связи от общества; − настройка механизмов гражданского участия в разработке, контроле и оценке деятельности органов государственной власти; − обеспечение свободы выражения мнения и собраний в работе некоммерческих организаций; − создание механизмов, способствующих активизации сотрудничества между органами государственной и муниципальной власти, с одной стороны, и организациями гражданского общества и бизнесом – с другой.
3. Применение новых стандартов профессиональной деятельности и этики в системе государственного управления:	− утверждение правил и норм, в соответствии с которыми министерства и ведомства, а также отдельные государственные и муниципальные служащие отчитываются о своей деятельности публично, принимают ответственность за результаты работы и целевые показатели, введение показателей и контракта эффективности государственных гражданских

Продолжение таблицы 4.

	− служащих, практики публичных отчетов и деклараций целей министерств и ведомств; − введение антикоррупционных механизмов и практик, обеспечивающих прозрачность управления государственными финансами и закупками; − установление и/или поддержание правовой основы предоставления общественности информации о доходах и активах государственных чиновников высокого ранга; − совершенствование механизмов оспаривания незаконных решений чиновников, защита интересов лиц, сообщающих о нарушениях; − повышение квалификации и развитие компетенций государственных гражданских служащих, создание региональных и межрегиональных центров компетенций.
4. Расширение доступа к новым технологиям в целях открытости, повышения качества работы и подотчетности правительств:	− применение инновационных технологий для обнародования значительных объемов информации, способствующих понятности и доступности деятельности органов власти, контролю бюджетных расходов со стороны граждан; − развитие доступных и защищенных онлайн платформ для оказания социальных услуг, привлечения общественности, обмена опытом и идеями; − обеспечение равного доступа к сети Интернет и мобильной связи как к инфраструктуре открытости; − продвижение альтернативных механизмов гражданского участия в процессе формирования и принятия решений; − стимулирование использования технологических инноваций как государственными служащими, так и гражданами; − обеспечение свободного доступа граждан к новым технологиям.

В целом, введение механизмов информационной открытости государственного и муниципального управления является важным в силу того, что:

- Механизмы содействуют увеличению подотчетности и прозрачности.
- Происходит удовлетворение граждан качеством государственного и муниципального управления.
- Расширение возможностей непосредственного участия граждан в процессах контроля, разработки и экспертизы исполнения управленческих решений.
- Формирование механизмов общественного контроля за деятельностью органов власти и исполнение ими управленческих решений и функций.
- Увеличение доступности государственных и муниципальных услуг.

Выявление общего вектора развития информационного противоборства возможно при помощи анализа возникающих и постоянно уточняемых теоретических построений. В отличие от предыдущих лет, в современный период основной интерес в научном дискурсе, уделяется уже не технической стороне проблемы, а психологическим и организационно-административным аспектам информационного противоборства, причем сведения рассматриваются как цель и способ действий, предпринимаемых для разрешения конфликта. Подобная смена приоритетов, безусловно, не убирает с повестки дня формирование и усовершенствование технических аспектов, так как информационные технологии являются важным элементом информационного противоборства.

По нашему мнению, информационные объекты в ходе конкретных информационных операций могут подвергаться различному воздействию. Например, компьютерная сеть или телекоммуникационные сети способны либо быть уничтожены или повреждены физически, либо могут быть изменены программно в результате вирусного проникновения или хакерской атаки. В результате подобного воздействия на информационные системы могут быть похищены важные сведения. Помимо этого, сами вышесказанные системы могут послужить механизмом информационного противоборства.

Исследование проблемы ведения информационного противоборства, в том числе установление возможностей с целью планирования мероприятий по исполнению или отражению информационного влияния, требует наиболее четкого раскрытия ключевых направлений информационного противоборства.

Нами были выделены такие направления:

1) Первое направление: борьба с системами управления.

Борьба с системами управления может быть определена как военная стратегия, предусматривающая ликвидацию систем и отсечение управленческих структур вооруженных сил противника от управляемых элементов для дестабилизации военного управления. Подобная борьба способна достигаться как непосредственным уничтожением управляющих структур, так и ликвидацией телекоммуникационных сетей связи, которые координируют структуру управления. Выбор метода борьбы определяется в соответствии с поставленными тактическими и стратегическими целями.

Особая важность информационных действий против систем управления заключается в том, что они имеют значимые шансы быть результативными на ранних стадиях зарождения конфликта, помимо этого, формируются предпосылки бескровной победы над противником. Но, данные «преимущества» могут быть в существенной степени нивелированы противником с помощью децентрализации управляющих систем и ведения так называемой «сетевой войны».

2) Второе направление: информационно-разведывательные операции.

Информационно-разведывательные операции в конкретном значении считаются развитием концепции оперативной разведки, несмотря на то, что между ними прослеживаются значительные отличия, сопряженные с тем, что получаемые в процессе информационно-разведывательных операций сведения, поступают напрямую участникам операции. Данные военной разведки направляются в командные центры, где они аккумулируются и затем в качестве приказов доводятся до подчиненных. Очевидно, что речь идет об приспособлении оперативной разведки к децентрализованной системе военного управления и

ведения боевых действий, требующих существенных поправок в сбор, обработку и распределение разведывательной информации.

В процессе информационно-разведывательных операций создаются новые децентрализованные и автоматизированные системы. В этой связи целесообразно рассмотреть два этапа таких операций. Первый, условно называемый «наступательным» этапом, обеспечивает сбор разведывательных сведений о противнике, а второй, «оборонительный» этап, связан с защитой сведений и ориентирован на противодействие информационно-разведывательным операциям противника.

3) Третье направление – это электронная борьба.

В первую очередь, необходимо выделить, что первые два рассмотренные выше направления информационного противоборства по сути предполагают борьбу с информационными системами, либо борьбу при помощи данных систем. В отличии от них, целью электронной борьбы, как практического способа ведения информационного противоборства, считается сокращение информационных способностей противника, в соответствии с чем она подразделяется: на борьбу с коммуникационными сетями противника, радиоэлектронную борьбу, криптографическую борьбу.

4) Четвертое направление – это психологическая борьба.

Речь идет о психологической борьбе в тех случаях, когда применение механизмов информационного противоборства ориентировано не против информационных систем противника, а напрямую против разума и психики человека. Психологическая борьба определяется как манипулирование общественным сознанием, мнением различных социальных групп. На Западе в рамках психологической борьбы принято выделять следующие основные виды информационно-психологических операций:

- операции по деморализации личного состава вооруженных сил;
- операции, ориентированные против структур военного командования;
- операции, направленные против структур государственного управления.

5) Пятое направление – это «хакерская» борьба.

Определение хакерской борьбы ориентировано главным образом на разнообразные элементы компьютерных сетей и информационные ресурсы. Главной характерной чертой хакерских «атак» является, что они носят не аппаратный, а программный характер. Некоторые западные аналитики считают, что информационное противодействие в основном должно сводится исключительно к хакерской борьбе. В современный период наиболее распространенными средствами хакерской борьбы считаются: «черви», компьютерные вирусы, «троянские кони», прошивка постоянного запоминающего устройства, логические бомбы. Приведенные выше средства могут анализироваться как примеры информационного оружия, реализованного в форме вредоносных программ.

6) Шестое направление ориентировано на «кибернетическую» и «сетевую» борьбу, которые, несмотря на вполне «техническое» звучание, в наименьшей степени связаны с информационными технологиями и содержат целый комплекс вопросов информационного противоборства, а именно: организационные, тактические, доктринальные, технические и стратегические задачи.

Таким образом, в современный период кибернетическая борьба, принадлежащая к информационно-ориентированным военным операциям, все более актуализируется в военной сфере, особенно это касается конфликтов значительной интенсивности. Кроме того, свое отражение кибернетическая борьба нашла в применении новых технологий в военной сфере.

С другой стороны, значимость сетевой борьбы увеличивается в конфликтах невысокой интенсивности и при проведении конфликтных операций, носящих невоенный характер. При этом понятие сетевой борьбы принадлежит скорее к организационной форме противоборства, применяющей информационные возможности по борьбе с противником. Применение информационных инфраструктур противника в этих случаях предполагает концепцию сетевой борьбы.

7) Седьмое направление связано с экономической информационной борьбой.

В современных условиях ведения информационной войны в экономической сфере выделяются две формы экономического информационного противоборства: информационная блокада и информационный империализм.

Информационная блокада в условиях глобализации и формирования цифровой экономики гибко воздействует на потенциального противника. В отличие от введения эмбарго на товары или другие экономические санкции, информационная блокада способна носить латентный характер, а информационные операции могут быть завуалированы под случайные хакерские проникновения компьютерных хулиганов или случайные сбои информационных систем. При этом, безусловно, не снимается вероятность открытого и прямого государственного давления в этой сфере.

По поводу информационного империализма, глобализация мировых экономических процессов гарантирует формирование современных информационных технологий. Наиболее адаптированными к результативной экономической деятельности являются США. Отметим, что разработка основных компонентов и программного обеспечения компьютерной техники сосредоточена, прежде всего, в Америке. Это дает США принципиальную возможность подчинять своим интересам функционирование мировых информационно-коммуникационных систем.

8) И наконец, восьмое направление – международный информационный терроризм.

К противоборству не может быть отнесен сам по себе терроризм (кроме государственного терроризма). Однако, в своей интернациональной форме и в связи с трансформацией терроризма в сторону применения современных высокотехнологичных методов влияния[206] террористические организации, не являясь субъектами международного права, могут выступать как самостоятельные субъекты международной политики. В условиях

[206] Федоров, А.В «Супертерроризм. Новый вызов нового века» – М.: «Права человека», 2003.

информационного противостояния, стремительного развития информационных технологий проблема международного терроризма обретает новое звучание. Это сопряжено, в первую очередь, с двумя аспектами: с применением террористическими организациями информационной структуры для формирования сетевых методов, а также террористическим влиянием на объекты информационных инфраструктур.

Террористические организации со временем трансформируются от иерархической структуры к информационно-ориентированной сетевой организации. Внутри организации личностное воздействие лидера все больше уступает место упрощенной децентрализованной системе.

Наравне с сохранением принципов влияния на объекты, распад которых способен спровоцировать за собой существенные жертвы у населения и вызвать значительный политический и общественный резонанс, осуществляется трансформация взглядов на террористическую борьбу как на прямой способ достижения власти.

Несвязанные инертностью формирования государственных институтов, террористические организации стремительно принимают на вооружение информационные технологии с целью выполнения конкретных террористических операций. Очевидно, что террористические организации нарушают целостность и работоспособность информационных сетей, что дает им возможность оперативно согласовывать свои действия, а также пропагандировать свои взгляды.

И, наконец, необходимо принимать во внимание возможность того, что государства, проводящие информационные операции, будут скрывать свои действия под террористическую деятельность некоторых известных или неизвестных групп. В этой связи наравне с трудностями поиска стратегии защиты от террористического влияния все большую актуальность приобретают задачи адекватного реагирования на возникающие вызовы в информационном пространстве.

Не исключается и вариант, когда в качестве агрессивной стороны способно выступать не государство, а террористическое сообщество, применяющее в собственных действиях информационную инфраструктуру государства. При этом четко устанавливается источник атаки и ответные меры.

Подводя итоги второй главы, целесообразно обозначить следующее:

1. При оценке информационных угроз выделяются факторы риска безопасности информации. Согласно «Доктрине информационной безопасности Российской Федерации» источники угроз делятся на внешние и внутренние. Наиболее существенными угрозами является уровень коррупции как государственных, так и муниципальных органов власти.

2. Проведён анализ проблем информационного обеспечения муниципальных образований Забайкальского края, выделены характеристики информационного обеспечения: «проектирование – создание – эксплуатация – замена». Показаны факторы, которые непосредственно влияют на реализацию информационной безопасности, сформированные по результатам социологического опроса муниципалитетов Забайкальского края:

– неквалифицированный персонал;

– нехватка ресурсов;

– отсутствие широкополосного интернета по всей территории Забайкальского края;

– изношенность информационного оборудования.

3. Информационная открытость муниципалитетов является основой имиджа. Информационная открытость означает соблюдение принципа информационной открытости административно-управленческой деятельности, прозрачности, а также создание механизмов эффективного и общественного контроля. Кроме того, информационная открытость органов муниципальной власти предполагает равный доступ граждан к информации о властных структурах.

4. Выделены направления информационного противоборства: борьба с системами управления, информационно-разведывательные операции,

электронное, психологическое, «хакерское», «кибернетическое», «сетевое», экономическое, информационное столкновения и международный информационный терроризм.

ГЛАВА 3 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПОЛИТИЧЕСКОГО ПРОЦЕССА НА ПРИМЕРЕ МУНИЦИПАЛИТЕТОВ ЗАБАЙКАЛЬСКОГО КРАЯ

3.1 Информационная открытость муниципальных районов Забайкальского края в контексте анализа их информационной освещённости

Информационная открытость органов муниципальной власти предполагает открытость действий и решений власти, возможность получения, поиска и распространения информации в сфере социально-политических отношений, равный доступ граждан к информации о властных структурах. К сожалению, в современный период многие чиновники заблуждаются в том, что уровень информационной открытости зависит от их личного усмотрения, а не от нормы закона.

По справедливому замечанию А.А, Вилкова и других авторов: «В России явление «закрытости» власти проявляется на протяжении всей нашей истории. Менялись политические режимы и формы правления, происходили революции, но неизменным оставалось состояние замкнутости, обособленности и связанное с ним непонимание действий власти обществом».[207]

Еще с советских времен засекреченной была фактически вся информация о деятельности муниципальной власти, но несмотря на процессы демократизации, проблема «открытости» муниципальной власти является актуальной и по сегодняшний день. К сожалению, власть воспринимается обществом как закрытый, не контролируемый обществом институт.

Несмотря на то, что главной обязанностью чиновников является оказание услуг населению, в настоящее время органы муниципалитетов осуществляют услуги дистанционно. В данной ситуации просматривается закономерная реакция

[207] Вилков, А.А., Некрасов, С.Ф., Россошанский, А.В. Политическая функциональность современных российских СМИ. Саратов: Издательский центр «Наука», 2011. – 268с.

граждан на деятельность властей, демонстрируется недоверие, отчуждение и конформизм.

Невозможно прослеживать динамику гражданского общества без обеспечения максимального и свободного доступа граждан к информации о деятельности органов муниципальной власти. Данный институт осуществляет помощь в контроле за действиями муниципальных органов, оказывает конструктивное влияние на принятие ими решений.

С принятием федерального закона «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»[208], возник институт свободы доступа к официальной информации, данный институт направлен на борьбу с коррупцией. Эффективность работы института апробирована на международной арене в контексте антикоррупционной политики. Недоработкой данного ФЗ является несформированность современных методов контроля над исполнением его норм по надлежащему качеству доступа к информации о деятельности государственных органов и органов местного самоуправления.

Потребность в «условиях глобального информационного общества более широкого применения альтернативных методов разрешения спорных моментов»[209] была установлена в «Окинавской хартии глобального информационного общества», которая была подписана лидерами стран «Большой Восьмерки» и Президентом Российской Федерации 22 июля 2000 г.

По опыту зарубежных стран, имеющих аналогичную законодательную базу, специализированные органы власти работают с информационной открытостью: по жалобам, надзору и контролю исполнения нормативных актов в сфере защиты информации. В качестве примера в 2000 г., Великобритания в своем законе «О свободе информации» сформировала специальный орган по рассмотрению споров

---

[208] Федеральный закон от 09.02.2009 N 8-ФЗ (ред. от 09.03.2016) «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_84602/.

[209] Окинавская хартия глобального информационного общества // 22 июля 2000 г. [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/supplement/3170.

Комиссара и Трибунала по вопросам информации или Комиссию по доступу к административным документам (CADA), которая является парламентским учреждением.[210]

Чтобы общество встало на путь демократии, власть должна быть открытой, этот тезис, все чаще обсуждают в современный период. Многие утверждают, что власть не заинтересована стать прозрачной для граждан. Вопросы открытости власти часто рассматриваются в аспекте, что открытость – это реализация права граждан на доступ к правовой информации, где формально право на доступ обеспечивается нормативно-правовой базой. Действует всем известный принцип, который гласит, что нормативно-правовой акт вступает в силу лишь после его официального опубликования. Но проблема не исчерпывается этим и является более сложной. Нужно признать, что потребности населения в информации о деятельности муниципальной власти, о принимаемых властных решениях, прямо влияющие на интересы граждан, не могут быть удовлетворены только фактом публикации. Очевидно, что формирование информационной политики представляется одним из приоритетных направлений сфер деятельности муниципальной власти.

Так, по Федеральному закону № 131 глава муниципального образования подконтролен и подотчетен населению и представительному органу муниципального образования. Подотчетность главы устанавливается в формах, указанных на рисунке 11.

Анализ правотворчества муниципалитетов показывает, что чаще всего принимаются нормативно-правовые акты, регулирующие порядок предоставления информации о проведенных торгах (конкурсах) на закупку товаров, работ и услуг для муниципальных нужд.

[210] С деятельностью данной комиссии можно познакомиться на ее сайте [Электронный ресурс]. – Режим доступа: http://www.cada.pt/.

Рисунок 11 – Формы подотчетности главы муниципалитета перед населением (составлена автором на основании ФЗ-131).

Большую роль в обеспечении информационной открытости органов местного самоуправления играют разные институты непосредственной демократии на местном уровне:

- публичные слушания;
- правотворческая инициатива граждан;
- собрание граждан;
- конференция граждан (собрание делегатов), опрос граждан.

Безусловно, муниципальное самоуправление играет особую роль в системе политических отношений.

С одной стороны, местное самоуправление – это элемент гражданского общества. Эти два феномена не тождественны, но тесно взаимосвязаны.

Муниципалитет – это не только элемент гражданского общества, но один из важнейших факторов развития данного общества.

С другой стороны, местное самоуправление в отличии от других институтов гражданского общества, не может существовать вне рамок государства. Это именно тот институт, который тесно связан с государством и его органами и, будучи автономным от государственной власти, осуществляет часть функций государства, являясь носителем публичной власти. Можно сделать вывод, что местное самоуправление выступает связующим звеном между гражданским обществом и государством. Именно этим определяется его значимость в системе политических отношений. Местное самоуправление предоставляет широкий спектр возможностей для участия населения в политическом процессе и здесь необходимо обеспечить максимальную доступность органов местного самоуправления для гражданина, поскольку ему предоставляется возможность сыграть активную политическую роль.

Информационная открытость предполагает освещённость населения о деятельности органов муниципальной власти, а также с помощью информационной освещенности формируется имидж района и, как вследствие, его инвестиционная привлекательность. Целесообразен анализ уровня и характера информированности населения относительно близлежащих к данным районам территорий, а также данные о существовании и функционировании данной административно–хозяйственной единицы. Для установления указанных факторов необходимо воспользоваться методом проведения контент – анализа средств массовой информации региона. Для нашего исследования мы взяли «Чернышевский», «Красночикойский», «Могочинский» и «Тунгиро-Олёкминский» районы.

Для социологических исследований мы использовали простую случайную выборку (Simple Random Sampling - SRS), где каждый компонент совокупности обладает известной и равной вероятностью отбора. Любая возможная выборка данного объема (n) может стать выборочной совокупностью. Это означает, что

каждый компонент отбирается вне зависимости друг от друга. Выборка создается случайным отбором компонентов из основы выборки (данный метод похож на лотерею). При простой случайной выборке вначале формируется база выборочного наблюдения, затем генерируются случайные числа, для определения номера компонента, которые будут включены в выборку.

SRS обладает следующими преимуществами. Данный метод прост для понимания, а результаты исследования распространяются на изучаемую совокупность. Для получения статистических выводов большинство подходов предусматривают сбор сведений с помощью простой случайной выборки. Однако, данный метод имеет четыре ограничения:

Во-первых, зачастую трудно сформировать базу выборочного наблюдения, позволяющую осуществить простую случайную выборку.

Во-вторых, результатом осуществления SRS может стать большая совокупность, либо совокупность, распределенная по большой географической территории, что значительно увеличивает время и стоимость сбора данных.

В-третьих, результаты применения простой случайной, в большинстве случаев, выборки характеризуются низкой точностью, чем результаты применения других вероятностных методов.

В-четвертых, в результате применения метода может сформироваться нерепрезентативная выборка. Хотя выборки, полученные SRS, в среднем, адекватно представляют генеральную совокупность, некоторые из них крайне не корректно представляют изучаемую совокупность.

В качестве каналов СМИ, по которым был проведен данный анализ, были взяты информационный интернет – «Читинский Городской портал» информационного агентства «Чита.ру», и портал «ЗабИНФО (Zabinfo.ru)» печатные издания Забайкальского края: газеты «Забайкальский рабочий», «Ваша реклама» и «Эффект – газета о жизни Забайкалья» .

Проведенный контент – анализ интернет – ресурса «Чита.ру», как одного из наиболее полного и надежного источника информации в современный период

развития технологий, включает в себя выявление интенсивности употребления ключевых слов среди общих массивов представляемой порталом новостной информации, так как именно эта информация рассчитана на широкие слои населения, а также сферу (раздел) употребления данных слов за период 01. 01. 2017 г. - 30. 04. 2018 г. Указанный интернет – портал позволяет осуществить поиск и анализ информации как по географическому признаку, так и по признаку сферы деятельности, что значительно облегчило проведение исследования. Необходимость проведения контент – анализа данного СМИ также важно и потому, что интернет – портал является общероссийским каналом информации. Именно интернет – ресурсы служат лицом края среди населения иных регионов России.

Для сравнения был проведен контент – анализ региональных СМИ с использованием ключевых слов «Чернышевский район» и «Красночикойский» районы. Также были проанализированы данные по запросам «Могочинский» и «Тунгиро-Олёкминский» районы. Результаты контент - анализа представлены в таблице 5.

Таблица 5 – Сравнительная таблица результатов контент – анализа Чернышевского, Красночикойского, Могочинского и Забайкальского районов на региональном информационном интернет – портале «Чита.ру» и «ЗабИНФО».

Разделы интернет – портала «Чита.ру» и «ЗабИНФО»	Интенсивность (частота) употребления ключевых слов (Чернышевский район)	Интенсивность (частота) употребления ключевых слов (Красночикойский район)	Интенсивность (частота) употребления ключевых слов (Могочинского района)	Интенсивность (частота) употребления ключевых слов (Тунгиро-Олёкминский район)
Здоровье	0	2	0	0
Происшествия и криминал	36	19	43	13
Человек и общество	11	7	9	7
Наука и образование	7	8	3	4

Продолжение таблицы 5.

Политика и власть	4	3	3	2
Сельское хозяйство	9	0	0	5
Спорт	0	0	0	0
Культура и искусство	2	8	1	0
Связь и телекоммуникации	1	1	2	2

Для более наглядного примера построим диаграмму данных (см рисунок 12).

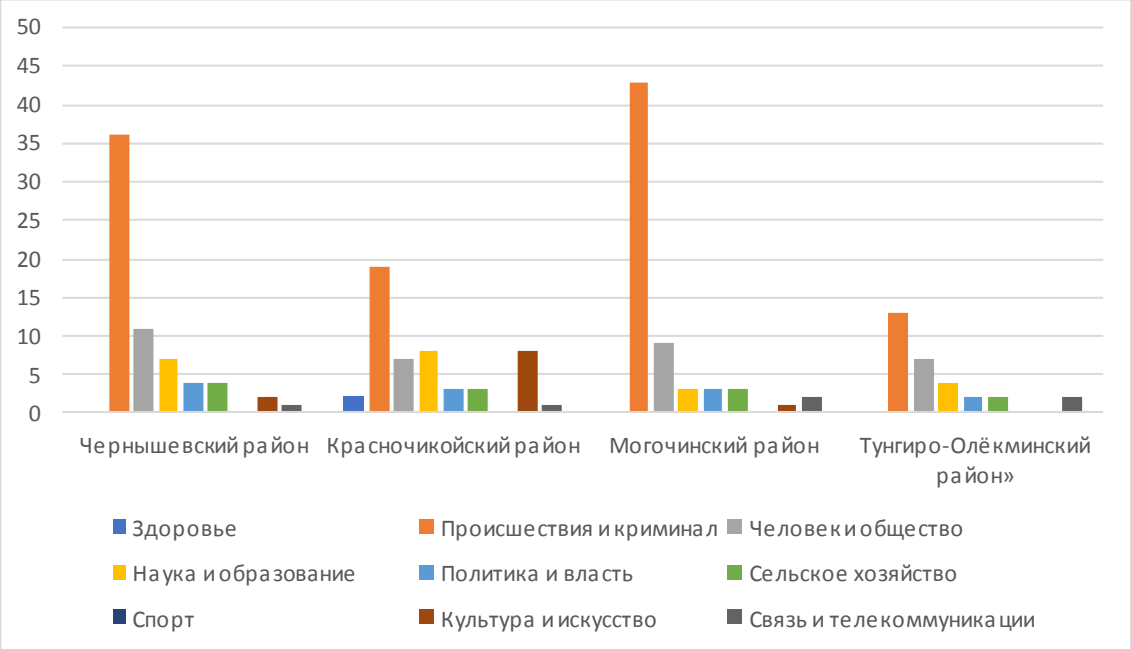


Рисунок 12 – Результаты контент – анализа муниципальных районов в региональном информационном интернет – портале «Чита.ру» и «ЗабИНФО».

На информационном интернет-портале «Чита.ру» указанные муниципальные образования позиционируются совершенно по-разному. Особое внимание стоит уделить таким критериям, как уровень криминогенности территорий, которые представлены в показателе «Происшествия и криминал». Мы наблюдаем тот факт, что муниципальный район «Могочинский район» позиционируется на интернет-портале, как более не стабильная в криминогенном плане территория, чем другие муниципальные районы.

Также стоит отметить тот фактор, что Красночикойский район практически по всем остальным показателям, в приведенных выше таблице и диаграмме, превосходит анализируемые районы. Это такие как «Наука и образование», «Спорт», «Культура и искусство», «Связь и телекоммуникации». Это служит дополнительным, но весьма важным аспектом в позиционировании указанных территориальных образований. Также можно заменить, что Тунгиро-Олёкминский район мало осведомлен в данный период в информационных порталах «Чита.ру» и «ЗабИНФО».

Для проведения контент – анализа печатных СМИ были взяты выпуски региональных газет «Забайкальский рабочий», «Ваша реклама» и «Эффект – газета о жизни Забайкалья» (за исключением рекламного блока издания) за период 2017-2018 г. В данном контент – анализе печатных источников информации интенсивность упоминания выбранных районов выше, чем в интернет – порталах.

Данные анализа приведены в таблицах 6 и 7.

Таблица 6 – Контент – анализ районов в региональной газете «Забайкальский рабочий».

Разделы региональной газеты «Забайкальский рабочий»	Интенсивность (частота) употребления ключевых слов (Чернышевский район)	Интенсивность (частота) употребления ключевых слов (Красночикой ский район)	Интенсивность (частота) употребления ключевых слов (Могочинского района)	Интенсивность (частота) употребления ключевых слов (Тунгиро-Олёкминский район)
Здоровье	4	3	2	1
Происшествия и криминал	21	12	31	9
Человек и общество	18	26	13	11
Наука и образование	5	8	4	3
Политика и власть	9	11	8	2

Продолжение таблицы 6.

Сельское хозяйство	8	13	4	3
Спорт	5	8	3	2
Культура и искусство	6	8	3	2
Связь и телекоммуникации	0	2	0	1

Таблица 7 – Контент – анализ районов в региональной газете «Ваша реклама» и ««Эффект – газета о жизни Забайкалья» (за исключением рекламного блока).

Разделы региональной газете «Ваша реклама» и ««Эффект – газета о жизни Забайкалья»	Интенсивность (частота) употребления ключевых слов (Чернышевский район)	Интенсивность (частота) употребления ключевых слов (Красночикойский район)	Интенсивность (частота) употребления ключевых слов (Могочинского района)	Интенсивность (частота) употребления ключевых слов (Тунгиро-Олёкминский район)
Здоровье	2	3	2	1
Происшествия и криминал	26	13	29	8
Человек и общество	14	17	15	10
Наука и образование	5	7	6	4
Политика и власть	10	14	9	8
Сельское хозяйство	9	12	7	4
Спорт	8	16	10	3
Культура и искусство	4	7	5	1
Связь и телекоммуникации	0	2	1	0

Из данных таблиц мы наблюдаем, что в печатных источниках информации Забайкальского края районы упоминаются чаще, чем в интернет – ресурсах. Однако, тем не менее, результаты контент – анализов печатной периодики и интернет – портала схожи. Могочинский район более часто упоминается в такой категории, как «Происшествия и криминал», чем другие районы. По всем остальным показателям, как мы видим, Красночикойский район превалирует над Чернышевским, Тунгиро-Олекминский район также слабо освещен в печатной периодике. Таким образом, итоговая таблица 8 проведенного контент-анализа по всем региональным СМИ включает следующие данные:

Таблица 8 – Контент – анализ Чернышевского, Красночикойского, Могочинского и Забайкальского районов в региональных СМИ.

	Интенсивность (частота) употребления ключевых слов (Чернышевский район)	Интенсивность (частота) употребления ключевых слов (Красночикойский район)	Интенсивность (частота) употребления ключевых слов (Могочинского района)	Интенсивность (частота) употребления ключевых слов (Тунгиро-Олёкминский район)
Здоровье	6	8	4	2
Происшествия и криминал	83	44	103	30
Человек и общество	43	50	37	28
Наука и образование	29	39	20	18
Политика и власть	23	28	20	12
Сельское хозяйство	26	25	11	12
Спорт	13	24	13	5
Культура и искусство	12	23	9	3
Связь и телекоммуникации	1	5	3	3

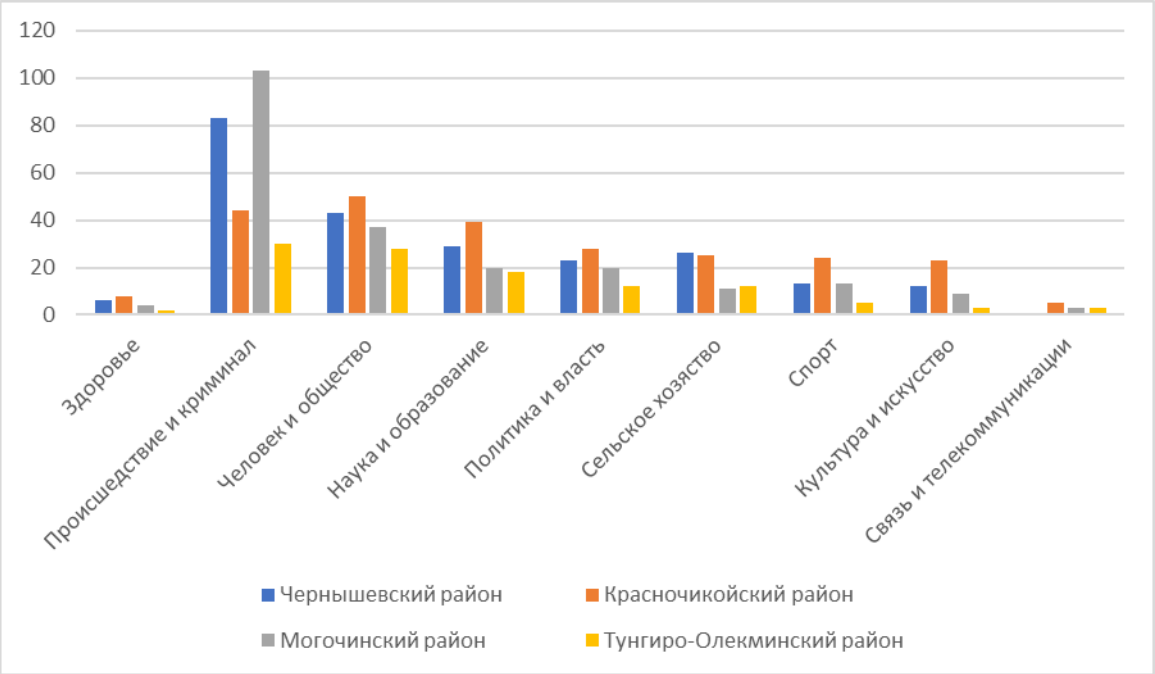


Рисунок 13 – Результаты контент – анализа Чернышевского, Красночикойского, Могочинского и Забайкальского муниципальных районов в региональном СМИ.

На приведенных выше таблицах и диаграмме (рисунок 13) отображены сведенные результаты контент-анализа муниципальных районов в указанных выше средствах массовой информации. Как можно наблюдать, по каждому отдельно взятому информационному источнику, так и в целом, муниципальный район «Могочинский район» и «Чернышевский район» позиционируются как неблагоприятные для инвестиционных процессов территорий с высоким уровнем криминогенности с низкой активностью в сфере культурной жизни и спорта и иных областях деятельности населения.

На диаграмме явно показано, что судить о муниципальном районе «Тунгиро-Олёкминский район» трудно, так как освещен данный район в региональных СМИ слабо. Мы видим, что криминогенность в Тунгиро-Олёкминском районе не высокая и развиваются следующие сферы: спорт, здоровье, наука, сельское хозяйство. Что касается «Красночикойского района», все рассматриваемые сферы жизнедеятельности на высоком уровне по сравнению с другими районами, но ниже уровень криминогенности. На данном этапе исследования из выбранных районов «Красночикойский район» считается самым благоприятным.

Таким образом, мы наблюдаем, что развитие и степень эффективности социально-экономического развития территориального образования напрямую зависит от уровня информационной освещенности данной территории в СМИ и иных источников региона и страны, а также качества и степени мощности инвестиционного позиционирования.

В проведенном нами исследовании следует учитывать дополнительный аспект в информационном позиционировании территориального образования – это официальные сайты муниципальных районов. При профессиональном и своевременном обеспечении функционирования данных информационных ресурсов (своевременном заполнении сайта, высоком качестве заполнения, использовании дополнительных свойств платформы) они на настоящий момент имеют в сфере муниципального управления не меньшую важность, чем материальные, трудовые, энергетические, финансовые и другие ресурсы.

Сайт муниципального образования является и средством информирования окружающих о событиях и процессах, происходящих на территории районов, и средством обратной связи с населением, проживающим на данной территории и еще осуществляет ряд функций.

Такой информационный ресурс, как сайт муниципального образования, является мощным инструментом в сфере продвижения территории.

Что касается официальных сайтов муниципальных районов Забайкальского края, то в данном случае ввиду отсутствия достаточно квалифицированных кадров и имеющихся достаточно слабых технических возможностей, уровень указанных информационных ресурсов очень низок.

Основным регулирующим документом в данной области является ФЗ №8 от 09.02.2009 (ред. от 09.03.2016) «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»[211]. Требования закона послужили основными критериями для оценки сайтов. Кроме

[211] Федеральный закон от 09.02.2009 N 8-ФЗ (ред. от 09.03.2016) «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» [Электронный ресурс]. – Режим доступа - http://www.consultant.ru/document/Cons_doc_LAW_84602/.

того, была определена группа критериев, выходящих за рамки федерального закона. К ним были отнесены: информация о действующих инвестиционных проектах, о достопримечательностях районов, новости, история районов, сведения об отдельных отраслевых структурах и т.д. В общей сложности Интернет-порталы муниципальных районов были оценены по 50 критериям. Каждый критерий оценивался по 5-балльной шкале, а итоговая оценка складывалась из расчета среднего арифметического значения.

Проведя исследования, был составлен рейтинг Интернет-порталов муниципальных районов. Таким образом, были получены следующие результаты[212] (см. таблицу 9).

Таблица 9 – Рейтинг интернет-порталов муниципальных районов.

№	Название района	Оценка	№	Название района	Оценка
1	Шилкииский	3,61	7	Улетовский	2,55
2	Агинский	3,4	18	Нерчинекий	2,47
3	Петровск-Забайкальский	3,33	19	Кыринский	2,4
4	**Могочинский**	**3,23**	20	Калганский	2,28
5	Могойтуйский	3,16	21	Газимуро-Заводский	2,18
6	Шелопуги некий	3,07	**22**	**Красночикойский**	**2,15**
7	Балейский	2,94	23	Карымский	2,1
8	Краснокаменский	2,94	24	Каларский	2,0
9	Борзинекий	2,92	25	Александрово-Заводский	1,88
10	Забайкальский	2,89	26	Дульдургинский	1,85

[212] Эпова, А.Н. Анализ интернет-порталов муниципальных районов / А.Н. Эпова // Молодежь Забайкалья: инновации в технологиях и образовании: материалы XV Международная молодежная научно-практическая конференция - Чита: ЗабГУ, 2012 - Часть III. – С.-111.

Продолжение таблицы 9.

11	Приаргунский	2,86	27	Оловяннинский	1,68
12	Читинский	2,83	28	Сретенский	1,51
13	Хилокский	2,63	**29**	**Тунгиро-Олекминский**	**1,2**
14	Нерчинско-Заводский	2,58	**30**	**Чернышевский**	**1,03**
15	Акшинский	2,57	31	Ононский	0,38
16	Тунгокоченский	2,56			

Исходя из приведенной выше таблицы, можно наблюдать, что в тройку лидеров по оценкам экспертов вошли порталы Шилкинского, Агинского, Петровск-Забайкальского и Могочинского муниципальных районов. Забайкальский район имеет среднее значение, Красночикойский район – уже пониженное значение. Аутсайдерами признаны порталы Тунгиро-Олекминского, Чернышевского, Ононского районов.

Рассматриваемые в данной работе муниципальные образования находятся в таблице оценки экспертов достаточно низко: муниципальный район «Чернышевский район» – на тридцатом месте из тридцати одного возможного, муниципальный район «Красночикойский район» – на двадцать втором, «Могочинский район» – на четвертом, а Тунгиро-Олекминский – на двадцать девятом из тридцати одного.

Как следствие, можно сделать вывод, что такие ресурсы, как официальные сайты муниципальных образований, являются очень слабыми в техническом отношении, а также в отношении информационного наполнения. Официальные сайты муниципальных образований явно не могут служить инструментом привлечения инвестиций в территориальные образования.

При этом даже у районов, занимающих лидирующие позиции, имеются существенные недостатки, что отразилось на их средней оценке:

1. Нестабильная частота обновлений, вследствие чего представленная информация теряет свою актуальность, дезинформирует пользователя и подрывает его доверие.

2. Наличие «мертвых» ссылок (указанные ссылки не содержат заявленной информации или ее невозможно скачать).

3. Неудобное расположение информации на сайте, часть данных не сгруппирована, а «стянута» в одну большую массу.

4. Нарушение неофициального правила навигации на сайте – правило 3 кликов, которое гласит: «пользователь должен иметь возможность найти любую информацию не более чем за 3 клика мышью».

5. Отсутствие ссылок на дополнительные ресурсы, расширяющие информационное поле о данном муниципальном районе.

6. Отсутствие дифференцированных разделов об отраслевых сферах.

7. Отсутствие визитной карточки района - ключевых особенностей, основной статистики, истории.

Так же были выявлены нестыковки в работе порталов: к некоторым сайтам районов нет доступа с официального портала Забайкальского края.

Ныне действующий портал региона www.e-zab.ru, дающий место для размещения сайтов муниципальных районов, в настоящее время прекратил свою работу. На базе программы «Электронное Забайкалье» произошел переход на новую платформу и создание нового доменного имени – Забайкальский край.рф. Муниципальным районам предложено подгружать сайты в одинаковом для всех интерфейсе, что предполагает легкость в ориентации для пользователя. Шаблон для сайтов создан в соответствии с критериями ФЗ-№8, но каждый орган местного самоуправления имеет право на творчество и добавление дополнительной согласованной с соответствующими структурами информации. Кроме того, было замечено, что созданные в сети Интернет-сайты органов местного самоуправления в Забайкальском крае не содержат в достаточном объеме сведений о необходимых условиях получения муниципальных услуг, что

затрудняет взаимодействие граждан с органами власти. Получение населением и организациями услуг, а также информации, связанной с деятельностью органов власти, в большинстве случаев требует их личного обращения в данные органы, а также представления запросов и другой необходимой информации в бумажном виде. Это приводит к соответствующим затратам времени, создает значительные неудобства для населения и лишает смысла реализацию проекта «Электронное правительство».

Таким образом, слабое развитие информационно-коммуникативных технологий на муниципальном уровне оставляет более предпочтительной для граждан классическую схему предоставления тех или иных услуг.

Что касается предложений относительно улучшений Интернет- порталов муниципалов, то к ним можно отнести следующие:

1. Контроль соблюдения ФЗ-№8 при переходе на новый портал.
2. Необходимость проведения курсов повышения квалификации лиц, обслуживающих порталы местных органов власти.

На наш взгляд, ситуация, сложившаяся в выбранных районах, характерна для многих муниципальных образований, а также поселков и малых городов Российской Федерации, находящихся в отдаленных регионах. Как уже было указано выше, для современного периода, который общепризнанно считают информационным веком, важнейшим и во многом определяющим фактором производства, характерным для данного времени, и является собственно информация. Не имея этого фактора, или имея неполные, либо недостоверные сведения, предприниматели, соответственно, не могут создавать и развивать какие-либо производства, а инвесторы не имеют возможности планировать и реализовывать какие-либо инвестиционные проекты.

Следовательно, территория с находящимися на ней ресурсами и перспективами развития, и неосвещенная в информационных источниках окружающего мира, так и остается неиспользованной, как следствие, неразвитой в экономическом отношении. Низкий уровень экономического прогресса служит

предпосылкой для неразвитости в социальной, культурной, демографической и иных сферах функционирования данной территории.

Таким образом, отсутствие информации негативно сказывается на жизнедеятельности людей. Что мы и наблюдаем на примере Чернышевского и Могочинского районов. Отсутствие позитивной информации о возможностях и перспективах данного территориального образования и наличие негативной оценки района в средствах массовой информации региона не привлекает инвестиции в муниципальный район «Чернышевский район».

Несмотря на небольшое различие между природными ресурсами и уровнем социально-экономического развития, инвестиции в муниципальном районе «Красночикойский район» в тысячи раз больше, чем в муниципальных районах «Чернышевский район» и «Могочинский район» Забайкалья . По нашему мнению, ключевой причиной этого является высокая мощность позиционирования Красночикойского района в региональных СМИ и положительная окраска данного позиционирования. Информационная открытость служит основой информационной безопасности органов власти.

3.2 Анализ информационной безопасности муниципалитетов Забайкальского края по итогам социологического исследования и пути ее совершенствования

Нами было проведено социологическое исследование для определения состояния информационной среды Забайкальского края и готовности муниципалитетов и их служащих к реализации информационной безопасности на местах. В исследовании приняли девять муниципальных районов Забайкальского края, а именно Агинский, Газимуро-Заводский, Карымский, Могойтуйский, Могочинский, Хилокский, Чернышевский, Читинский, Шилкинский и 300 муниципальных служащих.

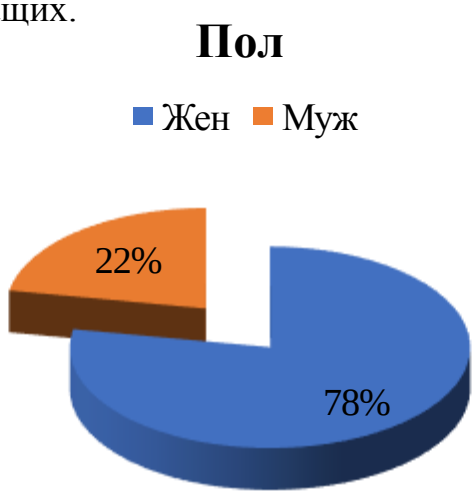


Рисунок 14 – Пол респондентов

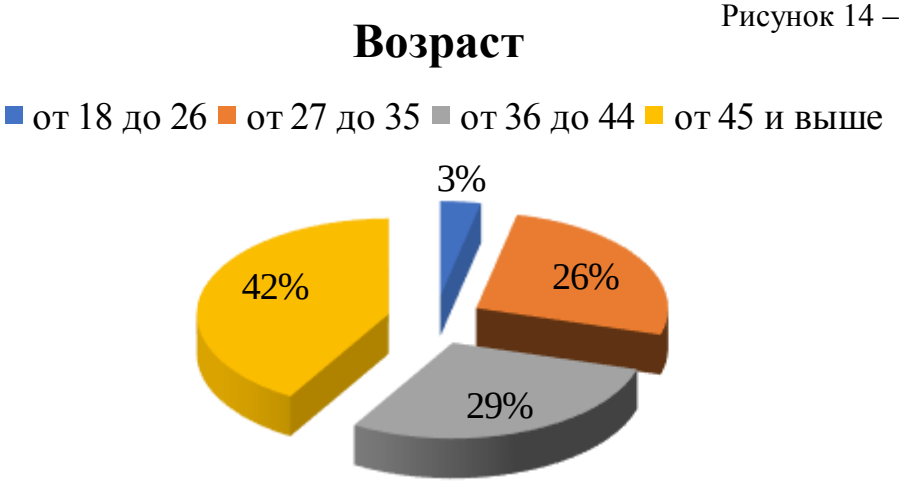


Рисунок 15 – Возраст респондентов

Как мы видим, из данных по гендерному и возрастному признаку в основном муниципалы – это женщины (78%), в соотношении мужчин – 22%. По возрастному цензу мы можем сделать вывод, что молодых людей от 18 до 26 малая часть – 3%. В основном, это муниципальные служащие от 27 до 35 и от 36 до 44, но почти половина (42 %) - это люди старше 45 лет. Это говорит о старении кадров, а значит о необходимости гибкости муниципальной системы к изменениям внешней среды.

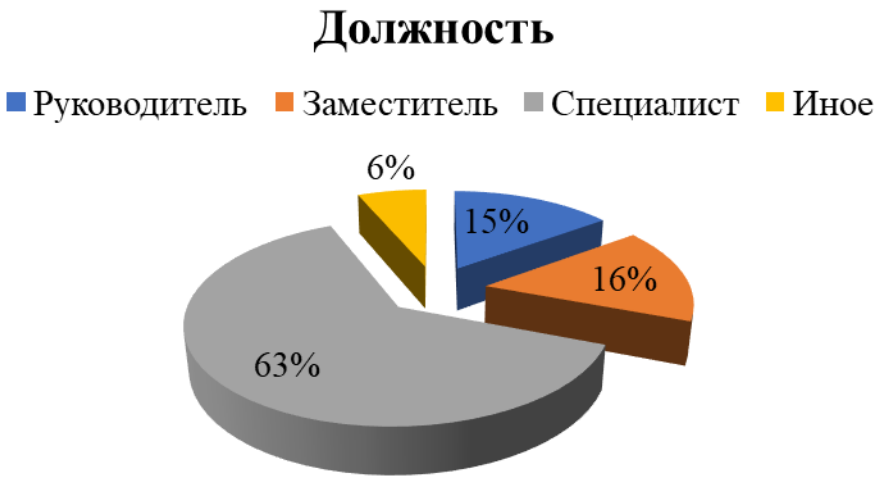
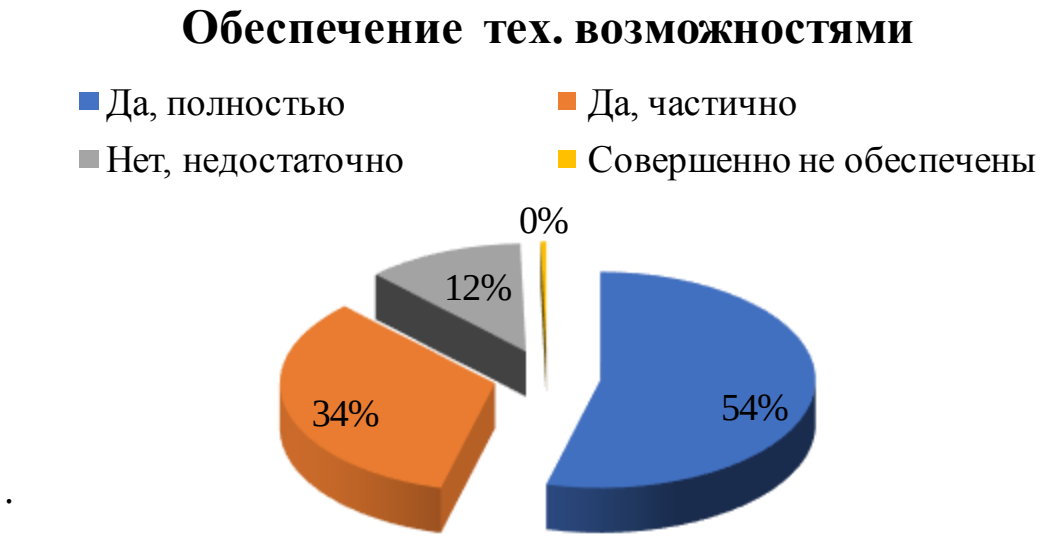


Рисунок 16 – Должность респондентов

Рисунок 17 – Образование респондентов

Что касается должности и образования муниципальных служащих Забайкальского края, то в основном в исследовании приняли участие специалисты в равной доли – руководители и заместители. Образование муниципалов прогрессирует вместе с условиями современного мира, радует, что появляются специалисты с профильным образованием «Государственное и муниципальное управление» – 16%, но лидируют экономическое и средне–специальное (17% и 19%), уменьшается тенденция по привлечению специалистов муниципальной службы с юридическим образованием, всего 9%, что показано на рисунке 16-17.



.

Рисунок 18 – Обеспечены ли вы техническими возможностями для реализации ваших полномочий?

Рисунок 19 – Удовлетворены ли вы уровнем состояния ваших технических средств?

Вопросы рисунков 18, 19 взаимосвязаны и ориентированы на выявление обеспеченности муниципального служащего техническими средствами и оценка их состояния для выполнения своих полномочий. Служащие, в основном, полностью или частично обеспечены ресурсами для выполнения своих полномочий и их состояние – отличное или хорошее. Это хорошие показатели для дотационного региона, но есть процент служащих, которые не обеспечены техническими возможностями или их средства устарели, что сказывается на обеспечении информационной безопасности.

Рисунок 20 – Пользуетесь ли вы сетью интернет?

Рисунок 21 – Имеется ли у вас – системный администратор?

Тенденции современного мира диктуют использование сети интернет, как в личных целях, так и в рабочих моментах, особенно это актуально при развитии электронного документооборот (ДЕЛО, СБИС). Большинство служащих при работе пользуются сетью интернет, что обуславливает поддержание информационной безопасность на высоком уровне. Одним из важных условий поддержания безопасности является наличие системного администратора, который следит за состоянием систем и их безопасности. Как показывает исследование в большинстве случаев в муниципальных органах имеется системный администратор. Для того, чтобы оценить осведомленность респондентов и их понимание сущности информационной безопасности, мы задали два вопроса по терминологии.

Первый вопрос: «Как вы понимаете определение информационная безопасность?». Определение мы брали с Доктрины информационной безопасности. В данном аспекте вопроса ответы разделились: 43% опрошенных ответили правильно, а 57%, к сожалению, не знают четкого ответа на данный вопрос.

Второй вопрос: «Как вы понимаете понятие конфиденциальная информация?». Определение мы взяли из ФЗ 149 от 27.07.2006 «Об информации, информационных технологиях и о защите информации». На данный вопрос 77% опрошенных ответили верно, а 23% – не верно. Данное определение муниципалы знают лучше, так как часто в работе сталкиваются с определением.

Рисунок 22 – Значима ли для вас лично экономическая безопасность?

Рисунок 23 – Значима ли для вас лично информационная безопасность?

Рисунок 24 – Значима ли для вас лично политическая безопасность?

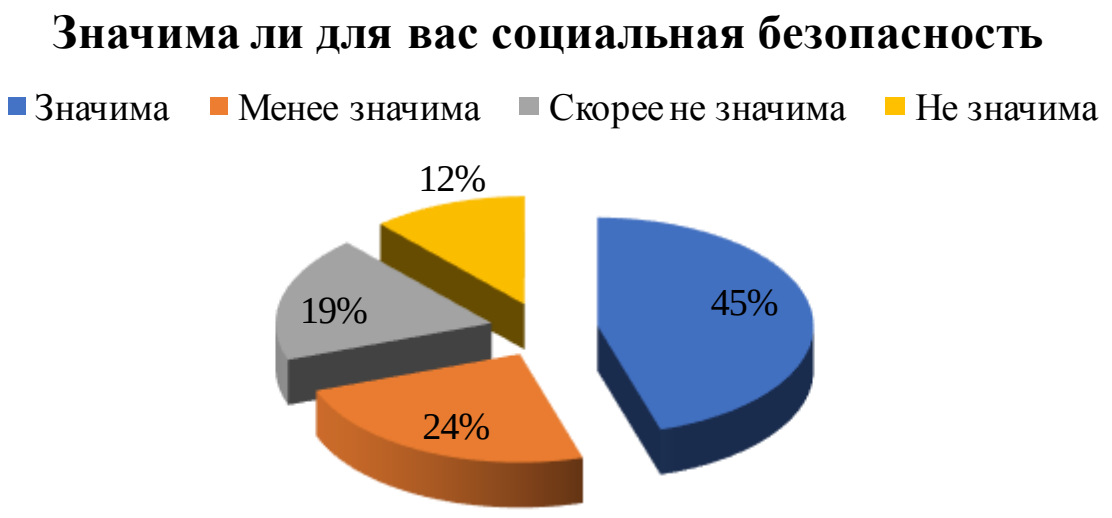


Рисунок 25 – Значима ли для вас лично социальная безопасность?

Рисунок 26 – Значима ли для государства, по вашему мнению, экономическая безопасность?

Рисунок 27 – Значима ли для государства, по вашему мнению, информационная безопасность?

Рисунок 28 – Значима ли для государства, по вашему мнению, политическая безопасность?

Рисунок 29 – Значима ли для государства, по вашему мнению, социальная безопасность?

Мы предложили респондентам расставить по значимости различные виды безопасности – экономическая, информационная, социальная, политическая. На первое место по личному рейтингу муниципалов встала экономическая безопасность. 32% всех опрашиваемых посчитали экономическую безопасность превыше всего, это аргументировано нехваткой ресурсов и нестабильной экономической ситуацией в стране. На втором месте – социальная и информационная, они набрали в общем объеме 25% и 24% и на последнем, третьем месте респонденты поставили политическую безопасность (19%). Связано это с политической стабильностью в стране и выборами президента в 2018г. Что касается рейтинга важности видов безопасности, по мнению респондентов, для государства, то тут ответы распределились почти равномерно – экономическая безопасность – 31%, информационная безопасность – 23%, политическая безопасность – 25%, социальная безопасность – 21%. Также можно подчеркнуть, что экономическая безопасность стоит на первом месте рейтинга, так как муниципалы считают, что экономическая стабильность в стране – залог прогресса в любой сфере жизнедеятельности.

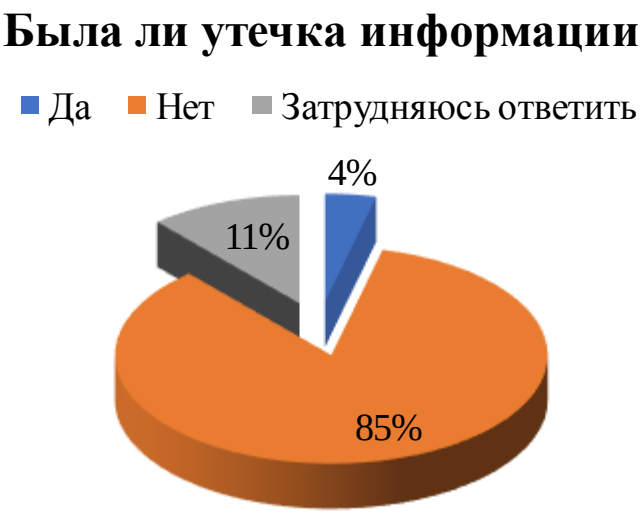


Рисунок 30 – Была ли утечка информации при выполнении ваших полномочий?

Данный вопрос компрометирующий, и ответы были ожидаемые, 85% ответили, что не было утечки информации, но 4% ответили положительно. Безусловно, это малый процент, но стоит задуматься о методах защиты информации.

Рисунок 31 – Какие угрозы информационной безопасности стали актуальными?

Среди угроз информационной безопасности на муниципальном уровне стали актуальными различные вирусы, данная угроза сопровождает информационные системы с момента их создания, но тревожный момент

актуализации на местном уровне угрозы − хакерский взлом, так как эта угрозы один из элементов киберпреступности и встречается чаще всего на федеральном уровне и реже не региональном.

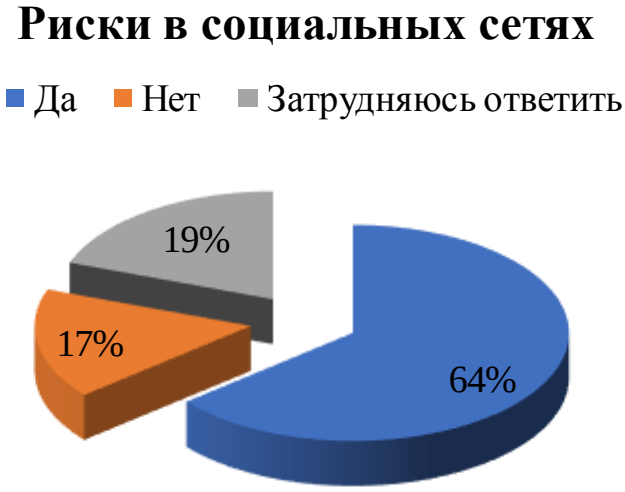


Рисунок 32 – Беспокоят ли вас риски информационной безопасности в социальных сетях?

Рисунок 33 – Рассматриваете ли вы информационную безопасность, как одно из основных направлений развития?

Так как риски в социальных сетях растут, мы не могли не задеть данную тему. Ведь большинство членов общества находится в виртуальной реальности часто и надо рассматривать социальные сети как одно из направлений развития информационной безопасности для защиты конфиденциальных данных, прав и

свобод человека и национальных интересов страны в целом. Так же муниципальные районы рассматривают в перспективе информационную безопасность как одно из основных направлений развития, так как инновация и глобализация не стоит на месте. Россия, как страна с растущим потенциалом и ресурсами, в современный период догоняет страны с высоким коэффициентом развития информационных технологий.

В условиях возрастания значения информационной составляющей необходимо обозначить пути ее совершенствования с точки зрения информационных технологий и глобализации. Одной из тенденций глобализации является совместная деятельность разных стран по развитию международного информационного общества. Информационное общество способно определяться как социальное, в котором орудием труда являются информационные технологии. В информационном обществе общественные отношения во многом определяются этими обстоятельствами, а экономика ориентирована на продукт информационной деятельности.

Данное общество представляет собой ассоциацию стран, которые достигли экономических и социальных высот и значительного уровня информатизации общества, развития науки, образования. Достижение данных параметров − это одно из главных условий экономического процветания и сохранения стратегической стабильности в мире. Однако, вхождение стран в глобальное информационное общество не отменяет наличия у стран национальных интересов и их защиты. Поэтому при формировании информационного общества обеспечивается защита национальных интересов в информационной сфере.

Концепцию к решению указанных задач определяет Доктрина информационной безопасности РФ, утвержденная Президентом РФ в декабре 2016 г. В ней обоснованы национальные интересы страны в информационной сфере и сформулированы принципы реализации этих интересов, и их защиты от различных угроз. В настоящее время идут активные работы по реализации положений Доктрины.

Выделены следующие основные направления информационной деятельности.

Первое направление – соблюдение прав и свобод человека и гражданина в области получения информации и пользования ею. Данное направление требует повысить эффективность использования информационной инфраструктуры в интересах общественного развития, что представляет собой непростую задачу. Так как в обстоятельствах расслоения общества на бедных и богатых трудно гарантировать равные доступы к современным информационным технологиям для социальных слоев населения. По этой причине государство обязано учитывать формирование социальных институтов поддержки.

Необходимо усовершенствовать систему формирования и рационального использования информационных систем, составляющих основу научно-технического и духовного потенциала страны, и обеспечить права и свободы человека и гражданина искать, получать, передавать и распространять информацию любым законным способом. Отметим, что право беспрепятственного доступа к информации не должно направляться к несоблюдению защиты чести и доброго имени человека и конституционного права гражданина на личную и семейную тайну, телефонных переговоров, почтовых, телеграфных и иных сообщений. Помимо этого, гарантируя независимость массовой информации, отсутствие цензуры, необходимо в тоже время усиливать методы нормативно-правового регулирования взаимоотношений в сфере охраны интеллектуальной собственности, формирование требований с целью соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации.

Благополучному решению данных задач мешают факторы и обстоятельства, которые в Доктрине отнесены к уровню угроз, среди которых можно выделить:

- вытеснение отечественных СМИ с внутреннего информационного рынка;
- создание монополий на получение и распространение информации;

– принятие органами власти РФ в области информационной деятельности нормативно-правовых актов, ущемляющих права и свободы граждан;

– незаконное использование специальных механизмов влияния на общественное сознание;

– противодействие, в том числе со стороны криминальных организаций, осуществлению гражданами своих прав на тайну переписки и охрану личной и семейной тайны;

– дезорганизация и разрушение системы накопления и сохранения культурных ценностей;

– девальвация духовных ценностей, пропаганда образцов массовой культуры;

– снижение духовного, нравственного и творческого потенциала населения России.

Второе направление – информационное обеспечение государственной политики РФ. В данном контексте существует потребность: усиления развития государственных отрытых информационных ресурсов; расширения возможностей СМИ по своевременному доведению достоверной и полной информации.

Основные угрозы в данной области:

– монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;

– блокирование деятельности государственных СМИ по информированию российской и зарубежной аудитории;

– низкая эффективность информационного обеспечения государственной политики РФ вследствие дефицита квалифицированных кадров, отсутствия результативной системы создания и осуществления государственной информационной политики.

Третье направление – формирование отечественной индустрии информации, реализация современных информационных технологий, обеспечение необходимой продукцией внутреннего рынка и выход данной

продукции на мировые рынки, а также обеспечение сохранности и результативности применения отечественных информационных ресурсов.

Для этого необходимо совершенствовать инфраструктуру единого информационного поля РФ: развивать отечественную отрасль информационных услуг с одновременным формированием результативности применения информационных ресурсов страны; изготавливать в РФ конкурентоспособные средства и телекоммуникации, системы информатизации; увеличивать участие России в интернациональной кооперации изготовителей этих систем.

Основной угрозой национальным интересам страны в данной области являются доступ РФ к новейшим информационным технологиям, взаимовыгодному участию отечественных производителей в мировом разделении труда, к индустрии информационных услуг, производство средств информатизации и связи, информационных продуктов, а также создание усиления технологической зависимости России в области современных технологий.

Четвертое направление – защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности телекоммуникационных систем. С этой целью требуется повысить безопасность, прежде всего, первичных сетей связи федеральных органов власти, органов власти субъектов РФ, муниципалитетов. Пристальное внимание в защите информационных ресурсов от несанкционированного доступа необходимо уделять: финансово-кредитной сфере, хозяйственной деятельности, а также системам и средствам информатизации вооружения и военной техники.

К числу основных угроз следует отнести:

– деятельность зарубежных разведок и преступных компонентов по незаконному сбору информации, введение в информационный продукт нелицензионных программ, которые реализуют функции, по разработке и программ, нарушающих стабильное функционирование информационных систем;

– нарушение специалистами процессов обработки информации;

– использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации;

– нарушение законных ограничений на распространение информации.

Осуществление мероприятий по реализации информационной безопасности политического процесса, отнесенных в Доктрине к первостепенным, невозможно без глубокой единой научной проработки: кадрового характера, гуманитарного, научно-технического.

Решение гуманитарных проблем реализации информационной безопасности РФ предполагает:

– определение путей и механизмов применения информационной среды с целью решения ключевых социально-политических задач России в современный период, выработку и подтверждение характеристик и методик анализа состояния информационной безопасности;

– создание теории информационной безопасности как междисциплинарной отрасли научного знания, развитие ее взаимоотношений с другими науками, формирование общеметодологических основ;

– анализ социальных процессов современного российского общества и исследование места и значимости вопросов обеспечения информационной безопасности индивидуального, группового и массового сознания, в том числе информационно-психологической безопасности личности и общества;

– формирование нормативного обеспечения и правового регулирования информационной безопасности государственной политики РФ, правовое сопровождение современных информационных технологии и отечественной отрасли информации, международно-правового регулирования в области информационной безопасности, безопасности информационных и телекоммуникационных систем.

Решение научно-технических проблем обеспечения информационной безопасности РФ предусматривает:

– определение путей обеспечения научно-технологической самостоятельности государства, формирование современных информационных технологий, отечественной индустрии средств информатизации, инфраструктуры единого информационного пространства РФ;

– разработку результативных методов защиты информационных и телекоммуникационных систем, информационных ресурсов, формирование систем вычислительной техники с высокой производительностью и принципами обработки данных, которые ориентированы на решение криптографических задач, создание методов защиты информации от технических разведок.

Решение проблем кадрового обеспечения информационной безопасности РФ требует:

– распространения знаний в сфере обеспечения информационной безопасности, формирование системы нормативно-правового и организационного обеспечения образовательного процесса в данной сфере;

– организации системы технологического обеспечения подготовки кадров в сфере информационной безопасности, в том числе исследование учебной литературы, развитие результативных методик применения современных информационных технологий в образовательном процессе;

– разработку научно-теоретических основ и механизмов государственного регулирования подготовки кадрового обеспечения, анализ путей применения современных образовательных технологий в целях увеличения результативности кадрового обеспечения.

Системное решение рассмотренных проблем даст возможность РФ войти в информационное общество, безусловно, при условии соблюдения ее национальных интересов в информационной сфере. Для этого необходима слаженная и заинтересованная работа органов государственной власти и муниципальных образований совместно с представителями деловых кругов, общественными и научными организациями, влиятельными политическими силами.

Подчеркнем, что для исполнения поставленных целей и управленческих задач следует осуществить мероприятия по совершенствованию информационной безопасности, которые включают в себя административный и организационный уровни защиты информации, характеристику этих уровней выделим ниже.

Первый уровень защиты информации – административный. Для реализации деятельности по информационной безопасности необходима четкая политика информационной безопасности. «Политика безопасности – это комплекс правил и норм поведения, характеризующих, как организация обрабатывает, защищает и распространяет информацию»[213]. При формировании политики безопасности, она должна не противоречить принятым нормативно-правовым актам страны и чем строже политика по информационной безопасности, тем надежнее система. Следует подбирать персональные способы защиты информации в зависимости от выбранной политики безопасности.

Второй уровень по обеспечению защиты информации – это организационный уровень. В данном контексте существуют мероприятия, улучшающие защиту информации:

− надзор над соблюдения норм и правил деятельности специалистов с конфиденциальной информацией;

− реализация мероприятий по обучению и профессиональной переподготовке специалистов по работе с современными программными продуктами;

− плановое осуществление дискуссий, вебинаров, семинаров по вопросам обеспечения информационной безопасности;

− формирование и улучшение мероприятий по усовершенствованию систем информационной безопасности;

− проведение инструктажей с каждым специалистом с целью осознания важности конфиденциальной информации, с которой он работает. Не редко

[213] Крупский, А. Ю., Феоктистова, Л. А. Информационный менеджмент: Учебное пособие – М.: Издательско-торговая корпорация «Дашков и К°». 2008 – 80 с.

недостаточное знание правил и норм защиты информации приводит к разглашению конфиденциальной информации специалистом;

- включение в деятельность системного администратора;
- контроль соблюдения правил и норм хранения документации;
- систематический надзор с целью проверки на дееспособность обслуживающих информационных систем и инфраструктуры.

Помимо того, прямым направлением развития является технический путь совершенствования безопасности. Рекомендуется осуществлять следующие направления повышения результативности программных средств, которые являются главным компонентом в реализации защиты информации:

1. Введение паролей пользователей. Целью данного направления считается контролирование доступа к информационным системам и следует с индивидуальным логином внедрить перечень пользователей, входящих в систему. Данные пароли переходят специалисту с надлежащим инструктажем, а также формируется срок действия пароля, по истечению которого необходимо его сменить, а также ограничение количества попыток входа в систему с неверным паролем.

2. Ограничение доступа к серверам. Данное ограничение будет осуществляется под контролем системного администратора, который обеспечивает доступ к надлежащей информации на сервере индивидуально для любого пользователя.

3. Регламентирование сканирования систем и базовое обновление антивирусных программ, что даст возможность выявлять вредоносные программы и устранить возникающие угрозы. Осуществление деятельности по установке средств противовирусной защиты позволит настроить антивирусную программу на плановое сканирование и обновление баз данных.

4. Установка на компьютер-сервер сетевого экрана например – «Agnitum Outpost FireWall, эта программа блокирует несекционный доступ из сети

интернет»[214]. Достоинства применения именно этого сетевого экрана Agnitum Outpost FireWall, связаны с тем, что путем блокирования несанкционированного доступа в систему достигается осуществление контроля соединения персонального компьютера с другими устройствами. Кроме того, отслеживается взаимодействие и деятельность локальных программ. Осуществляя тем самым блокировку неразрешенной активности и шпионские программы, в современный период хакерские методы взлома становятся все изощренные. Имеется ряд результативных сетевых кранов, способных автоматически изолировать вирусы и шпионские программы.

5. Исследование безопасности объектов вычислительной сети. При осуществлении данной задачи можно к примеру использовать программу «Сканер-ВС»[215], предназначенную для контроля безопасности сетей от внутренних и внешних угроз.

«Сканер-ВС» выполняет следующие функции:

a) осуществление анализа характеристик подсистемы защиты информации;

b) обеспечение контроля над ресурсами сертифицированных программ защиты информации;

c) контролирование безопасной загрузки системы;

d) анализ парольной системы и сетевого трафика;

e) обнаружение критических точек сервисов;

f) оценка результативности методов очистки памяти и поиск сведений на носителях информации.

Основные возможности системы:

- поиск критических точек;
- определение типологии ресурсов сети;
- анализ и перехват сетевого трафика;

---

[214] Agnitum Outpost FireWall [Электронный ресурс]. – Режим доступа: http://www.agnitum.ru/support/kb/-article.php?id=1000295&lang=ru.

[215] Сканер-ВС [Электронный ресурс]. – Режим доступа: http://npoechelon.ru/production/65/4291?yclid=2819-290500710796405.

- контроль целостности системы;
- поиск остаточных сведений информации на носителях;
- сетевой аудит стойкости паролей;
- аудит аппаратной конфигурации.

6. Информационной защитой персонального компьютера считается программа безопасности от спама. Защита от спама программного обеспечения возможно методами выявления вредоносных почтовых сообщений. Для таких целей, по нашему мнению, можно воспользоваться программой antispam - «Spamoed»[216], которая позволяет заблокировать спам на компьютере и произвести фильтрацию почты. Главный принцип функционирования состоит в том, что «Spamoed» автоматически перекрывает ненужную электронную почту.

Прогрессивным методом избежания потерь данных при перебоях электроэнергии считается источник бесперебойного питания. Данный прибор гарантирует питание всей сети или отдельного персонального компьютера в интервале времени, необходимого с целью восстановления электроэнергии или для сохранения данных. Информационной функцией устройств считается сигнал, получаемый системой о том, что прибор перешёл на работу от собственного блока питания и время данной автономной работы ограничено. Затем персональный компьютер переходит к отключению всех выполняемых процессов и завершает работу системы. Множество приборов выполняют одновременно функцию стабилизатора напряжения.

Криптографическая защита данных гарантирует режим целостности и конфиденциальности информации при ее передаче по каналам связи. Протоколирование считается главным элементом защиты данных. Подобная защита предполагает анализ и накопление команд, совершающихся в информационной системе.

Деятельность протоколирования и аудита решает следующие задачи:

- осуществление воспроизведения последовательности событий;

[216] Spamoed [Электронный ресурс]. – Режим доступа: http://www.spamoed.com/.

- предоставление данных для определения проблем;
- обеспечение отчетности пользователей;
- анализ нарушений работы по защите.

При протоколировании события следует фиксировать, следующие данные:

- тип и дату события;
- id-номер пользователя;
- источник запроса;
- результат действия;
- анализ изменений базы данных защиты;
- имена задействованных объектов.

Результативность системы безопасности и функционирование системного администратора будет низкой при отсутствии методов анализа и сбора сведений о состоянии защиты баз данных, централизованного управления всеми ее элементами. Дело в том, что любой механизм защиты сведений является элементом всей системы политики безопасности, которая задается набором параметров и требований на уровне подсистем. Анализ работоспособности системы, требует наличия средств мониторинга и управления всех правил и других элементов в системе информационной безопасности. Рычаги мониторинга необходимы для регламентированного анализа баз данных, и принятия управленческих решений.

Осуществление данных мероприятий позволит:

- ограничить доступ в систему;
- повысить уровень защищенности пользователя;
- уменьшить число спама;
- внедрить и сформировать эффективную политику информационной безопасности;
- повысить уровень защиты рабочих станций;
- блокировать вредоносные атаки через сеть.

Для любого муниципалитета необходима индивидуальная политика информационной безопасности с учетом рекомендаций указанных выше по сотрудничеству как региональных, государственных, так и муниципальных властей»[217].

Следовательно, анализ информационной безопасности муниципалитетов Забайкалья показал следующее.

1. Среди угроз информационной безопасности на муниципальном уровне стали актуальными различные вирусы, данная угроза сопровождает информационные системы с момента их создания, но тревожный момент актуализации угрозы на местном уровне − хакерский взлом, так как эта угроза – один из элементов киберпреступности и встречается чаще всего на федеральном уровне.

2. Таким образом, риски в социальных сетях растут, и большинство членов общества, находясь в виртуальной реальности, для развития информационной безопасности ориентируются на защиту конфиденциальных данных, прав и свобод человека и национальных интересов страны.

3. Существуют несколько путей совершенствования информационной безопасности муниципалитетов Забайкальского края. Административный путь предполагает улучшение нормативно-правовой базы информационной безопасности. Организационный уровень ориентирован на улучшение защиты информации путем технизации управления (введение паролей пользователей; ограничение доступа к серверам; плановое сканирование систем и обновление антивирусных программ; установка на компьютер-сервер сетевого экрана «Agnitum Outpost FireWall; анализ защищенности объектов вычислительной сети). Информационной защитой персонального компьютера является программа защиты от спама и защищенность рабочих станций муниципальных служащих.

[217] Кухарский, А.Н. Информационная безопасность муниципалитетов Забайкальского края и пути ее совершенствования // Постулат. 2017. №2 (16). Биробиджан. С.11.

ЗАКЛЮЧЕНИЕ

В проведенном исследовании была поставлена одна из важных научно-практических задач – совершенствование информационной безопасности политического процесса органов власти. На основе результатов проведенного исследования можно выделить основные выводы.

1. По нашему мнению, главными акторами регионального политического процесса являются:

– система органов государственной власти, муниципалитеты, партии, иные политические организации;

– деятели, реализующие информационную безопасность как необходимое условие функционирования органов власти любого уровня;

– население регионов и муниципалитетов;

– система международных отношений.

Под акторами информационной безопасности мы имеем ввиду, прежде всего, деятелей, осуществляющих информационную безопасность. Здесь мы акцентируем внимание на том, что информационная безопасность – это составляющая политического процесса, ориентированная на защищенность органов власти от манипулирования информацией.

2. Формирование информационного пространства, использовавшего современные методы и средства воздействия, является велением времени. Российское информационное пространство призвано играть фундаментальную роль в жизни российского государства. Условием эффективного функционирования информационного пространства считается наличие стабильной обратной связи в его информационных каналах, которое позволяет

учитывать и знать мнение граждан при определении приоритетов духовно-нравственного, экономического, политического развития общества.

Было отмечено, что согласно «Концепции региональной информатизации» информатизация региона направлена на повышение эффективности решения социально–экономических задач развития регионов, обеспечение функционирования и взаимодействия федеральных органов государственной власти, органов государственной власти субъектов РФ, органов местного самоуправления и учреждений. Кроме того, информатизация региона ориентирована на обеспечение прозрачности и информационной открытости органов управления, а также на формирование доступа гражданам к информационным ресурсам. Важную роль в развитии информационного пространства играют муниципалитеты, которые распространяют информацию в интересах органов власти и муниципальных образований, обеспечивая информационную поддержку. Все принятые в организациях технологии обработки информации основываются на федеральной нормативно-правовой базе в области информационной безопасности. И хотя вопросы информационной безопасности относятся к полномочиям федерального уровня, существует их региональное и муниципальное разнообразие.

3. Была охарактеризована информационная открытость как один из элементов информационной безопасности политического процесса. Информационная открытость – это целостный комплекс совместных мер системы государственного и муниципального управления, общественного контроля, направленных на предоставление сведений о деятельности государственных и муниципальных органов, предусмотренных законодательством, обществу в целом или конкретным лицам в целях обеспечения прозрачности и подотчетности органов власти в рамках установленного порядка на началах равенства доступа к информации.

По нашему мнению, к общим функциональным задачам информационной политики следует отнести:

– предоставление на базе формирования массовых коммуникаций и информационного обмена открытого информационного обслуживания общества;

– информационное обеспечение деятельности органов государственного и муниципального управления;

– реализация открытого информационного взаимодействия гражданского общества и власти;

– совершенствование информационных систем и телекоммуникационной инфраструктуры;

– формирование необходимой нормативно-правовой базы организации информационного общества.

Выделено, что информационная открытость и ее обеспечение не является односторонним процессом. Стремление гражданского общества к получению полных и достоверных сведений о деятельности органов государственной и муниципальной власти, контроль и активная позиция общественности и их институтов по отношению к власти соотносятся с желанием власти проинформировать о своей деятельности общество. Прозрачность опеределяется как освещение деятельности власти, содержания и механизма реализации, разъяснение целей публичной политики, а «открытость – как создание публичными органами власти условий для беспрепятственного доступа граждан к информации о его деятельности и к процессу принятия решений на всех этапах их приготовления.

4. Был рассмотрен политический процесс с различных научных подходов:

− Согласно структурно-функциональному подходу политический процесс рассматривается как механизм самоструктурирования системы, как политическая социализация граждан путем их участия в принятии решений политической жизни.

− Политический процесс в концепции системного подхода, считается и характеризуется как целостная система. Системный подход оценивает стабильность его элементов вследствие иерархичного расположения его

компонентов и наличия базовых элементов. Таким базовым компонентом или элементом является государство, которому общество предоставляет полномочия для управления взаимоотношениями и которое обладает для выполнения данных полномочий всеми ресурсами. Именно федеральный уровень государства позволяет выходить как на уровень регионов, так и муниципальных образований.

− По коммуникативному подходу политический процесс оценивается как обмен информационными данными акторами политики, как внутри политической системы, так и между системами. СМИ гарантирует данный процесс технологично, ориентируясь на политические партии, общественные движения, политические лидеры. Именно разработчики коммуникативного подхода делают ставку на координацию интегративных успехов.

− Институциональный подход оценивает политический процесс с позиции деятельности политических институтов. Благодаря институализации политический процесс имеет конституциональный и неконституционный, контролируемый и неконтролируемый характер.

В нашем представлении «политический процесс» содержит пространственно-временные трансформации, происходящие в политической системе государства. Их взаимодействие и функционирование, возможности движения и обновления, взаимодействие вне и внутри политических систем, формирование, деятельность политических институтов, динамика общепризнанных ценностей, распределение ролей политических акторов, характеризуют динамику политических субъектов, их информационное взаимодействие.

5. Были оценены характеристики власти. По утверждению А.В. Новиковой, понятие власти многозначно, имеет публичный, волевой и централизованный характер. Политическая власть – термин, обозначающий реальную возможность и способность определенного класса, социальной группы или части общества, а также представляющих их организаций и индивидов распространять свою волю относительно других групп, отдельных индивидов,

осуществлять общие интересы и цели насильственными и ненасильственными средствами. Политическую власть можно определить как способ реализации групповых интересов и достижения общих целей. Таким образом, в целом власть есть способность и возможность воздействовать на деятельность, поведение людей с позиции воли, авторитета, права, силы, знания. Каждый вид власти заслуживает внимания. Политическая власть, как и любой другой вид власти, означает право и способность одних проводить свою волю по отношению к другим. Именно через органы политической власти обеспечивается информационное взаимодействие.

6. Отмечено, что организационно-правовое обеспечение информационной безопасности предполагает реализацию комплекса законов, нормативов, управленческих решений, регламентирующих функционирование защиты сведений и информации, единые стандарты обеспечения информационной безопасности. К функционалу обеспечения информационной безопасности относятся:

− развитие основных методов и принципов отнесения сведений к защищаемой информации конфиденциального характера;

− регулирование системы органов власти и должностных лиц, имеющих ответственность за реализацию по защите информации;

− формирование системы различных видов документов, регулирующих механизмы по реализации системы защиты информации;

− детализация мер ответственности за нарушения норм защиты информации;

− закрепление регламента по решению конфликтных ситуаций по вопросам обеспечения защиты информации;

− становление экономических, налоговых взаимоотношений с целью эффективной борьбы с киберпреступностью и защиты информации в информационной сфере;

– улучшение компонентов экономического и налогового мотивирования научно-технологического прогресса в сфере информатизации и защиты информации».

Необходимо выделить, что нормативно-правовые базы государства в сфере информационной безопасности считаются необходимой мерой, которая удовлетворяет главную потребность в защите информации и сведений при формировании социально-экономических, политических, военных направлений деятельности государства. Особый интерес со стороны западных государств к реализации и становлению такой базы обусловлен возрастающими расходами на противоборство с угрозами в информационной сфере. Все это без исключения вынуждает западные государства всерьез работать над целями и задачами нормативно-правовой базы в области защиты информации.

7. Нами выделена разноаспектность защиты информации в органах государственной и муниципальной власти. Очевидно, что целый спектр государственных и муниципальных мероприятий зависит от числа опасностей и возможностей органов власти регулировать данные угрозы, используя надлежащие контрмеры. Одной из имеющихся угроз защиты информации служит потеря сведений по техническим каналам. Объектами допуска являются элементы информатизации органов государственной и муниципальной власти, в том числе технологическое оборудование, архивы, специализированные библиотеки, те объекты, в которых имеется информация ограниченного допуска. Для преодоления большей части технических каналов утечки сведений органы власти осуществляют технологически сложные методы защиты информации.

8. Была дана характеристика проекту «Открытый регион», который с точки зрения реализации повышает эффективность работы органов государственной и муниципальной власти. Для этого в рамках проекта формируются принципы открытого управления с учетом специфики конкретного субъекта РФ или муниципалитетов. В современный период в рамках проекта «Открытый регион» внедрение механизмов информационной открытости управления осуществляется

в 31 субъекте РФ. При осуществлении проектов в субъектах РФ для повышения открытости государственного управления в регионе требуется принятие комплексной нормативно-правовой базы. В целом, политика информационной открытости государственного управления выразилась в теории «Электронного правительства», которая предполагает обеспечение эффективного взаимодействия, базирующегося на увеличении открытости информационных ресурсов и объема информации, которую органы власти должны размещать в информационной системе и телекоммуникационных сетях (сети интернет).

9. Дана оценка информационной системе «Электронный муниципалитет» (далее ЭМ) представляющая программный комплекс, предназначенный для автоматизации функций органов местного самоуправления (далее ОМСУ).

Цели системы «ЭМ»:

– Унификация информации, обрабатываемой ОМСУ, с целью:

А) консолидации данных на уровне муниципального района для оценки социально-экономического развития региона в целом;

Б) организации регламентированного обмена информацией с государственными органами власти и учреждениями.

– Сокращение количества обработки данных хозяйственного и других видов учета, справок и выписок для населения и других видов отчетов администрацией ОМСУ.

– Сокращение времени получения государственных и муниципальных услуг гражданами.

Обозначим концепцию «ЭМ» в ракурсе муниципальной службы. Под сущностью муниципальной службы понимаем выполнение муниципальными служащими полномочий и взаимодействий с внешней средой в деятельности ОМСУ.

10. Отмечена важность проблемы информационной интеграции как этапа развития государственного и муниципального управления России в условиях глобализации. Очевидно, что интеграция в органах власти РФ – это процесс

объединения деятельности политических акторов, информационных систем и программных обеспечений. Следует отметить следующие основные подходы к ведению интеграции информационных систем политического процесса:

− «Стихийная» интеграция – интеграция систем при отсутствии единой инфраструктуры.

− На базе электронного документооборота формируется унифицированная информационная система для решения текущих и перспективных вопросов органов власти.

− Рекомендуется в органах власти использовать единую интеграционную систему ESB, которая характеризуется определенными параметрами.

Интеграция системы осуществляется при соблюдении технологических характеристик, включающих в себя следующие этапы:

− Обоснование рекомендаций к интеграции систем.

− Выполнение требований к эксплуатации систем.

− Стандартизация взаимодействия открытых информационных систем.

− Сквозной мониторинг к управлению.

− Единые методы к становлению информационной инфраструктуры.

− Набор механизмов технологической платформы для работы с интеграционными компонентами.

Интеграция процессов предполагает задействование сквозных процессов, где на отдельных этапах используются приложения. При этом обработка информации на данных этапах производиться в приложениях, а функции реализации процесса осуществляет специализированная подсистема. Для функционирования данного способа интеграции традиционно используют технологию WorkFlow.

Кроме того, в развитии информационной безопасности государственного и муниципального управления появились следующие инновации: программы «Электронное Правительство» и «Электронный муниципалитет». Включение всех уровней власти в систему электронного взаимодействия повышает качество

информационной безопасности политического процесса как государственного, так и муниципального управления. Для развития информационной интеграции и инновации органов власти применяется новый информационный продукт «СБИС», который обеспечивает оперативный доступ к информационным ресурсам.

11. Проанализированы наиболее значимые факторы, стимулирующие угрозы информационной безопасности деятельности органов власти. Органы муниципальной власти отмечают незащищенность в технологическом плане информационных систем, создаваемых на территории муниципального образования, которыми могут являться:

– незаконное использование и сбор информации;

– несоблюдение технологий обработки информации;

– внедрение нелицензированных программных компонентов;

– реализация элементов, дестабилизирующих деятельность систем защиты информации;

– повреждение средств обработки информационно-телекоммуникационных систем;

– активное вмешательство в ключевые системы защиты данных;

– взлом паролей и средств защиты информации;

– утечка информации по техническим каналам;

– внедрение средств-устройств перехвата информации по каналам связи;

– хищение, уничтожение носителей информации;

– перехват информации в сетях, дешифрование информации;

– использование нелицензионных и несертифицированных зарубежных и отечественных средств защиты данных;

– несанкционированный доступ к информации, находящейся в базах данных;

– нарушение нормативно-правовых актов, ограничивающих распространение информации.

Источники информационных угроз безопасности делятся на внутренние и внешние. Для местного самоуправления доминирующими являются внутренние источники, а внешние, чаще всего выходящие на государственный уровень, являются менее значимыми, но тесно связанными с ресурсами государства. Разграничить источники угроз сложно. Отметим наиболее существенные по своему влиянию на информационную безопасность. Самым значимым является уровень коррупции муниципалитетов.

В результате проведенного автором анализа организации политического управления информационным обеспечением в Забайкальском крае, выявлено, что необходимо уделить внимание таким аспектам, как:

– разработка организационных методов управления информации внутри администрации муниципальных образований;

– совершенствование законодательной базы информационной безопасности при взаимодействии муниципальных учреждений;

– персональная ответственность за возникновение информационных угроз в работе специалистов муниципальной администрации:

– защита электронного и бумажного документооборота.

Бумажный документооборот требует стабильности и архивного хранения в бумажном виде.

Можно сделать вывод, что вышеперечисленные направления по обеспечению информационной безопасности в администрациях муниципальных районах, связаны с развитием ноу-хау и современных инновационных технологий, имеющих новые способы защиты автоматизированных систем и программы для внедрения электронного документооборота. Необходимы формы персональной ответственности и контроля за использованием информации. Данный контроль обеспечат технические средства, но, на наш взгляд, эффективным методом будет совмещение технических средств с административными мерами контроля. Ограничение функций, осуществляемых с документами, которые содержат конфиденциальные сведения, позволит снизить

риск утечек информации во внешнюю среду. Оптимизация внутренних процессов и управление персоналом администраций муниципалитетов являются первоочередными мерами улучшения защиты информации. Также для эффективной организации информационной безопасности должна учитываться информационная открытость муниципалитетов и органов власти как инновационный фактор развития информатизации управления. Такова авторская оценка информационных угроз органов государственного и муниципального управления.

12. Анализ проблемы ведения информационного противоборства, включая определение возможностей для планирования мероприятий по осуществлению или отражению информационного воздействия, требует более четкого выявления основных направлений информационного противоборства. Выделены следующие направления информационного противоборства: борьба с системами управления, информационно-разведывательные операции, электронное, психологическое, «хакерское», «кибернетическое», «сетевое», экономическое, информационное столкновения и международный информационный терроризм.

13. Проведен анализ уровня и характера информированности населения муниципальных территорий, а также данные о существовании и функционировании административно–хозяйственных единиц Забайкалья. Для установления указанных характеристик воспользовались методом проведения контент – анализа средств массовой информации Забайкальского региона. Для нашего исследования взяли «Чернышевский», «Красночикойский» и «Могочинский», «Тунгиро-Олекминский» районы. В качестве каналов СМИ, по которым был проведен данный анализ, были взяты информационный интернет - портал «Читинский Городской портал» информационного агентства «Чита.ру», и портал «ЗабИНФО (Zabinfo.ru)» печатные издания Забайкальского края – газеты «Забайкальский рабочий», «Ваша реклама» и «Эффект – газета о жизни Забайкалья» .

Сделаны выводы, что такие ресурсы, как официальные сайты муниципальных образований Забайкалья, являются очень слабыми в техническом отношении, а также в отношении информационного наполнения. Официальные сайты муниципальных образований Забайкальского края явно не могут служить инструментом привлечения инвестиций в территориальные образования.

Ныне действующий портал Забайкальского региона – www.e-zab.ru, дающий место для размещения сайтов муниципальных районов, в настоящем времени прекратил свою работу. Муниципальным районам предложено подгружать сайты в одинаковом для всех интерфейсе, что предполагает легкость в ориентации для пользователя. Шаблон для сайтов создан в соответствии с критериями ФЗ-№8, но каждый орган местного самоуправления имеет право на творчество и добавление дополнительной согласованной с соответствующими структурами информации. Кроме того, было замечено, что созданные в сети Интернет-сайты органов местного самоуправления в Забайкальском крае не содержат в достаточном объеме сведений о необходимых условиях получения муниципальных услуг, что затрудняет взаимодействие граждан с органами власти. Получение населением и организациями услуг, а также информации, связанной с деятельностью органов власти, в большинстве случаев требует их личного обращения в данные органы, а также представления запросов и другой необходимой информации в бумажном виде. Это приводит к соответствующим затратам времени, создает значительные неудобства для населения и лишает смысла реализацию проекта «Электронное правительство».

Таким образом, слабое развитие информационно-коммуникативных технологий на муниципальном уровне оставляет более предпочтительной для граждан бумажную схему предоставления тех или иных услуг.

14. Нами было проведено социологическое исследование для определения состояния информационной среды Забайкальского края и готовности муниципалитетов и их служащих к реализации информационной безопасности на местах. В исследовании приняли участие девять муниципальных районов

Забайкальского края, а именно Агинский, Газимуро-Заводский, Карымский, Могойтуйский, Могочинский, Хилокский, Чернышевский, Читинский, Шилкинский и 300 муниципальных служащих. По гендерному и возрастному признаку в основном муниципалы – это женщины (78%), в соотношении мужчин – 22%. По возрастному цензу мы можем сделать вывод, что молодых людей от 18 до 26 малая часть – 3%. В основном это муниципальные служащие от 27 до 35 и от 36 до 44, но почти половина (42 %) - это люди старше 45 лет. Это говорит о старении кадров, а значит о необходимости гибкости муниципальной системы к изменениям внешней среды. Что касается должности и образования муниципальных служащих Забайкальского края, что в основном в исследовании приняли участие специалисты в равной доли – руководители и заместители. Образование муниципалов прогрессирует вместе с условиями современного мира, радует что появляются специалисты с профильным образованием «Государственное и муниципальное управление» – 16%, но, лидируют экономическое и средне–специальное (17% и 19%), уменьшается тенденция по привлечению специалистов муниципальной службы с юридическим образованием, всего – 9%.

Тенденции современного мира диктуют использование сети интернет, как в личных целях, так и в рабочих моментах, особенно это актуально при развитии электронного документооборот (ДЕЛО, СБИС). Большинство служащих при работе пользуются сетью интернет, что обуславливает поддержание информационной безопасности на высоком уровне. Одно из важных условий поддержания безопасности – наличие системного администратора, который следит за состоянием систем и их безопасности. Как показывает исследование в большинстве случаев в муниципальных органах имеется системный администратор, но качество не очень высокое, как показало исследование. Среди угроз информационной безопасности на муниципальном уровне стали актуальными различные вирусы, данная угроза сопровождает информационные системы с момента их создания, но тревожный момент актуализации на местном

уровне угрозы − хакерский взлом, так как эта угроза один из элементов киберпреступности и встречается чаще всего на федеральном уровне и реже не региональном и муниципальном уровнях.

15. Сформулированы направления по развитию информационной безопасности. Первое направление - информационное обеспечение государственной политики РФ. В этом направлении необходимо: интенсифицировать формирование государственных отрытых информационных ресурсов; укреплять государственные СМИ, расширять их возможности по своевременному доведению достоверной информации.

Второе направление – развитие современных информационных технологий, отечественной индустрии информации, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. Для этого требуется развивать инфраструктуру единого информационного пространства Российской Федерации; отечественную индустрию информационных услуг с одновременным повышением эффективности использования государственных информационных ресурсов; производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей информационных средств и систем.

Третье направление – защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности телекоммуникационных систем. С этой целью необходимо повышать безопасность, в первую очередь, первичных сетей связи, федеральных органов власти, органов власти субъектов РФ и местного самоуправления. Особое внимание по защите информационных ресурсов надо обратить на финансово-кредитную сферу, на административно-хозяйственную деятельность, на вооружение, военную технику, инфраструктуру всех органов власти и их ресурсное обеспечение.

16. Существуют следующие пути совершенствования информационной безопасности муниципалитетов Забайкальского края: административный и организационный уровни. Административный путь предполагает улучшение нормативно-правовой базы информационной безопасности. Организационный уровень ориентирован на улучшение защиты информации путем технизации управления (введение паролей пользователей; ограничение доступа к серверам; плановое сканирование систем и обновление антивирусных программ; установка на компьютер-сервер сетевого экрана «Agnitum Outpost FireWall. С целью защищенности объектов вычислительной сети должна применяться программа информационной защиты персональных компьютеров от спама и защита рабочих станций муниципальных служащих.

Перспективы дальнейшего изучения связаны с достижением эффективности системы обеспечения информационной безопасности, с созданием вариантов развития как государственной, так и муниципальной системы защиты информации. Обеспечение непрерывной коммуникации и взаимодействие между людьми в интересах как населения общественных пространств, так и органов государственной, муниципальной власти предполагает реализацию программ «Электронное правительство», «Электронный муниципалитет». Социально-политическую значимость перспективных исследований усиливает программа «Электронный муниципалитет» и деятельность негосударственных организаций, связанная с обработкой персональных данных, подлежащих государственному лицензированию.

Перспективное рассмотрение проблемы информационной безопасности связано с тем, что несмотря на процессы демократизации, проблема «открытости» государственной, муниципальной власти является актуальной и по сегодняшний день. К сожалению, власть воспринимается обществом как закрытый, не контролируемый обществом институт. С принятием федерального закона «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», возник институт свободы доступа к

официальной информации, который направлен на борьбу с коррупцией. Эффективность работы института апробировала себя на международной арене в контексте антикоррупционной политики. Недоработкой данного ФЗ является неэффективность современных методов контроля по исполнению норм над надлежащим качеством доступа к информации о государственных, муниципальных органах власти. Перспективным результатом нашего исследования должно быть рассекречивание информации и равный доступ граждан к информации о властных структурах. Данная информация актуальна как для городов, так и для муниципалитетов субъектов РФ. Перспективной она является и для Забайкальского края, особенно для Газимуро-Заводского района, где находится Быстринский горно-обогатительный комбинат (БГОК) построенный «Норникелем» в сжатые сроки в Забайкальском крае. Выход комбината на полноценный режим работы предусмотрен к концу 2018 г, на проектную мощность – после 2021 г. После выхода на проектную мощность БГОК будет производить около 3 млн т магнетитового концентрата, 260 тыс т медного концентрата и 9,5 млн тройских унций золота. Рынки сбыта для магнетитового и медного концентрата – Россиия и КНР, а также, потенциально – Япония и Южная Корея. «Норникель» владеет БГОКом через дочернюю компанию ООО «ГРК «Быстринское», в которой ему принадлежит 50,01%. Таковы прогнозируемые механизмы политического управления регионами мира и международным пространством отдельных стран: России, КНР, Японии и Южной Кореи.

СПИСОК ЛИТЕРАТУРЫ

1. Абрамов, А.В. Политический институт и политическая институционализация: определение понятия // Власть, май. 2010. -С. 55;

2. Аксенов, С.Г. Организационно-правовые основы обеспечения информационной безопасности органов государственной власти // Налоги – 2008, – N 3(2).

3. Актуальные киберугрозы – 2018. Тренды и прогнозы (дата опубликования 12 марта 2019 г.) компании Positive Technologies. [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/.

4. Алексеева, Е.В. Доктрина информационной безопасности Российской Федерации как ключевой аспект правового обеспечения национальной безопасности в информационной сфере // Ленинградский юридический журнал. 2016. – № 4 (46). – С. 97-103.

5. Антопольский, А.Б. Актуальные проблемы учета и регистрации информационных ресурсов // Проблемы информатизации. – 2001. – № 2.

6. Арканникова, М.С. Информационная открытость как ресурс конкурентоспособности регионов: концептуальные подходы. – М.: Полит. ин-т. 2008. – С. 49.

7. Арсентьев, М.В. Состояние информационной безопасности в России / М.В. Арсентьев // Информационные ресурсы России. 2003. – №2. – С. 19-21.

8. Артамонов, Г.Т. О противоречиях перехода к информационному обществу/ Г.Т.Артамонов//Вестник ВОИВТ. – 1998. – №3. – С.42–44.

9. Баранов, Н.А. Политические отношения и политических процесс в современной России. – СПб.: БГТУ, 2004. – 30 п.л.

10. Баскаков, А.В., Остапенко, А.Г., Щербаков, В.Б. Политика информационной безопасности как основной документ организации в создании системы информационной безопасности // Информация и безопасность. 2006. – Т.9. –№ 2. –С. 43-47.

11. Баталов, Э.Я. Политическое - «слишком человеческое» 2000. – 136 с.

12. Батурин, Ю. М., Жодзишскнй, А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юрид. лит., 1991. – 160 с.

13. Бачило, И.Л., Лопатин, В.Н., Федотов, М.А. Информационное право. / Под ред. академика РАН Б. Н. Топорнина. СПб.: Издательство Р. Асланова «Юридический центр Пресс», 2005.

14. Беззубцев, О.А. Ковалев, А.Н. О лицензировании и сертификации в области защиты информации [Электронный ресурс]. – Режим доступа: http://www.cryptopro.ru/sites/default/-files/docs/licen.pdf.

15. Березинская, М.Д., Азаров, А.Ю. Информационная безопасность современного общества // В сборнике: Информационное общество: состояние, проблемы, перспективы, 2017. – С. 45-52.

16. Бордюже, В.В., Белозеров, А.В., Софьина, И.В. Информационная безопасность: Монография / В.В. Бордюже, А.В. Белозеров, И.В. Софьина. – Пермь: Пермский центр научно-технической информации, 2009.- С 276.

17. Бородин, А. С. Информационная безопасность в современной России: политологический анализ: дис. … к-та полит. наук: 23.00.02 / Бородин Алексей Сергеевич. Санкт-Петербург, 2009. – 211 с.

18. Величко, М. Ю. Информационная безопасность в деятельности органов внутренних дел: теоретико-правовой аспект [Электронный ресурс]. – Режим доступа: http://lawtheses.com/informatsionnaya-bezopasnost-v-deyatelnosti-organov-vnutrennih-del-teoretiko-pravovoy-aspekt#ixzz5IfdhgH2A.

19. Венгеров, А.Б. Право и информационное обеспечение АСУ / А.Б. Венгеров // Советское государство и право. – 1972. – № 8. – С. 28-36.

20. Ветров, П.И. Уголовное право. – М., 1999. – С. 183-184.

21. Вехов, В.Б., Попова, В.В., Илюшин, Д.А. Тактические особенности расследования преступлений в сфере компьютерной информации: Науч.-практ, пособие. Изд. 2-е, доп. и испр. – М.: «ЛэксЭст», 2004. – 160 с.

22. Вилков, А.А., Некрасов, С.Ф., Россошанский, А.В. Политическая функциональность современных российских СМИ. Саратов: Издательский центр «Наука», 2011. – 268с.

23. Винер, Н. Кибернетика. −М.: 1968.

24. Временный регламент подготовки и размещения общедоступной информации Росстата в формате открытых данных / Утвержденного Заместитель руководителя Федеральной службы государственной статистики Г.К.Оксенойт 21.02.2017 [Электронный ресурс]. – Режим доступа: https://rulaws.ru/acts/Vremennyy-reglament-podgotovki-i-razmescheniya-obschedostupnoy-informatsii-Rosstata-v-formate-otkrytyh-dan/.

25. Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10.12.1948) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_120805/.

26. Галушкин, А.А. К Вопросу о значении понятий «национальная безопасность», «информационная безопасность», «национальная информационная безопасность» // Правозащитник. 2015. –№ 2. –С. 8.

27. Гафнер, В.В. Информационная безопасность / В.В. Гафнер. – Рн/Д: Феникс, 2015. – 324с.

28. Генне, О.В. Основные положения стеганографии // Защита информации Конфидент. – 2001. – №3. – С.20-25.

29. Гидденс, Э. Социология. – М.: 1999.

30. Горшков, Е. А. Саганова, В. Н. Обзор и анализ инструментальных средств обеспечения кадровой деятельности // Современные тенденции технических наук (II): материалы междунар. заоч. науч. конф. (г. Уфа, май 2013г.). – Уфа: Лето, 2013. – С. 5–7.

31. Гражданский кодекс Российской Федерации часть первая от 30 ноября 1994 г. N 51-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/Cons_doc_LAW_5142/.

32. Демин, В., Пак, Т. Организация работы пресс-служб – международные стандарты. –Алматы, 2005.

33. Дзялошинский, И.М. Информационная открытость органов местного самоуправления как основа социального партнерства [Электронный документ]. – Режим доступа: www.dzyalosh.ru.

34. Довлатов, А.С. Государственное регулирование информационной открытости как фактор повышения эффективности национальной экономики: диссертация ... канд. эконом. н. : 08.00.05. – М.: 2004. – С. 171.

35. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // Российская газета. – № 187. – 28.09.2000.

36. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) [Электронный ресурс]. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71456224/.

37. Донская, Е. Н., Панько, Ю. В. Отдельные аспекты обеспечения информационной безопасности деятельности органов местного самоуправления // Молодой ученый. – 2014. – №8. – С. 453-457.

38. Дорфман, Я.Г. Рецензия на книгу А.И. Михайлова, А.И. Черного, Р.С. Гиляревского «Основы научной информации» / Я.Г. Дорфман// Научно-техническая информация. – 1996. - № 7. – С. 46-47.

39. Дульщиков, Ю.С. Региональная политика и управление. - М.: Изд-во РАГС, 2001.- 257 с.

40. Емельянов, Г.В., Стрельцов, А.А. Информационная безопасность России. Учебное пособие / Под ред. А.А. Прохожева. −М.: Всероссийский научно-технический информационный центр. 2000. – С. 34

41. Зайцев, С.Е. Политики информационной безопасности в системах информационной безопасности // Научный вестник Московского государственного технического университета гражданской авиации. 2008. – № 137. –С. 37-44.

42. Закон Российской Федерации от 21.07.1993 N 5485-1 (ред. от 08.03.2015) «О государственной тайне» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/.

43. Здравомыслов, Б.В. Уголовное право Российской Федерации. Особенная часть / Под ред. Б.В. Здравомыслова. М., 1996. – С. 356.

44. Зеленков, М.Ю. Политология [Электронный ресурс]. – Режим доступа: https://psyera.ru/politicheskiy-process-ponyatie-sushchnost-i-soderzhanie_8232.htm.

45. Зеленков, М.Ю. Политология [Электронный ресурс]. – Режим доступа: https://psyera.ru/politicheskiy-process-ponyatie-sushchnost-i-soderzhanie_8232.htm.

46. Зеленков, М.Ю. Политология. – М.: Юрид. ин-т МИИТа, 2009. – 302с.

47. Иванченко, А.В. Обеспечение открытости органов власти для граждан и юридических лиц. – М.: 2007. – 178 с.

48. Информационная система (ИС) «Электронный муниципалитет» [Электронный ресурс]. – Режим доступа: http://r62.center-inform.ru/download/products_and_solutions/presentation_municipality.pdf.

49. Информационное агентство ТАСС. Глава ФСБ видит серьезную проблему в нежелании IT-компаний сотрудничать со спецслужбами. [Электронный ресурс]. – Режим доступа: https://tass.ru/obschestvo/7006012.

50. Ирхин, Ю.В. Гражданское общество и власть: проблемы взаимодействия и контроля в современной России // Социально-гуманитарные знания. 2007, – № 5.

51. Ищенко, А.Н., Прокопенко, А.Н., Страхов, А.А Новая доктрина информационной безопасности Российской Федерации как основа противодействия угрозам безопасности России в информационной сфере // Проблемы правоохранительной деятельности. 2017. – № 2. – С. 55-62.

52. Каменская, Е.А. Сущность и особенности информационной открытости органов власти в современной России/Е.А. Каменская //Общество: политика, экономика, право. – 2011. – № 2. – С. 19

53. Катуева, Я.В. Характеристики информационного пространства в задаче управления безопасностью субъекта федерации // Труды международного симпозиума Надежность и качество. 2010. – Т.1. –С. 23-24.

54. Кин, Д. Демократия и гражданское общество. – СПб.: 2001. – 400 с.

55. Конвенция о защите прав человека и основных свобод ETS N 005 (Рим, 4 ноября 1950 г.) (с изменениями и дополнениями) [Электронный ресурс]. – Режим доступа: https://base.garant.ru/2540800/.

56. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) (вместе с поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ N 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_121499/.

57. Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.) [Электронный ресурс]. – Режим доступа: https://base.garant.ru/4089723/.

58. Конвенция Содружества Независимых Государств о правах и основных свободах человека (заключена в Минске 26.05.1995) (вместе с «Положением о Комиссии по правам человека Содружества Независимых Государств», утв. 24.09.1993) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_6966/.

59. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N

2-ФКЗ, от 21.07.2014 N 11-ФКЗ) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_28399/.

60. Копылов, В.А. Информационное право. – 2-е изд., перераб. и доп. - М.: Юристь, 2002. – 512с.

61. Крупский, А. Ю., Феоктистова, Л. А. Информационный менеджмент: Учебное пособие – М.: Издательско-торговая корпорация «Дашков и К°». 2008 – 80 с.

62. Крутских, А., Крамаренко, Г. Дипломатия и информационно-коммуникационная революция / А. Крутских, Г. Крамаренко // Международная жизнь. 2003. – №7. – С.102-113.

63. Кузнецова, К.И. Информационная безопасность и проблема информационного неравенства в системе безопасности современного общества // В сборнике: ИНТЕЛЛЕКТУАЛЬНЫЙ ПОТЕНЦИАЛ XXI ВЕКА сборник статей международной научно-практической конференции: в 2 частях. 2018. – С. 192-195.

64. Кузнецова, Н., Кульбы, В. Информационная безопасность систем организационного управления: Теоретические основы // Под редакцией Н. Кузнецова и В. Кульбы. – М.: Наука, 2006. – С. 23.

65. Куликов, С.С. Управление информационной безопасностью информационно-телекоммуникационных систем, подвергающихся атакам типа «сетевой шторм» // Управление информационными рисками и обеспечение безопасности инфокоммуникационных систем Остапенко А.Г. Сборник научных трудов. под ред. чл.-корр. РАН В.И. Борисова. Воронеж, 2013. – С. 032-047.

66. Кулян, Р., Кулян, Р. Рогальский, Г.Л. Информационное обеспечение управления экономической безопасностью муниципального образования: временной аспект // Экономические науки. 2009. –№ 56. –С. 233-237.

67. Кухарский, А.Н. Информационная безопасность муниципалитетов Забайкальского края и пути ее совершенствования // Постулат. 2017. №2 (16). Биробиджан. С.11.

68. Лапкин, В.В. Сравнительные политические исследования России и зарубежных стран. –М.: 2008. – 292 с.

69. Лепихова, Л. А. Открытость политической власти: технологический анализ: дис. ... канд. полит. наук: 23.00.02 / Лепихова Лидия Алексеевна, –Ростов-на-Дону, 2007. – 164 с.

70. Лопатин, В. Н. Теоретико-правовые проблемы защиты единого информационного пространства и их отражение в системах российского права и законодательства [Электронный ресурс]. – Режим доступа:http:/for-expert.ru/problemy_inform_prava/15.

71. Лызь, Н.А., Веселов, Г.Е., Лызь, А.Е. Информационно-психологическая безопасность в системах безопасности человека и информационной безопасности государства // Известия ЮФУ. Технические науки. 2014. – № 8 (157). – С. 58-66.

72. Ляпунов, Ю.И., Пушкин, А.В. Преступления в сфере компьютерной информации // Уголовное право. Особенная часть / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. – М., 1998.

73. Малахова, О.В. Информационная открытость деятельности органов государственной власти: региональные практики/О.В. Малахова, В.А. Суханова//Среднерусский вестник общественных наук. – 2015. – № 2 (38). – С. 83

74. Махмадов, П. А. Информационная безопасность в системе политической коммуникации: состояние и приоритеты обеспечения (на материалах государств Центральной Азии): дис. … д-ра полит. наук: 23.00.04 / Махмадов Парвиз Абдурахмонович, Душанбе, 2018. 323 с.

75. Международный пакт о гражданских и политических правах (Нью-Йорк, 16 декабря 1966 г.) [Электронный ресурс]. – Ррежим доступа: https://base.garant.ru/2540295/.

76. Методика мониторинга и оценки открытости федеральных органов исполнительной власти утверждена протоколом заочного голосования Правительственной комиссии по координации деятельности открытого правительства от 26 декабря 2013 г. № АМ-П36-89пр [Электронный ресурс].

– Режим доступа: open.gov.ru/upload/iblock/f32/f32f65ebe06aa62bb1a9f247e5c85dda.doc.

77. Методические рекомендации по внедрению принципов и механизмов открытого государственного управления в субъектах Российской Федерации [Электронный ресурс]. – Режим доступа: http://open.gov.ru/upload/iblock/00f/00fe0e47c2b1d068ad07318689bb13c4.pdf.

78. Михеев, Ю.А. Типизация региональных ИТ-решений не панацея, а повод… // PC WEEK. 2006. – №16. – С. 42–43.

79. Михеева, Т.А. Информационная прозрачность и открытость органов государственной власти/Т.А. Михеева//Государственное и муниципальное управление в XXI веке: теория, методология, практика. – 2013. – № 9. – С. 98

80. Муниципальная власть и гражданское общество: проблемы диалога и перспективы развития: материалы межрегион. научн.-практ. конф. (25 февраля 2010 г.) / отв. ред. В.Б. Прокопьев. – Улан-Удэ: Изд-во Бурятского госуниверситета, 2010. – С.76.

81. Нестеров, А.В. Существует ли информационная безопасность, или некоторые аспекты законопроекта технического регламента «О безопасности информационных технологий» // Правовые вопросы связи. 2007. – № 1. – С. 31-35.

82. Новикова, А.В. Политическая власть и политическое управление в субъектах Российской Федерации: монография / А.В. Новикова; Забайкал гос. ун-т. – Чита: ЗабГУ, 2014. – С. 35-36.

83. Новикова, А.В. Политическая власть и политическое управление в субъектах Российской Федерации: монография / А.В. Новикова; Забайкал гос. ун-т. – Чита: ЗабГУ, 2014. – С. 37-38.

84. Новикова, А.В. Региональные особенности политических процессов субъектов Российской Федерации в условиях внешней и внутренней модернизации (монография). М.: МАКС Пресс, 2015. – 166 с.

85. Новикова, А.В. Регионы РФ в политическом процессе модернизирующейся России, и их влияние на обеспечение национальной безопасности /А.В. Новикова. – Забайкальский гос. ун-т. – Чита: ЗабГУ, 2016.-230с.

86. Новикова, А.В. Тенденции региональных политических процессов в Сибирском федеральном округе // Материалы «Десятые Байкальские социально-гуманитарные чтения» в двух томах, Иркутск, 2017г. С19-23

87. Окинавская хартия глобального информационного общества // 22 июля 2000 г. [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/supplement/3170.

88. Открытый регион [Электронный ресурс]. – Режим доступа: http://open.gov.ru/openregion/.

89. Отчёт Центра мониторинга за первое полугодие 2018 г. компании «Перспективный мониторинг». [Электронный ресурс]. – Режим доступа: https://amonitoring.ru/service/security-operation-center1/mssp/quarterly-reports/2018-1_amonitoring_halfyear_report.pdf.

90. Официальный сайт форума «Открытые инновации». [Электронный ресурс]. – Режим доступа: https://openinnovations.ru/press-center/news.

91. Панферова, В. В. Информационная политика в современной России / В. В. Панферова // Социально-гуманитарные знания. 2005. – № 5. – С. 53-68.

92. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федераци Федеральный проект «Нормативное регулирование цифровой среды» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 N 7) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_328854/.

93. Петров, В. П., Петров С. В. Информационная безопасность человека и общества / В. П. Петров, С. В. Петров. – М.: ЭНАС, 2007. – 336 с.

94. Полыхань, К.О. Проблемы и особенности состояния информационной безопасности в соответствии с доктриной информационной безопасности

Российской Федерации // Устойчивое развитие науки и образования. 2019. – № 5. – С. 154-160.

95. Постановление Правительства РФ от 24 ноября 2009 г. N 953 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти» (с изменениями и дополнениями) [Электронный ресурс]. – Режим доступа: http://base.garant.ru/196682/#ixzz3pGRuZncQ.

96. Постановление Правительства РФ от 4 сентября 1995 г. N 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_7686/.

97. Потрубач, Н.Н. Проблемы информационной безопасности / Н.Н. Потрубач // Социально-гуманитарные знания. 1999. – №2. – С.264-273.

98. Почепцов, Г.Г. Информационные войны, Серия: Образовательная библиотека. Издательство: Рефл-бук, 2001г. – 576 с.

99. Просвирнин, Ю.Г. Проблемы информационной открытости органов власти / Ю.Г. Просвирнин // Правовая наука и реформа юридического образования. – 2011. – № 1. – С. 112.

100.Проценко, Е. В. Информационная безопасность политической коммуникации в современной России: дис. … к-та полит. наук: 23.00.02 / Проценко Евгений Васильевич. Ставрополь, 2009. 199 с.

101.Проценко, Е.А. Информационная безопасность субъектов Российской Федерации как составная часть национальной безопасности России // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2006. –№ 25. –С. 111-115.

102. Распоряжение Правительства РФ от 10.07.2013 N 1187-р (ред. от 24.03.2018) «О Перечнях информации о деятельности государственных органов, органов местного самоуправления, размещаемой в сети «Интернет» в форме

открытых данных» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_149441/.

103. Распоряжение Правительства РФ от 29.12.2014 N 2769-р (ред. от 18.10.2018) «Об утверждении Концепции региональной информатизации» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_173678/.

104. Рассолов, И.М. Информационное право / Рассолов И.М. - М.: Норма, Инфра: –М.: 2010. – 352 с.

105. Региональная политика [Электронный ресурс]. – Режим доступа: http://uchebnik.online/regionalnaya-ekonomika_738/regionalnaya-ekonomika-regionalnaya-25532.html.

106. Риа новости. В Минобрнауки рассказали, для чего нужны центры по кибербезопасности. [Электронный ресурс]. – Режим доступа: https://ria.ru/20191101/1560464194.html.

107. С деятельностью данной комиссии можно познакомиться на ее сайте [Электронный ресурс]. – Режим доступа: http://www.cada.pt/.

108. Сайт «Стандарт открытости» [Электронный ресурс]. – Режим доступа: https://openstandard.ru/.

109. Сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. [Электронный ресурс]. – Режим доступа: https://digital.gov.ru/ru/activity/statistic/rating/mezhdunarodnye-rejtingi/.

110. Семененко, В.А. Информационная безопасность. В.А. Семененко. – М.: МГИУ, 2010. – 277 с.

111. Сиваков, О. Г. Актуальные проблемы информационной безопасности в научно-технической сфере / О.Г. Сиваков // Информационные ресурсы России. 2003. – № 4. – С. 25-28.

112. Сизьмин, М.А. Информационная (информационно-психологическая) безопасность в структуре национальной безопасности (на примере США и России) // Известия Иркутской государственной экономической академии

(Байкальский государственный университет экономики и права). 2014. –№ 3. –С. 28.

113. Систер, В.Г. Информационные технологии на службе города// Информационное общество, 2003. – №1. – С.143

114. Сканер-ВС [Электронный ресурс]. – Режим доступа: http://npoechelon.ru/production/65/4291?yclid=2819-290500710796405.

115. Степанов, О. А. Ключевые аспекты правового регулирования использования и развития информационно-электронных технологий // Государство и право. 2004, – N 4. – С. 70.

116. Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 07.02.2008 N Пр-212) [Электронный ресурс]. – Режим доступа: http://base.garant.ru/192762/.

117. Стуженко, Н.И., Шеметов, А.И. Информационное обеспечение управления безопасностью региона // Научный альманах. 2015. – № 10-3 (12). – С. 251-254.

118. Талимончик, В.П. Информационная безопасность в контексте всеобъемлющей системы международной безопасности // Известия высших учебных заведений. Правоведение. 2008. – № 2 (277). – С. 103-111.

119. Указ Президента Российской Федерации от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года» // Российская газета. - № 4912. – 12.05.2009.

120. Указ Президента РФ от 17.03.2008 N 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_75586/#dst0.

121. Указ Президента РФ от 22.05.2015 N 260 «О некоторых вопросах информационной безопасности Российской Федерации» (вместе с «Порядком подключения информационных систем и информационно-

телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети «Интернет») [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_179963/.

122. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» [Электронный ресурс]. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71570570/.

123. Федеральная служба государственной статистики (РОССТАТ). [Электронный ресурс]. – Режим доступа: http://www.gks.ru/free_doc/new_site/rosstat/os/doclad-2019%20.pdf .

124. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_220885/.

125. Федеральный закон от 02.05.1997 N 76-ФЗ (ред. от 23.05.2015) «Об уничтожении химического оружия» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_14292/.

126. Федеральный закон от 09.02.2009 N 8-ФЗ (ред. от 09.03.2016) «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_84602/.

127. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/-Cons_doc_LAW_61798/.

128. Федеральный закон от 27.07.2010 N 224-ФЗ (ред. от 27.12.2018) «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные

акты Российской Федерации» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?from=103037-0&rnd=F4D1A53C9769ABE7588C801F7519379F&req=doc&base=LAW&n=310162&REFDOC=103037&REFBASE=LAW#28d967a5p5s.

129. Федеральный закон от 28 декабря 2010 г. N 390-ФЗ «О безопасности» [Электронный ресурс]. – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=187049.

130. Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне». [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_48699/.

131. Федеральный закон от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности» [Электронный ресурс]. – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=113-658.

132. Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи». [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_112701/.

133. Федеральный закон от 7 июля 2003 г. N 126-ФЗ «О связи» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/Cons_doc_law_43224/.

134. Федоров, А.В «Супертерроризм. Новый вызов нового века» – М.: «Права человека», 2003.

135. Философская энциклопедия. Словари и энциклопедии на Академике [Электронный ресурс]. - Режим доступа: http://dic.academic.ru/dic.nsf/enc_philosophy/211/%D0%92%D0%9B%D0%90%D0%A1%D0%A2-%D0%AC.

136. Филяк, П.Ю., Шварев В.М. Обеспечение информационной безопасности организации на основе системы менеджмента информационной безопасности // Информация и безопасность. 2015. – Т.18. – № 4. – С. 580-583.

137. Чайка, И. Г. Политические технологии обеспечения информационной безопасности региона: на примере Краснодарского края: дис. … к-та полит. наук: 23.00.02 / Чайка Иван Геннадьевич, Краснодар, 2010. 210 с.

138. Чеботарева, А.А. Обеспечение информационной безопасности личности: роль международной информационной безопасности и стратегического партнерства // Вестник Академии права и управления. 2016. – № 1 (42). – С. 48-51.

139. Чеботарева, А.А. Человек и электронное государство. Право на информационную безопасность // монография / А. А. Чеботарева; М-во образования и науки Российской Федерации, Гос. образовательное учреждение высш. проф. образования «Читинский гос. ун-т» (ЧитГУ). Чита, 2011.

140. Черноусов, М.В. Совершенствование механизмов информационной открытости в системе муниципального управления // Вестник Самарского муниципального института управления: теоретический и научно-методический журнал. 2010, – № 2 (13). – 132 с.

141. Черняк, Л. Новые задачи информационной безопасности / Л. Черняк // Открытые системы. СУБД. 2005. – № 5/6. – С. 16-18.

142. Шабров, О.Ф. Политико-административное управление в Российской Федерации: состояние и актуальные проблемы // Власть.-2004.-№11

143. Шабров, О.Ф. Политическая власть, ее эффективность и легитимность / О.Ф. Шабров // Политология. – М.: Изд-во РАГС, 2002. – С. 135-136.

144. Шелупанов, А.А., Зайцев, А.П., Мещеряков, Р.В. Основы защиты информации. Изд. 5-е, перераб. И доп. – Томск: В-Спектр, 2011. – 244с.

145. Шерстюк, В.П. Информационная безопасность в системе обеспечения национальной безопасности России, федеральные и региональные аспекты обеспечения информационной безопасности // Информационное общество. 1999. – № 5. – С. 3-5.

146. Эпова, А.Н. Анализ интернет-порталов муниципальных районов / А.Н. Эпова // Молодежь Забайкалья: инновации в технологиях и образовании:

материалы XV Международная молодежная научно-практическая конференция - Чита: ЗабГУ, 2012 - Часть III. – С.-111.

147. Якимца, В.Н. Оценка состояния и развития гражданского общества России: проблемы, инструменты и региональная специфика / под. ред. В.Н. Якимца. Труды ИСА РАН. – Т.57. – М.: Красанд, 2010. – 200 с.

148. Ярочкин, В.И. Информационная безопасность. В.И. Ярочкин. – М.: Акад. Проект, 2008. – 544 с.

149. Agnitum Outpost FireWall [Электронный ресурс]. – Режим доступа: http://www.agnitum.ru/support/kb/-article.php?id=1000295&lang=ru.

150. Ahles, M.T. Information systems impact on national security execution: a model for the security assistance training program execution in security assistance offices // thesis, degree: Ph.D., degreeYear: 2002, Institute: Union Institute and University, adviser: Cherie Lohr.

151. Andress, J The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice // — Syngress, 2014. − 240 p.

152. Arquilla, J, and Ronfeldt D. eds., In Athena’s Camp: Preparing for Conflict in the Information Age, Santa Monica, Calif.: RAND, MR-880-OSD/RC, 1997. –P.460.

153. Beniger, J. The Control Revolution: Technological and Economic Origins of the Information Society, Cambridge, Mass., Harvard University Press, 1986.

154. Castells, M. The Power of Identity. Maiden (Ma.) Oxford, Blackwell Publishers, 1997. Цит.по: Новая постиндустриальная волна на Западе: Антология. −Москва: Academia, 1999. –С. 494.

155. Cherdantseva, Y. Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals // Organizational, Legal, and Technological Dimensions of Information System Administrator / Y. Cherdantseva, J. Hilton. — IGI Global Publishing, 2013.

156. Fiddner, D.M.J. Hhe information infrastructure system as a national security risk and united states information infrastructure system national security policy, 1990—

2000 // thesis, 2004, Degree: Ph.D. DegreeYear: 2003, Institute: University of Pittsburgh, Adviser: Phil Williams.

157. Freeman, L. Peace G. Information Ethics: Privacy and Intellectual Property. – Hersey: Information Science Publishing, 2005.

158. Gompert, D.C. National security in the information age // Naval War College Review. 1998. – Т.51. – № 4. – С. 22-40.

159. Gordon, L. The Economics of Information Security Investment : / Lawrence Gordon, Martin Loeb // ACM Transactions on Information and System Security. – 2002. – Vol. 5, no. 4 (November).

160. Gray, C. Review: information security policies, procedures and standards: guidelines for effective information security management // ITNOW. 2003. – Т.45. –№ 2. –С. 30-b.

161. Hughes, J. Quantitative Metrics and Risk Assessment : The Three Tenets Model of Cybersecurity : / J. Hughes, G. Cybenko // Technology Innovation Management Review. – Ottawa, Canada : Talent First Network (Carleton University), 2013. – August. – P. 15–24.

162. Lynne, R. Jessica Moyer Cyber-security, cyber-attack, and the development of governmental response: the librarian's view // New Library World. 2004. –Т.105. – № 7-8. – С. 248-255.

163. McCullagh, A. Non-Repudiation in the Digital Environment : / Adrian McCullagh, William Caelli // Technology Innovation Management Review. – Chicago, USA : First Monday, 2000. – Vol. 8, no. 8 (August).

164. Merwe, V. Characteristics and Responsibilities involved in a Phishing Attack : / Loock, Marianne, Dabrowski, Marek // WISICT '05 Proceedings of the 4th international symposium on Information and communication technologies. — Cape Town, South Africa, 2005. – 3 January. – P. 249–254.

165. Moore, R. Investigating High Technology Computer Crime: − 2nd ed.− Boston : Anderson Publ., 2011. − 318 p.

166. Noveck, B. Paradoxical Partners: Electronic Communication and electronic Democracy. In Democratization, –Vol.7, – No.1, Spring 2000. – P.32.

167. Peter Ferdinand. The Internet, Democracy and Democratization. In Democratization, –Vol.7, –No.1, Spring 2000. –P.6.

168. Pettey, C. Gartner Says Digital Disruptors Are Impacting All Industries; Digital KPIs Are Crucial to Measuring Success: – Gartner, Inc., 2017.

169. Ramirez, A.J. Globalizacion y derecho social en Mexico. El entorno latinoamericano y las politicas sociales // thesis, degree: Dr., degreeYear: 2005, Institute: Universidad de Navarra (Spain).

170. Samonas, S. The CIA Strikes Back : Redefining Confidentiality, Integrity and Availability in Security : [англ.] / Samonas, S., Coss, D. // Journal of Information System Security. – Washington DC, USA: Information Institute Publishing, 2014. – Vol. 10, no. 3.

171. Schlienger, T. Information security culture: From analysis to change / Thomas Schlienger, Stephanie Teufel // South African Computer Journal. – Pretoria, South Africa, 2003. – Vol. 31.

172. Shawn, P. Wilbur. «An Archaeology of Cyberspace. Virtuality, Community, Identity». In David Bell and Barbara Kennedy (Eds.) Cybercultures Reader. Routledge, 2000, – P.45.

173. Spamoed [Электронный ресурс]. – Режим доступа: http://www.spamoed.com/.

174. Stickman, J.F. Assessing United States information assurance policy response to computer-based threats to national security // thesis, degree: D.P.A., degreeYear: 2001, Institute: University of Southern California, adviser: Chester A. Newland.

175. Wiley, J. Security and Preservation Considerations // Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management / Bidgoli, H. – John Wiley & Sons, 2006. – Vol. 3.

176. Wright, R. Three Scientists and Their Gods: Looking for Meaning in an Age of Information. −New York: Harper and Row, 1989. – P.5.

Приложение А.

Основные направления обеспечения информационной безопасности (составленная автором на основании Доктрины информационной безопасности России).

Сфера:	**Направления развития:**
В области обороны страны являются:	а) стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий (далее ИТ); б) совершенствование системы обеспечения информационной безопасности (далее ИБ) Вооруженных Сил РФ, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства; в) прогнозирование, обнаружение и оценка информационных угроз (далее ИУ), включая угрозы Вооруженным Силам РФ в информационной сфере (далее ИС); г) содействие обеспечению защиты интересов союзников РФ в ИС; д) нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества.
В области государственной и общественной безопасности являются:	а) противодействие использованию ИТ для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности; б) пресечение деятельности, наносящей ущерб национальной безопасности РФ, осуществляемой с использованием технических средств и ИТ специальными службами и организациями иностранных государств, а также отдельными лицами; в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения ИУ и ликвидации последствий их проявления, повышение защищенности граждан; г) повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов; д) повышение безопасности функционирования образцов вооружения, военной и специальной техники и автоматизированных систем управления.
В экономической сфере являются:	а) инновационное развитие отрасли ИТ и электронной промышленности, увеличение доли продукции этой отрасли в валовом внутреннем продукте, в структуре экспорта страны; б) ликвидация зависимости отечественной промышленности от зарубежных ИТ и средств обеспечения ИБ за счет создания, развития и широкого внедрения отечественных разработок, а также производства продукции и оказания услуг на их основе; в) повышение конкурентоспособности российских

	компаний, осуществляющих деятельность в отрасли ИТ и электронной промышленности, разработку, производство и эксплуатацию средств обеспечения ИБ, оказывающих услуги в области обеспечения ИБ, в том числе за счет создания благоприятных условий для осуществления деятельности на территории РФ; г) развитие отечественной конкурентоспособной электронной компонентной базы и технологий производства электронных компонентов, обеспечение потребности внутреннего рынка в такой продукции и выхода этой продукции на мировой рынок.
В области науки, технологий и образования являются:	а) достижение конкурентоспособности российских ИТ и развитие научно-технического потенциала в области обеспечения ИБ; б) создание и внедрение ИТ, изначально устойчивых к различным видам воздействия; в) проведение научных исследований и осуществление опытных разработок в целях создания перспективных ИТ и средств обеспечения ИБ; г) развитие кадрового потенциала в области обеспечения ИБ и применения ИТ; д) обеспечение защищенности граждан от ИУ, в том числе за счет формирования культуры личной ИБ.
В области стратегической стабильности и равноправного стратегического партнерства являются:	а) защита суверенитета РФ в информационном пространстве посредством осуществления самостоятельной и независимой политики, направленной на реализацию национальных интересов в информационной сфере; б) участие в формировании системы международной ИБ, обеспечивающей эффективное противодействие использованию ИТ в военно-политических целях, противоречащих международному праву, а также в террористических, экстремистских, криминальных и иных противоправных целях; в) создание международно-правовых механизмов, учитывающих специфику ИТ, в целях предотвращения и урегулирования межгосударственных конфликтов в информационном пространстве; г) продвижение в рамках деятельности международных организаций позиции РФ, предусматривающей обеспечение равноправного и взаимовыгодного сотрудничества всех заинтересованных сторон в ИС; д) развитие национальной системы управления российским сегментом сети «Интернет».

Приложение Б.

Анкета при проведении социологического опроса муниципалитетов Забайкальского края.

Уважаемые друзья!

Для сбора информации с целью улучшения деятельности органов местного самоуправления нами проводиться опрос на тему

«Информационное обеспечение органов местного самоуправления как основа информационной безопасности».

Мы гарантируем конфиденциальность полученной информации. Результаты будут использованы в обобщенном виде.

Вы должны отметить выбранные ВАМИ варианты ответов любым способом (О;+;V)

1. Ваша должность:
   1.1 руководитель;
   1.2 заместитель;
   1.3 специалист.
   1.4 укажите иное_____
2. Ваш пол:
   2.1 мужской;
   2.2 женский.
3. Ваш возраст:
   3.1 от 18 до 26;
   3.2 от 27 до 35;
   3.3 от 36 до 44;
   3.4 от 45 и старше.
4. Ваше образование:
   4.1 высшее профильное (Государственное и муниципальное управление);
   4.2 высшее образование, указать какое (педагогическое юридическое, инженерное, техническое со знанием информационных технологий и т.д.)_____;
   4.3 незаконченное высшее;
   4.4 средне-специальное;
   4.5 иное.
5. Обеспечены ли вы техническими возможностями для реализации ваших полномочий (технические средства, программное обеспечение и т.д.):
   5.1 да, полностью обеспечены;
   5.2.да, частично обеспечены;
   5.3 нет, недостаточно ресурсов;
   5.4 совершенно не обеспечены.
6. Удовлетворены ли вы уровнем состояния ваших технических средств:
   6.1 да, мы идет в ногу со временем;
   6.2 да, но хотелось бы лучше;
   6.3 уровень состояния ресурсов средний;
   6.4 нет, все устарело.
7. Пользуетесь ли вы сетью интернет?
   7.1 да, пользуемся часто;
   7.2 да, пользуемся редко;
   7.3 планируем пользоваться;
   7.4 нет, не пользуемся.
8. Имеется ли у вас системный администратор:
   8.1 да, у нас отдельная должность – системный администратор;
   8.2 да, специалист совмещает несколько должностей;
   8.3 приглашенный специалист;

8.4 нет системного администратора;

8.5 нет необходимости в системном администраторе.

9. Как вы понимаете сущность определения «информационная безопасность»?

9.1 это – состояние защищенности личности, общества и государства в информационной сфере…;

9.2 это – осуществление мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз…;

9.3 это – совокупность сил обеспечения информационной безопасности…

10. Распределите, пожалуйста, виды безопасности по значимости шкал от 1 до 4 (1 – значимо, 2 – менее значимо, 3 – скорее незначимо, 4 – незначимо):

	Лично для вас	Для муниципального образования и государства в целом
Экономическая		
Информационная		
Политическая		
Социальная		

11. Как вы понимаете определение «конфиденциальная информация»?

11.1 это – совокупность баз данных, технологий и технических средств;

11.2 это – обязательное требование не передавать такую информацию третьим лицам;

11.3 это – зафиксированная на специальном материальном носителе информация, в порядке, установленном законодательством Российской Федерации;

12.Была ли утечка информации при выполнении ваших полномочий? Случалась ли у вас утечка…

12.1 да;

12.2 нет;

12.3 затрудняюсь ответить.

13. Какие угрозы информационной безопасности стали актуальными в современный период? (выберите несколько вариантов):

13.1 хакерский взлом;

13.2 халатность работников;

13.3 различные вирусы;

13.4 использование систем не по значению;

13.5 использование несертифицированного программного обеспечения;

13.6 таких угроз нет.

14. Беспокоят ли вас риски информационной безопасности, связанные с социальными сетями?

14.1 да;

14.2 нет.

14.3 затрудняюсь ответить.

15. Рассматриваете ли вы информационную безопасность как одно из основных направлений развития: Нужно ли, на ваш взгляд, работу по обеспечению информационной безопасности включать в перечень основных направлений развития муниципального образования?

15.1 да, безусловно;

15.2 данный аспект рассматривается в перспективе;

15.3 у нас есть более важные направления развития;

15.4 нет, не рассматривается.

СПАСИБО ЗА УЧАСТИЕ!