ВЫСШЕЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ

В. П. МЕЛЬНИКОВ, С. А. КЛЕЙМЕНОВ, А. М. ПЕТРАКОВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Под редакцией профессора С. А. КЛЕЙМЕНОВА

Допущено
Учебно-методическим объединением
по университетскому политехническому образованию
в качестве учебного пособия для студентов высших учебных заведений,
обучающихся по специальности «Информационные системы и технологии»

6-е издание, стереотипное

ACADEMIA

Москва
Издательский центр «Академия»
2012

УДК 621.391(075.8)
ББК 32.81я73
М48

Рецензент —
зав. кафедрой «Информационная безопасность» МГТУ им. Н. Э. Баумана,
канд. техн. наук, доцент *Н. В. Медведев*

Мельников В. П.

М48 Информационная безопасность и защита информации : учеб. пособие для студ. учреждений высш. проф. образования / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под. ред. С. А. Клейменова. — 6-е изд., стер. — М. : Издательский центр «Академия», 2012. — 336 с.

ISBN 978-5-7695-9222-5

Представлены основные положения, понятия и определения обеспечения информационной безопасности деятельности общества, его различных структурных образований, организационно-правового, технического, методического, программно-аппаратного сопровождения. Особое внимание уделено проблемам методологического обеспечения деятельности как общества, так и конкретных фирм и систем (ОС, СУБД, вычислительных сетей), функционирующих в организациях и фирмах. Описаны криптографические методы и программно-аппаратные средства обеспечения информационной безопасности, защиты процессов переработки информации от вирусного заражения, разрушающих программных действий и изменений.

Для студентов учреждений высшего профессионального образования.

УДК 621.391(075.8)
ББК 32.81я73

ISBN 978-5-7695-9222-5

ПРЕДИСЛОВИЕ

В связи с усилением взаимосвязи и взаимозависимости между государствами наблюдается активизация политической деятельности субъектов международной жизни, направленной на реализацию собственных национальных интересов. Вследствие этого обостряется геополитическая борьба между странами за обладание природными ресурсами и достижение более высокого жизненного уровня своих граждан. Формы этой борьбы различны, но ее ожесточенность и бескомпромиссный характер свидетельствуют об актуализации для каждого государства в отдельности вопросов обеспечения национальной безопасности, решения проблем выживания и развития. При этом глобализация и информационная революция XX—XXI вв. в современном мире являются определяющими, диалектически связанными между собой геополитическими процессами.

Геополитические процессы и тенденции развития мирового сообщества не являются случайными, они формируются и управляются ведущими западными государствами, прежде всего США, в ходе геополитического информационного противоборства (ГИП) на базе:

1) политического прогнозирования развития событий при сохранении существующих тенденций и без активного вмешательства;

2) постановки целей;

3) формирования стратегии и тактики достижения целей;

4) принятия (осознания) базовых ценностей существования и приоритетов развития (решения вопросов самоидентификации и цивилизационного выбора);

5) видения и осознания существующей реальности (моделирования элементов, связей и простейших систем);

6) поиска, сбора и обработки информации;

7) стратегического многофакторного анализа внешнего и внутреннего положения (моделирования структур, построения сложных многоуровневых моделей взаимодействия систем);

8) обнаружения, определения и формулирования проблем;

9) определения информационных, временных, финансовых, организационных и прочих ресурсных ограничений;

10) разработки конкретных технологий, методов и способов решения поставленных задач (для достижения целей);

11) формулирования альтернативных вариантов решения задач;

12) выбора критерия оценки эффективности принимаемых (реализуемых) вариантов решения задач;

13) выбора наилучшего варианта решения и его исполнения;

14) анализа реакции на принятое (реализованное) решение;

15) прогнозирования последствий, к которым приведет реализация той или иной альтернативы;

16) коррекции решения (внесения поправок на всех уровнях данной схемы).

Геополитическое информационное противоборство — одна из современных форм борьбы между государствами, а также система мер, проводимых одним государством с целью нарушения информационной безопасности (ИБ) другого государства при одновременной защите от аналогичных действий со стороны противостоящего государства.

Информационное противоборство — это форма борьбы, представляющая собой использование специальных (политических, экономических, дипломатических, военных, технических и др.) методов, способов и средств для воздействия на информационную среду противостоящей стороны и защиты собственной в интересах достижения поставленных целей.

Основные сферы ведения информационного противоборства:

- политическая;
- дипломатическая;
- техническая;
- финансово-экономическая;
- духовная;
- военная;
- энергоинформационная.

Для организации ГИП в России принята Доктрина информационной безопасности.

Доктрина информационной безопасности Российской Федерации (ИБ РФ), появившаяся практически одновременно с Окинавской Хартией глобального информационного общества, символизирует прочное вхождение России в единое мировое информационное сообщество. Основные положения Доктрины ИБ РФ отражают интересы России в условиях многополярного мира и полностью соответствуют глобально-космическим проблемам человечества в XXI в.

Доктрина ИБ РФ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения ИБ РФ.

Она служит основой:

- для формирования государственной политики в области обеспечения ИБ РФ;

• подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения ИБ РФ;

• разработки целевых программ обеспечения ИБ РФ.

Доктрина ИБ РФ развивает концепцию национальной безопасности Российской Федерации применительно к информационной сфере.

Начало XXI в. знаменуется бурным развитием информационных технологий во всех сферах жизни человечества. При этом информация все в большей мере становится стратегическим ресурсом государства, производительной силой и дорогим товаром. Это не может не вызывать стремления государств, организаций и отдельных граждан получить преимущества за счет овладения информацией, не доступной оппонентам, а также за счет нанесения ущерба информационным ресурсам противника (конкурента) и защиты своих информационных ресурсов. Поэтому национальная безопасность Российской Федерации существенным образом зависит от обеспечения ИБ, и в ходе технического прогресса эта зависимость будет усиливаться.

Остроту межгосударственного информационного противоборства можно наблюдать в оборонной сфере, высшей формой которой являются информационные войны в различных областях информационных технологий, в стремлении криминальных структур противоправно использовать информационные ресурсы, в необходимости обеспечения прав граждан на информационный обмен. При этом важно обеспечить конституционные права граждан на получение достоверной информации, на ее использование в интересах осуществления законной деятельности, а также на защиту информации, обеспечивающую личную безопасность, на обеспечение защиты информации в компьютерных системах (КС), являющихся материальной основой информатизации общества.

Комплексное обеспечение ИБ на всех уровнях может быть реализовано, если создана и функционирует система защиты информации, охватывающая весь жизненный цикл прохождения информации — от идеи и разработки проекта до утилизации изделия — и всю технологическую цепочку сбора, хранения, обработки и выдачи информации в КС и коммуникациях.

В данном учебном пособии описаны и раскрыты методологии обеспечения ИБ в деятельности общества, государства, фирм, систем и отдельных граждан.

В гл. 1 представлены основные положения, понятия и определения, термины, методы обеспечения ИБ РФ, различные виды и источники угроз ИБ РФ. В гл. 2, 3 и 4 описано организационно-правовое методологическое обеспечение ИБ деятельности общества, фирм и систем по различным направлениям ее жизненного цикла. В гл. 5 представлены программно-аппаратные средства обес-

печения функционирования предприятий и, в частности, средства защиты персональной электронно-вычислительной машины (ПЭВМ), их программное обеспечение и данные, в том числе в типовых операционных системах (ОС), системах управления базами данных (СУБД), вычислительных сетях, Интернет и Интранет.

Авторы выражают благодарность академику Академии проблем безопасности, обороны и правопорядка, генеральному директору ООО «Петровка-Р» Н. Н. Ролдугину за предоставленные материалы по практическому применению средств защиты информации в телефонных и вычислительных сетях.

СПИСОК СОКРАЩЕНИЙ

АБП — агрегат бесперебойного питания
АДМ — адаптивная дельта-модуляция
АИТ — автоматизированные информационные технологии
АОН — автоматический определитель номера
АРМ — автоматизированное рабочее место
АС — автоматизированная система
АСКД — автоматизированная система контроля доступом
АСОД — автоматизированная система обработки данных
АСУ — автоматизированная система управления
АТС — абонентская телефонная станция
БД — база данных
БПОС — блок питания и обработки сигналов
БУ — блок уплотнения (сигналов датчиков)
ВЗУ — внешнее запоминающее устройство
ВР — виртуальная реальность
ВС — вычислительная система
ГА — Генеральная Ассамблея (ООН)
ГИП — геополитическое информационное противоборство
ГМД — гибкий магнитный диск
ГТС — городская телефонная станция
ДЗУ — дисковое запоминающее устройство
ЕС — Европейский Союз
ЗУ — запоминающее устройство
ИА — идентификация и аутентификация
ИБ — информационная безопасность
ИК — идентификационная карточка
ИПВ — информационно-психологическое воздействие
ИПС — изолированная программная среда
ИС — интегральная схема
ИТ — информационные технологии
КМ — коммуникационный модуль
КС — компьютерная система
КСА — комплекс средств автоматизации
КСЗИ — комплексная система защиты процессов переработки информации
ЛВС — локальная вычислительная сеть
ЛС — локальный сегмент
МБ — модель безопасности

МБО — монитор безопасности объекта
МБС — монитор безопасности системы
НИС — несанкционированное изменение структур
НСД — несанкционированный доступ
НСДИ — несанкционированный доступ к информации
ОБИ — обеспечение безопасности информации
ОБСЕ — Организация по безопасности и сотрудничеству в Европе
ОВО — отказ в обслуживании
ОЗУ — оперативное запоминающее устройство
ООА — объектно-ориентированный анализ
ООН — Организация Объединенных Наций
ООП — объектно-ориентированное программирование
ОП — оперативная память
ОРК — открытое распределение ключей
ОС — операционная система
ПБ — политика безопасности
ПЗС — прибор с зарядовой связью
ПЗУ — постоянное запоминающее устройство
ПИК — пластиковая идентификационная карточка
ПИН — персональный идентификационный номер
ПК — персональный компьютер
ПО — программное обеспечение
ПП — процедура преобразования
ПРД — пользователь распределенного доступа
ПС — программное средство
ПСЧ — псевдослучайное число
ПЦ — процессор
ПЭВМ — персональная электронно-вычислительная машина
ПЭМИН — побочное электромагнитное излучение и наводки
РД — руководящий документ
РКС — распределенная компьютерная система
РПВ — разрушающие программные воздействия
РПС — разрушающее программное средство
СБ — стратегия безопасности
СВТ — средства вычислительной техники
СЗИ — система защиты процессов переработки информации
СЗИК — система защиты от исследования и копирования
СКВУ — система контроля вскрытия устройств
СМИ — средства массовой информации
СНГ — Содружество Независимых государств
СНПИ — средства негласного получения информации
СОК — система с открытым ключом
СОО — система охраны объекта
СПД — система передачи данных
СРД — система разграничения доступа

СУБД — система управления базами данных
ТЛФ — телефонный аппарат
ТПО — телекоммуникационное программное обеспечение
ТС — техническое средство
УВК — устройство ввода кода
ФАПСИ — Федеральное агентство правительственной связи и информации
ФК — функциональный контроль
ФПУ — фильтр прикладного уровня
ЦПУ — центральный пульт управления
ЦРК — центр распределения ключей
ЭВТ — электронно-вычислительная техника
ЭЛТ — электронно-лучевая трубка
ЭМИ — электромагнитное излучение
ЭСОД — электронная система обработки данных

Глава 1

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЕЯТЕЛЬНОСТИ ОБЩЕСТВА И ЕЕ ОСНОВНЫЕ ПОЛОЖЕНИЯ

1.1. Информационные геополитические и экономические процессы современного общества

1.1.1. Основные положения информатизации общества и обеспечение безопасности его деятельности

Современный этап развития общества характеризуется возрастающей ролью информационных взаимодействий, представляющих собой совокупность информационных инфраструктур и субъектов, осуществляющих сбор, формирование, распространение и использование информации. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации.

Массовая компьютеризация, внедрение и развитие новейших информационных технологий привели к прорыву в сферах образования, бизнеса, промышленного производства, научных исследований и социальной жизни.

Информация превратилась в глобальный неистощимый ресурс человечества, вступившего в новую эпоху развития цивилизации — эпоху интенсивного освоения этого информационного ресурса.

Идея, что информацию можно рассматривать как нечто самостоятельное, возникла вместе с новой наукой — кибернетикой, доказавшей, что информация имеет непосредственное отношение к процессам управления и развития, обеспечивающим устойчивость и выживаемость любых систем.

Нарастание темпов ускорения прогресса в обществе — одно из самых существенных и наименее изученных социальных явлений. Научное объяснение причины ускорения темпов общественного прогресса может быть дано, если процессы развития в человеческом обществе будут рассмотрены с точки зрения системно-кибернетического подхода, т.е. как целенаправленная информационно-управленческая деятельность людей с обязательным учетом факторов времени и социальных аспектов его развития, уровней организации.

В основу системно-кибернетического подхода должны быть положены четыре фундаментальных аспекта кибернетики: информационный, управленческий, организационный и социальный.

Новым в системно-кибернетическом подходе является то, что составляющие его аспекты рассматриваются в динамическом единстве с обязательным учетом в каждом из них социальной составляющей управления.

В результате анализа информации о взаимодействиях с внешней средой психика человека формировала понимание того, что ускорение информационных процессов, усиление коммуникативности и целенаправленных взаимодействий повышают живучесть индивида, популяций, социальных систем. Это привело к интенсификации информационных процессов в человеческом обществе.

Неустанная, не прекращающаяся по сей день борьба за скорость и эффективность обращения и взаимодействия особенно ярко проявилась в интенсивном развитии средств непосредственной передачи информации через книгопечатание, телеграф, телефон, радио, телевидение, компьютер, Интернет, мобильные средства связи и т.д.

Выдающийся русский ученый В.М.Бехтерев в 1921 г. сформулировал 23 основных закона поведения человеческих коллективов.

1. Закон сохранения энергии. Общественная или коллективная энергия составляется из совокупности запасных энергий всех участвующих в общей работе лиц, далеко не вся переходит в полезную или действительную работу; часть ее тратится на преодоление инерции коллектива, внутреннее трение между участниками работы, преодоление внешних препятствий в работе, в чем бы они ни проявлялись.

2. Закон пропорционального соотношения скорости движения с движущей силой. В каждый данный момент общество, находясь в недвижном равновесии, является результатом взаимодействия возбуждающих и тормозящих условий, причем всякое общественное движение протекает в направлении равнодействующих тех и других условий, выливаясь опять-таки в такую форму, которая определяется соответственным преобладанием возбуждающих сил над тормозящими влияниями.

3. Закон тяготения.

4. Закон отталкивания.

5. Закон противодействия, равного действию.

6. Закон подобия.

7. Закон периодичности, или ритма. Фактически всякое государство в жизненном цикле своего существования, подвергаясь закону ритма, проходит сначала период первоначального развития, следующий за ним период расцвета, после чего следует пе-

риод упадка, а затем в обновленной форме государство может вновь проявить свою энергию и мощь, достичь нового расцвета, за которым опять неизбежно последует его упадок, и т. д.

8. Закон инерции.
9. Закон непрерывного движения и изменчивости.
10. Закон рассеивания энергии, или энтропии.
11. Закон относительности.
12. Закон эволюции.
13. Закон дифференцирования.
14. Закон воспроизведения.
15. Закон избирательного обобщения, или синтеза.
16. Закон исторической последовательности.
17. Закон экономии.
18. Закон приспособления.
19. Закон отбора.
20. Закон взаимодействия.
21. Закон компенсации, или замещения символами или знаками.
22. Закон зависимых отношений.
23. Закон индивидуальности.

В.М.Бехтерев выделил основные типы человеческих коллективов (рис. 1.1).

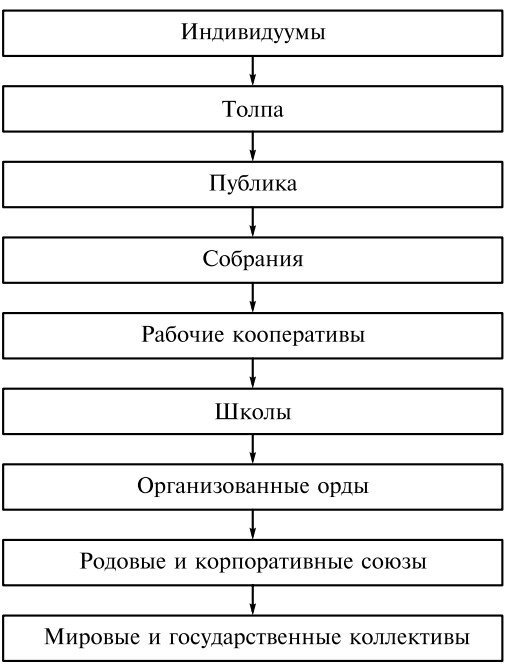

Рис. 1.1. Основные типы человеческих коллективов

Современные естественно-научные знания служат теоретико-методологической предпосылкой для построения логически стройной единой развивающейся картины мира на базе социальной информации. Феномен социальной информации привел общество к возможностям эффективно использовать ее во всех процессах жизненного цикла общества, а особенно эффективно — в вопросах управления и взаимодействия.

В соответствии с концептуальным подходом профессора Р. Ф. Абдеева можно выделить следующие виды информации:

- физическая, присущая процессам отражения в неорганической природе;
- биологическая, циркулирующая в живой природе и формирующая ее структуры;
- социальная, передающаяся в человеческом обществе в процессе коммуникаций между людьми.

Можно также выделить классы информационных структур:

- естественно возникшие информационные структуры неорганической природы;
- естественно возникшие информационные структуры органической природы;
- искусственные информационные структуры, созданные целенаправленной деятельностью человека (так называемая вторая природа, или ноосфера).

«Ноос» — древнегреческое название человеческого разума, следовательно, ноосфера — сфера человеческого разума.

Термин «ноосфера» был предложен в 1927 г. французским математиком и философом Эдуардом Леруа для использования его в описании состояния биосферы. Вскоре после Э. Леруа этот термин стал употреблять известный французский палеолонтолог, антрополог и член ордена иезуитов Пьер Тейяр де Шарден. Однако в соответствии со своим мировоззрением он придал термину «ноосфера» несколько иное понимание, так как считал, что разум не является неизбежным результатом эволюции мыслительного аппарата, но дан человеку Богом.

В. И. Вернадский лично знал французских ученых, но не спешил воспользоваться термином «ноосфера». Этот термин понадобился В. И. Вернадскому лишь тогда, когда он стал разрабатывать идею об эволюции биосферы. Первое упоминание его в письмах относится к 1935 г., а первое упоминание в печати — в 1937 г.

В работе «Живое вещество и биосфера»* В. И. Вернадский дает свое понимание ноосферы: «Исторический процесс на наших глазах коренном образом меняется... Человечество, взятое в целом, становится мощной геологической силой. И перед ним, перед его

---

* *Вернадский В. И.* Живое вещество и биосфера / В. И. Вернадский. — М. : Наука, 1994.

мыслью и трудом, становится вопрос о перестройке биосферы в интересах свободно мыслящего человечества как единого целого. Это новое состояние биосферы, к которому мы, не замечая этого, приближаемся, и есть ноосфера».

Другой взгляд на информационные процессы окружающего нас мира представляет их как науку — информациологию, которую сформулировал и обосновал И. И. Юзвишин в работе «Основы информациологии»*. Она значительно расширяет и углубляет методологию изучения и переработки информации.

В конце XX в. усиливается внимание мировой политической элиты к феномену социальной информации, так как социальная информация может являться индикатором (показателем) функционирования мировой политики, которая базируется в основном на социально-экономических аспектах жизненного цикла государства.

Социальную информацию в мировом процессе классифицируют по следующим признакам:

- по объему циркуляции — на региональную; национальную; континентальную; глобальную;
- по времени циркуляции — на краткосрочную; среднесрочную; долгосрочную;
- по характеристикам — на позитивную, негативную, нейтральную;
- по способу представления информации — на передаваемую с помощью СМИ; через спецслужбы; через неформальные связи; с помощью дипломатических источников; через бизнес-структуры; через компьютерные, телекоммуникационные и мобильные сети;
- по назначению информации — для убеждения; управления и коррекции принятия решений; воздействия; получения ответной реакции; компрометации; создания новых ценностей и правил взаимодействий.

Другую характеристику типов и видов социальной информации дал академик В. Г. Афанасьев в книге «Социальная информация»**. Он выделил типы и виды социальной информации.

Типы социальной информации:

- о прошлом;
- о настоящем;
- о будущем: прогностическая; ориентировочная; нормативная; предупредительная; плановая.

Виды социальной информации:

- по направленности: горизонтальная; вертикальная (прямая — директивно-нормативная, обратная — контрольно-отчетная);
- по объему циркуляции: внутренняя; внешняя.

---

* *Юзвишин И. И.* Основы информациологии : учебник / И. И. Юзвишин. — 3-е изд., перераб. и доп. — М. : Высш. шк., 2001.

** *Афанасьев В. Г.* Социальная информация / В. Г. Афанасьев. — М. : Наука, 1994.

По Н. А. Бердяеву* социальная информация определяется традиционной матрицей сознания, в основе которой на современном этапе лежит триада: самоуважение, самоорганизация и самореализация.

В XX в. управление информационными потоками превращается в решающий фактор завоевания, сохранения и удержания руководства и власти. Пожалуй, первыми это осознали американцы. Они создали официальную общегосударственную систему «Социальные показатели».

Система «Социальные показатели» состоит из восьми блоков, включающих в себя 167 показателей. Количество показателей распределяется по блокам в следующем соотношении:

1) здоровье — 29;
2) общественная безопасность — 23;
3) образование — 20;
4) труд (выбор ценностей — удовлетворенность трудом) — 28;
5) доход — 24;
6) жилище — 17;
7) досуг — рекреация (т. е. отдых) — 11;
8) демография — 15.

В отличие от созданной системы текущей социальной информации организация системы перспективной социальной информации все еще находится в стадии становления. Но первые результаты ее воздействия на политику США уже имеются. В частности, характерно, что одной из основных целей стратегии национальной безопасности США в последние десятилетия является защита образа жизни.

С помощью общегосударственной системы «Социальные показатели» американской политической элите удается определить основные параметры образа жизни рядовых граждан США. Это позволяет политической элите США проводить стратегический анализ психического состояния не только американцев, оперативно реагировать на возникающие проблемы в «социальном самочувствии нации», фиксировать источники негативных внешних и внутренних информационно-психологических воздействий в довольно значительном количестве стран мира.

Таким образом, в США создана эффективная система диагностики внутренней социальной информации (в интересах власти), а в конце XX в. началось создание систем диагностики внешней социальной информации с помощью международных информационных систем (Интернет и др.), ЮСИА и т. д.

В настоящее время система диагностики социальной информации является ключевым звеном в ходе стратегического информационного противоборства национальных политических элит.

---

* *Бердяев Н. А.* Судьба России / Н. А. Бердяев. — М. : Политиздат, 1990.

По мнению доктора психологических наук М. Н. Решетникова, основу американского лидерства также составляет проведение специальной политики по привлечению в страну со всех континентов одаренной молодежи и научной элиты, независимо от национальности и расы, включая создание особых условий для того, чтобы они оставались в США.

В *специальную политику* были положены основополагающие исследования, проведенные в XX в.:

1) определено количество людей, способных к формированию новых прорывных идей (в науке, культуре, управлении и т. д.), которое в любой национальной популяции весьма ограничено и не превышает 3...5 %;

2) установлено, что интеллектуальная элита общества формируется столетиями и тысячелетиями и является самовоспроизводящей и чрезвычайно хрупкой системой;

3) установлено, что интеллектуал — это особый, в определенной степени искусственный, тип личности, для проявления которого именно в этом качестве требуется ряд особых условий:

- наличие задатков (генетический фактор) — абсолютное большинство интеллектуалов являются прямыми потомками столь же интеллектуальных родителей;
- максимально раннее (с 3...5 лет) погружение в высокоинтеллектуальную семейную или профессиональную среду определенной направленности (химия, физика, медицина, законотворчество и т. д.), получившее название «фактор специфически социального исследования»;
- максимально раннее (до 5...7 лет) выявление преобладающих способностей и склонностей, которые имеют свои периоды «манифестации» (если конкретная способность не была замечена и не было начато ее развитие в этот период, то она может быть утрачена навсегда);
- наличие талантливых учителей (одаренный ребенок, погруженный в обычную образовательную среду, в большинстве случаев очень быстро усредняется и как талант — утрачивается навсегда);
- отсутствие у одаренной личности материальных и бытовых проблем.

Абсолютное большинство одаренных личностей отличается высоким уровнем самоуважения, чрезмерной чувствительностью к любым психотравмирующим факторам, аполитичны, не склонны к сотрудничеству (в том числе с коллегами, представителями власти и т. д.). Значительная часть высокоодаренных личностей отличается специфической моральной динамичностью (отсутствием склонности следовать принятым в обществе нормам и правилам, в том числе в сфере сексуального поведения и т. д.).

Исходя из этих исследований в США на протяжении последних десятилетий чрезвычайно активно работает система приглашений и обеспечения солидными грантами талантливых учащихся школ, стажеров, аспирантов и докторантов из зарубежных стран, государственная система выявления талантливых детей.

Особенностью состояния процессов организации, управления и использования социальной информации в современной России является нахождение этих процессов в зачаточном состоянии, т. е. становление (организационное, теоретическое и практическое) как текущего, так и перспективного социального информационного комплекса.

Российские специалисты считают, что политической элите России нужна своя национальная система анализа социальной информации (текущей и перспективной), причем информационные ресурсы такой системы должны быть надежно защищены от негативных информационных воздействий со стороны геополитических противников (важно полностью исключить возможности подмены или уничтожения социальной информации по важнейшим вопросам образа жизни российского народа). В рамках этих программ сделаны определенные шаги в создании российской государственной системы выявления талантливых детей, стимулирования их творческой деятельности и др.

Россия должна быть готова к глобальному бескомпромиссному информационно-психологическому противоборству мировых элит (т. е. защите *матриц сознания* россиян от негативных информационных потоков), в том числе и в ходе избирательных процессов.

В связи с этим существенно возрастает значение и объем информационно-аналитической работы. Для организации информационного мониторинга *матриц сознания* политической элиты и населения России необходима система стратегического анализа социальной информации России. Такая система должна проводить анализ на различных уровнях (федеральном, региональном, местном). Результаты этого мониторинга должны постоянно учитываться при организации и проведении избирательных кампаний. Такая система должна быть одним из ключевых звеньев диагностики состояния информационной среды общества и всего Российского государства.

До недавнего времени в теории и на практике основное внимание уделялось обеспечению военной безопасности государств. Сегодня уже стала очевидной ограниченность данного подхода, так как научно-техническая революция привела к созданию информационного общества и информация является основным инструментом власти.

Элвин и Хэйди Тоффлер — известные всему миру американские социальные мыслители — в книге «Создание новой цивили-

зации. Политика третьей волны»* уделяют особое внимание информационным технологиям: «Сегодня расстановка сил в мире изменилась. Мы движемся к совершенно другой структуре сил, разделяющей мир не на две, а на три четко определенные противоположные враждующие цивилизации. Символ Первой, как и прежде, — мотыга, Второй — конвейер, а Третьей — компьютер».

Следует отметить, что проблема обеспечения ИБ в нашей стране длительное время не только не выдвигалась, но и фактически игнорировалась. При этом считалось, что путем тотальной секретности и различными ограничениями можно обеспечить ИБ страны.

Только сейчас Российское государство начинает серьезно и ответственно подходить к проблеме определения и отстаивания жизненно важных интересов, реальных и потенциальных угроз в информационной сфере. Российская политическая и техническая элита начинает осознавать необходимость решения проблем обеспечения ИБ.

1.1.2. Составляющие национальных интересов Российской Федерации в информационной сфере

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению ИБ.

Выделены четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая 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 включает в себя информационное обеспечение государственной политики Российской Федерации, связанное с доведением достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни до российской и международной общественности. При этом необходимо обеспечить доступ граждан к открытым государственным информационным ресурсам.

Третья составляющая включает в себя развитие современных информационных технологий, отечественной индустрии инфор-

---

* *Тоффлер Э.* Создание новой цивилизации. Политика третьей волны / Э. Тоффлер, Х. Тоффлер. — М. : Гардарика, 1995.

мации, 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 включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

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

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Основными составляющими в интенсификации информационных процессов при системно-кибернетическом и социальном подходе к формализации хода общественного развития являются:

- неуклонное возрастание скоростей информационного обмена;
- увеличение объема добываемой и передаваемой информации;
- ускорение процессов обработки информации;

• расширение применения адаптивного управления (с использованием обратных связей);

• расширение наглядного (визуального) представления информации в процессах управления;

• бурный рост технической оснащенности управленческого труда;

• учет особенностей социально-психологических взаимодействий человеческого социума и образований.

1.1.3. Основные свойства и характеристики информационного обеспечения безопасности функционирования информационных систем управления предприятий и фирм

Информация, создаваемая, потребляемая и хранимая в процессе функционирования и взаимодействия социальных, технических и организационно-технических систем друг с другом и с внешней средой (чаще всего это одно и тоже), может быть условно разделена на два основных рода: внутреннюю и внешнюю.

Внутренняя информация — это структурная или преобразующая информация (последнее название адекватно для частного вида организационно-технических структур, например для автоматизированных систем управления (АСУ)). Внутренняя структурная информация создается, потребляется и распространяется самой системой. Ее использование санкционировано только для внутреннего потребления, т.е. для управления элементами и подсистемами, обеспечения основного и вспомогательных производственных процессов и т.д. Эту информацию содержат массивы данных, документы и файлы, не предназначенные для передачи внешней среде или через внешнюю среду.

Внешняя информация циркулирует в каналах обмена с иными системами, составляющими в совокупности внешнюю среду. В процессе информационного обмена с внешней средой может участвовать информация, являющаяся основным продуктом деятельности системы, и контрольная информация о состоянии системы (финансовая, отчетная, плановая и т.д.), правовая и нормативная информация, регламентирующая условия функционирования системы, рекламная и другая информация. В ряде случаев к внешней информации приходится относить и внутреннюю информацию, к которой осуществляется несанкционированных доступ посредством технических каналов утечки.

Определение качественно различных форм проявления информации двух указанных родов можно провести на основе анализа модели процесса управления сложным динамическим объектом. В соответствии с этой моделью (рис. 1.2) управление основным процессом функционирования $P_o(S)$ динамического объекта S осуществляется в замкнутом контуре, в котором протекают процес-

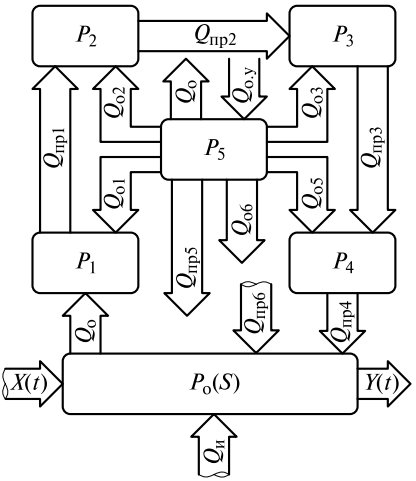

Рис. 1.2. Структура модели управления сложным динамическим объектом

сы P_i, $i \in 1, ..., 5$, и циркулируют сообщения (происходит обмен информационными массивами, документами) Q.

Множество процессов P_i объединяет наблюдение, измерение, идентификацию, выработку управляющих решений, координацию совместных действий, информационный обмен между подсистемами — участниками процесса $P_о(S)$ функционирования динамического объекта.

При этом информация, которую содержат сообщения Q, проявляется в следующих формах.

1. Осведомляющая информация, которая заключена в массивах $Q_о \in \{Q_0, ..., Q_6\}$ и содержит все сведения о системе S и свойствах управляемого процесса $P(S)$, а также о действующих на него управляющих ($Q_{о.у}$, $X(t)$) и искажающих (дестабилизирующих) воздействиях информации $Q_и$ внешней среды.

2. Преобразующая информация, объединяемая массивами $Q_{пр i}$, $i \in 1, ..., 5$. Эта информация заключена в устройствах и подсистемах системы S.

3. Преобразующая информация в массивах $Q_{пр\,i}$, $i \in 1, ..., 6$, среди которых $Q_{пр1}$ — массивы результатов измерения (восприятия) свойств и характеристик осведомляющих данных $Q_о$; массивы данных $Q_{пр2}$ наблюдения (распознавания) ситуаций, определяемых осведомляющей информацией $Q_о$; совокупности результатов $Q_{пр3}$ идентификации (предсказания) хода протекания основного производственного процесса $P_о(S)$, которые необходимы для эффективного управления; документы $Q_{пр4}$ с результатами решений о целях функционирования системы и управления; данные $Q_{пр5}$, необходимые для координации целей и координируемости процессов в системе; данные $Q_{пр6}$ о структуре и взаимодействии подсистем в составе $P_о(S)$.

4. Управляющая информация $Q_{о.у}$, к которой относятся все сведения, нужные для целенаправленного изменения состава, характеристик и параметров основного процесса $P(S)$ функционирования системы. В частности, процессом $P_о(S)$ может быть управляемый производственный процесс.