Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

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

Автореферат
диссертации на соискание ученой степени
кандидата политических наук

Екатеринбург – 2020

Работа выполнена на кафедре государственного, муниципального управления и политики Федерального государственного бюджетного образовательного учреждения высшего образования «Забайкальский государственный университет»

Научный руководитель: доктор политических наук, профессор
Бейдина Татьяна Евгеньевна,

Официальные оппоненты: **Чеботарева Анна Александровна,**
доктор юридических наук, доцент, ФГАОУ ВО «Российский университет транспорта», г. Москва, заведующая кафедрой «Административное право, экологическое право, информационное право»;

Пронин Эдуард Анатольевич,
доктор политических наук, профессор, Московский областной филиал НОУ ВПО «Санкт-Петербургский Гуманитарный университет профсоюзов» «Институт искусств и информационных технологий», г. Москва, профессор кафедры «Рекламы и социально-культурных технологий»;

Козыкина Наталья Владимировна,
кандидат политических наук, ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б. Н. Ельцина», г. Екатеринбург, доцент кафедры теории и истории международных отношений.

Защита состоится «04» марта 2020 г. 10:00 часов на заседании диссертационного совета УрФУ 23.01.05 по адресу: 620000, г. Екатеринбург, пр. Ленина, 51, зал заседаний диссертационных советов, комн. 248.

С диссертацией можно ознакомиться в библиотеке и на сайте ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»: https://dissovet2.urfu.ru/mod/data/view.php?d=12&rid=924

Автореферат разослан «___» _____ 2020 г.

Ученый секретарь
диссертационного совета Керимов Александр Алиевич

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИССЕРТАЦИИ

Актуальность исследования. Изменение конфигурации международного политического пространства, возникновение в условиях глобализации новых центров силы и политических акторов вызывают научный интерес к исследованию проблемы информационной безопасности политического процесса, ее предпосылок и факторов обеспечения. Один из наиболее влиятельных мировых политических трендов современного периода – это взаимозависимость стран и народов. Это является внешней предпосылкой для развития информационной безопасности политического процесса. Информационная безопасность сопровождается не только позитивными феноменами, но и появлением и усилением глобальных информационных угроз национальным интересам государств в политической и других сферах.

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

Поэтому в центре внимания ученых находятся проблемы, которые связаны с исследованием новых принципов и технологий информационного взаимодействия в политической сфере, а также выявление возможностей противостояния возникших угроз и обеспечения информационной безопасности на глобальном, региональном и национальном уровнях. Показ значимости внешнеполитических и внутриполитических составляющих информационной безопасности, в совокупности, составляет теоретический аспект актуальности темы диссертационной работы. Теоретическую и практическую актуальность имеет научное осмысление вопроса, ориентированное на определение понятия «информационная безопасность», которая одними исследователями трактуется как кибербезопасность (безопасность информационных сетей и систем); другими – как манипулирование информацией, пропаганда с помощью Интернета, информационное воздействие на сознание целевых групп. Информационная безопасность может оцениваться как составляющая национальной безопасности. Поэтому сравнительный анализ подходов, изучение целей и ключевых проблем обеспечения безопасности политического процесса представляется актуальным.

Актуализирует проблему необходимость подготовки специалистов по кибербезопасности, которых мало как во власти, так и в коммерческой среде. Например, в лаборатории «Касперского» существуют 134 вакансии на специалистов по кибербезопасности. 01 ноября 2019г. Минобрнауки объявили о том, что нужны учебно-научные центры по безопасности для информатизации государственных и муниципальных органов власти, а также для обеспечения «единого многомерного образовательного пространства»[1].

Формирование и становление информационной безопасности – комплексная проблема, в которой можно выделить правовой, административный, программно-технический и процедурный уровни. Исходя из данных уровней, существует необходимость развития методологических положений информационной безопасности

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

органов власти. Актуализация исследования рычагов управления информационной безопасностью в условиях интеграции информационных систем обусловлена тем, что данные проблемы рассматривают, прежде всего, с технических позиций.

Степень научной разработанности проблемы.

С технической точки зрения оценка информационной безопасности началась с 1816 г. и связана с защитой информации государства, с появлением средств электро и радиосвязи, с повышением защищённости радиолокационных средств, с внедрением в деятельность органов власти электронно-вычислительной техники. 1965 г. характеризуется созданием информационно-коммуникационных сетей и передачей администратору управления сетевыми ресурсами. С 1973 г. обеспечение информационной безопасности связано с разработкой новых критериев безопасности, сгруппировалось новое сообщество «хакеров», целью которых было нанесение ущерба информационным каналам отдельных пользователей, организаций и целым странам. В данный период сформировалась новая отрасль международного права − информационное право. 1985 г. обусловлен созданием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения.

В изучении политического процесса активно участвовали классики политической мысли Д. Истон, Г. Алмонд, Б. Пауэлл, К. Ганс, Д. Норт. 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[3], А. С. Панариным, Ю.С. Дульщиковым, А. В. Новиковой[4], 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. Субъектами политического процесса являются «политические системы, политические институты (государство, гражданское общество, политические партии и т. д.), организованные и неорганизованные группы людей, индивиды»[5]. 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 в системе политического процесса, в управлении и реализации государственной и муниципальной службы такие исследователи как: М.Д. Березинская, А.Ю. Азаров[6], А.Е. Лызь, К.О. Полыхань[7], В.П. Талимончик,

---

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

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

[4] 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.

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

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

[7] 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.

В.М. Шварев, J. Andress[8], L. Gordon, R. Moore, T. Schlienger, J. Wiley. Информационную безопасность в системе национальной безопасности изучали: Е.В. Алексеева[9], А.А. Галушкин, Е.А. Проценко, М.А. Сизьмин[10], В.П. Шерстюк, М.Т. Ahles, D.M.J. Fiddner, D.C. Gompert, J.F. Stickman[11]. Можно отметить работы по информационной безопасности в политико-правовой сфере: Я.В. Катуева, К.И. Кузнецова, Н.И. Стуженко, А.А. Чеботаревой [12], А.И. Шеметова, L. Freeman, S. Gartner, J. Hughes[13], M. Jessica, R. Lynne, A. Merwe, G. Peace. Отметим авторов, изучавших информационную безопасность в системе муниципального и государственного управления, среди которых: А.В. Баскаков, С.Е. Зайцев, А.Н. Ищенко, А.В. Нестеров, Г.Л. Рогальский, Y. Cherdantseva, C. Gray, A. McCullagh, A.J. Ramirez, S. Samonas[14].

Теоретико-методологической основой исследования являются работы зарубежных и отечественных исследователей по защите информации и информационной безопасности, среди которых работы: М.В. Арсентьева, Ю.М. Батурина, Н.И. Ветрова, В.Б. Вехова, Б.В. Здравомыслова, А. Кудрявцева, Ю.И. Ляпунова, В.В. Панферова, Н.Н. Потрубач, О. Г. Сивакова, Л. Черняк.

Проблемы государственного регулирования в информационной сфере стали изучаться во второй половине XX в., когда стал развиваться международный обмен научно-техническими достижениями. Неоценимый вклад в данную область внесли: А.Б. Антопольский, Г.Т. Артамонов, М.Д. Березинская, А.Ю.Азаров, И.Л. Бачило, А.Б. Венгеров, А.А.Галушкин[15], Я.Г. Дорфман, Г.В. Емельянов, В.А.Копылов, С.С. Куликов, В.Н. Лопатин, Г.Г. Почепцов, М.М. Рассолов[16], А.А. Чеботарева[17] и др. Среди зарубежных ученых можно отметить работы J. Arquilla, J.Beniger, M. Castells, P. Ferdinand, S. Noveck, W. Robert, P. Wilbur, N Wiener.

Единственным политологом, рассматривающим информационную безопасность с позиции внешнего политического процесса, был доктор политических наук П.А. Махмадов[18]. С позиции внутреннего политического процесса информационная

---

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

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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

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

[17] 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.

[18] 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

безопасность рассматривалась в Краснодаре[19], Ставрополе[20], а политологический анализ был осуществлен в Санкт-Петербурге[21]. 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.

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. Выявить направления информационных угроз для государственных и муниципальных органов власти, охарактеризовать информационную открытость как основное условие развития России и создать модель информационной открытости.
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

Абдурахмонович, Душанбе, 2018. 323 с.

[19] 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.

[20] 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.

[21] 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.

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 национальной безопасности, политологии, геополитике и 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 муниципальными образованиями по обеспечению безопасности личности, общества и государства.

Методология и методы 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 муниципали-

тетов 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, основанных на утвержденной в 2019 г. национальной программе «Цифровая экономика Российской Федерации»[22], предполагающей цифровое государственное управление. Достоверность подтверждается развитой источниковой базой кандидатской диссертации, среди которой:

1. Нормы международного права, правовая база Российской Федерации по защите информации.

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

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

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, Душанбе, Иркутска, Благовещенска, Таджикистана, 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; мате-

[22] 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/.

риалах 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-на-Дону; материалах XIV международной научно-практической конференции: Фундаментальные и прикладные науки сегодня. 20-21 февраля 2018г. North Charleston, USA; материалах IX всероссийской (с международным участием) научно-практической 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 по списку ВАК, а также в сборниках международных и всероссийских научно-практических конференций.

Структура исследования. Диссертация состоит из введения, трех глав, включающих семь параграфов, заключения, списка литературы, содержащего 176 названия. В работе представлены 33 рисунка и 9 таблиц. Общий объем работы – 199стр.

2. ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обосновывается актуальность темы, дается степень ее научной разработки и анализ литературы по проблеме, определяются цель и задачи исследования, научная новизна и практическая значимость.

Первая глава − «Теоретико-методологические основы информационной безопасности как политического процесса» посвящена рассмотрению теоретических и методологических основ информационной безопасности политического процесса.

В параграфе 1.1 «Взаимосвязь понятий «политический процесс», «информационная безопасность», «национальная безопасность», «информационная открытость»» диссертантом дается обоснование места информационной безопасности в политическом процессе и в системе национальной безопасности.

Помимо классического подхода к структуре и субъектам политического процесса, изложенным в диссертации, мы подчеркиваем, что к субъектам политического процесса можно отнести информационную составляющую с учетом информатизации политических процессов, системы государственного и муниципального управления и значимости информации для органов власти. 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. Данное определение универсально и используется всеми структурами власти, оно содержит общее определение защиты информации как государства, так и его гражданина. Деятельность в области информационной безопасности призвана обеспечить защиту законных интересов граждан, общества и государства в информационной сфере. По утверждению 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»[23].

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 характеризуется 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. Таким базовым компонентом или 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 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.

---

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

С точки зрения коммуникативного подхода политический процесс оценивается 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.

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.

Так же отмечаем информационный подход, где выделены реально действующие информационные акторы. Здесь мы акцентируем внимание на том, что информационная безопасность – это составляющая политического процесса ориентированная на защищенность органов власти от манипулирования информации.

Очевидно, что политический процесс включает объекты и субъекты (государство, политические партии, гражданское общество и т. д.). По нашему мнению, к субъектам политического процесса можно отнести информационную составляющую с учетом значимости информации для органов власти.

Характеристика регионального аспекта позволяет отметить, что 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.

Такой подход к региональным политическим процессам позволяет лучше и точнее выявлять группы влияния, действующие в субъектах Российской Федерации. В XXI в. стало значительно проявляться влияние деструктивных факторов на различные сферы общества. Началась дезинтеграция политических структур и традиционных систем, которые в предшествующие этапы развития государства которые стали обладать более или менее стабильным характером. Устойчивостью стал ха-

рактеризоваться и политический процесс. На данные оценки обращал внимание отечественный исследователь А. С. Панарин и исследователи философии постмодернизма. Будучи общественным явлением, 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. Благодаря этим сигналам 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.

Автором дана характеристика информационной безопасности политического процесса. В современный период текущие и стратегические задачи внешней и внутренней политики государства по обеспечению информационной безопасности основываются на «Стратегии национальной безопасности РФ до 2020 г.» (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. Для «обеспечения информационной безопасности Российской Федерации нужно преодолеть технологическое отставание в важнейших областях информатизации, телекоммуникаций и связи, определяющих 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 условия для гармонизации национальной информационной инфраструктуры»[24].

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. Главная цель зарубежного информационного воздействия в современный период – культивирование эгоцентризма, навязывание западных стандартов и дезинформация населения. Условием эффективного функционирования пространства является наличие устойчивой обратной связи в информационных каналах, позволяющей учитывать мнение населения при определении приоритетов экономического, политического и духовно-нравственного развития общества.

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

В параграфе 1.2 «**Теоретико-методологический анализ системы управления информационной безопасностью: организационно-правовые характеристики**» анализируется организационно-правовое обеспечение информационной безопасности как совокупность законов, управленческих решений, нормативов, регламентирующих как общую деятельность по обеспечению информационной безопасности, так и создание, функционирование специализированных систем информационной защиты. Основополагающими функциями организационно-правового обеспечения информационной безопасности являются:

1) формирование основных принципов и методов отнесения сведений конфиденциального характера к защищаемой информации;

2) регламентирование системы органов и должностных лиц, несущих ответственность за обеспечение информационной безопасности;

3) создание комплекса различных видов документов, регламентирующих систему обеспечения информационной безопасности.[25]

Как отмечал С.Г. Аксенов: «Основными принципами формирования организационно-правового обеспечения защиты информации являются:

1) обязательность соблюдения норм и правил защиты информации всеми лицами, имеющими отношение к защищаемой и конфиденциальной информации;

2) нормативное правовое закрепление всех мер ответственности за нарушение порядка и правил защиты информации;

3) придание юридической силы всем решениям в области организационно-правового обеспечения защиты информации»[26].

Очевидно, что законодательные основы любого государства в области информационной безопасности являются необходимой мерой, удовлетворяющей первейшую потребность в защите информации при развитии социально-экономических, политических, военных направлений функционирования этого государства. Особое внимание со стороны западных стран к формированию и развитию такой основы вызвано всевозрастающими затратами на борьбу с преступностью в информационной сфере. Все это заставляет страны Запада серьезно заниматься вопросами законодательства в области информационной безопасности и защиты информации. Так, в США первый Закон в этой области был принят еще в 1906 г., а к настоящему времени уже имеется более 500 законодательных актов по защите информации, ответственности за ее разглашение и компьютерные преступления.

Важной характеристикой информационной безопасности является государственная тайна. Государственная тайна − это основной элемент системы информационной безопасности в деятельности органов власти. Главным источником в сфере информационной безопасности, составляющим государственную тайну, является Закон РФ «О государственной тайне», в котором понятие «государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации»[27]. Теоретический анализ организационно-правовых характери-

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

[26] Там же.

[27] 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/.

стик информационной безопасности предполагает оценку функций, приемов, ресурсов, методов обеспечения информационной безопасности. Специфической является информационная безопасность в органах государственной власти и муниципального управления. Для предотвращения утечки информации в данных органах формируется целый комплекс мероприятий, в том числе регулирование на предмет государственной тайны и конфиденциальной информации.

В параграфе 1.3 **«Информационная интеграция и инновация как этап развития государственного и муниципального управления России»** дана оценка и перспектива одного из стратегических направлений, обозначенных Президентом РФ В. В. Путиным в качестве целевого вектора на будущее – это создание информационного высокотехнологичного общества страны. Достижению этой установки призвана служить федеральная целевая программа – «Информационное общество», которая охватывает все сферы жизнедеятельности России. Для реализации данной задачи создан Совет при Президенте РФ по развитию информационного общества (2008). Первые же заседания Совета касались реализация программы «Электронного правительства» (2009).

23 октября 2019г. в инновационном центре «Сколково» завершился VIII международный Форум «Открытые инновации», который посетили более 20 000 человек. География участников Форума включала 102 страны, в том числе Германию, Корею, США, Японию, Францию, Великобританию, Австралию, Тунис. На площадках Форума состоялось свыше 150 деловых сессий, где было подписано 29 соглашений между российскими и международными компаниями, фондами и институтами развития. «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.

Главной 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).

Цели системы «ЭМ»:

1. Унификация информации, обрабатываемой ОМСУ.
2. Сокращение количества обработки данных хозяйственного и других видов учета, выписок для населения и других видов отчетов администрацией ОМСУ.
3. Сокращение времени получения государственных и муниципальных услуг.

В настоящее время существует неоднозначность в восприятии концепции «электронного правительства», как правило, идет ассоциация только с государственными учреждениями, хотя, «электронное правительство» включает в себя и ОМСУ. 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.

Во второй главе «Информационная безопасность в деятельности органов государственного и муниципального управления России» автор исследовал информационные угрозы, открытость органов государственной и муниципальной власти и основные направления обеспечения информационной безопасности.

В параграфе 2.1 **«Оценка информационных угроз органов государственного и муниципального управления»** проанализированы информационные угрозы и факторы риска, изложенные в «Доктрине информационной безопасности» и проявляющиеся в практике государственного и муниципального управления. Очевидно, что растет угроза внедрения террористами вредоносных программ на объекты инфраструктуры РФ с целью провоцирования масштабных аварий. Возможность при 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 противодействовать информационным угрозам для безопасного и достоверного доступа граждан ко всей информации, необходимой для государственных и муниципальных органов власти.

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 выражается в местном самоуправлении, так как их деятельность напрямую связана со всеми сферами жизнедеятельности человека и накоплением оперативной информации. Е.А. Горшков подчеркивает значимость информации: «Активный рост процессов информатизации общества, предоставление государственных и муниципальных услуг в электронном виде и развитие систем электронного документооборота способствуют возрастанию зависимости органов муниципалитета от используемой ими информации, качества, достоверности, своевременности ее получения»[28].

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

В нашем исследовании мы определили факторы риска, которые по источникам угроз информационной безопасности принято разделять на внутренние и внешние. Нами проанализированы все виды угроз и показаны риски их реализации в органах власти. Специфика органов местного самоуправления дает возможность учи-

[28] 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.

тывать внутренние источники, а внешние сложно распределить, в связи с тем, что муниципальные информационные ресурсы тесно связаны с ресурсами страны.

В параграфе 2.2 **«Информационная открытость и основные направления политического процесса по реализации информационной безопасности»** рассматривается информационная открытость государственного и муниципального управления России. В XXI в. демократическими называются те государства, которые обеспечивают как нормативно, так фактически на своей территории режим «открытого правления». Под «открытым правлением» понимается 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[29], И.М. Дзялошинский, А.С. Довлатов[30], А.В. Иванченко, М.В. Черноусов[31] и другие. Характеристика открытости муниципалитетов характеризуется чаше постановкой проблемы, чем ее решением.

Анализу установления гражданского общества в России как необходимого фактора развития открытого государственного управления посвящены работы Э.Я. Баталова, Ю.В. Ирхина[32], Д. Кина, В.В. Лапкина[33], В.Н. Якимца[34]. Данные работы уделяют внимание политической трансформации гражданского общества и органов государственной и муниципальной власти при переходе от одного политического режима к другому. Так же рассматривается возможность и перспективы внедрения новейших информационных технологий и сети интернет в политической сфере для обеспечения открытости государственной и муниципальной власти[35].

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»[36]. Таким образом, обеспечение непрерывной коммуникации в социально-политической системе является стержнем ее функционирования. Муниципальное управление также представ-

---

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

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

[31] 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.

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

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

[34] 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.

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

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

ляет особую систему, 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»[37].

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. 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. С принятием федерального закона «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»[38], возник институт свободы доступа к официальной информации, который направлен на борьбу с коррупцией. Эффективность работы института была апробирована 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.

Диссертант рассматривает основные варианты развития систем по обеспечению информационной безопасности в основном на примере муниципалитета. Стабильное функционирование региональных социально-политических комплексов управления зависит от состояния информационной безопасности (далее ИБ) муниципалитета, под которой 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. Решение поставленных задач невозможно без участия в системе обеспечения ИБ РФ ее муниципальных образований[39].

К основным направлениям деятельности по обеспечению ИБ муниципалитета, сформулированным на основе анализа содержания Доктрины информационной безопасности Российской Федерации относятся: формирование, и рациональное управление муниципальными информационными ресурсами; выявление угроз ИБ и их источников; защита информационных прав личности, общества от негативных информационных воздействий.

Указанные направления реализуются конкретными видами деятельности, выполняемыми ОМСУ, предприятиями, учреждениями в соответствии с их компетенцией. Слаженность деятельности по обеспечению ИБ и сложности возникающих

[37] Демин, В., Пак, Т. Организация работы пресс-служб – международные стандарты. −Алматы, 2005.
[38] ФЗ 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/.
[39] Шелупанов, А.А., Зайцев, А.П., Мещеряков, Р.В. Основы защиты информации. Изд. 5-е, перераб. И доп. – Томск: В-Спектр, 2011. – 244с.

проблем, требуют скоординированных действий в этой сфере. К основным координируемым проблемам на муниципальном уровне относятся:

1. Прогнозирование угроз ИБ, их реализации. Создание моделей угроз применительно к направлениям обеспечения ИБ.

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

3. Реализация единой политики в области систематизации, учета и обеспечения доступа к информационным ресурсам муниципалитета.

4. Совершенствование информационно-телекоммуникационных средств и систем в муниципалитете.

Каждая из проблем требует специфических подходов и методов решения. Общая координация решения данных проблем может осуществляться созданным специализированным советом, а решение конкретных организационно-технических вопросов целесообразно возложить на компетентные учреждения муниципалитета или региона по каждой из проблем. Для этого могут быть созданы соответствующие координационные советы. Рассмотрены варианты развития муниципальной системы защиты информации.

В третьей главе «Информационная безопасность политического процесса на примере муниципалитетов Забайкальского края» автор исследовал состояние информационной безопасности на примере муниципальных образований Забайкальского края.

В параграфе 3.1 **«Информационная открытость муниципальных районов Забайкальского края в контексте анализа их информационной освещённости»** диссертант провел контент–анализ средств массовой информации Забайкальского региона. 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 территорий, а также данные о существовании и функционировании административно–хозяйственных единиц. Для нашего исследования мы взяли «Чернышевский», «Красночикойский», «Могочинский» и «Тунгиро-Олёкминский» районы Забайкалья. 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.

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. 2017г. – 30. 04. 2018 г.

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. 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.

В проведенном 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.

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

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 является информация, имеющая также экономический эффект. 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 муници-

пальных 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.

В параграфе 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. Были опрошены 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.

По вопросу: «Удовлетворены ли вы уровнем состояния ваших технических средств?», ориентированному на выявление обеспеченности муниципального служащего техническими средствами и их состояния для выполнения своих полномочий, служащие ответили «в основном полностью или частично обеспечены ресурсами для выполнения своих полномочий и их состояние отличное или хорошее». Это нормальные показатели для дотационного региона, но есть процент служащих, которые не обеспечены техническими возможностями или их средства устарели.

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. Одним из важных условий поддержания безопасности – является наличие системного администратора, который следит за состоянием систем и их безопасностью. Как показывает исследование в большинстве случаев в муниципальных органах имеется системный администратор. Но качество его работы – невысокое.

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%). Очевидно, что это связано с политической стабильностью в стране и выборами президента в 2018г. Что касается рейтинга важности для государства видов безопасности, по мнению респондентов, то тут ответы распределились почти равномерно: экономическая безопасность – 31%, информационная безопасность – 23%, политическая безопасность – 25%, социальная безопасность – 21%. Таким образом, муниципалы считают, что экономическая стабильность в стране – залог прогресса в государстве.

Среди угроз информационной безопасности на муниципальном уровне стали актуальными различные вирусы, данная угроза сопровождает информационные системы с момента их создания, но тревожный момент актуализации угроз на местном уровне − хакерский взлом, так как эта угроза – один из элементов киберпреступности и встречается чаще всего на федеральном уровне. В связи с тем, что риски в социальных сетях растут, а большинство членов общества находится в виртуальной реальности, то социальные сети – одно из направлений развития информационной безопасности для защиты конфиденциальных данных, прав и свобод человека и национальных интересов страны.

Диссертант дает обоснование, что для выполнения поставленных целей и управленческих задач, необходимо провести мероприятия по совершенствованию информационной безопасности, которые включают в себя административный и организационный уровни защиты информации. Что касается организационного уровня, то существуют мероприятия, помогающие улучшить защиту информации:

– проведение работ по обучению и повышению профессиональных знаний специалистов по работе с современными программными продуктами;

– совершенствование систем информационной безопасности;

– организация инструктажа каждого специалиста для осознания всей важности и конфиденциальности информации, с которой он работает. Нередко разглашению конфиденциальной информации специалистом предшествует недостаточное знание правил защиты информации.

Кроме того, ключевым моментом является технический путь совершенствования безопасности, а программные средства – это основные элементы в реализации защиты информации. Например, установка на компьютер-сервер сетевого экрана Agnitum Outpost FireWall блокирует несекционный доступ из сети Интернет, а введение «Сканер-ВС» предназначено для контроля защищенности сетей от угроз.

Эффективность системы информационной безопасности и действий системного администратора будет низкой при отсутствии методов анализа, хранения и сбора информации о состоянии защиты информации, централизованного управления всеми субъектами безопасности. Дело в том, что каждое средство защиты является составляющей всей системы политики безопасности, которая на уровне подсистем задается набором параметров и требований. Аудит работоспособности системы, всех правил и других элементов в системе информационной безопасности муниципалитетов требует наличия средств мониторинга и управления. Для планового анализа данных и принятия управленческих решений необходимы рычаги мониторинга. Для каждого муниципалитета должна быть индивидуально создана политика информационной безопасности с учетом рекомендаций по сотрудничеству как государственных, так и муниципальных властей.

В заключении обобщены результаты исследования, сформулированы основные выводы и намечены перспективы дальнейшего изучения проблемы.

3. СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ АВТОРОМ ПО ТЕМЕ ДИССЕРТАЦИИ:

Статьи в рецензируемых научных журналах, рекомендуемых ВАК:

1. ***Кухарский, А.Н.,*** Бейдин, С.В. Антикризисное управление в социально-экономической сфере с учетом антироссийских санкций // Вестник Забайкальского государственного университета. Чита. 2016.– Т. 22. – № 10. – С.55-60 (0,4 п.л. / 0,3 п.л.).

2. ***Кухарский, А.Н.*** Информационная безопасность в аспекте защищенного электронного документооборота в информационных системах муниципальных образований // Вестник Забайкальского государственного университета. Чита. 2017.– Т. 23. – № 7. – С. 86-90 (0,3 п.л.).

3. ***Кухарский, А.Н.,*** Бейдина, Т.Е., Попов, Ю.А. Мягкая и твердая сила как стратегия развития США в различных регионах мира // Вестник Забайкальского государственного университета. Чита. 2018. – Т. 24. – № 7. – С. 61-67 (0,4 п.л / 0,1 п.л.).

4. ***Кухарский, А.Н.,*** Зимина, Н.В., Новикова, А.В. Усовершенствование систем местного самоуправления в рамках организационно-кадрового обеспечения муниципального управления // Вестник Забайкальского государственного университета. Чита. 2018. – Т. 24. – № 3. – С. 83-92 (0,6 п.л. / 0,4п.л.).

5. ***Кухарский, А.Н.*** Пути совершенствования информационно-коммуникационных технологий России и регионов // Вестник Забайкальского государственного университета. Чита. 2018. – Т. 24. – № 1. – С. 59-64 (0,4 п.л.).

6. ***Кухарский, А.Н.,*** Бейдина, Т.Е., Попов, Ю.А., Денисов, Ю.В. Снижение влияния ведущих партий США в избирательном политическом процессе: динамика изменений // Политика и общество. М.: 2018. – № 4 (161). – С. 39-52 (0,9 п.л / 0,4 п.л.).

7. ***Кухарский, А.Н.,*** Бейдина, Т.Е., Бейдин, С.В., Новикова, А.В. Местное самоуправление в Российской Федерации: организационно-правовые и кадровые проблемы // Вестник Забайкальского государственного университета. Чита. 2019. – Т. 25. – № 1. – С. 37-45 (0,6 п.л. / 0,2 п.л.).

Статьи в сборниках научных трудов, материалах конференций и других изданиях:

8. ***Кухарский, А.Н.*** Информатизация муниципального управления на примере Могочинского района // Материалы 15 международной научной студенческой конференции «Студент и научно-технический прогресс», 12-18 апреля 2013 г.: Управление / отв. и науч. ред. И.В. Князева; РАНХиГС, Сиб. ин-т упр. – Новосибирск: Изд-во СибАГС, 2013. – 339 с. (0,1 п.л.).

9. ***Кухарский, А.Н.,*** Бейдина, Т.Е. Информационное обеспечение региональных и муниципальных органов власти в интересах информационной безопасности // В сборнике: Местное самоуправление на современном этапе: теория и практика IV международная научно-практическая конференция: сб. ст. отв. ред. Т. О. Третьякова. Чита. 2015. – С. 77-82 (0,4 п.л. / 0,3 п.л.).

10. ***Кухарский, А.Н.,*** Новикова, А.В. Кадровое обеспечение как направление инновационного развития муниципальных образований // В сборнике: Муниципальное управление в Российской Федерации: реалии и инновации Материалы III всероссийской научно-практической конференции: сборник статей. Под редакцией Т. И. Сапожниковой. Чита. 2015. – С. 76-81 (0,4 п.л. / 0,2 п.л.).

11. ***Кухарский, А.Н.,*** Погулич, О.В. Совершенствование организационно-правовой основы и антикоррупционного управления в сельских поселениях // В сборнике: Муниципальное управление в Российской Федерации: реалии и инновации Материалы III всероссийской научно-практической конференции: сборник статей. под редакцией Т. И. Сапожниковой. Чита. 2015. – С. 70-76 (0,4 п.л. / 0,3 п.л.).

12. ***Кухарский, А.Н.,*** Бейдин, С.В. Организация избирательного процесса на муниципальных выборах на примере муниципального района «Улетовский район» // В сборнике: Муниципальное управление в Российской Федерации: реалии и инновации Материалы III всероссийской научно-практической конференции: сборник статей. под редакцией Т. И. Сапожниковой. Чита. 2015. – С. 65-70 (0,4 п.л. / 0,3 п.л.).

13. ***Кухарский, А.Н.,*** Бейдин, С.В. Направления обеспечения информационной безопасности в ракурсе деятельности органов федеральной инспекции труда по Забайкальскому краю // В сборнике: Местное самоуправление на современном этапе: теория и практика IV Международная научно-

практическая конференция: сб. ст. отв. ред. Т. О. Третьякова. Чита. 2015. – С. 19-23 (0,3 п.л. / 0,2 п.л.).

14. ***Кухарский, А.Н.,*** Бейдина, Т.Е., Новикова, А.В. Тенденции региональных политических процессов в Сибирском федеральном округе // В сборнике: Десятые Байкальские социально-гуманитарные чтения Материалы: в 2 томах. Иркутск. 2017. – С. 19-23 (0,3 п.л / 0,1 п.л.).

15. ***Кухарский, А.Н.*** Обеспечение информационной безопасности в органах муниципальных образований Забайкальского края // В сборнике: Инновационное развитие муниципальных образований Материалы V международной научно-практической конференции. Ответственный редактор К.И. Галынис. Чита. 2017. – С. 75-79 (0,3 п.л.).

16. ***Кухарский, А.Н.*** Информационная безопасность муниципалитетов Забайкальского края // Результаты научных исследований, выполненных в ходе подготовки выпускных квалификационных работ: материалы студенческой научно-практической конференции / Частное образовательное учреждение высшего образования Центросоюза Российской Федерации Сибирский университет потребительской кооперации Забайкальский институт предпринимательства. – Чита: ЗИП СибУПК, 2017. – 151с. (0,5 п.л.).

17. ***Кухарский, А.Н.*** Информационная безопасность муниципалитетов Забайкальского края и пути ее совершенствования // Постулат. 2017. – № 2 (16). г. Биробиджан. – С. 11 (0,5 п.л.).

18. ***Кухарский, А.Н.,*** Бейдина, Т.Е. Основные аспекты обеспечения информационной безопасности муниципалитетов России // Международная научно-практическая конференция: Современные проблемы развития экономики России и Китая. 20-21 ноября 2017. Благовещенск (0,4 п.л. / 0,2п.л.).

19. ***Кухарский, А.Н.,*** Бейдина, А.Р. Российский и зарубежный опыт устойчивого развития как фактор экологизации // Защита окружающей среды как фактор социально-экономического развития территорий муниципальных образований: опыт и проблемы: Материалы всероссийской научно-практической конференции с международным участием 14-15 апреля 2017г., Ростов-на-Дону. Ред.-изд. гр.: А.Ю. Шутов (руков.), О.В. Локота, А.В. Понеделков, А.В. Буров и др. Ростов-на-Дону: ЮРИУ РАНХиГС, 2017. – 928 с. (0,6п.л. / 0,3 п.л.).

20. ***Кухарский, А.Н.,*** Бейдина, Т.Е., Денисов, Ю.В., Попов, Ю.А. Евразийцы, современные политические изменения и политические процессы // Евразийство: теоретический потенциал и практические приложения. Барнаул. 2018. – № 9. – С. 209-214 (0,4 п.л. / 0,1 п.л.).

21. ***Кухарский, А.Н.,*** Бейдина, Т.Е., Денисов, Ю.В. Перспективы развития непосредственной демократии с учетом современных информационных технологий // Наука Красноярья. Красноярск. 2018. – Т. 7. – № 1. – С. 7-21 (1 п.л. / 0,4 п.л.).

22. ***Кухарский, А.Н.,*** Бейдина, Т.Е., Новикова, А.В. Реформа местного самоуправления и политика делегирования полномочий муниципальным образованиям Российской Федерации: теория и практика // Наука Красноярья. Красноярск. 2018. – Т. 7. – № 1. – С. 22-37 (1 п.л. / 0,4 п.л.).

23. ***Кухарский, А.Н.,*** Новикова, А.В. Информационные аспекты взаимодействия общества и власти: практика государственных и муниципальных органов // В сборнике: Развитие политических институтов и процессов: зарубежный и отечественный опыт Материалы IX всероссийской научно-практической конференции. Ответственный редактор И.А. Ветренко. Омск. 2018. – С. 77-80 (0,2 п.л. / 0,1 п.л.).

24. ***Кухарский, А.Н.,*** Бейдина, Т.Е. Основные аспекты обеспечения информационной безопасности деятельности муниципалитетов России // В сборнике: Современные проблемы развития экономики России и Китая Материалы международной научно-практической конференции. Под общ. ред. О.А. Цепелева. Благовещенск. 2018. – С. 105-107 (0,2 п.л. / 0,1 п.л.).

25. ***Кухарский, А.Н.,*** Бейдина, Т.Е., Новикова, А.В. Проблемы развития местного самоуправления в Забайкальском крае // Российский политический процесс в региональном измерении: история, теория, практика: сборник материалов всероссийской научно-практической конференции / под ред. Я.Ю. Шашковой, Н.П. Коробковой, Т.А. Асеевой. – Барнаул: Изд-во Алт. гос. ун-та, 2018. – С. 17-20 (0,2 п.л. / 0,1 п.л.).

26. ***Кухарский, А.Н.*** Информационно-коммуникационные технологии как индекс развития России и регионов // Материалы XIV международной научно-практической конференции: Фундаментальные и прикладные науки сегодня. 20-21 февраля 2018г. – Т3 North Charleston, USA. – С.53-55 (0,1 п.л.).

27. ***Кухарский, А.Н.,*** Бейдина, Т.Е., Денисов, Ю.В., Попов, Ю.А. Перспективы развития частного военного бизнеса на мировой и политической арене // Вестник Центра стратегических исследований при Президенте Республики Таджикистан «Таджикистан и современный мир». – №2 (61). Душанбе. 2018. – С.29-39 (0,7 п.л. / 0,3 п.л.).

28. ***Кухарский, А.Н.,*** Бейдина, Т.Е., Денисов, Ю.В. Демократия в информационную эпоху с использованием телекоммуникационных технологий // Russian studies in law and politics. Красноярск, 2018. – Т.2. №1. – С. 4-14 (0,7 п.л. / 0,4 п.л.).

29. ***Кухарский, А.Н.*** Информационные технологии в системе управления // Политика развития, государство и мировой порядок. Материалы VIII всероссийского конгресса политологов. Под общ. ред. О.В. Гаман-Голутвиной, Л.В. Сморгунова, Л.Н. Тимофеевой. М.: 2018. – С. 297 (0,1 п.л.).

30. ***Кухарский, А.Н.,*** Бейдина, Т.Е., Новикова, А.В. Проблемы формирования имиджа губернатора и политического лидера Забайкальского края // В сборнике: Российская элитология: инновационные ответы на вызовы современного мира Материалы Третьего всероссийского элитологического конгресса с международным участием. Ростов-на-Дону. 2019. – С. 245-253 (0,6 п.л / 0,4 п.л.).

31. ***Кухарский, А.Н.,*** Бейдина Т.Е., Новикова А.В., Погулич О.В. Развитие современных политических процессов в целях обеспечения управления коммуникациями и информационной безопасностью // Развитие политических институтов и процессов: зарубежный и отечественный опыт [Электронный ресурс]: материалы X всероссийской научно-практической конференции (Омск, 26 апреля 2019 г.) / [редкол.: Д.И. Попов (отв. ред.), И.А. Ветренко (отв. ред.) и др.]. Электрон. текст. дан. Омск: Изд-во Ом. гос. ун-та, 2019 (0,4 п.с / 0,1 п.л.).

Подписано в печать
Формат 60х90/16. Бумага офсетная. Способ печати цифровой.
Усл. печ. л. 1,5. Уч.-изд. л. 1,5. Заказ № _____. Тираж 100 экз.
ФГБОУ ВО «Забайкальский государственный университет»
672039, г. Чита, ул. Александро-Заводская, 30