

УДК 338

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ И ЕЕ РЕГИОНАХ

¹Ахметьянова А.И., ²Кузнецова А.Р.

¹ФГБОУ ВО «Башкирский государственный университет», Уфа, e-mail: ai-albina@mail.ru;

²ФГБОУ ВО «Башкирский государственный аграрный университет»,
Уфа, e-mail: alfia_2009@mail.ru

Настоящая статья посвящена исследованию вопросов национальной безопасности страны и ее регионов. В статье отмечается, что в современных условиях национальная безопасность напрямую зависит от уровня информационного обеспечения и от существующих условий информационной безопасности. Информационная безопасность играет ключевую роль в обеспечении жизненно важных интересов Российской Федерации и ее регионов. Революция в сфере информационных технологий (появление глобальной сети Интернет, мобильных средств и коммуникаций и т.п.) качественно расширила технические возможности специалистов в области информационной безопасности. Информационная безопасность во многом зависит от защищенности технических структур (компьютерных систем управления, баз данных и т.п.), вывод из строя которых способен привести к нарушению работы комплексной системы безопасности. В современном обществе информационные и коммуникационные технологии являются основными факторами, определяющими уровень социально-экономического развития и состояние международной информационной безопасности. В этой связи основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года призваны способствовать активизации внешней политики Российской Федерации на пути достижения согласия учета взаимовыгодных интересов в рамках интернационализации глобального информационного пространства.

Ключевые слова: информационная безопасность, информационные технологии, компьютерное обеспечение, субъекты Российской Федерации, затраты

PROBLEMS OF INFORMATION SECURITY IN RUSSIA AND ITS REGIONS

¹Akhmetyanova A.I., ²Kuznetsova A.R.

¹Bashkir State University, Ufa, e-mail: ai-albina@mail.ru;

²Bashkir State Agrarian University, Ufa, e-mail: alfia_2009@mail.ru

This article is devoted to the study of national security of the country and its regions. The article notes that in modern conditions the national security is directly dependent on the level of information security and information security from the existing conditions. Information security plays a key role in ensuring the vital interests of Russia and its regions. The revolution in information technology (the emergence of the global Internet, mobile tools and utilities, etc.) qualitatively expanded technical capabilities of experts in the field of information security. Information security depends on the security of the technical structures (computer management systems, databases, and TR), disabling that can lead to disruption of the integrated security system. In modern society, information and communication technologies are the main factors determining the level of socio-economic development and the state of international information security. In this connection, the Russian Federation's state policy framework in the field of international information security for the period up to 2020 are designed to boost the foreign policy of the Russian Federation in the way of reaching an agreement account mutual interests within the framework of the internationalization of global information space.

Keywords: information security, information technology, computer software, subjects of the Russian Federation, expenses

Национальная безопасность страны и ее регионов в современных условиях напрямую зависима от уровня информационного обеспечения и от существующих условий информационной безопасности. Информационная безопасность играет ключевую роль в обеспечении жизненно важных интересов Российской Федерации и ее регионов. Революция в сфере информационных технологий (появление глобальной сети Интернет, мобильных средств и коммуникаций и т.п.) качественно расширила технические возможности специалистов в области информационной безопасности. Информационная безопасность во многом зависит от

защищенности технических структур (компьютерных систем управления, баз данных и т.п.), вывод из строя которых способен привести к нарушению работы комплексной системы безопасности.

В последние годы в сфере информационных технологий происходят прогрессивные изменения. Об этом свидетельствуют данные официальной статистики. Рассмотрим удельный вес организаций, использовавших информационные и коммуникационные технологии в своей работе за период с 2003 по 2014 гг. по данным Федеральной службы государственной статистики Российской Федерации на рис. 1.



Рис. 1. Удельный вес организаций, использовавших информационные и коммуникационные технологии за период с 2003 по 2014 гг. [4]

Из данных, представленных на рис. 1, отчетливо видно, что удельный вес персональных компьютеров, используемых в работе, за анализируемый период возрос с 84,6 до 93,8%, т.е. на 9,2 п.п. Возрос также удельный вес локальных вычислительных сетей с 45,8 до 67,2%, т.е. рост составил 21,4 п.п. Удельный вес использования электронной почты возрос с 48,6 до 85,2%, т.е. на 36,6 п.п. Использование Интернета в работе возросло с 43,4 до 86,9%, т.е. на 43,5 п.п., что в целом свидетельствует о наличии положительных тенденций в области развития информационных и коммуникационных технологий в стране.

Проведенный анализ показал, что число персональных компьютеров в обследованных организациях за период с 2003 по 2014 г. возросло в 2,8 раза, из которых число

компьютеров, обладающих доступом к глобальным информационным сетям, возросло в 6,8 раза, в том числе к сети Интернет – в 7,4 раза. Количество приобретенных персональных компьютеров за период с 2003 по 2014 г. возросло на 79,5%. В расчете на каждые 100 человек работников организаций число персональных компьютеров увеличилось в 2,6 раза: с 18 компьютеров в 2003 г. до 47 компьютеров в 2014 г., что, несомненно, является положительной тенденцией. Позитивно и то, что в расчете на каждые 100 человек работников число компьютеров, имеющих доступ к сети Интернет, возросло в 7,3 раза: с 4 до 29 единиц.

Рассмотрим удельный вес организаций, использовавших Интернет, по субъектам Российской Федерации на рис. 2.

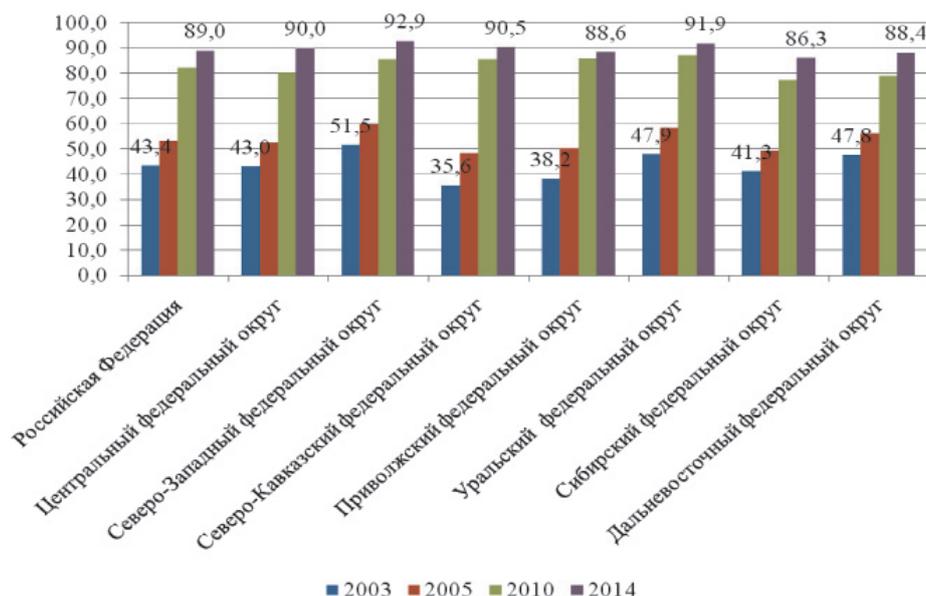


Рис. 2. Удельный вес организаций, использовавших Интернет, по субъектам Российской Федерации [4]

Из данных, представленных на рис. 2, следует, что удельный вес организаций, использовавших Интернет, по субъектам Российской Федерации за период с 2003 по 2014 г. имел устойчивую тенденцию к росту. В общероссийском масштабе удельный вес организаций, использовавших Интернет, возрос с 43,4 до 89%. При этом в 2003 г. округом – лидером по использованию сети Интернет выступал Северо-Западный федеральный округ (51,5%), на втором месте был Уральский федеральный округ (47,9%), затем на 3 месте был Дальневосточный федеральный округ (47,8%), на четвертом – Центральный федеральный округ (43%), на 5 месте – Сибирский федеральный округ (41,3%), на 6 месте – Приволжский федеральный округ (38,2%), на 7 месте – Северо-Кавказский федеральный округ (35,6%).

Таким образом, к уровню 2014 г. первое и второе места по использованию сети Интернет сохранились за Северо-Западным (92,9%) и Уральским федеральным (91,9%) округами. Третье место стало принадлежать Северо-Кавказскому федеральному округу (90,5%). Четвертое место сохранилось за Центральным федеральным округом (90%), 5 место стало принадлежать Приволжскому федеральному округу (88,6%), 6 место – Дальневосточному федеральному округу (88,4%), 7 место принадлежит – Сибирскому федеральному округу (86,3%).

Согласно данным Федеральной службы государственной статистики Российской Федерации, в 2003 году в структуре затрат организаций на информационные и коммуникационные технологии по видам наибольший удельный вес принадлежал за-

тратам на приобретение вычислительной техники (52,3%), на оплату услуг электросвязи – 20,9%, на оплату услуг сторонних организаций – 11,3%, на приобретение программных средств затрачивалось 7,7%, прочим затратам стало принадлежать 7,1%. В 2014 г. затратам на оплату услуг электросвязи стало принадлежать 23,8%, затратам на приобретение вычислительной техники – 22,1%, затратам на оплату услуг сторонних организаций – 17%, на приобретение программных средств затрачивалось 13,8%, приобретению телекоммуникационного оборудования стало принадлежать 13,1%, прочим затратам стало принадлежать 9,1%.

Рассмотрим удельный вес организаций, использовавших специальные программные средства, на рис. 3.

Из данных, представленных на рис. 3, следует, что за период с 2003 по 2014 г. удельный вес организаций, использовавших специальные программные средства, возрос с 68,7 до 86,3%, т.е. на 17,6 процентных пункта. При этом если в 2003 г. для решения организационных, управленческих задач использовалось 53,4% специальных программных средств, то в 2014 г. – 56,2%, увеличение удельного веса использования программных средств для организационных, управленческих и экономических задач в общероссийском масштабе составило 2,8 п.п. Для финансовых расчетов в 2003 г. использовалось 30% специальных программных средств, а в 2014 г. – 57%, т.е. рост составил 27 п.п. Для получения электронно-справочной правовой информации в 2014 г. используется почти 54% специальных программных средств.



Рис. 3. Удельный вес организаций, использовавших специальные программные средства, в процентах [4]

Информационная безопасность является частью национальной безопасности. В 2014 г. была принята Концепция Евразийской безопасности [1], в соответствии с которой основными угрозами информационной безопасности являются:

- стремление ряда стран к доминированию в мировом информационном пространстве, разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним;

- использование информационных технологий в целях манипуляции общественным мнением;

- использование информационных технологий в целях дезинформации мирового сообщества, информационного обеспечения санкций экономического, политического и военного характера вплоть до военной агрессии;

- использование информационных технологий в качестве инструмента культурного разложения, пропаганды асоциального образа жизни, отрицания норм морали и общекультурных ценностей;

- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

- компрометацию ключей и средств криптографической информации;

- утечку информации по техническим каналам;

- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

- уничтожение, повреждение, разрушение или хищение машин и других носителей информации;

- перехват информации в сетях передачи данных и на линиях связи, дешифрова-

ние этой информации и навязывание ложной информации;

- несанкционированный доступ к информации, находящейся в базах данных [2].

В качестве основных направлений создания системы коллективной информационной безопасности, в соответствии с концепцией Евразийской национальной безопасности определены:

- реализация конституционных прав и свобод граждан в сфере информационной безопасности;

- совершенствование и защита информационной инфраструктуры, интеграция государств (Белоруссии, России, Казахстана, Кыргызстана, Узбекистана) в мировое информационное пространство;

- противодействие угрозе развязывания протывоборства в информационной сфере;

- ограничение доступа к информации, содержащей пропаганду террористической, экстремистской и преступной деятельности, травмирующей личность информации, особенно в отношении несовершеннолетних;

- создание системы противодействия монополизации отечественными и зарубежными структурами составляющих информационной инфраструктуры, включая рынок информационных услуг и средства массовой информации;

- разработку, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения.

Основная часть

Для преодоления ключевых угроз информационной безопасности в Российской Федерации принята и реализуется Концепция информационной безопасности, являющаяся составной частью Концепции национальной безопасности Российской Федерации [2].

Она служит основой для разработки стратегии обеспечения информационной безопасности страны, включающей в себя цели, задачи и комплекс основных мер по ее практической реализации; формирования и проведения государственной политики Российской Федерации в области обеспечения информационной безопасности; подготовки предложений правового, нормативно-методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации; разработки целевых программ защиты информационных ресурсов и средств информатизации.

Заключение

Экономический потенциал государства все в большей степени определяется объемом информационных ресурсов и уровнем развития информационной инфраструктуры. Информационная среда, являясь системообразующим фактором во всех сферах национальной безопасности, активно влияет на состояние политической, экономической, оборонной и других составляющих национальной безопасности Российской Федерации.

В качестве основных направлений государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года определены задачи формирования системы международной информационной безопасности, создание условий, обеспечивающих снижение риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств, представляющих угрозу международному миру, безопасности и стратегической стабильности; создание условий для обеспечения технологического суверенитета государств в области информационных и коммуникационных технологий и преодоления информационного неравенства между развитыми и развивающимися странами [3].

В современном обществе информационные и коммуникационные технологии являются основными факторами, определяющими уровень социально-экономического развития и состояние международной информационной безопасности. В этой связи основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года призваны способствовать активизации внешней политики Российской Федерации на пути достижения согласия учета взаимовыгодных интересов в рамках интернационализации глобального информационного пространства.

Список литературы

1. Доктрина информационной безопасности Российской Федерации. Утв. Указом Президента РФ от 09.09.2000 г. № 1300. Источник: <http://www.zakonprost.ru/content/base/39613>. – Режим доступа: 05.06.2016.
2. Концепция Евразийской Безопасности от 22.04.2014 г. Источник: http://www.imemo.ru/files/File/magazines/rossia_i_novay/2012_03/round%20table.pdf. – Режим доступа: 05.06.2016.
3. Кузнецова А.Р., Валиева Г.Р. Интеллектуальный потенциал инновационной деятельности в сельском хозяйстве // Экономика сельского хозяйства России. – 2013. – № 1. – С. 031–036.
4. Кузнецова А.Р., Валиева Г.Р. Проблемы формирования инноваций в аграрной сфере экономики Республики Башкортостан // Вестник Башкирского государственного аграрного университета. – 2013. – № 1 (25). – С. 129–130.
5. Кузнецова А.Р., Ягафарова В.А. Образование как ключевой фактор повышения конкурентоспособности страны // Высшее образование сегодня. – 2013. – № 1. – С. 31–33.
6. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Утв. Президентом Российской Федерации от 24.07.2013 № Пр-1753. Источник: http://www.consultant.ru/document/cons_doc_LAW_178634. – Режим доступа: 06.06.2016.
7. Федеральная служба государственной статистики Российской Федерации. Источник: http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/science_and_innovations/it_technology/#. – Режим доступа: 06.06.2016.

References

1. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii. Utv. Ukazom Prezidenta RF ot 09.09.2000 g. no. 1300. Istochnik: <http://www.zakonprost.ru/content/base/39613>. Rezhim dostupa: 05.06.2016.
2. Konceptija Evrazijskoj Bezopasnosti ot 22.04.2014 g. Istochnik: http://www.imemo.ru/files/File/magazines/rossia_i_novay/2012_03/round%20table.pdf. Rezhim dostupa: 05.06.2016.
3. Kuznecova A.R., Valieva G.R. Intellektualnyj potencial innovacionnoj dejatelnosti v selskom hozjajstve // Jekonomika selskogo hozjajstva Rossii. 2013. no. 1. S. 031–036.
4. Kuznecova A.R., Valieva G.R. Problemy formirovanija innovacij v agrarnoj sfere jekonomiki Respubliki Bashkortostan // Vestnik Bashkirskogo gosudarstvennogo agrarnogo universiteta. 2013. no. 1 (25). pp. 129–130.
5. Kuznecova A.R., Jagafarova V.A. Obrazovanie kak kljuchevoj faktor povysheniya konkurentosposobnosti strany // Vysshee obrazovanie segodnja. 2013. no. 1. pp. 31–33.
6. Osnovy gosudarstvennoj politiki Rossijskoj Federacii v oblasti mezhdunarodnoj informacionnoj bezopasnosti na period do 2020 goda. Utv. Prezidentom Rossijskoj Federacii ot 24.07.2013 no. Pr-1753. Istochnik: http://www.consultant.ru/document/cons_doc_LAW_178634. Rezhim dostupa: 06.06.2016.
7. Federalnaja sluzhba gosudarstvennoj statistiki Rossijskoj Federacii. Istochnik: http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/science_and_innovations/it_technology/#. Rezhim dostupa: 06.06.2016.