ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УЧЕБНИК И ПРАКТИКУМ
ДЛЯ БАКАЛАВРИАТА И МАГИСТРАТУРЫ

Под редакцией доктора юридических наук, профессора,
заслуженного юриста Российской Федерации **Т. А. Поляковой**
и доктора юридических наук, доктора технических наук,
профессора, заслуженного деятеля науки
Российской Федерации **А. А. Стрельцова**

Рекомендовано Учебно–методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по юридическим направлениям и специальностям

Книга доступна в электронной библиотечной системе
biblio-online.ru

Москва ▪ Юрайт ▪ 2019

УДК 34(075.8)
ББК 67я73
О64

***Ответственные редакторы*:**

Полякова Татьяна Анатольевна — доктор юридических наук, профессор, заслуженный юрист Российской Федерации, действительный государственный советник юстиции Российской Федерации 3 класса, заведующая сектором информационного права Института государства и права Российской академии наук, профессор кафедры информационного права, информатики и математики Всероссийского государственного университета юстиции;

Стрельцов Анатолий Александрович — доктор юридических наук, доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, действительный государственный советник Российской Федерации 3 класса, заместитель директора Института проблем информационной безопасности Московского государственного университета имени М. В. Ломоносова.

***Рецензенты*:**

Бачило И. Л. — доктор юридических наук, профессор, главный научный сотрудник Института государства и права Российской академии наук, заслуженный юрист Российской Федерации;

Кузнецов П. У. — доктор юридических наук, профессор, заведующий кафедрой информационного права Уральской государственной юридической академии.

Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2019. — 325 с. — Серия : Бакалавр и магистр. Академический курс.

О64

ISBN 978-5-534-03600-8

В учебнике изложены общие теоретический и методологический подходы к формированию правового и организационного обеспечения информационной безопасности человека, общества и государства. Подробно освещены основные институты правового обеспечения информационной безопасности: правовые режимы защиты информации, государственной, служебной и коммерческой тайн, персональных данных, юридической ответственности за правонарушения в области информационной безопасности, а также структура организационного обеспечения информационной безопасности. Рассмотрены проблемы формирования правового режима международной информационной безопасности. Значительное внимание уделено организационным аспектам управления защитой информационных систем.

Соответствует актуальным требованиям Федерального государственного образовательного стандарта высшего образования.

Предназначен для студентов, обучающихся по программам академического бакалавриата и магистратуры дисциплины «Правовое и организационное обеспечение информационной безопасности», будет полезен для аспирантов, преподавателей юридических и экономических высших учебных заведений, юридических и экономических факультетов университетов.

УДК 34(075.8)
ББК 67я73

ISBN 978-5-534-03600-8

Оглавление

Авторский коллектив

Полякова Татьяна Анатольевна, доктор юридических наук, доцент, заслуженный юрист Российской Федерации, действительный государственный советник юстиции Российской Федерации 3 класса, заведующая сектором информационного права Института государства и права Российской академии наук, профессор кафедры информационного права, информатики и математики Всероссийского государственного университета юстиции — гл. 2 (параграфы 2.2 и 2.3), 3, 7;

Стрельцов Анатолий Александрович, доктор юридических наук, профессор, доктор технических наук, заслуженный деятель науки Российской Федерации, действительный государственный советник Российской Федерации 3 класса, заместитель директора Института проблем информационной безопасности Московского государственного университета имени М. В. Ломоносова, член-корреспондент Академии криптографии Российской Федерации — гл. 1, 2 (параграфы 2.1, 2.4—2.6);

Чубукова Светлана Георгиевна, кандидат юридических наук, доцент, заместитель заведующего кафедрой правовой информатики Московского государственного юридического университета имени О. Е. Кутафина (МГЮА), почетный работник высшего профессионального образования Российской Федерации — гл. 4, 5;

Ниесов Владимир Александрович, кандидат технических наук, профессор кафедры информационного права, информатики и математики Российского государственного университета правосудия, советник юстиции 1 класса, лауреат Государственной премии СССР, почетный работник высшего профессионального образования Российской Федерации — гл. 6.

Предисловие

Одним из важных направлений обеспечения устойчивого развития человечества в обозримом будущем является освоение результатов продолжающейся научно-технической революции, в том числе результатов, полученных в области автоматизации процессов получения, передачи, хранения и распространения информации, формирования глобального информационного пространства. Расширяется применение современных информационных и коммуникационных технологий, компьютерной техники в социально-экономической, политической и духовной сферах жизнедеятельности общества, в выполнении задач государственного управления. Потенциал информационно-коммуникационных технологий активно используется для повышения качества жизни граждан, содействия реализации ими конституционных прав и свобод человека и гражданина, формирования институтов гражданского общества, расширения участия граждан в решении их насущных проблем, повышении эффективности деятельности органов государственной власти и местного самоуправления.

Эти процессы с неизбежностью повышают зависимость человека, организаций, государственных органов и учреждений от устойчивости функционирования информационной инфраструктуры общества, безопасности ее использования для реализации основных прав и свобод, законных интересов граждан, интересов общества и государства. Устойчивость функционирования и безопасность использования информационной инфраструктуры становятся важным фактором повышения конкурентоспособности страны, обеспечения ее национальной безопасности.

Влияние данного фактора на жизнь общества и государства становится особенно заметно в условиях обострения межгосударственных отношений, разработки методов и способов использования информационно-коммуникационных технологий для оказания «силового» давления на политическое руководство государства и население, для усиления потенциала вооруженных сил зарубежных государств, для нарушения социальной стабильности, вмешательства во внутренние дела других государств.

Противодействие новым вызовам и угрозам связано в том числе с обеспечением информационной безопасности человека, организаций, общества и государства в целом. В его составе выделяются организационное, правовое, кадровое, техническое, финансовое и иные виды обеспечений. В данном учебнике основное внимание сосредоточено на правовом и организационном обеспечении информационной безопасности, играющих системообразующую роль в данном противодействии. Усилиями законодателя правовое обеспечение информационной безопасности, по существу, сложилось в самостоятельную подотрасль информационного права. Организационное обеспечение — действенный инструмент координации усилий

субъектов обеспечения информационной безопасности на наиболее опасных угрозах устойчивости функционирования и безопасности использования информационной инфраструктуры общества.

Многие вышедшие в последнее время учебники и учебные пособия по дисциплине «Организационно-правовое обеспечение информационной безопасности» содержат систематизированное изложение материалов по данной тематике, однако практически все они ориентированы на использование при подготовке специалистов. Внимание, уделяемое изложению выделенных вопросов в учебных материалах по дисциплине «Информационное право», как правило, не позволяет подробно рассмотреть основные тенденции развития правового и организационного обеспечений информационной безопасности.

В предлагаемом учебнике на основе авторских исследований и концептуальных подходов систематизировано изложены наиболее актуальные аспекты правового обеспечения информационной безопасности, а также важнейшие аспекты его организационного обеспечения как учебной дисциплины.

Учебник включает семь глав основного материала, отражающих как вопросы развития теории правового и организационного обеспечения информационной безопасности, так и наиболее важные вопросы применения теории для решения практических задач.

В главе 1 изложены общие вопросы обеспечения информационной безопасности в проблематике формирования информационного общества в России, противодействия угрозам использования информационно-коммуникационных технологий для ущемления национальных интересов, снижения уровня информационной безопасности человека, общества и государства.

Глава 2 посвящена рассмотрению наиболее важных вопросов формирования теории и методологии правового и организационного обеспечения информационной безопасности.

В главе 3 изложены авторские подходы к изучению организационно-правовых проблем формирования системы международной информационной безопасности.

В главе 4 основное внимание сосредоточено на вопросах обеспечения безопасности информации ограниченного доступа.

В главе 5 рассматриваются правовые механизмы ограничения распространения информации в информационной инфраструктуре общества в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Особенности организационно-правового обеспечения защиты информационных систем раскрываются в главе 6.

Вопросам юридической ответственности за правонарушения в информационной сфере посвящена глава 7.

Каждая глава учебника сопровождается перечнем вопросов для самостоятельной подготовки.

В учебнике также представлен Перечень рекомендованной литературы, которая может быть полезна при изучении соответствующих разделов учебной дисциплины.

Авторский коллектив

Принятые сокращения

1. Нормативные правовые акты

Конституция РФ — Конституция Российской Федерации, принята всенародным голосованием 12 декабря 1993 г. (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ)

Устав ООН — Устав Организации Объединенных Наций, принят в Сан-Франциско 26 июня 1945 г.

ГК РФ — Гражданский кодекс Российской Федерации: часть первая от 30.11.1994 № 51-ФЗ; часть вторая от 26.01.1996 № 14-ФЗ; часть третья от 26.11.2001 № 146-ФЗ; часть четвертая от 18.12.2006 № 230-ФЗ

КоАП РФ — Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ

НК РФ — Налоговый кодекс Российской Федерации: часть первая от 31.07.1998 № 146-ФЗ; часть вторая от 05.08.2000 № 117-ФЗ

ТК РФ — Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ

УК РФ — Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ

Закон об информации — Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Закон о СМИ — Закон РФ от 27.12.1991 № 2124-1 «О средствах массовой информации»

Доктрина информационной безопасности — Доктрина информационной безопасности Российской Федерации (утверждена Президентом РФ от 09.09.2000 № Пр-1895)

2. Прочие сокращения

абз. — абзац(-ы)

БРИКС — объединение Федеративной Республики Бразилии, Российской Федерации, Республики Индии, Китайской Народной Республики и Южно-Африканской Республики

гл. — глава(-ы)

ЕАЭС — Евразийский экономический союз

ИКТ — информационно-коммуникационные технологии

ОДКБ — Организация договора коллективной безопасности

ООН — Организация Объединенных Наций

п. — пункт(-ы)

подп. — подпункт(-ы)

разд. — раздел(-ы)

РФ — Российская Федерация
СМИ — средства массовой информации
СНГ — Содружество Независимых Государств
ст. — статья(-и)
ч. — часть(-и)
ШОС — Шанхайская организация сотрудничества
ЭВМ — электронная вычислительная машина

Глава 1
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

В результате изучения данной главы студент должен:

знать содержание понятий «обеспечение информационной безопасности», «правовой режим информационной безопасности» и «организационный режим информационной безопасности»; предметную область правового и организационного режимов информационной безопасности; методику определения функциональной направленности режимов обеспечения безопасности; политические причины возникновения информационного противоборства; затрагиваемые им сферы общественной жизни; методику выявления угроз информационной безопасности Российской Федерации;

уметь определять объект обеспечения информационной безопасности; субъект информационной безопасности; функциональную направленность режимов обеспечения информационной безопасности человека, организации, государства; выявлять субъектов проявления угроз информационной безопасности; общественные отношения, возникающие в связи с деятельностью данных субъектов; определять основные направления установления правового режима информационной безопасности;

владеть навыками определения функциональной направленности режимов обеспечения информационной безопасности, а также выявления и анализа направлений установления правового режима информационной безопасности личности, организации, государства.

Принцип оценивания степени овладения компетенциями. Оценивание степени овладения компетенциями осуществляется на основе проверки качества выполнения самостоятельных работ, защиты сделанных учащимся выводов поставленных проблемных вопросов, раскрытия содержания понятия «обеспечение информационной безопасности», определения функциональной направленности правовых и организационных режимов обеспечения информационной безопасности.

1.1. Информационная безопасность в информационном обществе

1.1.1. Обеспечение информационной безопасности

Понятие «информационная безопасность» получило широкое распространение как в международных, так и в национальных политических документах и правовых нормативных актах.

Впервые понятие «*информационная безопасность*» в национальном законодательстве и политических документах появилось в ст. 2 Закона РФ от 05.03.1992 № 2446-1 «О безопасности», где «информационная безопасность» была выделена в качестве одной из составляющих безопасности Российской Федерации.

В то же время было введено понятие «национальная безопасность Российской Федерации», под которой понималась «безопасность ее многонационального народа как носителя суверенитета и единственного источника власти в Российской Федерации». Впервые в России оно было определено в 1997 г. в Концепции национальной безопасности Российской Федерации. В новой редакции Федерального закона от 28.12.2010 № 390-ФЗ «О безопасности» термины «безопасность» и «национальная безопасность» используются в качестве синонимов.

В проекте концепции информационной безопасности Российской Федерации (1997 г.) национальные интересы России в информационной сфере охватывали три основных аспекта:

— соблюдение конституционных прав и свобод граждан;

— развитие современных телекоммуникационных технологий;

— защита государственных информационных ресурсов от несанкционированного доступа.

Отдельно были выделены национальные интересы в духовной сфере, которые включали сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Данные трактовки понятия «национальная безопасность» и содержания национальных интересов в информационной сфере получили развитие в Доктрине информационной безопасности. В этом документе понятие «информационная безопасность Российской Федерации» было раскрыто как «состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства».

В международных правовых документах понятие «информационная безопасность» впервые появилось в принятой по инициативе Российской Федерации 4 декабря 1998 г. резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности». В резолюции отмечалось, что информационные технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами ООН.

В развитых зарубежных государствах (США, государства Европейского Союза, Канада и др.) защита национальных интересов от злоупотреблений в использовании ИКТ трактуется в контексте «кибербезопасности» и «сетевой безопасности».

«*Кибербезопасность*» рассматривается как защищенность от внешних и внутренних угроз безопасности киберпространства. Данное пространство образуется взаимосвязанной сетью инфраструктур, обеспечивающих реализацию информационных технологий различного назначения. В Стратегии обеспечения национальной безопасности киберпространства США (2011 г.)

отмечается, что политика государства направлена на «защиту от нанесения ущерба работе информационных систем критических инфраструктур и, таким образом, на содействие защите людей, экономики и национальной безопасности США». При этом государство стремится, с одной стороны, уменьшить уязвимость объектов киберпространства к угрозам «прежде, чем они могут нанести ущерб кибернетическим системам, поддерживающим критические инфраструктуры страны, а с другой — гарантировать, что такие нарушения киберпространства будут нечастыми, будут иметь минимальную длительность, с нарушениями можно будет справиться и такие нарушения будут причинять наименьший возможный ущерб».

Понятие «*сетевая безопасность*» связано с явлением более частного порядка — защищенностью глобальных и национальных телекоммуникационных сетей от нежелательного доступа в сеть со стороны третьих лиц, от нарушения сохранности данных и эффективного функционирования сети в целом. Данное понятие можно рассматривать как составляющую понятия «кибербезопасность».

Общая схема явлений, охватываемых понятиями «информационная безопасность», «кибербезопасность» и «сетевая безопасность» представлена на рис. 1.1.

Рис. 1.1. **Соотношение понятий «информационная безопасность», «кибербезопасность» и «сетевая безопасность»**

Комплексное изучение проблем «обеспечения информационной безопасности», в том числе в рамках юридических наук, началось в Российской Федерации сравнительно недавно. Первые результаты комплексных исследований проблемы применительно к юриспруденции были опубликованы в монографиях Ю. М. Батурина[1], И. Л. Бачило, В. Н. Лопатина, М. А. Федотова[2], А. А. Стрельцова[3].

---

[1] *Батурин Ю. М., Жодзишский А. М.* Компьютерная преступность и компьютерная безопасность. М., 1991; *Батурин Ю. М.* Проблемы компьютерного права. М., 1991.

[2] *Бачило И. Л., Лопатин В. Н., Федотов М. А.* Информационное право / под ред. Б. Н. Топорнина. СПб. : Юридический центр Пресс, 2001.

[3] *Стрельцов А. А.* Обеспечение информационной безопасности России. М., 2003; *Стрельцов А. А.* Правовое обеспечение информационной безопасности России: теоретические и методологические основы. Минск : Литфонд, 2005.

В настоящее время количество работ, в которых затрагивается данная тематика, довольно велико. К их числу можно, например, отнести учебники И. Л. Бачило[1], П. У. Кузнецова[2], О. И. Городова[3], монографии Л. В. Тумановой, А. А. Снытникова[4], Л. К. Терещенко[5], А. В. Морозова и Т. А. Поляковой[6] и некоторые другие публикации. Значителен объем статей в периодических изданиях[7]. Правовые вопросы в контексте «информационной безопасности» заняли устойчивое место как отдельное научное направление в интенсивно развиваемой комплексной отрасли российского права — «Информационное право».

В зарубежной литературе первые результаты исследований по данной тематике появились еще в 1994 г.[8] В настоящее время значительное внимание специалистов привлекают проблемы правового регулирования общественных отношений в области обеспечения безопасности киберпространства и сетевой безопасности. В этой области можно выделить, например, работу G. Cecchine, V. Moore[9]. Учитывая, что безопасность киберпространства (кибербезопасность) и сетевая безопасность представляют собой относительно самостоятельные аспекты информационной безопасности, в дальнейшем основное внимание будет уделено рассмотрению положений правовой теории в области обеспечения информационной безопасности.

В структуре регулируемых правом общественных отношений в области обеспечения информационной безопасности выделяются следующие основные составляющие:

— объекты информационной безопасности;

— угрозы информационной безопасности;

— субъекты информационной сферы.

Информационная сфера образуется совокупностью информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Объектами информационной безопасности являются те объекты информационной сферы, которые защищаются от угроз.

---

[1] *Бачило И. Л.* Информационное право. М. : Юрайт ; Высшее образование, 2009.

[2] Информационные технологии в юридической деятельности / под ред. П. У. Кузнецова. М. : Юрайт, 2011.

[3] *Городов О. И.* Информационное право. М. : Проспект, 2009.

[4] *Туманова Л. В., Снытников А. А.* Обеспечение и защита права на информацию. М., 2001.

[5] *Терещенко Л. К.* Правовой режим информации. М. : Юриспруденция, 2007.

[6] *Полякова Т. А.* Правовые основы информационной безопасности в России. М. : Триумф, 2008; *Морозов А. В., Полякова Т. А.* Организационно-правовое обеспечение информационной безопасности. М. : РПА Минюста России, 2013.

[7] Журналы: «Информационное право», «Государство и право», «Информационное общество», «Право и государство» и др.

[8] *Mefford A.* 'Lex Informatica: Foundations of Law on the Internet' (1997/1998). Ind. J. Global Legal Studies. URL: http://lawdigitalcommons.bc.edu/iclr/vol32/iss2/16; DR Johnson and D Post, 'Law and Borders — The Rise of Law in Cyberspace' (1996) 48 Stanford L Rev 1367.

[9] *Cecchine G., Moore V.* Infectious disease and National Security. National Defense Research Institute/ RAND Corporation. (pbk. : alk. paper), WA 110 C387i 2006.

К числу таких объектов могут быть отнесены:

— информация;

— объекты информационной инфраструктуры общества;

— интересы субъектов информационной сферы, которые используют информацию и объекты информационной инфраструктуры для удовлетворения законных интересов человека, общества и государства.

Согласно законодательству *информация* представляет собой сведения, сообщения и данные независимо от формы их представления.

Для обеспечения удобства использования информации субъектами информационной сферы она, как правило, объединяется с помощью соответствующих информационных технологий и компьютерных средств в *базы данных* или *информационные системы*. В данном случае под *базами данных* понимаются представленные в объективной форме совокупности самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью ЭВМ. В свою очередь *информационные системы* рассматриваются как совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Доступ к базам данных и к информационным системам, к необходимой информации осуществляется с использованием информационных технологий. Данные технологии базируются на применении компьютеров, сетей компьютеров, средств и систем телекоммуникационной связи, образующих совместно с необходимыми организационными структурами информационную инфраструктуру общества.

В этом контексте *информационные технологии* могут рассматриваться как процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов, ориентированные на решение конкретных прикладных задач обработки информации, а *информационная инфраструктура* — как система технических средств и организационных структур, обеспечивающих возможность выполнения задач обработки и передачи информации в рамках реализации субъективных прав и позитивных обязанностей субъектов информационной сферы.

Развивая терминологию Стратегии национальной безопасности Российской Федерации[1], под *угрозой информационной безопасности* информации и информационной инфраструктуры будем понимать совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба национальным интересам Российской Федерации.

Национальные интересы РФ, как отмечено в Стратегии национальной безопасности, заключаются:

— в укреплении обороны страны, обеспечении незыблемости конституционного строя, суверенитета, независимости, государственной и территориальной целостности Российской Федерации;

---

[1] Стратегия национальной безопасности Российской Федерации: утверждена Указом Президента РФ от 31.12.2015 № 683.

— укреплении национального согласия, политической и социальной стабильности, развитии демократических институтов, совершенствовании механизмов взаимодействия государства и гражданского общества;

— повышении качества жизни, укреплении здоровья населения, обеспечении стабильного демографического развития страны;

— сохранении и развитии культуры, традиционных российских духовно-нравственных ценностей;

— повышении конкурентоспособности национальной экономики;

— закреплении за Российской Федерацией статуса одной из лидирующих мировых держав.

Субъекты информационной сферы могут быть разделены по целям их участия в общественных отношениях, связанных с информацией и информационной инфраструктурой:

— на участвующих в регулируемых правом общественных отношениях по поводу объекта безопасности в качестве обладателей информации или обладающих правомочиями владеть, пользоваться и распоряжаться составляющими информационной инфраструктуры;

— реализующих интересы, направленные на нанесение ущерба свойствам объектов информационной безопасности;

— осуществляющих деятельность в области обеспечения информационной безопасности информации и информационной инфраструктуры.

Термин **«информационная безопасность»** может трактоваться, с одной стороны, как состояние защищенности человека, общества и государства в информационной сфере, а с другой — как результат деятельности по обеспечению информационной безопасности.

В свою очередь, **обеспечение информационной безопасности** логично рассматривать как деятельность по противодействию угрозам безопасности человека, общества и государства в информационной сфере, осуществляемую с использованием выделенных для этого сил и средств.

Задание для размышления

Специалисты высказывают различные взгляды на формулировку дефиниции «безопасность». Так, в Законе РФ «О безопасности», в Концепции национальной безопасности Российской Федерации, в Доктрине информационной безопасности понятие «безопасность» раскрывалось как «состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства».

Позже, в Стратегии национальной безопасности Российской Федерации данное понятие раскрывается как «состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечивается реализация конституционных прав и свобод граждан, достойное качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие»[1].

Попытайтесь определить, в чем заключаются различия между приведенными формулировками и предметами нормативных и политических актов Президента РФ?

[1] Стратегия национальной безопасности Российской Федерации. Указ Президента Российской Федерации от 31.12.2015 № 683.

Важно запомнить

Понятия «информационная безопасность» и «обеспечение информационной безопасности» всегда связаны с конкретным объектом, который представляет интерес для субъекта обеспечения информационной безопасности. Определение объекта обеспечения информационной безопасности осуществляется заинтересованным субъектом (человеком, организацией, руководителем органа государственной власти или муниципального образования, государственным должностным лицом).

Система обеспечения информационной безопасности Российской Федерации образуется соответствующими силами и средствами.

Силы обеспечения информационной безопасности Российской Федерации включают Вооруженные Силы РФ, другие войска, воинские формирования и органы, в которых федеральным законодательством предусмотрена военная и (или) правоохранительная служба, а также федеральные органы государственной власти, принимающие участие в обеспечении национальной безопасности государства на основании законодательства РФ.

Средства обеспечения информационной безопасности Российской Федерации образуются совокупностью технологий (технические, программные, лингвистические, правовые, организационные средства, включая телекоммуникационные каналы), используемых в системе обеспечения информационной безопасности для сбора, формирования, обработки, передачи или приема информации о состоянии национальной безопасности и мерах по ее укреплению.

Реализация функций обеспечения информационной безопасности осуществляется управомоченными лицами, федеральными органами исполнительной власти или государственными должностными лицами посредством использования сил и средств, предназначенных для противодействия угрозам объектам информационной безопасности, видов обеспечения информационной безопасности и прежде всего правового и организационного обеспечения.

1.1.2. Правовое обеспечение информационной безопасности

Правовое обеспечение общественных отношений, связанных с противодействием угрозам информационной безопасности субъекта (человека, общества и государства), является одним из важнейших видов обеспечения информационной безопасности.

Правовое обеспечение информационной безопасности представляет собой относительно самостоятельное направление информационного права, образуемое совокупностью правовых режимов, принципов и норм, закрепленных в законодательстве РФ и источниках международного права. В рамках данного направления информационного права регулируются общественные отношения по поводу обеспечения безопасности, прежде всего информации и информационной инфраструктуры, используемых человеком, обществом и государством для удовлетворения законных интересов, реализации прав и выполнения юридических обязанностей.

Понятие «*правовой режим*» широко используется в праве. Как отмечал С. С. Алексеев[1], «правовой режим» представляет собой порядок регулирования, выраженный в многообразном комплексе правовых средств, характеризующих особое сочетание взаимодействующих между собой дозволений, запретов и позитивных обязываний, создающих особую направленность регулирования.

В данном случае эту особую направленность правового регулирования задает использование правовых средств для противодействия угрозам информационной безопасности. Именно это отражает стремление использовать потенциал права для решения важной социальной задачи — обеспечения безопасности информации, информационных технологий и информационной инфраструктуры в интересах человека, организаций, в деятельности которых проявляется жизнь общества либо государства и его органов.

Правовой режим информационной безопасности определяется правомочиями субъектов правоотношений по обладанию защищаемой информацией, свойствами защищаемых объектов безопасности, направленностью на противодействие угрозам нарушения потребительски важных свойств объекта безопасности, степенью определенного законодателем участия федеральных органов исполнительной власти, других органов и организаций в выявлении угроз, в пресечении их проявлений, в определении субъектов, виновно осуществляющих действия по реализации угроз, в предупреждении проявления угроз информационной безопасности и в ликвидации последствий их проявления, в применении установленной законом ответственности к лицам, виновным в проявлении угроз.

Правовой режим обеспечения информационной безопасности образуется совокупностью субъективных прав, позитивных обязанностей и запретов, образующих функциональную направленность правового регулирования на противодействие угрозам безопасности объектов информационной сферы, на безопасное удовлетворение законных интересов человека, общества и государства.

По *механизму формирования* правовые режимы информационной безопасности могут быть разделены на международные и национальные.

Международные правовые режимы информационной безопасности образуются совокупностью принципов и норм, закрепленных в основных источниках международного права: в международных конвенциях, устанавливающих правила, определенно признанные государствами; в международном обычае как доказательстве всеобщей практики, признанной в качестве правовой нормы; в общих принципах права, признанных цивилизованными нациями. При определении трактовок норм международного права могут быть использованы судебные решения и доктрины наиболее квалифицированных специалистов по публичному праву различных наций.

Национальные правовые режимы информационной безопасности образуются совокупностью институтов, принципов и норм, закрепленных в источниках международного права, национальном законодательстве, а также в актах нормативного технического регулирования в области обе-

---

[1] *Алексеев С. С.* Право: азбука — теория — философия. Опыт комплексного исследования. М., 1999. С. 372.

спечения безопасности информации, баз данных, информационных технологий и систем, информационной инфраструктуры.

Субъекты регулируемых правом общественных отношений по поводу обеспечения безопасности информации и информационной инфраструктуры разделяются на три основные группы.

Субъекты, заинтересованные в использовании информации и информационной инфраструктуры для осуществления экономической, культурной, политической и иной деятельности, осуществления функций государства. Такие субъекты действуют в рамках правомочий, предоставленных им как обладателям информации, как владельцам или собственникам средств, составляющих информационную инфраструктуру, как операторам информационных систем различного вида, как управомоченным лицам в области установления правовых режимов тайн.

Субъекты, уполномоченные в области осуществляения деятельности по обеспечению информационной безопасности, т.е. в деятельности по противодействию угрозам безопасности, обладают правомочиями, позволяющими им планировать и осуществлять мероприятия по защите объектов информационной безопасности от угроз, заниматься надзорной и правоприменительной практикой, правоохранительной деятельностью, проведением оперативно-следственных мероприятий.

Субъекты, использующие уязвимости в системах обеспечения безопасности информации и информационной инфраструктуры для разработки и применения специальных вредоносных информационных технологий в противоправных политических или корыстных целях, с помощью правового режима информационной безопасности приобретают статус лиц с деликтным поведением, наносящим ущерб интересам и объектам интересов других лиц. Против таких лиц направлена деятельность правоохранительных органов, независимо от того, находятся ли они на территории нашего государства или за рубежом.

Угроза информационной безопасности информации и информационной инфраструктуры представляет собой совокупность условий и факторов, наносящих или потенциально способных нанести ущерб объектам обеспечения информационной безопасности.

Правовое обеспечение информационной безопасности регулирует отношения в области противодействия угрозам информационной безопасности человека, отдельных организаций и Российской Федерации в целом, во многом определяя структуру и принципы других видов обеспечения информационной безопасности и, в частности, организационного обеспечения.

Нормы и институты правового обеспечения информационной безопасности закреплены в международных договорах РФ, нормативных правовых актах национального законодательства. К числу важных источников права в данной области следует отнести Конституцию РФ, Устав ООН, Закон об информации, Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне», Стратегию национальной безопасности Российской Федерации и другие нормативные правовые акты Президента РФ, уполномоченных федеральных органов исполнительной власти.

Общая структура правового режима информационной безопасности представлена на рис. 1.2.

Рис. 1.2. **Общая структура правового режима информационной безопасности**

1.1.3. Организационное обеспечение информационной безопасности

Вторым не менее важным видом обеспечения информационной безопасности является организационное обеспечение.

Организационное обеспечение информационной безопасности образуется совокупностью нормативных и методических документов, разрабатываемых и вводимых в действие уполномоченными лицами в рамках правоприменительной практики по реализации правовых режимов информационной безопасности, а также мероприятий, осуществляемых специально выделяемыми силами и с применением средств обеспечения информационной безопасности.

Мероприятие, осуществляемое в рамках организационного обеспечения информационной безопасности, представляет собой систему согласованных по целям, времени и субъектам их осуществления взаимосвязанных мер и действий сил обеспечения информационной безопасности.

Виды мероприятий условно могут быть классифицированы по областям деятельности: формирование и обеспечение функционирования системы нормативных и технических средств противодействия угрозам; формирование, подготовка и использование кадрового потенциала; финансовое обеспечение; методическое обеспечение выполнения мероприятий и т.д.

В рамках организационного обеспечения принимаются в том числе меры, направленные на развитие научных исследований в области повышения устойчивости информационной инфраструктуры к проявлению угроз; на содействие в установленном законодательством порядке работе общественных организаций, ставящих своей целью противодействие угрозам информационной безопасности и определение форм возможного взаимодействия с ними; на согласование деятельности федеральных органов исполнительной власти и органов исполнительной власти субъектов РФ в области противодействия угрозам; на развитие системы массовой информации, способной содействовать предоставлению гражданам, другим лицам, проживающим на территории государства, возможности получения доступа к достоверной информации об интересующих их событиях общественной

жизни как внутри страны, так и за рубежом; на принятие мер по недопущению пропаганды и агитации, возбуждающей социальную, расовую, национальную или религиозную ненависть и вражду, пропаганды социального, расового, национального, религиозного или языкового превосходства.

Общая схема организационного режима информационной безопасности представлена на рис. 1.3.

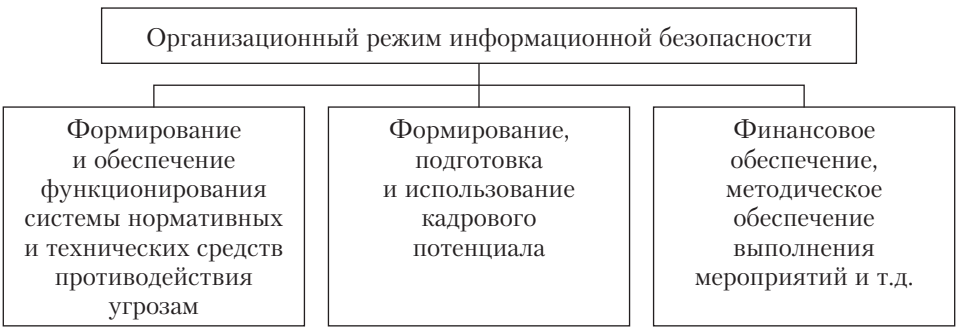

Рис. 1.3. **Общая схема организационного режима информационной безопасности**

1.1.4. Методика выявления функциональной направленности режима информационной безопасности

Как было отмечено выше, важной характеристикой режима информационной безопасности объекта является его функциональная направленность. Она определяется следующими основными факторами:

— свойствами объекта, на который направлен режим безопасности;

— видами угроз безопасности информации и информационной инфраструктуры, на противодействие которым сориентирован режим информационной безопасности;

— целью противодействия угрозам информационной безопасности.

Определение свойств объекта, на которые направлен режим информационной безопасности, осуществляется на основе анализа правоустанавливающих документов, объема и содержания субъективных прав и позитивных обязанностей уполномоченного лица, его интересов, связанных с объектом информационной безопасности.

Так, если объектом обеспечения безопасности является информационная система персональных данных, то субъектом, устанавливающим режим информационной безопасности, может быть оператор информационной системы. При этом режим информационной безопасности в соответствии с федеральным законодательством должен обеспечить противодействие всем возможным угрозам безопасности сбора, хранения и обработки персональных данных граждан.

Виды угроз безопасности информации и информационной инфраструктуры объекта безопасности классифицируются, как правило, либо по способу их реализации (несанкционированный доступ, неправомочное использование, нарушение целостности или конфиденциальности и т.п.), либо по субъектам реализации этих угроз: государства, террористические и другие

преступные организации либо физические лица. Выявление видов наиболее опасных угроз осуществляется на основе анализа уязвимостей объекта безопасности и возможности их использования для нанесения ущерба объекту.

Цели противодействия угрозам безопасности информации и информационной инфраструктуры устанавливаются уполномоченным лицом в соответствии с требованиями законодательства в рамках его субъективных прав и позитивных обязанностей.

При выявлении целей обеспечения информационной безопасности Российской Федерации необходимо базироваться на положениях политических документов Президента РФ, который в соответствии с Конституцией РФ определяет основные направления государственной внешней и внутренней политики, в том числе в области обеспечения информационной безопасности.

При выявлении цели обеспечения информационной безопасности коммерческой организации основным источником нормативных установок являются положения уставных документов данной организации.

Общая схема методики выявления функциональной направленности режима информационной безопасности представлена на рис. 1.4.

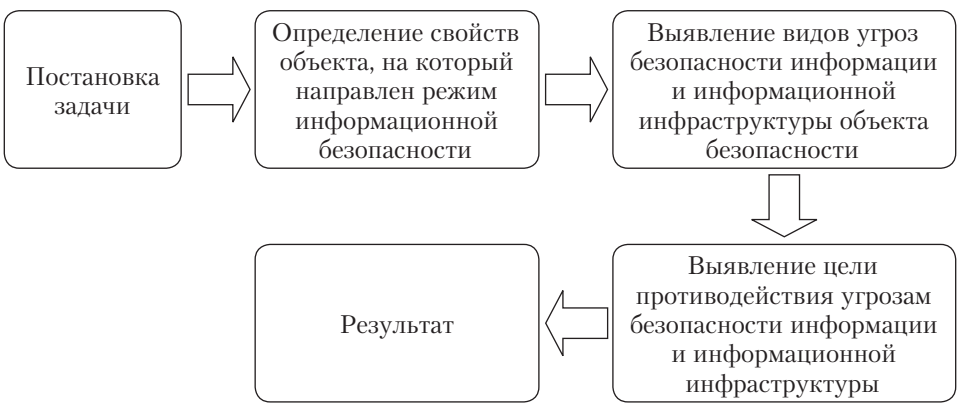

Рис. 1.4. **Общая схема методики выявления функциональной направленности режима информационной безопасности**

Задание для размышления

Выявите цели правового режима обеспечения безопасности персональных данных (см. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»), а также цели установления международного правового режима обеспечения международной безопасности, формирование которого предусмотрено Основами государственной политики Российской Федерации в области международной информационной безопасности до 2020 года (утверждены Президентом РФ 24.07.2013 № Пр-1753).

1.1.5. Информационное общество и развитие института правового и организационного обеспечения информационной безопасности

Современный период характеризуется формированием информационного общества. Что же такое информационное общество? Оно представляет собой стадию развития цивилизации, на которой основным фактором

развития производственных сил и производственных отношений, наряду с потребностями субъектов социальной жизни и возможностями общества по их удовлетворению, становятся[1]:

— сокращение издержек производства, связанных с его адаптацией к увеличению и глобализации рынка товаров и услуг;

— возможность использования информационной инфраструктуры системы массовой информации для формирования спроса за счет виртуального управления потребностями людей;

— повышение потребительских свойств товаров и услуг за счет использования накопленных человечеством знаний и совершенствования методов обработки информации;

— сокращение времени продвижения инновационных товаров и услуг на глобальный рынок.

Уровень влияния данных факторов в значительной степени определяется: динамичностью развития информационной инфраструктуры; уровнем и интенсивностью модернизации промышленности, отрасли информационных услуг; соответствием потенциала производительных сил общества потребностям развития экономики; степенью развитости культуры массового производства товаров и услуг и системы массового потребления; степени интеграции в международную систему разделения труда и глобализации потребления; оперативности использования в производстве новых знаний и достижений науки и других факторов.

В обществе с обостренным противостоянием политических сил, недостаточно высоким уровнем политической культуры неизбежно возникают угрозы использования ИКТ для разрешения политических противоречий. В связи с этим противодействие угрозам становится неотъемлемой составляющей обеспечения безопасности общества, социальной стабильности и устойчивого прогрессивного развития.

В международных декларациях[2], в материалах Всемирной встречи на высшем уровне по информационному обществу, прошедшей в 2003 и 2005 гг. в Женеве (Швейцария) и Тунисе (Тунис)[3], в политических документах Президента РФ по вопросам развития информационного общества в Российской Федерации была отмечена важность решения вопросов обеспечения информационной безопасности. В частности, в документах Рабочей группы по управлению Интернетом[4] отмечалась обязанность правительств: разрабатывать, координировать и осуществлять соответствующую государственную политику на национальном, региональном и международном уровнях; принимать соответствующие законы, положения и стан-

---

[1] Стратегия развития информационного общества в Российской Федерации (утверждена Президентом РФ 07.02.2008 № Пр-212).

[2] Окинавская хартия глобального информационного общества 2000 г., Форталезская (15 июля 2014 г.) и Уфимская (9 июля 2015 г.) декларации глав государств БРИКС, Душанбинская (12 сентября 2014 г.) и Уфимская (10 июля 2015 г.) декларации глав государств — членов ШОС.

[3] Построение информационного общества — глобальная задача в новом тысячелетии: Декларация принципов, 12 декабря 2003 г., Женева; Тунисское обязательство. 2005 г. Тунис.

[4] См. п. 29—82 Тунисской программы для информационного общества, 2005 г.

дарты; выполнять надзорные функции; бороться против киберпреступности; регулировать споры и проводить арбитраж.

Формирование информационного общества сопровождается расширением области общественных отношений, объектами которых являются информация и информационная инфраструктура. Часть таких общественных отношений регулируется правом, что создает основу для влияния правовых средств, составляющих содержание правовых режимов информационной безопасности, на данные отношения; для стимулирования эффективного использования информации и информационной инфраструктуры в практической жизни человека, организаций, органов государственной власти; для укрепления государственных гарантий пользования признанными правами и свободами человека и гражданина в соответствии с принципами и нормами международного права, а также принципами и нормами национального законодательства.

Данное обстоятельство обусловливает возрастание роли права в жизни общества, создает условия для обособления правовых норм и институтов, а также закрепляющих их нормативных правовых актов, в отдельное направление информационного права — правовое обеспечение информационной безопасности. Предмет данного направления составляют правовые воздействия на общественные отношения в области противодействия угрозам безопасности информации и информационной инфраструктуры.

1.2. Современное информационное противоборство и обеспечение информационной безопасности

Особое значение в условиях глобализации приобретают вопросы информационного противоборства в целях обеспечения информационной безопасности.

1.2.1. Общие положения

Информационное противоборство представляет собой особый способ разрешения межгосударственных противоречий посредством:

— использования «силовых» механизмов давления на политических противников угрозой нарушения устойчивости функционирования и безопасности использования глобальной и национальной информационных инфраструктур, нарушения целостности, доступности и конфиденциальности информации, передаваемой по каналам связи, хранящейся и обрабатываемой в информационных и компьютерных сетях;

— навязывания международному общественному мнению определенных политических трактовок тех или иных важных событий международной и национальной жизни посредством использования значительного преимущества в контролируемом потенциале международной системы массовой информации;

— провоцирования политических сил общества противостоящего государства на насильственную смену политического (в том числе демократического) режима, оказания финансовой и иной помощи данным поли-

тическим силам в пропаганде их идеологических позиций и взглядов для захвата власти и последующего разрешения межгосударственных противоречий на условиях, выгодных государству — инициатору переворота.

Сегодня принято выделять два основных вида информационного противоборства между государствами: информационно-техническое и идеологическое.

Информационно-техническое противоборство — это способ разрешения межгосударственных противоречий между двумя и более государствами посредством нанесения ущерба информационным системам, процессам и ресурсам, критически важным и иным структурам; подрыва политической, экономической и социальной систем; дестабилизации общества и государства.

Идеологическое информационное противоборство — это способ разрешения межгосударственных противоречий посредством использования информационного пространства и информационных технологий для оказания «давления» на политическое руководство противостоящего государства (государств).

В данном случае не рассматриваются вопросы использования для достижения тех же целей так называемых «традиционных (кинетических)» видов оружия.

Классификация видов информационного противоборства представлена на рис. 1.5.

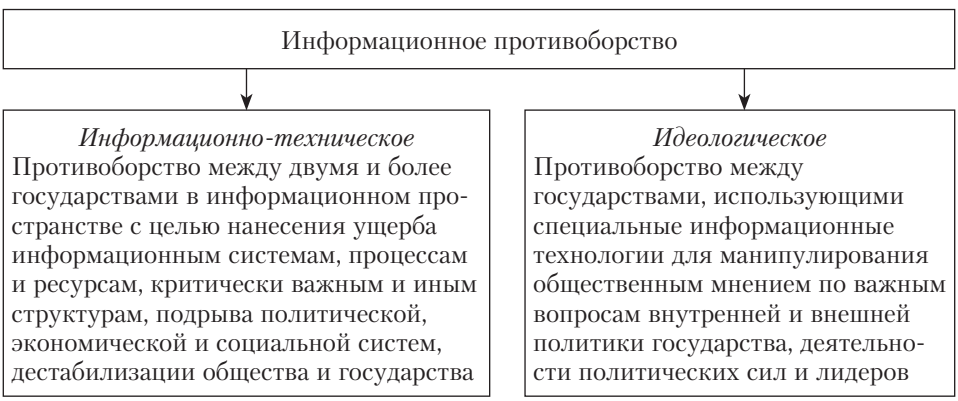

Рис. 1.5. **Классификация видов информационного противоборства**

Опасность угроз национальной безопасности Российской Федерации, возникающих в связи с использованием другими государствами средств и методов информационного противоборства, отмечена в Основах государственной политики в области международной информационной безопасности на период до 2020 года, где к числу основных угроз международной информационной безопасности отнесены:

— использование информационных и коммуникационных технологий в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных действий и актов агрессии, направленных на ущемление суверенитета, нару-

шение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

— вмешательство во внутренние дела суверенных государств, нарушение общественного порядка, разжигание межнациональной, межрасовой и межконфессиональной вражды, пропаганда расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию.

1.2.2. Информационно-техническое противоборство

Появление информационных технологий (процессов, методов поиска, сбора, хранения, обработки, предоставления, распространения информации и способов осуществления таких процессов и методов, ориентированных на решение конкретных прикладных задач обработки информации), которые могут быть использованы в качестве средства «силового» воздействия на объекты информационной инфраструктуры противостоящей стороны, давления на ее политическое руководство, представляет собой новое явление в системе международных отношений.

Впервые опасность такого использования средств информатизации была отмечена в 1998 г. в специальном послании по проблеме международной информационной безопасности Министра иностранных дел РФ в адрес Генерального секретаря ООН. В документе особый акцент был сделан на необходимость предотвращения появления принципиально новой — информационной — сферы конфронтации и развязывания принципиально новых конфликтов.

С тех пор по просьбе Генеральной Ассамблеи ООН и поручению Генерального Секретаря ООН четырежды собиралась Группа правительственных экспертов ООН, в итоговых докладах которой отмечается[1]: «...все страны заинтересованы в поощрении использования ИКТ в мирных целях. Страны также заинтересованы в предотвращении конфликтов, возникающих в результате использования ИКТ. Общее понимание в отношении норм, правил и принципов, применимых к использованию ИКТ государствами, и добровольные меры укрепления доверия могут играть важную роль в поддержании мира и безопасности».

В рамках реализации государственной политики Российской Федерации в области формирования системы международной информационной безопасности Президент РФ В. В. Путин поставил задачу «содействия подготовке и принятию государствами — членами ООН, международных актов, регламентирующих применение принципов и норм международного гуманитарного права в сфере использования ИКТ»[2].

В чем же заключается принципиальное отличие информационных технологий как средства «силового» воздействия на международные отно-

---

[1] Доклад группы правительственных экспертов ООН: представлен Генеральным Секретарем ООН 68-й сессии Генеральной Ассамблеи ООН 24 июня 2013 г.

[2] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24.07.2013 № Пр-1753).

шения от традиционных видов оружия и чем обусловлены трудности применения существующего международного права безопасности к киберпространству?

Во-первых, несмотря на общее мнение о возможности использования ИКТ в военных целях, практически все специалисты сходятся во мнении, что ИКТ не являются оружием. И в российской, и в англоязычной литературе ИКТ часто рассматривается как синоним понятия «информационные технологии». В Законе об информации термин «*информационные технологии*» раскрывается как «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов». В англоязычной литературе он трактуется в более общем смысле как понятие, интегрирующее все телекоммуникационные средства, компьютеры, а в случае необходимости — специальное и общее программное обеспечение, память, системы аудио-, видеовизуализации, используемые пользователем для накопления, передачи, обработки информации. Термин «оружие» в российской литературе определяется как «всякое средство, приспособленное, технически пригодное для нападения или защиты, а также совокупность таких средств»[1]. В англоязычной литературе термин «оружие» определяется почти аналогично.

Во-вторых, общеизвестно, что любое использование информационных технологий (в том числе и вредоносное использование в военно-политических целях) является невидимым для человека, и поэтому для фиксации особенностей реализации технологии на том или ином компьютере или в компьютерной сети требуются специальные технические и программные средства.

Следствием этого являются практически неограниченные возможности фальсификации заинтересованными государствами:

— фактов вредоносного использования против них информационных технологий;

— сведений, позволяющих идентифицировать государство, осуществляющее или допустившее вредоносное использование информационных технологий во вред государству-жертве, что позволяет произвольным образом приписывать тому или иному государству ответственность за такую деятельность;

— сведений о превышении в рамках вредоносного использования информационных технологий так называемых «пороговых значений», которые, по мнению специалистов, порождают право на индивидуальную или коллективную самооборону в смысле ст. 51 Устава ООН.

Таким образом, при использовании информационных технологий в качестве средства «силового» давления отсутствует возможность доверять информации других государств о фактах использования ИКТ в качестве угрозы силой или силы в международных отношениях, а также о возникновении правоотношений по поводу права на индивидуальную или коллективную самооборону.

---

[1] *Ожегов С. И.* Словарь русского языка. М. : Русский язык. 1986. С. 394.

Задание для размышления

Подумайте, что необходимо сделать для решения проблемы объективизации фактов вредоносного использования информационных технологий против объектов информационной инфраструктуры других государств и для атрибуции субъектов такого использования информационных технологий?

В современной внешней политике трудно основывать свои решения на предположениях о соблюдении всеми государствами — членами ООН начал нравственности и о наличии у этих государств доверия к имеющимся у государства-жертвы данным о факте и последствиях вредоносного использования против нее информационных технологий. Новая история редко дает основания не сомневаться в нравственности поведения политиков некоторых государств, а современная история дает очень много оснований для недоверия к информации, которая официально распространяется некоторыми государствами (например, анонсированное в свое время Государственным секретарем США К. Пауэллом с трибуны Совета Безопасности ООН утверждение о наличии оружия массового поражения в Ираке, которое так и не было найдено, но дало США возможность применения вооруженной силы против Ирака).

Важной особенностью использования информационных технологий в качестве средства «силового» давления на национальную информационную инфраструктуру других государств является отсутствие у государств-членов ООН каких бы то ни было международных обязательств, связанных с обеспечением устойчивости функционирования сети Интернет. Вряд ли таковыми можно считать обязательства организации *ICANN*, которая записала себе в уставные документы обеспечение безопасности управления системой доменных имен. Одновременно не вызывает сомнений, что нарушение функционирования сети Интернет как основы глобальной информационной инфраструктуры при определенных политических обстоятельствах может спровоцировать международный спор (вооруженный конфликт), не связанный с вредоносным использованием информационных технологий.

В-третьих, национальные правоприменители (лица, принимающие политические решения) при решении вопроса о придании тем или иным сведениям значимости юридических фактов, подтверждающих противоправную угрозу силой или ее применения посредством злонамеренного использования ИКТ, а также злонамеренное использование ИКТ для осуществления вооруженного нападения, вынуждены основывать свои решения на информации, полученной от технических средств регистрации. Регистрируемые события, по мнению правоприменителя, с достаточной степенью уверенности позволяют ему судить о наличии явных или скрытых признаков нападений на объекты национальной или региональной информационных инфраструктур.

Этими обстоятельствами обусловлено интенсивное развитие правоохранительными и правоприменительными структурами соответствующих национальных и региональных систем выявления признаков нарушения

международного права посредством злонамеренного использования ИКТ против объектов национальной и региональной информационных инфраструктур.

Задание для размышления

Попробуйте объяснить, почему при проведении оперативно-следственных мероприятий в пределах юрисдикции государства проблемы невидимости последствий вредоносного использования информационных технологий менее актуальны, чем в международных отношениях?

В то же время такие национальные и региональные системы малопригодны для разрешения межгосударственных споров по данному поводу, так как единственными средствами доказывания позиций сторон, которые могут быть приняты к рассмотрению как в Совете Безопасности ООН, так и в Международном Суде, являются официальные заявления уполномоченных лиц. Политическое рассмотрение значительной части подобных обращений в Совете Безопасности ООН имеет перспективу лишь в том случае, когда интересы постоянных членов Совета Безопасности ООН совпадают или близки. В остальных случаях единственным средством разрешения споров становится рассмотрение их юридической составляющей в Международном Суде. В то же время, как отметил Международный Суд в решении по делу Никарагуа[1], он «...может по своему усмотрению оценивать значимость различных элементов доказательства». «Что касается заявлений представителей государств, порой на самом высоком уровне, то Суд придерживается мнения, что такие заявления имеют особую доказательную ценность, когда они подтверждают факты или поведение неблагоприятного характера для государства, представленного лицом, сделавшим это заявление». «Что касается письменных свидетельств под присягой и заявлений под присягой, сделанных членами правительства, Суд считает, что может, конечно, сохранить части этого средства доказывания, которые могут рассматриваться в качестве противоречащих интересам или утверждениям того государства, представителем которого является данный свидетель; в остальном к доказательствам следует относиться с большой осторожностью».

Таким образом, для создания условий справедливого рассмотрения споров по поводу нарушения международного права посредством злонамеренного использования ИКТ в киберпространстве представляется важным создание единой системы (возможно, на базе соответствующих национальных и региональных систем) регистрации фактов угрозы силой или ее применения, а также «вооруженного нападения» посредством злонамеренного использования ИКТ. При этом национальные и региональные элементы системы регистрации должны быть сертифицированы по единым стандартам, а обслуживающий эти устройства персонал — обладать необходимыми международными иммунитетом и привилегиями.

[1] Дело о военной и военизированной деятельности в Никарагуа и против Никарагуа (Никарагуа против Соединенных Штатов Америки): решение Международного Суда от 27 июня 1986 г.

К системе сертификации можно было бы предъявить следующие требования:

— доверие к показаниям средств технической фиксации нарушений норм международных договоров со стороны участников спора;

— мониторинг всех событий, составляющих юридические факты, порождающие право индивидуальной или коллективной самообороны;

— объективность информации технических средств мониторинга и возможность их представления в качестве средства доказательства в Международном Суде при рассмотрении соответствующих споров.

Общая структура проблем применения международного права для противодействия информационно-техническому противоборству представлена на рис. 1.6.

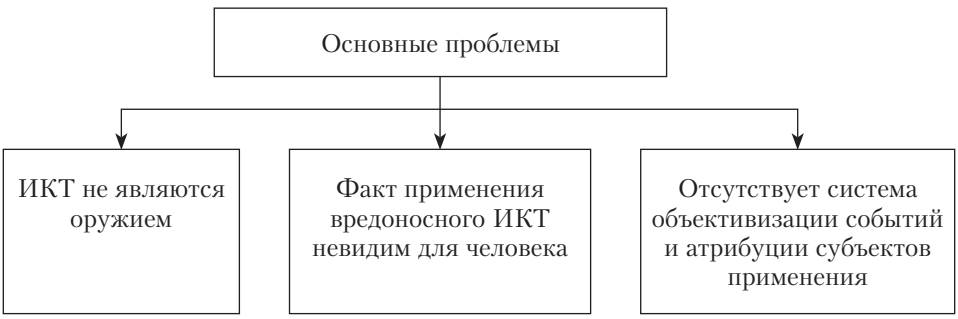

Рис. 1.6. **Общая структура проблем применения международного права для противодействия информационно-техническому противоборству**

Задание для размышления

Попробуйте объяснить, зачем нужна система сертификации элементов системы регистрации опасных событий в киберпространстве?

1.2.3. Идеологическое противоборство

На современном этапе развития международных отношений важным фактором обеспечения социальной стабильности общества является противодействие угрозам вмешательства государств во внутренние дела других государств, и в частности в дела Российской Федерации. Недопустимость такого вмешательства закреплена в Декларации о принципах международного права[1], Заключительном акте Совещания о безопасности и сотрудничеству в Европе[2] и других международных правовых договорах.

Реальная политика некоторых государств в нарушение данного обязательства часто включает мероприятия по пропаганде на территории дру-

[1] Принцип, касающийся обязанности в соответствии с Уставом не вмешиваться в дела, входящие во внутреннюю компетенцию любого другого государства. Декларация о принципах международного права, касающихся дружественных отношений и сотрудничества между государствами в соответствии с Уставом Организации Объединенных Наций, 1970.

[2] Заключительный Акт Совещания по безопасности и сотрудничеству в Европе, 1975. Декларация принципов, которыми государства-участники будут руководствоваться во взаимных отношениях (п. VI «Невмешательство во внутренние дела»).

гих государств идеологии сил, не получивших легитимного права участия в политической жизни общества, — политических сил других государств.

Информационное противоборство в идеологической области (идеологическое противоборство) представляет собой форму разрешения межгосударственных противоречий посредством использования пропаганды в глобальной и национальной информационных инфраструктурах для снижения уровня социальной устойчивости общества, доверия населения к политическому руководству и реализуемой им политике, а в конечном итоге — для смены политического руководства путем вооруженного или невооруженного политического переворота, демократических перевыборов.

В этих условиях одной из важных составляющих государственной политики является противодействие такому вмешательству как правовыми, так и организационными методами.

Правовые средства противодействия использованию идеологической пропаганды для вмешательства во внутренние дела государства, включающие нормы и институты национального законодательства и нормы международного права, только начинают формироваться.

Основными объектами идеологического противоборства выступают прежде всего общественные отношения, связанные с процессами развития политического сознания и формирования общественного мнения, так как именно эти социальные явления определяют, с одной стороны, «предрасположенность» общества к поддержке тех или иных политических установок и выдвигающих их политических сил, а с другой — к поддержке конкретных политических мероприятий и лидеров данных политических сил.

Политическое сознание может быть определено как отражение политического бытия в общественном сознании.

Политическое бытие представляет собой совокупность проявлений деятельности человека в сфере политики, которая существует в форме политических отношений, власти, деятельности политических институтов и политических лидеров. Политическое бытие образуется совокупностью политической деятельности субъектов общественной жизни, проявляющейся в «организации и проведении политических акций в целях воздействия на принятие государственными органами решений, направленных на изменение проводимой ими государственной политики, а также в формировании общественного мнения в указанных целях»[1].

В философии общественное сознание раскрывается как «воззрения людей в их совокупности на явления природы и социальную реальность, выраженные в созданных обществом естественном или искусственном языках, творениях духовной культуры, социальных нормах и взглядах социальных групп, народа и человечества в целом»[2].

«Воззрения людей» существуют в виде информации, которая представляет собой «результаты отражения движения объектов материального

---

[1] Федеральный закон от 13.07.2012 № 121-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования деятельности некоммерческих организаций, выполняющих функции иностранного агента». ст. 2, п. 2.

[2] *Спиркин А. Г.* Философия. М. : Гардарики, 2002. С. 637.

мира, запечатленные в организме или сообществе организмов и используемые ими для адаптации к изменениям окружающей действительности»[1]. Как известно, философская категория «отражение» охватывает проявления свойств одних объектов материального мира воспроизводить в своей природе особенности других, взаимодействующих с ними материальных объектов[2], т.е. свойство сохранять «следы» некоторых свойств объектов взаимодействия.

К числу «объектов», обладающих свойством отражения, относятся индивид и социум. Результаты отражения реальной действительности индивидом (индивидуальное сознание) проявляются в сведениях, знаниях, оценках, предпочтениях, потребностях, интересах и мотивах поведения и других свойствах индивида как личности. Они также проявляются в знаниях, оценках, идеях, нормах, традициях, обычаях, языке, пользование которыми поощряется или не поощряется социальными единениями, обществом в целом на данном историческом этапе общественного развития. Результаты отражения реальной действительности в индивидуальном и общественном сознании проявляются, прежде всего, в духовной культуре индивида, его поведении и предпочтениях, правилах взаимодействия с другими индивидами, в отношениях с определенными социальными группами и обществом, а также в традициях, обычаях, языках, предпочтениях социальных групп, составляющих общество.

В культурологии под духовной культурой понимается совокупность знаний, нравственных ценностей, обычаев, традиций, стереотипов поведения, политических, идеологических, религиозных и иных мировоззренческих представлений о рациональном общественном устройстве, востребованных социальными единениями на данном историческом этапе развития. Духовная культура объединяет наиболее характерные для членов общества образы мысли и действий, основанные на нравственных ценностях, нормах, традициях, обычаях, критериях, оценках, объединяющих людей по этим признакам в единую социальную общность[3]. В этом качестве духовная культура является тем социальным преобразователем, посредством которого информация, получаемая в результате отражения реальной действительности (включая ее проявление в виде общественного мнения), становится мотивацией политической деятельности наиболее активных социальных сил.

Как явление духовной жизни индивидов, духовная культура определяет индивидуальное мировоззрение членов общества. Она формируется на основе источников информации о культуре (слов, символов, знаков, изображений: печатной продукции, в том числе научной, художественной и иной литературы, произведений устного народного творчества, произведений искусства, таких как картины, фрески, ноты, исполнительские произведения, схемы, чертежи и т.п.), фиксирующих исторический опыт данного

---

[1] *Стрельцов А. А.* Обеспечение информационной безопасности России. М. : Изд-во МЦНМО, 2002. С. 20.

[2] Там же. С. 150.

[3] Общая социология / под общ. ред. А. Г. Эфендиева. М. : ИНФРА-М, 2002. С. 330.

общества и позволяющих осуществлять передачу составляющих духовной культуры другим социальным единениям, другим поколениям. Тем самым она выступает в качестве средства детерминирования (стандартизации[1]) с помощью прошлого, накопленного опыта поведения конкретной социальной общности в условиях бесконечного многообразия современной политической жизни. Можно сказать, что духовная культура — это историческое наследие, которое формирует наше политическое сознание и тем самым обрекает нас на определенное поведение в настоящем и в будущем.

Политическое сознание является наиболее общей категорией, отражающей всю совокупность чувственных и теоретических, ценностных и нормативных, рациональных и подсознательных представлений человека, которые опосредуют его отношения как с политическими институтами власти, так и между собой по поводу участия в управлении делами общества и государства[2]. В общепринятой мировой традиции политическое сознание рассматривается в широком контексте, как вся совокупность психического отражения политики, как ее субъектный компонент, проявляющий себя на разных уровнях, в различных ситуациях[3].

Задание для размышления

Попробуйте объяснить, что такое «политика» и как это явление общественной жизни соотносится с «правом»?

Политическое сознание проявляется, в частности, в общественном мнении, в связи с чем общественное мнение становится объектом идеологического противоборства. В данном случае общественное мнение может рассматриваться как прежде всего ценностное отношение (позиция: одобрение, поддержка, приемлемость и т.д.) общества к жизненно значимому для него вопросу (проблеме), которое формируется на основе обобщения мнений наиболее влиятельных общественных групп. Специалисты в области взаимодействия с общественностью[4], в чью компетенцию входит определение способов, механизмов, средств воздействия на общественное мнение, полагают, что основными субъектами общественного мнения являются социальные группы, способные оказать заметное влияние на реализацию политики.

Формирование общественного мнения является показателем важности, значимости вопроса для общества, а группового мнения — включенности группы в определенную систему отношений, степени развитости самой группы и ее общественных интересов. Общественное мнение имеет ценностно-регулятивный характер, отражающийся в позиции общества по любому социально важному вопросу или проблеме, в деятельности

[1] *Зиновьев А. А.* На пути к сверхобществу. М. : Центрполиграф, 2000. С. 149.

[2] *Соловьев А. И.* Политология. М. : Аспект-пресс, 2003. С. 330; Политология. М. : РАГС, 2002. С. 213.

[3] *Коваленко В. И., Костин А. И.* Политические идеологии: история и современность // Вестник Московского университета. 1997. № 2. Серия 12. С. 45—75.

[4] *Комаровский В. С.* Государственная служба и СМИ. Воронеж: Изд-во ВГУ, 2003. С. 105.