

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт экономики и управления	Кафедра «Экономическая теория и международные отношения»
Направление подготовки	41.03.05 «Международные отношения»
Профиль	Мировая политика и международный бизнес

БАКАЛАВРСКАЯ РАБОТА

на тему

**Политика России, США, Китая по обеспечению информационной
безопасности**

Студент	<hr/>	Куницын Максим Сергеевич
	подпись, дата	
Руководитель	<hr/>	Питайкина И. А.
	подпись, дата	
Нормоконтролер	<hr/>	Влазнева С. А.
	подпись, дата	

Работа допущена к защите (протокол заседания кафедры от _____ № _____)

Заведующий кафедрой	<hr/>	Рожкова Л. В.
	подпись, дата	

Работа защищена с отметкой _____ (протокол ГЭК от _____ № _____)

Секретарь ГЭК	<hr/>	Рассказова Н. В.
	подпись, дата	

Пенза 2022

ФГБОУ ВО «Пензенский государственный университет»
Институт экономики и управления
Кафедра «Экономическая теория и международные отношения»
Направление подготовки 41.03.05 «Международные отношения», профиль
Мировая политика и международный бизнес

«УТВЕРЖДАЮ»:
Зав. кафедрой
д.с.н., доцент Рожкова Л.В.

« ____ » _____ 20 ____ г.

ЗАДАНИЕ
НА БАКАЛАВРСКУЮ РАБОТУ

студенту Куницыну М. С., группа 18ЭА2, обучение очное

1 Тема бакалаврской работы: Политика России, США, Китая по обеспечению информационной безопасности

утверждена приказом по университету

от « ____ » _____ 20 ____ г. № _____

2 Срок сдачи студентом законченной бакалаврской работы: 14.06.2022.

3 Исходные данные к бакалаврской работе: нормативно-правовая база, научная и справочная литература, данные сети Интернет.

4 Перечень подлежащих разработке вопросов: политика России по обеспечению информационной безопасности, политика США по обеспечению информационной безопасности, политика Китая по обеспечению информационной безопасности.

5 Перечень графического материала: таблицы, рисунки.

6 Дата выдачи задания: 30.12.2021.

График подготовки бакалаврской работы

№ п/п	Содержание работы	Срок выполнения	Дата выполнения, подпись руководителя
1	Составление плана ВКР	30.01.2021 – 10.01.2022	
2	Изучение исходных данных к бакалаврской работе	11.01.2022 – 23.01.2022	
3	Написание Главы 1	24.01.2022 – 20.03.2022	
4	Написание Главы 2	21.03.2022 – 1.05.2022	
5	Написание введения и заключения	2.05.2022 – 15.05.2022	
6	Оформление ВКР	16.05.2022 – 29.05.2022	
7	Сдача ВКР нормоконтролю, проверка в системе «антиплагиат.вуз»	30.05.2022 – 12.06.2022	
8	Ознакомление с отзывом руководителя	13.06.2022	
9	Представление законченной бакалаврской работы, передача в ГЭК	14.06.2022	

Руководитель _____ / И. А. Питайкина /
(подпись) (инициалы, фамилия)

Задание принял к исполнению студент _____ / М. С. Куницын /
(подпись) (инициалы, фамилия)

Реферат

Бакалаврская работа 42 с., 3 ч., 1 рис., 1 табл., 40 источников.

МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ, ВНЕШНЯЯ ПОЛИТИКА, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РОССИИ, США, КИТАЯ

Объект исследования – информационная безопасность России, США, Китая.

Цель работы состоит во всестороннем изучении содержания, практических и теоретических особенностей и перспектив развития информационной безопасности России, США и Китая на современном этапе.

Методологическую основу работы составили принципы объективности, историзма, системности, единства исторического и логического, социально-исторической обусловленности деятельности человека, взаимосвязи общественного бытия и общественного сознания.

Результаты работы: Путем анализа были выявлены понятие и содержание информационной безопасности стран и их правовое обеспечение. Выделены основные цели обеспечения информационной безопасности в новых условиях мировой политики и геополитики. Представлены три сценария развития информационной деятельности стран. Выделен приоритетный путь развития информационной безопасности для России, США, Китая.

Рекомендации по внедрению. Анализ информационной безопасности может быть использован органами государственной власти и научным сообществом для повышения эффективности выстраивания новой экономической и политической системы и расширения теоретической базы проводимых исследований.

Теоретическая значимость работы состоит в комплексном анализе теоретических основ обеспечения информационной безопасности России, США, Китая и выявлении перспектив развития в кибербезопасности.

Прогнозные предположения о развитии объекта исследования. Перспективы реализации и обеспечения успешной информационной политики достижимы в полном объеме.

Summary

Bachelor's thesis 42 pages, 2 parts, 1 figure, 1 table, 40 sources.

INTERNATIONAL RELATIONS, FOREIGN POLICY, INFORMATION SECURITY OF RUSSIA, USA, CHINA

The object of the study is the information security of Russia, USA, China.

The purpose of the work is to comprehensively study the content, practical and theoretical features and prospects of the information security of Russia, USA and China at the present stage.

The methodological basis of the work was the principles of objectivity, historicism, consistency, unity of historical and logical, socio-historical conditionality of human activity, the relationship of social being and social consciousness.

Results of the work: The analysis revealed the concept and content of the information security of countries and their legal support. The main goals of ensuring information security in the new conditions of world politics and geopolitics are highlighted. Three scenarios for the development of information activities of countries are presented. A priority path for the development of information security for Russia, the USA, and China has been identified.

Recommendations for implementation. Foreign policy analysis can be used by public authorities and the scientific community to improve the efficiency of building a new economic and political system and expand the theoretical base of ongoing research.

The theoretical significance of the work lies in a comprehensive analysis of the theoretical foundations of the information security of Russia, USA, China and identifying development prospects in cybersecurity.

Forecast assumptions about the development of the object of study. The prospects for the implementation and maintenance of a successful information policy are achievable in full.

Оглавление

Введение.....	3
Глава 1 Политика России по обеспечению информационной безопасности	5
1.1 Понятие и содержание информационной безопасности России.....	5
1.2 Правовое обеспечение информационной безопасности в России	11
Глава 2 Политика США по обеспечению информационной безопасности	20
2.1 Политика США с сфере информационной безопасности.....	20
2.2 Правовое обеспечение информационной безопасности в США	24
Глава 3 Политика Китая по обеспечению информационной безопасности	29
3.1 Политика Китая в сфере информационной безопасности	29
3.2 Правовое обеспечение информационной безопасности в Китае	31
Заключение	34
Список использованных источников	36
Приложение А	40

Введение

Актуальность данной темы обусловлена тем, что характерной чертой современного общества является его информатизация – активная разработка и внедрение во все сферы человеческой деятельности информационных технологий и средств. Информация и информационные ресурсы становятся одним из решающих факторов развития личности, общества и государства. Широкие возможности компьютеров и информационных технологий позволяют автоматизировать процессы мониторинга и управления государственными, экономическими, социальными, оборонными и другими объектами и системами, получать, накапливать, обрабатывать и передавать информацию об этих процессах практически с любой требуемой скоростью, в любом количестве.

Все это дает основание утверждать, что информатизация играет сегодня решающую позитивную роль в развитии человечества, что информационное общество объективно неизбежно. Но история учит нас тому, что многие достижения научно-технической мысли использовались не только во благо людей. Достаточно вспомнить достижения ядерной физики – атомное оружие, оптоэлектроники – лазерное оружие, химии – отравляющие газы, биологии – биологическое оружие и т. д. Всегда находились силы, которые стремились использовать в своих интересах открытия в научно-технической сфере.

Сегодня у определенных субъектов (коалиций, государств, организаций, личностей) возникает стремление единолично обладать информационными ресурсами, средствами и технологиями и использовать их для удовлетворения своих интересов и противодействия интересам вероятных конкурентов в экономическом, коммерческом и даже военном противоборстве. Информация и информационные технологии при этом начинают выступать в качестве объектов угроз, что порождает проблему информационной безопасности.

Таким образом, тема изучения сущности и содержания информационной безопасности в современных условиях очень актуальна. Особенной эта тематика является в свете глобальных геополитических тенденций последних лет.

Проблемы и пути информационного обеспечения безопасности государства не являются новейшими с точки зрения исследовательского вопроса. Они активно рассматриваются в работах отечественных и зарубежных авторов в контексте тех или иных научных интересов.

Объект исследования – политика обеспечения информационной безопасности России, США и Китая.

Предмет исследования – формы и методы реализации политики информационной безопасности в киберпространстве.

Цель данной дипломной работы – выявить перспективы развития информационной безопасности России, США и Китая на современном этапе.

Исходя из поставленной цели, можно выделить следующие задачи работы:

- рассмотреть понятие и содержание информационной безопасности России;
- проанализировать правовое обеспечение информационной безопасности в России;
- изучить политику США в сфере информационной безопасности;
- проанализировать правовое обеспечение информационной безопасности в США;
- изучить политику Китая по обеспечению информационной безопасности;
- проанализировать правовое обеспечение информационной безопасности в Китае.

Методы исследования: анализ, синтез, описание, сравнение.

Структура работы отражает логику и содержание исследования. Работа состоит из введения, трех глав, разделенных на параграфы, заключения и списка использованных источников.

Глава 1 Политика России по обеспечению информационной безопасности

1.1 Понятие и содержание информационной безопасности России

Под информационной безопасностью Российской Федерации понимается состояние защищенности национальных интересов Российской Федерации в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Информационная сфера представляет собой совокупность информационных ресурсов и информационной инфраструктуры объекта защиты.

Совокупность хранимой, обрабатываемой и передаваемой информации, используемой для обеспечения процессов управления, называют информационным ресурсом.

К информационным ресурсам относятся:

- информационные ресурсы предприятий оборонного комплекса, содержащие сведения об основных направлениях развития вооружения, о научно-техническом и производственном потенциале, об объемах поставок и запасах стратегических видов сырья и материалов;

- информационное обеспечение систем управления и связи;

- информация о фундаментальных и прикладных НИР, имеющих государственное значение и др.

Информационная инфраструктура – это совокупность информационных подсистем, центров управления, аппаратно-программных средств и технологий обеспечения сбора, хранения, обработки и передачи информации.

Информационная инфраструктура включает:

- информационную инфраструктуру центральных, местных органов государственного управления, научно-исследовательских учреждений;

- информационную инфраструктуру предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих государственные оборонные заказы либо занимающихся оборонной проблематикой;

– программно-технические средства автоматизированных и автоматических систем управления и связи.

Под угрозой безопасности информации понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее. Угрозы информационной безопасности Российской Федерации подразделяются на внешние и внутренние.

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения, являются:

- все виды разведывательной деятельности зарубежных государств;
- информационно-технические воздействия (в том числе радиоэлектронная борьба, проникновение в компьютерные сети);
- диверсионно-подрывная деятельность специальных служб иностранных государств, осуществляемая методами информационно-психологического воздействия;
- деятельность иностранных политических, экономических и военных структур, направленная против интересов Российской Федерации в сфере национальной обороны [2].

К внутренним угрозам, которые будут представлять особую опасность в условиях обострения военно-политической обстановки, относятся:

- нарушение установленного регламента сбора, обработки, хранения и передачи информации, находящейся в штабах и учреждениях силовых структур Российской Федерации, на предприятиях оборонного комплекса;
- преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем специального назначения;
- ненадежное функционирование информационных и телекоммуникационных систем специального назначения;
- возможная информационно-пропагандистская деятельность, подрывающая престиж силовых структур Российской Федерации и их боеготовность;

– нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов [6].

К угрозам безопасности уже развернутых и создаваемых информационных и телекоммуникационных средств и систем относятся:

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- 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;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств, предназначенных 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 машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;

- несанкционированный доступ к информации, находящейся в банках и базах данных;

- нарушение законных ограничений на распространение информации.

Основными направлениями совершенствования системы обеспечения информационной безопасности Российской Федерации являются:

- систематическое выявление угроз и их источников, структуризация целей обеспечения информационной безопасности и определение соответствующих практических задач;

- проведение сертификации общего и специального программного обеспечения, пакетов прикладных программ и средств защиты информации в существующих и создаваемых автоматизированных системах управления и связи, имеющих в своем составе элементы вычислительной техники;

- постоянное совершенствование средств защиты информации, развитие защищенных систем связи и управления, повышение надежности специального программного обеспечения;

- совершенствование структуры функциональных органов системы, координация их взаимодействия.

Оценка состояния информационной безопасности базируется на анализе источников угроз (потенциальной возможности нарушения защиты) [20].

Деятельность, направленную на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на нее, называют защитой информации. Объектом защиты является информация или носитель информации, или информационный процесс, которые нужно первоначально защищать [17].

Защита информации организуется по трем направлениям: от утечки, от несанкционированного воздействия, от преднамеренного и от непреднамеренного воздействия. На рисунке 1 представлены направления защиты информации.

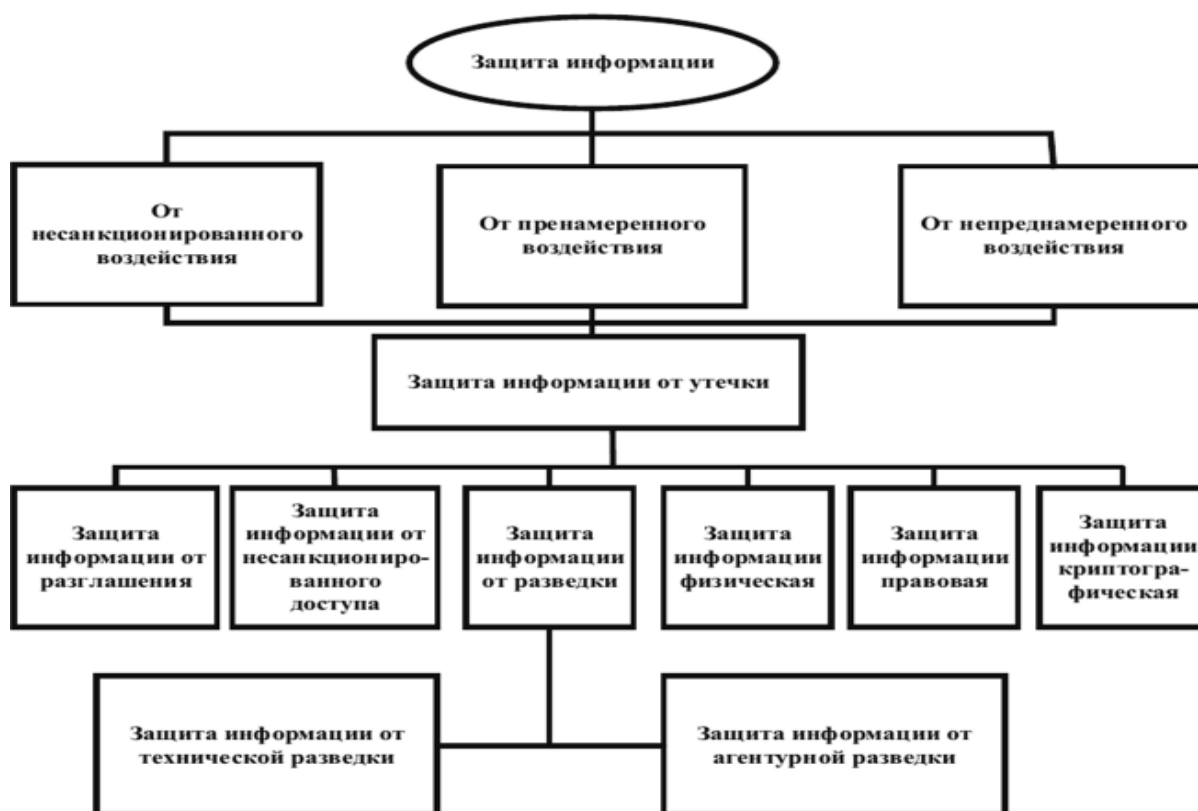


Рисунок 1 – Направления защиты информации [7]

Первое направление – защита информации от утечки – деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

Защита информации от разглашения направлена на предотвращение несанкционированного доведения ее до потребителя, не имеющего права доступа к этой информации [7].

Защита информации от несанкционированного доступа направлена на предотвращение получения информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может быть: государство; юридическое лицо; группа

физических лиц, в том числе общественная организация; отдельное физическое лицо.

Защита информации от технической разведки направлена на предотвращение получения информации разведкой с помощью технических средств.

Второе направление – защита информации от несанкционированного воздействия – деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Третье направление – защита информации от непреднамеренного воздействия – деятельность, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Организовать защиту информации – значит создать систему защиты информации, а также разработать мероприятия по защите и контролю эффективности защиты информации.

Выделяются четыре основные составляющие национальных интересов РФ в информационной сфере.

Первая составляющая национальных интересов РФ в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая составляющая национальных интересов РФ в информационной сфере включает в себя информационное обеспечение государственной политики РФ, связанное с доведением до российской и международной общественности

достоверной информации о государственной политике РФ, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая национальных интересов РФ в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

Четвертая составляющая национальных интересов РФ в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

1.2 Правовое обеспечение информационной безопасности в России

Право в целом и каждая его отрасль проявляют себя как организационный механизм, как действующая научная или практическая юридическая система, пользуясь при этом определенным инструментарием.

Для информационного права – молодой и только формируемой отрасли – важно определить основные институты и одновременно найти пути наиболее эффективного применения других инструментов права, позволяющих выразить суть регулирования в сфере практической информатики. Поскольку ведущим звеном в

развитии информационного права, как и любой отрасли, является его нормативная часть, то первостепенное внимание должно быть направлено на дефиниции.

В работе В. А. Никитова «Информатика в терминах и определениях российского законодательства» на базе действующего законодательства выявлено и систематизировано более семисот терминов и их определений. Названная работа по выявлению и систематизации правовой терминологии в информатике использовала в качестве источника только федеральное законодательство – действующие законодательные акты РСФСР, законы РФ, акты российского парламента, указы и распоряжения президентов РСФСР и Российской Федерации, постановления и распоряжения Совета Министров РСФСР и Правительства РФ, а также не утратившие юридическую силу правовые акты СССР.

Перечень актов, отнесенных к категории источников, свидетельствует о том, что, во-первых, законодательство в самом широком смысле уделяет большое внимание информационной проблематике и, во-вторых, тема информации и других компонентов информатики рассредоточена по всем отраслям законодательства, а также по всем уровням нормативно-правовой системы.

Два вопроса требуют ответа по теме правовых дефиниций в информационном праве.

Первый вопрос связан с выявлением сугубо правовых терминов, имеющих отношение к сфере регулирования информационного права. Он касается отбора тех правовых определений, которые необходимы и без которых правовое регулирование не будет эффективным (имеется в виду ситуация, когда в правовые дефиниции попадают термины не правового характера). Многие термины, касающиеся предметной области информатики, попадают в сферу правового регулирования потому, что теория и социальная информатика не построили прочной основы в терминологическом срезе своих дисциплин. Не созданы еще и теории информации, информатизации как направлений и сфер социальной деятельности. Потому многие термины становятся по определению правовыми. Тем самым образуется перекрестная система использования дефиниций в разных направлениях информатики. Социальная информатика использует правовые дефиниции, а

правовая – социальные. Например, такие определения, как документ», «документированная информация», «информатизация», «информационная безопасность», в строгом смысле не являются правовыми дефинициями. Это предметы и области деятельности, в которых совершаются правовые отношения. Но отсутствие устоявшихся понятий этих выражений в системной, информационной, управленческой практике, в документалистике и т.д. вынуждают законодателя вводить их в число правовых дефиниций.

Не случайно в некоторых проектах законов, связанных с информацией в определенных системах, разработчики пытаются увязать информацию, документ с категорией «юридической силы». В толковом словаре по информатике термин «документ» определен как «материальный объект, содержащий в зафиксированном виде информацию, оформленную установленным порядком и имеющую в соответствии с действующим законодательством правовое значение».

Все же следует иметь в виду, что право может установить требования к определенной категории документов, но предусмотреть юридическую силу любых документов заранее невозможно. Такое значение документов устанавливается всякий раз компетентными органами с учетом юридических фактов (обстоятельств) ситуаций, событий. Поиск истины в этом направлении, очевидно, должен завершиться такой формулировкой, которая бы исключила использование одного и того же термина в смежных законах с различным определением его дефиниции. Второй вопрос связан с учетом разнообразия юридических дефиниций [10].

Правовые дефиниции являются стержнем словарей в информационно-поисковых системах. Поэтому к их выбору и определению следует подходить более требовательно и, в конечном счете, добиваться их унификации, своеобразной стандартизации в рамках права.

Так, например, в правилах подготовки документов, связанных с разработкой законопроектов федеральными органами исполнительной власти дано определение слова «термин». Под термином понимается «слово (или словосочетание) однозначно означающее содержание понятия предмета, явления, процесса». Предложено различать термины общеправовые, межотраслевые, отраслевые. Сформулированы

правила работы с терминами. Норма – дефиниция должна содержать определения новообразуемого правового понятия, используемого в тексте закона. Правовая дефиниция понимается как определение правового понятия, отражающего существенные, главные признаки того или иного правового предмета, явления. В ходе проектирования документа разработчик с учетом концепции акта выбирает из уже существующих словарей термины, необходимые для его цели, вычисляет из них базовые понятия для своего акта и дополнительно формулирует те дефиниции, которые в действующие словари не вошли.

Учитывая, что дефинитивная часть информационного права только формируется, важно провести инвентаризацию терминов в уже действующих законах и наметить перспективное распределение терминов недостающих с учетом планов подготовки проектов законов в данной области. Иными словами, этим процессом также надо управлять. В настоящее время ощущается дефицит нормативного определения таких терминов, как «электронно-цифровая подпись», «электронный документ», «электронный документооборот», «электронная библиотека», «информационная система» (есть разночтения), «общественный интерес», «информационный продукт», «информационный объект». Это все термины предметного свойства. Вместе с тем еще много терминов, нуждающихся в правовом определении. К таковым относятся те, которые касаются видов субъектов, видов их деятельности. Например, все компоненты права на информацию - сбор, обработка, распространение и т.д. – ждут своего легитимного определения.

Таким образом, правовые дефиниции и образуемые на их основе поисковые слова и словосочетания – важная часть инструментария составителей нормативно-правовых актов, органов, принимающих и издающих такие акты, а также организаторов и персонала информационно-поисковых, аналитических и экспертных систем, обслуживающих интересы и потребности различных категорий пользователей, и, наконец, самих пользователей, которые при наличии техники имеют широкие возможности самостоятельно обращаться с информационными системами.

Началом формирования законодательства России в информационной сфере можно считать 1992 г., когда были приняты законы о правовой охране программ для ЭВМ и баз данных, о правовой охране технологий интегральных микросхем. С момента принятия базового Федерального закона «Об информации, информатизации и защите информации» прошло более 10 лет. За это время сформировался достаточно разнообразный массив законодательства и других нормативно-правовых актов, регулирующих отношения в областях:

- формирования и использования информационных ресурсов;
- создания и использования информационных технологий;
- формирования необходимой инфраструктуры для информатизации на федеральном, региональном, отраслевом, ведомственном уровнях, в структурах местного самоуправления, а также для удовлетворения информационных потребностей граждан, средств массовой информации, различных юридических лиц, других структур общества [10].

Сегодня никого не удивит констатация факта, что решается задача формирования информационного общества, что Россия заняла свою нишу и структуре Интернета и что население, производственные, научные и управленческие структуры широко пользуются глобальными сетями для получения необходимой информации и представления своей собственной для обозрения всеми заинтересованными пользователями всемирной паутины.

Действующая нормативно-правовая основа практической информатики (так называется совокупность и взаимодействие информационных ресурсов, технологий, средств и сетей связи – коммуникаций), представляет достаточно сложное образование. Все уровни законодательства имеют самое непосредственное отношение к регулированию информационной деятельности, отношений, процессов реальной информатики, обеспечивают формирование многообразия информационной среды, а, в конечном счете, и всей информационной сферы.

Конституция Российской Федерации, федеральные конституционные законы содержат немало норм, напрямую посвященных проблемам информации и информатизации, действует более десятка специальных федеральных законов,

имеющих своим предметом исключительно информацию или инфраструктуру информатизации. Множество норм об информационных отношениях рассредоточены по другим федеральным законам. В рассматриваемый период шло активное формирование информационного законодательства субъектов Российской Федерации: около сорока ее субъектов имеют специальные законы либо об информационных ресурсах, либо об информатизации региона.

Жизнь ставит все новые и новые проблемы, которые не могут быть решены без участия права. Процессы глобализации в экономической, культурной, научной и иных областях жизни могут быть реализованы только на основе информационных технологий, которые формируют инфраструктуру обмена документами, мнениями, знаниями и позволяют принимать соответствующие решения. Остро стоит вопрос не только о развитии и применении международного законодательства, международного частного права, но и о гармонизации правовых норм в случаях, когда отношения проходят через ряд границ и систем права. Глобализация диктует вопросы о формировании наднационального права и создании соответствующей нормативной базы [9].

Закономерно ставить вопрос о включении в этот ранг и информационных отношений, выходящих за рамки национального регулирования.

Учитывая интерес населения ко всем событиям как внутри страны, так и за рубежом, чувствительность к состоянию дел средств массовой информации, к государственным решениям по всем проблемам жизни общества и граждан, можно с уверенностью утверждать, что развитие законодательства к области информационной сферы включает понятие «законность» и «беззаконие» и что состояние правовой основы информатики в социальном ее облике - один из острейших вопросов общественного интереса и безопасности не только в информационной сфере.

Призывы к деполитизации общества, к деидеологизации, к разгосударствлению жизни с середины 80-х гг. XX в. нанесли огромный ущерб массовому сознанию в оценке и доверии к государственным, а следовательно, и к правовым институтам. В то же время на основе развития концепций элитарности

определенных кругов общества, опирающихся на механизмы полугласного признания ценза собственников, обеспечили выброс в сферу политики самых разных сил. И в сфере информационной деятельности на первом месте стоит вопрос не об удовлетворении потребностей общества в целом (именно это диктуется природой глобализации), а вопросы завоевания монополии, достижения дохода.

Действуют и традиции, согласно которым государство и общество находятся в конфронтации и именно государство обязано быть открытым (голос налогоплательщика) и прозрачным, что совсем не обязательно для других структур – негосударственных. Система тайн не балансируется в идеале. Государственная тайна – это обеспечение интересов «всех», всей страны, а коммерческая, частная, личная – сфера отдельных субъектов, как бы отстраненных от забот и притязаний социума [8].

За последнее время выстроилась линия «государственная безопасность, судебная, правовая, экономическая, административная, военная реформы». Такого изобилия концепций, доктрин, прогнозов, стратегий страна не знала давно. Постепенно политика государства приобретает систему. В ней не последнее место занимают проблемы информационной сферы. Доктрина информационной безопасности органически вытекает из Концепции государственной безопасности и создает импульс для постановки и решения очень сложных для общества вопросов в этой предметной области.

Осмысление проблем информационных процессов в настоящее время идет почти во всех направлениях современной науки – философии, социологии, психологии, политологии, праве, экономических науках, математике, логике, лингвистике и т.д. Все стороны научного понимания мироздания и социальной жизни затронуты процессами информатизации, компьютеризации общества. Общество нуждается в выстраивании правил поведения, правил отношений различных субъектов в новых условиях. Нужны не только коридоры власти, но и системы регуляторов, создающие необходимые указатели, куда и как идти и чего нельзя допускать при этом в целях сохранения безопасности человека, его

ассоциаций, государства и иных обеспечивающих безопасность институтов общества [6].

Теоретических правовых исследований в области информационного права пока немного. Преобладают исследования прикладного характера, публикации малых, журнальных форм. И все же в этой области уже накоплены знания, которые приближают возможность структурировать область правовых исследований по информационной проблематике. Большинство из них ориентировано на законодательную, нормативную область права, что характеризует центростремительную технологию формирования правовой науки в данной области. Весьма существенной проблемой является и исследование вопросов, связанных с влиянием информатики на всю систему правовой науки и правовую систему в целом, на государственное управление. Это специальные проблемы, и они еще требуют своего развития, нежели простая констатация факта наличия новых факторов социального значения. Проект Концепции совершенствования правового обеспечения информационной безопасности Российской Федерации следующим образом формулирует национальные интересы России в информационной сфере. Это сфера общественной жизни, образуемая совокупностью субъектов информационного взаимодействия или воздействия; собственно информации, предназначенной для использования в информационной сфере; информационной инфраструктуры; общественных отношений в области работы с информацией. Возможно, выстроить этот ряд с учетом следующих приоритетов. Новый материал для ответа на эти вопросы представлен Доктриной информационной безопасности и итогами работы ряда Международных конференций, которые прошли в первой половине 2001г. в г. Москве. Международная конференция «Информационное общество и интеллектуальные информационные технологии XXI века» состоялась 28-30 марта с участием Совета Федерации Федерального Собрания РФ, Британского совета в России (один из организаторов конференции), социально-инженерного парка «Будущая Россия», представителей ряда зарубежных стран и специалистов России. Ряд проблем информационной политики затронут и на 2-й международной конференции «Модернизация экономики России», прошедшей с 3 по 5 апреля, в

рамках которой работали секции «Правовое обеспечение устойчивого развития экономики» и «Модернизация государства и экономическое развитие». Плодотворные обобщения по некоторым вопросам достигнуты конференцией «Проблемы правового и организационно-технического обеспечения информационной безопасности России», состоявшейся с 22 по 24 мая в Екатеринбурге. Политической основой для решения проблем информатики являются такие документы, как Послание Президента РФ В. В. Путина Федеральному Собранию Российской Федерации 2004 г. Путеводным документом является Окинавская хартия «Глобальное информационное общество» и развивающие его решения различных стран, в том числе России.

Однако в настоящее время есть немало вопросов, возникающих в связи с отсутствием так необходимой координации в любом деле, а в развитии нормативно-правовой основы – в особенности. Единого центра, который бы аккумулировал все наиболее значимые для развития страны информационные проблемы нет. Важнейшими центрами являются Правительство РФ и Совет Безопасности и множество органов исполнительной власти России. Наибольшее внимание данным вопросам в соответствии со своей компетенцией уделяют Минсвязи, Минюст России, ФСБ России и некоторые другие структуры. Но проблемы перспектив развития законодательства все же оказываются размытыми, и в структуру законодательной власти в Федеральное Собрание РФ поступают предложения от многих инициаторов, не будучи скоординированными и ориентированными на генеральные направления. Тем не менее в настоящее время обстановка меняется под влиянием идей Доктрины информационной безопасности и развивающей ее Концепции развития правовой основы.

Глава 2 Политика США по обеспечению информационной безопасности

2.1 Политика США в сфере информационной безопасности

В настоящее время ФБР совместно с Агентством национальной безопасности (АНБ) ведут работы по созданию системы контроля за электронной почтой в Интернет. На программу технического перевооружения АНБ «*GroundBreaker*» Конгресс выделил свыше 5 млрд долл. и еще около 1 млрд долл. дополнительно на переоснащение многоцелевой атомной подводной лодки класса «*Sea wolf*» для прослушивания подводных кабелей связи с помощью специальной аппаратуры. Названная в честь президента США Джими Картера новая субмарина SSN-23 должна была быть спущена на воду в декабре этого года, но по настоянию АНБ было принято решение провести ее переоборудование, а спуск лодки отложить до июня 2009 г. По сведениям, просочившимся в печать, после ввода в строй новой субмарины АНБ рассчитывает прослушивать не только обычные электрические кабели связи, что оно делало и раньше, но и волоконно-оптические! Как это удастся сделать американцам – пока не ясно: для бесконтактного перехвата экранированного светового луча еще не придуман способ. Между тем, подводная лодка-шпион будет нести на своем борту специальный контейнер-камеру, из которой может быть осуществлен беспрепятственный доступ к любым подводным объектам [13].

Ежегодно США расходуют на информационные технологии только из федерального бюджета порядка 38 млрд долл., из которых около 20 млрд долл. (более 50 %) составляют расходы военного ведомства. И это без учета десятков млрд долл. затрачиваемых на бортовые системы управления спутников, ракет, самолетов, танков и кораблей. Сегодня Пентагон это не только один из крупнейших владельцев, арендаторов и пользователей информационных и телекоммуникационных ресурсов, ведущих заказчиков программного обеспечения, компьютерного оборудования и средств цифровой связи, но и, по сути дела, законодатель государственной политики и промышленных стандартов в области

информационной безопасности. Только в 2007 г. на защиту национальных информационных ресурсов в США было выделено 2 млрд долл., в то время как Пентагон истратил на защиту военных информационных систем 1 млрд долл.

В определенной степени это сказывается и на самих понятиях, связанных с защитой информации, которые постепенно трансформируясь из чисто военных терминов приобретают характер общегосударственных и промышленных стандартов. Производители оборудования и разработчики программных продуктов, заинтересованные в крупных государственных и военных заказах, начинают прислушиваться к тому, что говорят в коридорах Пентагона об информационной безопасности.

Осознав на собственном опыте бессмысленность защиты информационных ресурсов без участия всех заинтересованных сторон, каковыми в США являются фактически не только все государственные структуры, промышленность, частный капитал, но и рядовые граждане, военное ведомство в буквальном смысле пошло в народ, активно пропагандируя свое видение общенациональной проблемы № 1. Одним из примеров такого новаторского подхода является программа DIAP (*Defense Information Assurance Program*), в рамках которой с участием таких ведущих фирм как *Lucent Technologies, IBM, Microsoft, Intel, Cisco, Entrust, HP, Sun, GTE, Bay Networks, Axent, Network Associates, Motorola* закладывается фундамент информационной безопасности не только военной инфраструктуры, но и всего американского общества в целом на ближайшие 10 лет.

В соответствии с секретной директивой Пентагона S-3600.1 гарантия информации определяется как «информационная операция или операции, связанные с защитой информации и информационных систем за счет обеспечения их готовности (доступности), целостности, аутентичности, конфиденциальности и непротиворечивости. Данные операции включают в себя восстановление информационных систем за счет объединения возможностей защиты, обнаружения и реагирования. При этом информация не будет раскрыта лицам, процессам или устройствам, не имеющим к ней прав доступа, будет обеспечена полная достоверность факта передачи, наличия самого сообщения и его отправителя, а

также проверка прав на получение отдельных категорий информации, данные остаются в исходном виде и не могут быть случайно или преднамеренно изменены или уничтожены, будет обеспечен своевременный и надежный (по требованию) доступ к данным и информационным службам установленных пользователей, а отправитель данных получит уведомление факта доставки, также как получатель – подтверждение личности отправителя, и таким образом никто не сможет отрицать своего участия в обработке данных».

Тем самым классическое понятие информационной безопасности (*INFOSEC – information security*) как состояние информационных ресурсов было расширено и дополнено гарантированием их надлежащего использования даже в том случае, если эти ресурсы будут подвергнуты деструктивному воздействию как извне, так и изнутри. Иными словами в политике информационной безопасности четко обозначился сдвиг в сторону активных организационно-технических мероприятий защиты информационных ресурсов. Похоже, что американцы взяли за основу пропаганды знаний в области информационной безопасности советскую систему гражданской обороны 60-х, 70-х гг. XX в., когда население учили не только тому, как надевать индивидуальные средства защиты и укрываться в бомбоубежищах, но и как вести радиационный, химический и бактериологический контроль и восстанавливать объекты народного хозяйства после применения оружия массового поражения [16].

Заметим, что это не единственное нововведение Пентагона в лексиконе информационных технологий, которое стало достоянием общественности не смотря на гриф секретности первоисточника. К числу таковых можно отнести следующие: «информационное противоборство», «информационное превосходство», «информационные операции (общие и специальные)», «информационная среда», «атака на компьютерные сети», «вторжение в информационные системы» и др. С некоторых пор американское военное ведомство считает полезным публиковать отдельные несекретные фрагменты из своих засекреченных официальных нормативных документов (директив, инструкций, меморандумов, уставов и наставлений), повышая информированность общества о потенциальных угрозах

национальной безопасности. Военные терпеливо и настойчиво приучают все слои населения к своей терминологии, постепенно стирая грань между государством и обществом, обороной и производством, разведкой и предпринимательством, учебой и досугом.

Профессиональная подготовка персонала в соответствии с новыми требованиями в области информационной безопасности является ключевым направлением реализации программы *DIAP*, в рамках которой на учебный процесс выделяется в общей сложности около 80 млн долл. на период до 2005 г. При этом предполагается открыть специализированные курсы дистанционного обучения (свыше 20) в так называемом «виртуальном университете информационной безопасности» на базе сайтов в Интернете, в которых будут обучаться основам «стратегии глубокой эшелонированной защиты информационных ресурсов» администраторы (2 недели) и специалисты (3–5 дней) практически из всех федеральных ведомств, включая ЦРУ, ФБР, НАСА, Минфина, Минюста, Минэнерго и др. Ожидается, что за 5 лет в области информационной безопасности в общей сложности будет подготовлено не менее 100 тыс. дипломированных специалистов, готовых к любым неожиданностям в киберпространстве [30].

В каждом штате на период чрезвычайных условий (землетрясений, ураганов, наводнений, катастроф, террористических актов) создаются так называемые резервные центры обработки информации, в которых периодически собирается, накапливается и обновляется наиболее важная информация, необходимая для организации управления всех жизненно важных служб (полиции, скорой помощи, пожарной охраны и др.) в случае выхода из строя основных центров обработки информации и телекоммуникационных систем. Как правило такие центры оснащаются автономными источниками энергоснабжения (дизель – генераторами), способными поддерживать нормальный режим функционирования резервных информационных центров в течение нескольких суток до восстановления стационарной системы энергоснабжения. В повседневных условиях работу таких центров обеспечивает ограниченный по численности технический персонал,

имеющий все необходимые навыки для организации работы центра в чрезвычайных условиях.

Таким образом, краткий обзор только некоторых наиболее важных и дорогостоящих программ развития информационных технологий в США на примере Пентагона показывает, что проблема информационной безопасности отдельно взятого ведомства по своему масштабу уже давно является общенациональной и для своего решения требует пересмотра устоявшихся подходов, принятия единых стандартов как в промышленности, так и в бизнесе, создания национальной системы подготовки специалистов соответствующего профиля, широкого информирования населения об угрозах и мерах по их предотвращению.

2.2 Правовое обеспечение информационной безопасности в США

Ключевую роль в правовом регулировании информационной безопасности США играет американский «Закон об информационной безопасности». Его цель – реализация минимально достаточных действий по обеспечению безопасности информации в федеральных компьютерных системах, без ограничений всего спектра возможных действий.

Характерно, что уже в первом разделе закона называется конкретный исполнитель – Национальный институт стандартов и технологий (НИСТ), отвечающий за выпуск стандартов и руководств, направленных на защиту от уничтожения и несанкционированного доступа к информации, а также от краж и подлогов, выполняемых с помощью компьютеров. Таким образом, имеется в виду, как регламентация действий специалистов, так и повышение информированности всего общества.

Согласно закону, все операторы федеральных информационных систем, содержащих конфиденциальную информацию, должны сформировать планы обеспечения ИБ. Обязательным является и периодическое обучение всего персонала таких ИС. НИСТ, в свою очередь, обязан проводить исследования природы и масштаба уязвимых мест, вырабатывать экономически оправданные меры защиты.

Результаты исследований рассчитаны на применение не только в государственных системах, но и в частном секторе.

Закон обязывает НИСТ координировать свою деятельность с другими министерствами и ведомствами, включая Министерство обороны, Министерство энергетики, Агентство национальной безопасности и т.д., чтобы избежать дублирования и несовместимости.

Помимо регламентации дополнительных функций НИСТ, Закон предписывает создать при Министерстве торговли комиссию по информационной безопасности, которая должна:

- выявлять перспективные управленческие, технические, административные и физические меры, способствующие повышению ИБ;
- выдавать рекомендации Национальному институту стандартов и технологий, доводить их до сведения всех заинтересованных ведомств.

С практической точки зрения, важен раздел 6 закона, обязывающий все правительственные ведомства сформировать план обеспечения информационной безопасности, направленный на то, чтобы компенсировать риски и предотвратить возможный ущерб от утери, неправильного использования, несанкционированного доступа или модификации информации в федеральных системах. Копии плана направляются в НИСТ и АНБ.

В 1997 г. появилось продолжение описанного закона – законопроект «О совершенствовании информационной безопасности» (*Computer Security Enhancement Act of 1997*), направленный на усиление роли Национального института стандартов и технологий и упрощение операций с криптосредствами [21].

В законопроекте констатируется, что частный сектор готов предоставить криптосредства для обеспечения конфиденциальности и целостности (в том числе аутентичности) данных, что разработка и использование шифровальных технологий должны происходить на основании требований рынка, а не распоряжений правительства. Кроме того, здесь отмечается, что за пределами США имеются сопоставимые и общедоступные криптографические технологии, и это следует учитывать при выработке экспортных ограничений, чтобы не снижать

конкурентоспособность американских производителей аппаратного и программного обеспечения.

Перед тем как защитить федеральные информационные системы, рекомендуется более широко использовать технологические решения, основанные на разработках частного сектора. А также предлагается провести оценку возможностей зарубежных производителей в данной сфере деятельности.

Очень важен раздел 3, в котором от НИСТ требуется по запросам частного сектора готовить добровольные стандарты, руководства, средства и методы для инфраструктуры открытых ключей, позволяющие сформировать негосударственную инфраструктуру, пригодную для взаимодействия с федеральными ИС.

В разделе 4 особое внимание обращается на необходимость анализа средств и методов оценки уязвимых мест других продуктов частного сектора в области ИБ.

Приветствуется разработка правил безопасности, нейтральных по отношению к конкретным техническим решениям, использование в федеральных ИС коммерческих продуктов, участие в реализации шифровальных технологий, позволяющее, в конечном итоге, сформировать инфраструктуру, которую можно рассматривать как резервную для федеральных ИС.

Важно, что в соответствии с разделами 10 и далее предусматривается выделение конкретных (и немалых) сумм, называются точные сроки реализации программ партнерства и проведения исследований инфраструктуры с открытыми ключами, национальной инфраструктуры цифровых подписей. В частности, предусматривается, что для удостоверяющих центров должны быть разработаны типовые правила и процедуры, порядок лицензирования, стандарты аудита.

В 2001 г. был одобрен Палатой представителей и передан в Сенат новый вариант рассмотренного законопроекта – *Computer Security Enhancement Act of 2001*. В этом варианте примечательно как то, что, по сравнению с предыдущей редакцией, было убрано, так и то, что добавилось.

За четыре года (1997–2001 гг.) на законодательном и других уровнях информационной безопасности США было сделано многое. Смягчены экспортные

ограничения на криптосредства, сформирована инфраструктура с открытыми ключами, разработано большое число стандартов (например, новый стандарт электронной цифровой подписи – *FIPS 186*, январь 2000 г.). Все это позволило не заострять больше внимание на криптографии как таковой, а сосредоточиться на одном из ее важнейших приложений – аутентификации, рассматривая ее по отработанной на криптосредствах методике. На базе всех вышеперечисленных законов в США сформирована общенациональная инфраструктура электронной аутентификации [19].

Программа безопасности, предусматривающая экономически оправданные защитные меры и синхронизированная с жизненным циклом ИС, упоминается в законодательстве США неоднократно. Согласно пункту 3534 («Обязанности федеральных ведомств») подглавы II («Информационная безопасность») главы 35 («Координация федеральной информационной политики») рубрики 44 («Общественные издания и документы»), такая программа должна включать:

- периодическую оценку рисков с рассмотрением внутренних и внешних угроз целостности, конфиденциальности и доступности систем, а также данных, ассоциированных с критически важными операциями и ресурсами;
- правила и процедуры, позволяющие, опираясь на проведенный анализ рисков, экономически оправданным образом уменьшить риски до приемлемого уровня;
- обучение персонала с целью информирования о существующих рисках и об обязанностях, выполнение которых необходимо для их (рисков) нейтрализации;
- периодическую проверку и (пере)оценку эффективности правил и процедур;
- действия при внесении существенных изменений в систему;
- процедуры выявления нарушений информационной безопасности и реагирования на них; эти процедуры должны помочь уменьшить риски, избежать крупных потерь, организовать взаимодействие с правоохранительными органами.

Таким образом, помимо этого, в законодательстве США имеются в достаточном количестве и положения ограничительной направленности, и

директивы, защищающие интересы таких ведомств, как Министерство обороны, АНБ, ФБР, ЦРУ.

Глава 3 Политика Китая по обеспечению информационной безопасности

3.1 Политика Китая в сфере информационной безопасности

При составлении отчетов и докладов органов различных государств Китай традиционно лидирует среди стран, которые осуществляют хакерские атаки или акты кибершпионажа. На основе оценки американских экспертов китайские военные подразделения, специализирующиеся на кибервойнах и способны в случае необходимости уничтожить большинство объектов американской информационной инфраструктуры. С другой стороны, китайская сторона не слишком преувеличивает свои достижения в киберпространстве. КНР часто указывает на то, что безопасность информационных систем страны находится только в начальной стадии развития и очень уязвима перед мерами безопасности, прописанными в киберстратегиях ведущих мировых держав.

Руководство Китая опасается в случае масштабной кибератаки потерять контроль над узловыми точками информационной инфраструктуры, чем могут воспользоваться для дискредитации страны внешние силы. Эти опасения небеспочвенны. В Индексе кибермогущества, составленном *Economist Intelligence Unit* и консалтинговой компанией *Booz Allen Hamilton*, Китай занял лишь 13-е место, а в рейтинге стран с наиболее развитым сектором ИКТ – лишь 36-е.

Не является ли это доказательством того, что данные западных спецслужб о кибермощи Китая противоречат представлениям составителей рейтингов и самих китайцев? Нет, совсем не так. Китай понимает, что в случае прямого противостояния с США его армия и вооружение не смогут обеспечить адекватный ответ. Поэтому для достижения и сохранения паритета с Западом власти активно разрабатывают киберсредства, которые при нападении на Китай могут вывести из строя всю информационную инфраструктуру противника. Главная слабость КНР заключается в неспособности самостоятельно создавать новые технологии. ИКТ, функционирующие в Китае, – это, как правило, искусно скопированные и доработанные технологии, ставящие страну на путь догоняющей модернизации,

пока не способной генерировать собственные разработки⁶. Тем не менее в последнее время наблюдается резкое увеличение инвестиций в сферу кибербезопасности, а реализация собственных проектов в области ИКТ стала приоритетным направлением инновационного развития [13].

Китайская государственная стратегическая программа инновационного развития содержит важные положения о развитии киберпространства и обеспечении его безопасности. Общие принципы информационной безопасности Китая: в первую очередь безопасность инноваций, а также ответственность за обеспечение информационной безопасности. В этом важная особенность подхода страны к вопросам информационной и кибербезопасности. Китайская модель инновационного развития основывается на четком следовании национальным интересам, непрерывном расширении научной и технической базы страны, активном привлечении инвестиций в разработку НИОКР, постоянном совершенствовании законодательства в сфере защиты интеллектуальной собственности. В программе признается, что в производстве высокотехнологичных продуктов в области ИКТ Китай все еще зависим от западных технологий, которые при помощи встроенных шпионских программ могут нанести вред всей китайской информационной инфраструктуре, инновационным разработкам и создать угрозу национальной безопасности страны. Снижение зависимости от западных ИКТ рассматривается как одно из важных средств обеспечения кибербезопасности КНР.

В Китае отсутствует единая стратегия развития киберпространства и обеспечения безопасности информационных систем, но это вовсе не означает, что отсутствует концептуальное обоснование значимости проблемы. Основным документом, в котором подчеркивается значимая роль ИКТ в жизни китайского народа, является Всеобъемлющая концепция национальной безопасности КНР [22].

Таким образом, в концепции отмечено, что информация в современном мире не только открывает много возможностей, но и создает угрозы политической, экономической, военной безопасности КНР. Большое внимание в документе уделено интернету как наиболее значимому, но наименее управляемому сегменту глобального информационного пространства.

3.2 Правовое обеспечение информационной безопасности в Китае

Сфера кибербезопасности попала в поле зрения китайских властей во второй половине 1990-х гг.

Одним из стимулов развития законодательства в этой области послужило создание в 1999 году системы электронного государственного управления (*Government Online Project, GOP*) и появление необходимости адекватного правового регулирования. Так, в 2000 году были приняты руководящие принципы для системы электронного государственного управления (*Guidelines of National Electronic Government Construction, NEGC*).

В 2011 г. положения о кибербезопасности были внесены в национальное уголовное законодательство КНР, а в 2013 г. – в Закон о защите прав и интересов потребителей.

В июле 2015 г. Всекитайское собрание народных представителей опубликовало проект первого Закона о кибербезопасности.

7 ноября 2016 г. Закон о кибербезопасности КНР был одобрен в третьем чтении на сессии постоянного комитета ВСНП. Официально вступил в силу 1 июня 2017 г.

Закон о кибербезопасности носит сводный характер и представляет собой первую попытку китайских властей сформулировать и обобщить стратегические принципы, определяющие действия Китая в области кибербезопасности.

Текст закона состоит из 79 статей, объединенных в 7 разделов:

- Основные принципы;
- Обеспечение и стимулирование кибербезопасности;
- Безопасность сетевых операций;
- Информационная безопасность;
- Контроль, предупреждение, чрезвычайное реагирование и меры наказания;
- Юридическая ответственность;
- Дополнительный раздел.

Главным образом, закон затрагивает деятельность поставщиков сетевых продуктов и услуг. Согласно Статье 22, поставщики сетевых продуктов и услуг должны своевременно информировать пользователей и соответствующие компетентные власти о любых известных уязвимостях в области безопасности и принимать необходимые меры по их устранению. В случае, если продукты или услуги собирают личные данные, поставщики обязаны уведомлять об этом пользователей. Сбор и хранение личных данных пользователей должны осуществляться исключительно в целях, официально обозначенных поставщиком. Запрещены раскрытие, изменение, удаление и передача данных третьим лицам, исключение составляет проведение перечисленных операций по требованию самого пользователя [10].

Закон существенно ограничивает анонимность пользователей за счет введения требования об обязательной верификации для доступа к сети. Если пользователь не предоставляет реальные идентификационные данные, провайдер не имеет права открывать доступ к сети.

Особое внимание уделяется безопасности критически важной инфраструктуры, к которой относятся государственные коммуникационные и информационные услуги, энергетика, транспорт, ирригация, финансы, оборонная сфера, электронное правительство и другие ключевые отрасли и сектора, нанесение ущерба, незаконное использование и утечка данных в которых могут нести серьезную угрозу национальной безопасности и общественным интересам. В том числе, ужесточаются требования к профессиональной подготовке сотрудников, работающих на объектах КВИИ, вводится запрет на хранение данных за пределами Китая; согласно положениям закона, закупка сетевых продуктов и услуг для объектов КВИИ должна осуществляться под контролем уполномоченных государственных органов, предприятия в критически важных отраслях обязаны проводить ежегодные оценки рисков безопасности и отражать полученные результаты в отчетах.

В случае выявления нарушений закон предусматривает штрафы в размере от 10 тыс до 1 млн юаней, в зависимости от тяжести киберпреступления, при этом

весь полученный незаконным путем доход подлежит конфискации. В соответствии со Статьей 75, власти КНР имеют возможность замораживать активы иностранных учреждений, организаций и физических лиц, если они подозреваются в организации и осуществлении атаки, взлома, вмешательства, нанесении вреда критически важной информационной инфраструктуре Китая.

Нормативно-правовой акт также предусматривает проведение мер по повышению уровня грамотности населения в области кибербезопасности при участии государственных органов всех уровней и СМИ [7].

Таким образом, принятие закона ведет к усилению государственного контроля над деятельностью китайских и иностранных компаний в сети Интернет.

Закон может оказать существенное влияние на структуру внутреннего ИТ-рынка КНР и позиции национальных производителей. Его имплементация ограничивает доступ западных ИТ-компаний к китайскому рынку, так как требует от них прохождения специальной сертификации, что, в том числе, предполагает необходимость раскрытия исходных кодов поставляемого программного обеспечения [23].

Китайским и иностранным компаниям, планирующим заниматься реализацией ИТ-продуктов на китайском рынке, необходимо производить полную или частичную корректировку своих бизнес- и операционных практик в соответствии с положениями нового Закона [24].

Заключение

Подводя итоги вышесказанного, следует сделать следующие выводы.

Информатизация общества порождает проблемы информационной безопасности, главные из которых – проблема информационных войн и информационного терроризма. Они носят глобальный характер, но для России, США и Китая приобретают особую остроту, что обусловлено их геополитическим и экономическим положением.

Информационная безопасность государства – защита конституционного строя, суверенитета, территориальной целостности с использованием информационных средств. Жизненно важные интересы государства в информационной сфере:

- создание условий для реализации интересов личности и общества в информационной сфере;
- формирование институтов общественного контроля за органами государственной власти;
- безусловное обеспечение законности и правопорядка;
- создание условий для развития собственной информационной инфраструктуры;
- формирование системы подготовки и реализации решений органов государственной власти, обеспечивающих национальные интересы страны;
- защита государственной информационной системы и информационных ресурсов (в том числе защита государственной тайны);
- защита единого информационного пространства страны;
- развитие равноправного и взаимного международного сотрудничества.

Национальная безопасность России, США и Китая существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Под информационной безопасностью в этих понимается состояние защищенности их национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества

и государства. На основе национальных интересов России, США и Китая в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Угрозы информационной безопасности государства:

- разрушение единого информационного пространства;
- вытеснение информационных агентств и средств массовой информации с внутреннего информационного рынка;
- монополизация информационного рынка;
- блокирование деятельности государственных средств массовой информации по информированию гражданских лиц и зарубежной аудитории;
- ослабление роли государственного языка;
- несанкционированное целенаправленное вмешательство и проникновение в деятельность и развитие информационных систем;
- низкая эффективность информационного обеспечения государственной политики (дефицит кадров, отставание информационных систем от международных стандартов).

Угрозы информационной безопасности России, США и Китая подразделяются по общей направленности (угрозы государственным устоям и свободам граждан, духовной жизни общества, информационной структуре, информационным ресурсам) и по способам воздействия (собственно информационные, программно-математические, физические и организационные).

В современном обществе информационная безопасность является важнейшим компонентом национальной безопасности. От нее в значительной степени зависит уровень экономической, оборонной, социальной, политической и других видов безопасности.

Список использованных источников

- 1 Авинова Н. Н. Исторические аспекты информационных войн. М. : Юрайт, 2018. 276 с.
- 2 Белов Е. С. Основы информационной безопасности. М. : Юрайт, 2017. 544 с.
- 3 Ветров С. А., Лоткин И. В. Современные международные отношения. М. : Юрайт, 2019. 91 с.
- 4 В Китае вступает в силу резонансный закон о кибербезопасности. URL: <https://ria.ru/20170601/1495523455.html> (дата обращения: 05.05.2022).
- 5 Гаджиев К. С. Место и роль России в трансформирующейся системе международных отношений (материалы семинара). Н. Новгород : Нижегородский государственный университет им. Н. И. Лобачевского, 2002. 236 с.
- 6 Глобальный отчет по информационным технологиям 2010–2011 гг. Всемирный экономический форум. URL: <http://strategy.ru/the-report-on-information-technology> (дата обращения: 05.05.2022).
- 7 Глобальная программа кибербезопасности (ГПК) МСЭ. Основа для международного сотрудничества в области кибербезопасности. URL: <http://www.ifap.ru/pr/2008/080908aa.pdf> (дата обращения: 05.05.2022).
- 8 Доктрина информационной безопасности РФ. URL: <http://www.scrf.gov.ru/security/information/document5/> (дата обращения: 05.05.2022).
- 9 Закон о кибербезопасности позволит замораживать счета иностранцев. URL: <https://ria.ru/20161101/1480433700.html> (дата обращения: 05.05.2022).
- 10 Заявление министров иностранных дел стран НАТО. URL: <https://www.nato.int/nrcwebsite/ru/articles/20140327announcement/index.html> (дата обращения: 05.05.2022).
- 11 КНР. Закон о кибербезопасности принят. URL: <https://www.imemo.ru/news/events/text/knr-zakon-o-kiberbezopasnosti-prinyat> (дата обращения: 05.05.2022).

12 Концепция стратегии кибербезопасности Российской Федерации. URL: <http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf> (дата обращения: 05.05.2022).

13 Лапина М. А. Информационное право. М. : ЮНИТИ-ДАНА, Закон и право, 2018. 390 с.

14 Линников А. Геополитические факторы обеспечения экономической безопасности современной России в условиях технологического отставания. Федерализм. 2020. № 4. С. 127–140.

15 Положение интернета в Китае. Пресс-канцелярия госсвета КНР. URL: http://russian.china.org.cn/government/archive/baipishu/txt/02/01/content_21857458_8 (дата обращения: 05.05.2022).

16 Роговский Е. А. США. Информационное общество. Экономика и политика. Международные отношения. М. : Юрайт, 2019. 324 с.

17 Рейтинг стран по уровню кибербезопасности. URL: <https://nonews.co/directory/lists/countries/cybersecurity-index> (дата обращения: 05.05.2022).

18 Сунь Цзы Искусство войны. М. : София, 2021. 160 с.

19 Шаклеина Т. Россия и США в мировой политике. М. : Aspekt Press, 2017. 332 с.

20 Шакиров А. Р. Экономика США. Мировая экономика и международные отношения. М. : София, 2018. 203 с.

21 Шацкий М. Ю. Мировые информационные войны и конфликты. М. : Юрайт, 2017. 432 с.

22 Щеголев Б. Н. США: экономическое развитие и проблемы внешней торговли. М. : Юрайт, 2016. 138 с.

23 Юриш И. Р. Экономические системы мира. М. : Аспект, 2019. 445 с.

24 Ярунов И. И. Информация как мировая ценность. М. : Юрайт, 2006. 177 с.

25 An Act to establish the Department of Homeland Security, and for other purposes. URL: https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf (дата обращения: 05.05.2022).

26 Average annualized cost of cyberattacks on companies in selected countries as of August 2020 (in million U.S. dollars). URL: <https://www.statista.com/statistics/293274/countries/> (дата обращения: 05.05.2022).

27 Ball D. China's Cyber Warfare Capabilities. URL: <http://www.securitychallenges.org.au/ArticlePages/vol7no2Ball.html> (дата обращения 05.05.2022)

28 Budget in brief. Fiscal year 2020. URL: https://www.dhs.gov/sites/default/files/publications/FY2017_BIB-MASTER.pdf (дата обращения: 05.05.2022).

29 China's First Cyber Security Law | Institute for Defence Studies and Analyses. URL: https://idsa.in/backgrounder/china-first-cyber-security-law_apsingh_231216 (дата обращения: 05.05.2022).

30 Department of Defense Strategy for Operating in Cyberspace. URL: <http://csrc.nist.gov/groups/SMA/isab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf> (дата обращения: 05.05.2022).

31 Department Of Homeland Security. Statement On The President's Fiscal Year 2019 Budget. URL: <https://www.dhs.gov/news/2018/02/12/department-homeland-security-statement-president-s-fiscal-year-2019-budget> (дата обращения: 05.05.2022).

32 Digital Attack Map. Top daily DDoS attacks worldwide. URL: <http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=17650&view=map> (дата обращения: 05.05.2022).

33 First U.S. – China High – Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes. URL: <http://worldjpn.grips.ac.jp/documents/texts/USC/20151201.D1E.html> (дата обращения: 05.05.2022).

34 Global Cybersecurity Index (GCI) 2017. ITU 2020. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.2017-R1-PDF-E.pdf (дата обращения: 05.05.2022).

35 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98 (дата обращения: 05.05.2022).

36 International respect needed in cyber security: official. URL: <http://english.peopledaily.com.cn/90883/8278445.html> (дата обращения: 05.05.2022).

37 International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. URL: <https://www.whitehouse.gov/sites> (дата обращения: 05.05.2022).

38 Joint Summary of Outcomes: Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue. URL: <http://worldjpn.grips.ac.jp/documents/texts/USC/20160615.D1E.html> (дата обращения: 05.05.2022).

39 Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. Prepared for the U. S.–China Economic and Security Review Commission by Northrop Grumman Corp. URL: [http://http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_Capabilitiesfor omputer_NetworkOperationsand CyberEspionage.pdf](http://http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_Capabilitiesfor%20omputer_NetworkOperationsandCyberEspionage.pdf) (дата обращения: 05.05.2022).

40 Segal A. Is China a Paper Tiger in Cyberspace? Council on Foreign Relations. URL: <http://blogs.cfr.org/asia/2012/02/08/is-china-a-paper-tiger-in-cyberspace/> (дата обращения: 05.05.2022).

Приложение А

Глобальный индекс кибербезопасности 2020 г.

Таблица А.1 – Глобальный индекс кибербезопасности 2020 г.

№	Страна	Индекс
1	США	100
2	Великобритания	99,54
3	Саудовская Аравия	99,54
4	Эстония	99,48
5	Южная Корея	98,52
6	Сингапур	98,52
7	Испания	98,52
8	Россия	98,06
40	Китай	92,53