УДК 378.046.4+349
DOI: 10.15827/0236-235X.118.320-323
Дата подачи статьи: 30.01.17
2017. Т. 30. № 2. С. 320–323

УРОВНИ И ПРАВОВАЯ МОДЕЛЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ЗАЩИТЫ ИНФОРМАЦИИ)

С.В. Голубчиков, к.т.н., начальник отдела, gsv_64@list.ru
(ПАО «НПО «Алмаз», Ленинградский просп., 80, стр. 16, г. Москва, 125190, Россия);
В.К. Новиков, к.в.н., доцент
(Военная академия РВСН им. Петра Великого,
ул. Карбышева, 8, г. Балашиха, Московская обл., 143900, Россия);
А.В. Баранова, аспирант, abv92@list.ru
(МГИМО (университет) МИД России, просп. Вернадского, 76, г. Москва, Россия)

В контексте определения информации как стратегического ресурса любого государства, производительной силы и дорогого товара рассматриваются проблемы информационной безопасности (защиты информации). Для их разрешения одним из направлений деятельности государства является правовое регулирование.

Так как информационная безопасность – это неотъемлемая часть общей и национальной безопасности, содержание которой базируется прежде всего на Конституции Российской Федерации, а также на основных базовых документах, в работе выделены уровни безопасности, дано понятие жизненно важных интересов, вытекающее из понятия безопасности.

Формулируются важнейшие задачи обеспечения информационной безопасности Российской Федерации. Задаются направления обеспечения информационной безопасности, а также организационно-технические мероприятия по защите информации в общегосударственных информационных и телекоммуникационных системах.

Предлагается к рассмотрению разработанная правовая модель обеспечения информационной безопасности, где выделены объекты защиты информации: персональные данные человека, различные технические средства, ПО, информационно-технические системы, документы и др.

В работе делается вывод о том, что информационная безопасность является составной частью общей и национальной безопасности и охватывает все сферы деятельности.

***Ключевые слова**: информация, информационная безопасность, защита информации, информационная сфера, правовая модель.*

Начало XXI века ознаменовано бурным развитием информационных технологий во всех сферах государственной деятельности и общественной жизни. Информация все в большей мере становится стратегическим ресурсом любого государства, производительной силой и дорогим товаром. Это не может не вызывать стремления государств, организаций и отдельных граждан получить преимущества за счет завладения информацией, нанесения ущерба информационным ресурсам конкурента, а также защиты своих информационных ресурсов [1–3].

В настоящее время вопрос информационной безопасности остро стоит на уровне как государства, различных организаций, так и отдельных граждан. Важно обеспечить их конституционные права на получение достоверной информации, на ее использование в интересах осуществления законной деятельности учреждений, а также на защиту государственной, коммерческой, семейной, личной и других видов тайн.

Рассмотрим систему информационной безопасности, сложившуюся в России.

Проблема защиты информации от постороннего доступа и нежелательных воздействий возникла с развитием общественных отношений. Наиболее ценной становится информация, позволяющая ее владельцу получить какой-либо материальный, политический, военный и другой выигрыш [4–6].

Однако создание индустрии переработки информации порождает целый ряд сложных проблем, одной из которых является надежное обеспечение сохранности и установленного правового статуса информации в отдельных технических средствах, в информационно-вычислительных системах и информационно-телекоммуникационных сетях. Данная проблема вошла в обиход как проблема информационной безопасности [7–8].

Для ее разрешения необходимо урегулировать на государственном уровне правовые аспекты данной области.

Информационная безопасность является неотъемлемой составной частью общей и национальной безопасности, содержание которой базируется в первую очередь на Конституции России, а также на основных базовых документах: Федеральном законе «О безопасности», «Стратегии национальной безопасности Российской Федерации до 2020 года» и Доктрине информационной безопасности Российской Федерации.

Анализ приведенных документов позволяет выделить уровни безопасности, представленные на рисунке 1.

Под безопасностью понимается состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Из понятия «безопасность» вытекает другое понятие – «жизненно важные интересы» как совокуп-

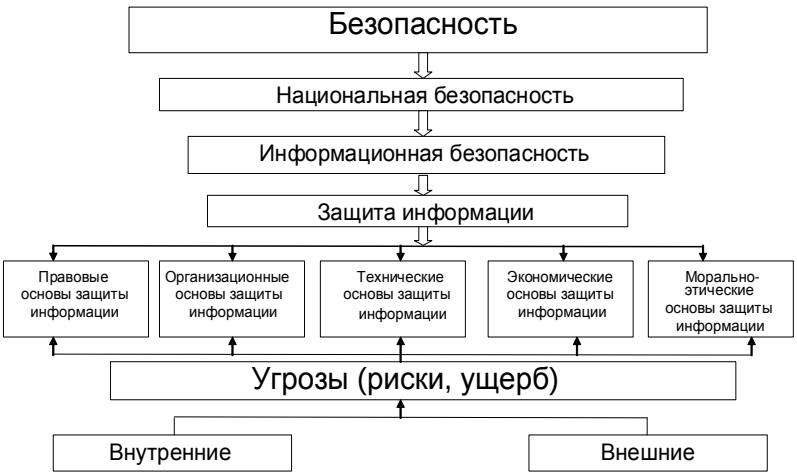

Рис. 1. Уровни безопасности

Рис. 1. Security levels

ность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

Рассмотрим суть информационной безопасности через понимание национальной безопасности.

Национальная безопасность – состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства.

При этом в рамках национальной безопасности национальные интересы России в информационной сфере заключаются в соблюдении конституционных прав и свобод в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

Угрозами национальной безопасности России в информационной сфере, представляющими серьезную опасность, являются:

– стремление ряда стран к доминированию в мировом информационном пространстве;

– вытеснение России с внешнего и внутреннего информационных рынков;

– разработка рядом государств концепций информационных войн;

– возможность нарушения нормального функционирования информационных и телекоммуникационных систем, получения несанкционированного доступа к ним.

Важнейшие задачи обеспечения информационной безопасности:

– реализация конституционных прав и свобод граждан в сфере информационной деятельности;

– совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;

– противодействие угрозе развязывания противоборства в информационной сфере.

Направлениями обеспечения информационной безопасности [9] Российской Федерации в общегосударственных информационных и телекоммуникационных системах являются:

– предотвращение перехвата информации из помещений и с объектов, а также информации, передаваемой по каналам связи с помощью технических средств;

– исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;

– предотвращение утечки информации по техническим каналам, возникающей при эксплуатации технических средств ее обработки, хранения и передачи;

– предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации;

– обеспечение информационной безопасности при подключении общегосударственных информационных и телекоммуникационных систем к внешним информационным сетям, включая международные;

– обеспечение безопасности конфиденциальной информации при взаимодействии информационных и телекоммуникационных систем различных классов защищенности;

– выявление внедренных на объекты и в технические средства электронных устройств перехвата информации.

Защитить информацию в общегосударственных информационных и телекоммуникационных системах позволят организационно-технические мероприятия:

– лицензирование деятельности организаций в области защиты информации;

– аттестация объектов информатизации по выполнению требований обеспечения защиты информации при проведении работ, связанных с использованием сведений, составляющих государственную тайну;

– сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи;

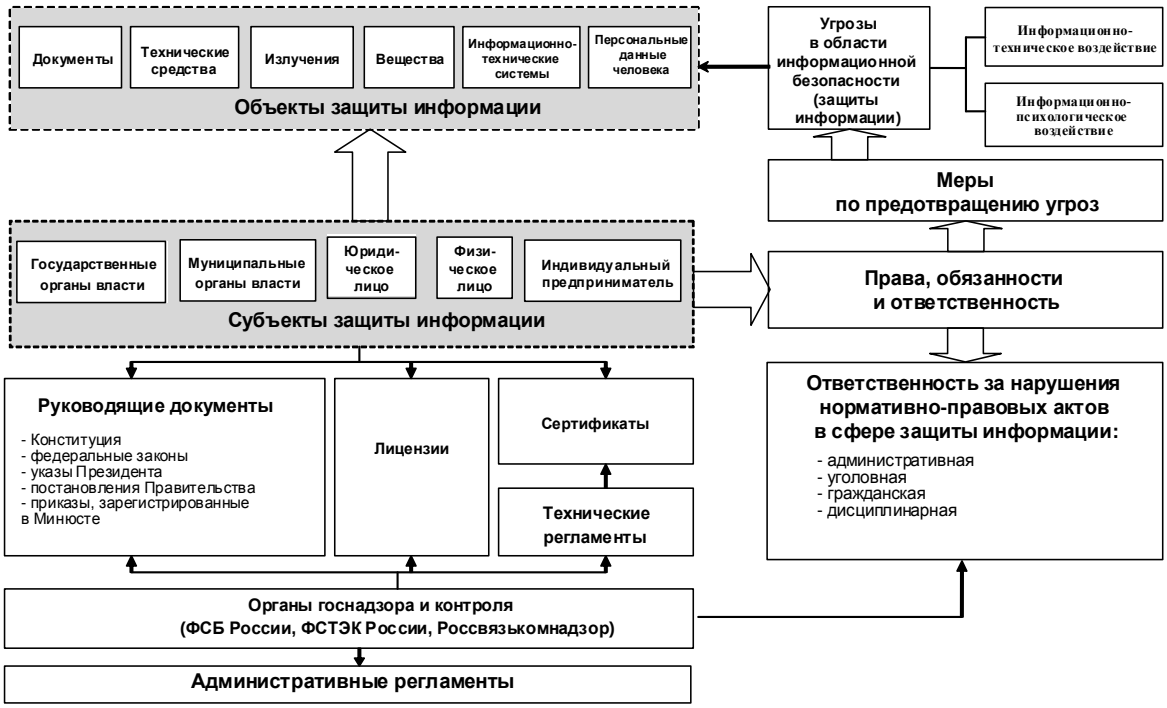

Рис. 2. Правовая модель информационной безопасности (защиты информации)

Рис. 2. A legal model of information security

– введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств, подлежащих защите;

– создание и применение информационных и автоматизированных систем управления в защищенном исполнении.

Анализ сущности и содержания нормативных правовых актов Российской Федерации в области информационной безопасности (защиты информации) позволил сформулировать правовую модель информационной безопасности (защиты информации) [10], которая дает более полное понятие правовой основы защиты информации (рис. 2).

Правовая модель информационной безопасности (защиты информации) позволяет представить область деятельности организаций и ее участников, правовые отношения, возникающие при восприятии (сборе), обработке, хранении, передаче и уничтожении и других действиях, производимых с информацией.

Таким образом, информационная безопасность является составной частью общей и национальной безопасности и охватывает все сферы деятельности государства, гражданина, а также различных организаций и бизнеса [11, 12].

Литература

1. Буданцев Ю.П. Информационное оружие и информационная война в современных условиях // Безопасность. 1999. № 3–4. С. 103–115.

2. Манилов В.Л. Национальная безопасность: ценности, интересы, цели // Военная мысль. 2005. № 9. С. 7–8.

3. Мухин В., Лось А., Новиков В. Информационная война в Персидском заливе // Безопасность. 1996. № 1–2. С. 60–63.

4. Новопашин А.П. Информационная политика России: состояние и пути совершенствования // Безопасность. 2010. № 11–12. С. 5–23.

5. Панарин И.Н., Панарина Л.Г. Информационная война и мир. М.: ОЛМА-ПРЕСС, 2003. 384 с.

6. Кириленко В.И., Лось В.П. Информационная борьба и проблемы обеспечения информационной безопасности Российской Федерации // Информационное право. Информационная культура и информационная безопасность: матер Всерос. науч.-практич. конф. СПб: Изд-во ГУП, 2002. С. 59–63.

7. Киреенко А.Е. Современные проблемы в области информационной безопасности: классические угрозы, методы и средства их предотвращения // Молодой ученый. 2012. № 3. С. 40–45.

8. Петров В.П., Петров С.В. Информационная безопасность человека и общества. М.: ЭНАС, 2007. 336 с.

9. Новиков В.К., Галушкин И.Б., Аксенов С.В. Информационная безопасность и защита информации. Организационно-правовые основы. М.: Горячая линия–Телеком, 2016. 312 с.

10. Голубчиков С.В., Новиков В.К., Баранова А.В. Правовая модель информационной безопасности (защиты информации) в образовательном процессе // Муниципальное образование: инновации и эксперимент. 2017. № 1. С. 55–58.

11. Новиков В.К. Организационное и правовое обеспечение информационной безопасности. Ч. I. Правовое обеспечение информационной безопасности. М.: Изд-во МИЭТ, 2013. 184 с.

12. Новиков В.К., Галушкин И.Б., Аксенов С.В. Организационно-правовые основы информационной безопасности (защиты информации). Ч. II. Правовые и организационные основы информационной безопасности (защиты информации). М.: Изд-во ВА РВСН им. Петра Великого, 2015. 395 с.

Software & Systems Received 30.01.17
DOI: 10.15827/0236-235X.118.320-323 2017, vol. 30, no. 2, pp. 320–323

A SYSTEM AND LEGAL MODEL OF INFORMATION SECURITY (DATA PROTECTION)

S.V. Golubchikov [1], *Ph.D. (Engineering), Head of Department, gsv_64@list.ru*
V.K. Novikov [2], *Ph.D. (Military Sciences), Associate Professor*
A.V. Baranova [3], *Postgraduate Student, abv92@list.ru*

[1] *PJSC NPO "Almaz", Leningradsky Ave. 80/16, Moscow, 125190, Russian Federation*
[2] *The Military Academy of Strategic Rocket Troops after Peter the Great, Karbysheva St. 8, Balashikha, Moscow Reg., 143900, Russian Federation*
[3] *MGIMO University, Vernadsky Ave. 76, Moscow, Russian Federation*

Abstract. The paper considers the problems of information security (data protection) in the context of information as a strategic resource of any state, a productive force and an expensive commodity. One of the state activities to solve these problems is the legal regulation of this area.

Since information security is an integral part of the overall and national security with its content based on the Constitution of the Russian Federation, as well as on the core documents, the article identifies the levels of security of the Russian Federation.

Security is defined as a condition of protection of the vital interests of an individual, society and the state from internal and external threats. Therefore the paper gives the definition of "vital interests" arising from the definition of "security".

The authors formulate the most important purposes for ensuring information security of the Russian Federation.

The paper specifies the directions of ensuring the information security of the Russian Federation, as well as organizational and technical measures to protect information in the national information and telecommunication systems.

The article presents the developed legal model for ensuring information security. The model reveals the objects of information security that may be under different kinds of influences, such as personal data; various technical means; software; information and technical systems involved in sensing, processing, storage and transmission of information (data); documents (paper, electronic); radiation; substances.

There is a conclusion that information security is an integral part of the overall and national security and covers all spheres of activities of the state, citizens, as well as various organizations and businesses.

Keywords: information, information security, data protection, information sphere, legal model.

References

1. Budantsev Yu.P. Information weapon and information war under current conditions. *Bezopasnost* [Security]. 1999, no. 3–4, pp. 23–29 (in Russ.), pp. 103–115.

2. Manilov V.L. National security: values, interests, purposes. *Voennaya mysl* [Military Thought]. 2005, no, 9, pp. 7–8 (in Russ.).

3. Mukhin V., Los A., Novikov V. Information war in the Persian Gulf. *Bezopasnost* [Security]. 1996, no. 1–2, pp. 60–63 (in Russ.).

4. Novopashin A.P. Information policy of Russia: status and ways to improve. *Bezopasnost* [Security]. 2010, no. 11–12, pp. 5–23 (in Russ.).

5. Panarin I.N., Panarina L.G. *Informatsionnaya voyna i mir* [Information War and Peace]. Moscow, OLMA-PRESS, 2003, 135 p.

6. Kirilenko V.I., Los V.P. Information war and information security problems in the Russian Federation. *Informatsionnoe pravo. Informatsionnaya kultura i informatsionnaya bezopasnost: mater. Vseros. nauch.-praktich. konf.* [Information Right. Information Culture and Information Security: Proc. All-Russian Science and Practice Conf.]. St. Petersburg, GUP Publ., 2002, pp. 59–63 (in Russ.).

7. Kireenko A.E. Modern problems in information security: classical threats, preventing methods and instruments. *Molodoy ucheny* [Young Scientist]. 2012, no. 3 (38), pp. 40–45 (in Russ.).

8. Petrov V.P., Petrov S.V. *Informatsionnaya bezopasnost cheloveka i obshchestva* [Information Security for a Human and Society]. ENAS Publ., 2007.

9. Novikov V.K., Galushkin I.B., Aksenov S.V. *Informatsionnaya bezopasnost i zashchita informatsii. Organizatsionno-pravovye osnovy* [Information Security and Protection. Procedural and Institutional Basics]. V.K. Novikov (Ed.). Moscow, Goryachaya liniya–Telekom Publ., 2016, 312 p.

10. Golubchikov S.V., Novikov V.K., Baranova A.V. Information Security Legal Model in an Educational Process. *Munitsipalnoe obrazovanie: innovatsii i eksperiment* [Municipal Entity: Innovations and Experiments]. 2017, no. 1, pp. 55–58 (in Russ.).

11. Novikov V.K. *Organizatsionnoe i pravovoe obespechenie informatsionnoy bezopasnosti. Ch. I. Pravovoe obespechenie informatsionnoy bezopasnosti* [Procedural and Institutional Support for Information Security. Part 1. Legal Support for Information Security]. Moscow, MIET Publ., 2013, 184 p.

12. Novikov V.K., Galushkin I.B., Aksenov S.V. *Organizatsionno-pravovye osnovy informatsionnoy bezopasnosti (zashchity informatsii). Ch. II. Pravovye i organizatsionnye osnovy informatsionnoy bezopasnosti (zashchity informatsii)* [Procedural and Institutional Basics of Information Security. Part 2. Legal and Institutional Basis of Information Security]. Moscow, VA RVSN im. Petra Velikogo Publ., 2015, 395 p.