Кучерявый М. М., Косов Ю. В., Вовенда Ю. В.

Деятельность органов государственной власти Северо-Западного федерального округа по обеспечению безопасности информации

DOI 10.22394/1726-1139-2017-10-8-14

Кучерявый Михаил Михайлович
Администрация Ленинградской области (Санкт-Петербург)
Вице-губернатор Ленинградской области — руководитель аппарата Губернатора и Правительства Ленинградской области
Доктор политических наук, доцент
priemnaya@lenreg.ru

Косов Юрий Васильевич
Северо-Западный институт управления — филиал РАНХиГС (Санкт-Петербург)
Заместитель директора
Доктор философских наук, профессор
kosov-yuv@sziu.ranepa.ru

Вовенда Юлия Владимировна
Северо-Западный институт управления — филиал РАНХиГС (Санкт-Петербург)
Аспирант кафедры государственного и муниципального управления
Администрация Ленинградской области (Санкт-Петербург)
Помощник Вице-губернатора Ленинградской области — руководителя аппарата Губернатора и Правительства Ленинградской области
vovenda-yv@sziu.ru

РЕФЕРАТ
В статье рассматривается деятельность органов государственной власти Северо-Западного федерального округа по обеспечению безопасности информации. Освещаются вопросы формирования и функционирования системы защиты информации в Северо-Западном федеральном округе. Особое внимание уделено государственным информационным системам, процессам регулирования и контроля обеспечения безопасности информации Управлением ФСТЭК по СЗФО.

КЛЮЧЕВЫЕ СЛОВА
органы государственной власти, обеспечение информации, система защиты информации, государственные информационные системы, техническая защита информации

Kucheryavyy M. M., Kosov Yu. V., Vovenda Yu. V.

The Activities of Public Authorities of the North-West Federal District to Ensure Information Security

Kucheryavyy Mikhail Mikhailovich
Administration of the Leningrad Region (Saint-Petersburg)
Vice-governor of the Leningrad Region — Chief of Staff of the Governor and the Government of the Leningrad Region
Doctor of Science (Political Sciences), Associate Professor
priemnaya@lenreg.ru

Kosov Yury Vasilyevich
North-West Institute of Management, Branch of RANEPA (Saint-Petersburg, Russian Federation)
Deputy Director
Doctor of Science (Philosophy), Professor
kosov-yuv@sziu.ranepa.ru

Vovenda Yulia Vladimirovna
North-West Institute of Management — branch of RANEPA (Saint-Petersburg, Russian Federation)
Postgraduate student of the Chair of the State and Municipal Management
Administration of the Leningrad Region (Saint-Petersburg)
The assistant to the Vice-governor of the Leningrad Region — Chief of Staff of the Governor and the Government of the Leningrad Region
vovenda-yv@sziu.ru

ABSTRACT
The article is considered the activities of public authorities of the North-West Federal District to ensure information security. Highlights the issues of formation and functioning of the information security system in the North-West Federal District. The main attention is paid to the state information systems, control and monitoring of security information by the FSTEC Office for the North-West Federal District.

KEYWORDS
public authorities, providing information, information security system, state information systems, technical protection of information

Ключевой тенденцией развития современного общества является всеохватывающее влияние информации на все сферы общественной жизни. Обеспечение информационной безопасности сегодня играет важнейшую роль в устойчивости системы государственного управления.

На заседании Совета Безопасности 26 октября 2017 г. Президент Российской Федерации В. В. Путин отметил, что «устойчивая работа информационных систем, средств коммуникации и связи, их защищенность имеют для страны стратегическое значение. Это важный фактор обеспечения суверенитета, обороноспособности, безопасности государства, эффективного развития экономики, социальной сферы, государственного управления на базе передовых, в том числе цифровых, технологий»[1].

В данных условиях на первый план выдвигаются вопросы реализации государственной политики в области защиты суверенитета, территориальной целостности и конституционного строя Российской Федерации с учетом существующих и возможных угроз национальной безопасности.

Геополитическая ситуация, сложившаяся в начале XXI в., потребовала переосмысления содержания понятия «национальная безопасность» и смены приоритетов в сфере обеспечения национальной безопасности.

В стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации 31 декабря 2015 г.[2], дано определение понятию «национальная безопасность», как «состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации».

Необходимо отметить, что в сегодняшнем глобальном мире одним из основных приоритетов обеспечения национальной безопасности Российской Федерации является информационная сфера.

[1] О защите информационной инфраструктуры государства и мерах по ее развитию // Совет Безопасности Российской Федерации [Электронный ресурс]. URL: http://www.scrf.gov.ru/council/session/2301/ (дата обращения: 27.10.2017).

[2] Стратегия национальной безопасности Российской Федерации // КонсультантПлюс [Электронный ресурс]. URL:http://www.consultant.ru/document/cons_doc_LAW_191669/61a97f7ab0f2f3757fe034d11011c763bc2e593f/ (дата обращения: 19.07.2017)

В Доктрине информационной безопасности дано определение понятию информационная безопасность Российской Федерации, как «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»[1].

Сегодняшний мир, в котором мы живем, — это мир, который характеризуется глобальным развитием, усовершенствованием информационно-коммуникационных технологий и сложившаяся к настоящему времени новая политическая реальность, характеризующаяся трансформацией разрозненных и суверенных информационных систем в единое глобальное пространство [3].

Надежная работа информационных ресурсов, систем управления и связи имеет исключительное значение для обороноспособности страны, для устойчивого развития экономики и социальной сферы, для защиты суверенитета России.

Доктриной информационной безопасности Российской Федерации[2] предусматривается повышение эффективности функционирования системы государственного управления, обеспечение информационного взаимодействия между органами власти при решении задач в области обороны и безопасности.

Определяя в качестве приоритетов построение в Российской Федерации информационного общества, государственная политика нацелена на усиление внимания к защите государственных информационных ресурсов.

Существующие современные угрозы в информационной сфере направлены в первую очередь против действующих органов государственной власти и управления всех регионов Российской Федерации.

В Северо-Западном федеральном округе проживает около четырнадцати миллионов человек. В состав округа входит одиннадцать субъектов Российской Федерации, более трех тысяч органов государственной власти субъектов Российской Федерации и около полутора тысяч органов местного самоуправления.

В государственных и муниципальных информационных системах органов власти субъектов Российской Федерации обрабатываются значительные массивы информации ограниченного доступа.

Зарегистрированных государственных информационных систем в округе около четырехсот, муниципальных более пятисот. В более чем 4500 информационных систем персональных данных обрабатывается информация о населении округа. Такие данные очень привлекательны для технических разведок иностранных государств.

Северо-Западный федеральный округ непосредственно граничит со странами блока НАТО — Норвегией, Эстонией, Латвией, Литвой и Польшей, где размещены современные технические средства ведения разведки и управления. На территории округа расположены стратегические командования Минобороны России, органы военного управления, крупнейшие объединения вооруженных сил Российской Федерации, а также стратегически важные полигоны и испытательные площадки.

Большая часть объектов защиты, находящихся в пределах округа, доступны для средств космической, морской, наземной и воздушной разведок. Возможности разведок позволяют:

- непрерывно контролировать каналы сотовой связи;

[1] Доктрина информационной безопасности Российской Федерации. Новая редакция. [Электронный ресурс]. URL: http://infosystems.ru/assets/files/files/doktrina_IB.pdf (дата обращения: 31.10.2017).

[2] Доктрина информационной безопасности Российской Федерации. Новая редакция [Электронный ресурс]. URL: http://infosystems.ru/assets/files/files/doktrina_IB.pdf (дата обращения: 03.07.2017).

- осуществлять перехват интернет-трафика;
- осуществлять мониторинг органов государственного управления, военных объектов и объектов оборонно-промышленного комплекса.

При этом официально, в соответствии с «Договором по открытому небу»[1], осуществляется детальная фотосъемка объектов по маршруту полета.

Также легально, в рамках международных научно-исследовательских программ, ведется разведка с использованием иностранных технических средств наблюдения и контроля, которые позволяют получать сведения об экономическом и военном потенциалах Северо-Западного региона. Такие средства размещены в Республике Коми, Мурманской и Ленинградской областях, в Санкт-Петербурге.

В границах административных центров субъектов Российской Федерации — Санкт-Петербурга, Петрозаводска, Мурманска, Пскова — размещены более пятидесяти генеральных консульств и представительств иностранных государств. Из них тридцать два представляют интересы стран блока НАТО. Из зданий консульских учреждений ведется техническая разведка деятельности органов власти и предприятий оборонно-промышленного комплекса различными средствами.

Часть территории Республики Карелия, Мурманской, Псковской и Ленинградской областей и вся Калининградская область доступны для наземных систем разведки с территории приграничных государств, что представляет угрозу безопасности информации в каналах связи и государственных информационных системах.

Технические средства более двадцати стран НАТО объединены в систему глобального контроля международных линий связи «Эшелон» [1, с. 165]. Часть пунктов сбора и обработки информации стран-участниц размещены вдоль внешней границы Северо-Западного федерального округа. Средствами системы «Эшелон» перехватывается и анализируется информация, передаваемая по линиям связи, а также с международных и национальных спутниковых систем. Возможности этой системы позволяют анализировать десятки миллионов сообщений в минуту.

Наибольшую угрозу для государственных информационных систем Северо-Западного федерального округа представляет техническая компьютерная разведка, реализованная в системе электронного наблюдения PRISM, созданной Агентством национальной безопасности США для сбора информации с крупнейших интернет-сервисов, включая электронную почту, поисковые запросы, разговоры в Skype, мобильные приложения, транзакции в системах Visa и MasterCard [2, с. 160].

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» защита информации «представляет собой принятие правовых, организационных и технических мер, направленных на: обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации»[2].

---

[1] Договор по открытому небу // Организация по безопасности и сотрудничеству в Европе [Электронный ресурс]. URL: http://www.osce.org/ru/library/14131 (дата обращения: 07.08.2017).

[2] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.07.2017) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.11.2017) // КонсультантПлюс [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_61798/0e9ec16b786dcbdaaa7f44abfc4a15e601d5be22/ (дата обращения: 31.09.2017).

Для обеспечения своевременной и адекватной реакции на возникающие и прогнозируемые угрозы утечки информации ограниченного доступа в округе сформирована и функционирует система защиты информации, которая охватывает все уровни и ветви органов власти Северо-Западного федерального округа.

Общее руководство деятельностью по защите информации в округе осуществляют полномочный представитель Президента Российской Федерации и Межведомственный совет по защите информации.

В субъектах Российской Федерации — главы высших органов исполнительной власти субъектов Российской Федерации и комиссии по защите информации. В органах власти и организациях ответственность за обеспечение защиты информации возлагается на их руководителей.

Управление Федеральной службы по техническому и экспортному контролю (ФСТЭК) по Северо-Западному федеральному округу осуществляет координацию деятельности по защите информации в пределах федерального округа, организует функционирование сформированной системы защиты информации.

Управление Федеральной службы по техническому и экспортному контролю по Северо-Западному федеральному округу осуществляет реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

- обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в том числе в функционирующих в составе критически важных объектов Российской Федерации информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям;
- противодействия иностранным техническим разведкам на территории Российской Федерации;
- обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носителей информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации;
- защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;
- осуществления экспортного контроля[1].

Итоги контроля органов государственной власти Северо-Западного федерального округа показали, что не везде в полной мере выполняются рекомендации нормативных и методических документов ФСТЭК России, что приводит к серьезным нарушениям безопасности информации и к возможной вероятности раскрытия сведений, составляющих государственную тайну.

Характерными нарушениями, которые можно классифицировать как типовые, для всех проверенных органов власти являются следующие:

- недостаточное руководство системой информационной безопасности в регионах уполномоченными должностными лицами;
- назначение специалистов, не имеющих профильного высшего образования и не прошедших переподготовку и повышение квалификации;

[1] Сведения о полномочиях ФСТЭК России; перечень нормативных правовых актов, определяющих эти полномочия // ФСТЭК России [Электронный ресурс]. URL: http://fstec.ru/obshchaya-informatsiya/polnomochiya (дата обращения: 07.08.2017).

- недостаточное финансирование для приобретения лицензионного и сертифицированного информационно-коммуникационного оборудования;
- назначение на должности специалистов по защите информации без соответствующего согласования с Управлением ФСТЭК России по Северо-Западному федеральному округу.

Сравнительная оценка результатов контроля свидетельствует об увеличении в три раза общего количества нарушений в области технической защиты информации.

В пять раз увеличилось число нарушений в общей организации работ, что говорит об ослаблении контроля со стороны руководства регионов, организаций и учреждений.

Не принимаются меры по устранению нарушений и недостатков, которые выявлялись в ходе предыдущих проверок.

Наибольшее количество нарушений связано с низкой организацией работ и недостаточной профессиональной подготовкой специалистов.

Система органов государственной власти и управления в Северо-Западном федеральном округе является центральным звеном обеспечения информационного противоборства в регионе.

Важное значение имеет обеспечение защиты информации в государственных информационных системах (ГИС).

В информационных системах органов власти циркулирует информация, имеющая значение для деятельности государства и региона, в том числе в социальной сфере, здравоохранении и образовании, преждевременное раскрытие которой может привести к нежелательному, негативному общественному резонансу.

Безопасность информации в ГИС достигается путем проведения большого комплекса работ, в том числе по аттестованию ГИС и созданию систем по технической защите информации.

В органах власти субъектов Российской Федерации, по представленным данным, функционируют более шестнадцати тысяч информационных систем. При этом из восьми тысяч информационных систем, функционирующих в органах государственной власти, зарегистрировано порядка четырехсот государственных информационных систем, что составляет 6,5% от их общего количества.

В органах местного самоуправления из восьми с половиной тысяч информационных систем зарегистрировано около пятисот муниципальных информационных систем, что составляет 6%.

Работа по определению статуса информационных систем в органах власти находится на начальном этапе, в то время как решениями Межведомственного совета по защите информации в Северо-Западном федеральном округе руководителям органов власти рекомендовалось выполнить данные работы в 2014 г. При этом, необходимая правовая база, определяющая порядок и содержание работ по защите информации в государственных информационных системах, уже сформирована.

На сегодняшний день из зарегистрированных в округе государственных информационных систем, аттестовано по требованиям безопасности информации только двадцать пять, что составляет 7% от общего числа зарегистрированных систем.

Такая же ситуация складывается и с аттестацией информационных систем органов местного самоуправления, где аттестованных информационных систем около 3%.

Фактическое состояние работ по защите информации в государственных информационных системах органов государственной власти и органов местного самоуправления оценивается в ходе контроля, проводимого Управлением ФСТЭК России по СЗФО.

За последнее время проверены на соответствие требованиям законодательства Российской Федерации, нормативных и методических документов ФСТЭК России информационные системы органов государственной власти Санкт-Петербурга, Мурманской и Архангельской областей.

Результаты контроля показали, что основные организационные и технические требования приказа ФСТЭК России от 11 февраля 2013 г. № 17[1] в полном объеме выполнены только в проверенных государственных информационных системах Санкт-Петербурга.

В информационных системах Архангельской и Мурманской областей требования к защите информации не выполняются или выполняются частично.

Уровень защищенности информационных систем в органах государственной власти не в полной мере соответствует существующим угрозам и масштабам информатизации.

Темпы совершенствования региональных систем защиты информации отстают от возрастания и усложнения требований в области информационной безопасности.

Без усиления внимания руководства к подбору, подготовке специалистов и необходимому финансированию работ, эффективность по обеспечению безопасности информации будет недостаточной.

Литература

1. *Кучерявый М. М.* Основные факторы влияния политики информационной безопасности на национальную безопасность современной России // Евразийская интеграция: экономика, право, политика. 2013. № 14. С. 164–168.
2. *Кучерявый М. М.* Роль информационной составляющей в системе политики обеспечения национальной безопасности Российской Федерации // Известия Российского государственного педагогического университета им. А.И. Герцена. 2014. № 164. С. 155–163.
3. *Косов Ю. В., Кучерявый М. М.* Статус России в мировом сообществе и обеспечение глобальной безопасности // Грядущий мировой порядок в оценках российских и американских экспертов: материалы XXII Ежегодного Российско-американского семинара в Санкт-Петербургском государственном университете, 15–21 мая 2013 года. СПб. : СПбГУ, 2013. С. 131–137.

References

1. Kycheryavyy M. M. *Major factors of influence of policy of information security on national security of modern Russia* [Osnovnye faktory vliyaniya politiki informatsionnoi bezopasnosti na natsional'nuyu bezopasnost' sovremennoi Rossii] // Eurasian Integration: Economy, Law, Policy [Evraziiskaya integratsiya: ekonomika, pravo, politika]. 2013. N 14. P. 164–168. (rus)
2. Kycheryavyy M. M. *Role of information component in the system of policy of ensuring of national security of the Russian Federation* [Rol' informatsionnoi sostavlyayushchei v sisteme politiki obespecheniya natsional'noi bezopasnosti Rossiiskoi Federatsii] // News of the Herzen State Pedagogical University of Russia [Izvestiya Rossiiskogo gosudarstvennogo pedagogicheskogo universiteta im. A. I. Gertsena]. 2014. N 164. P. 155–163. (rus)
3. Kosov Yu. V., Kycheryavyy M. M. *Status of Russia in the world community and ensuring global safety* [Status Rossii v mirovom soobshchestve i obespechenie global'noi bezopasnosti] // Future world order in estimates Russian and American experts [Gryadushchii mirovoi poryadok v otsenkakh rossiiskikh i amerikanskii ekspertov]: materials of the XXII Annual Russian-American seminar in St. Petersburg State University, on May 15–21, 2013. SPb. : St. Petersburg State University, 2013. P. 131–137. (rus)

[1] Приказ Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // ФСТЭК России [Электронный ресурс]. URL: http://fstec.ru/normativnye-pravovye-akty-tzi/110-deyatelnost/tekushchaya/tekhnicheskaya-zashchita-informatsii/normativnye-pravovye-akty/prikazy/703-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 19.08.2017).