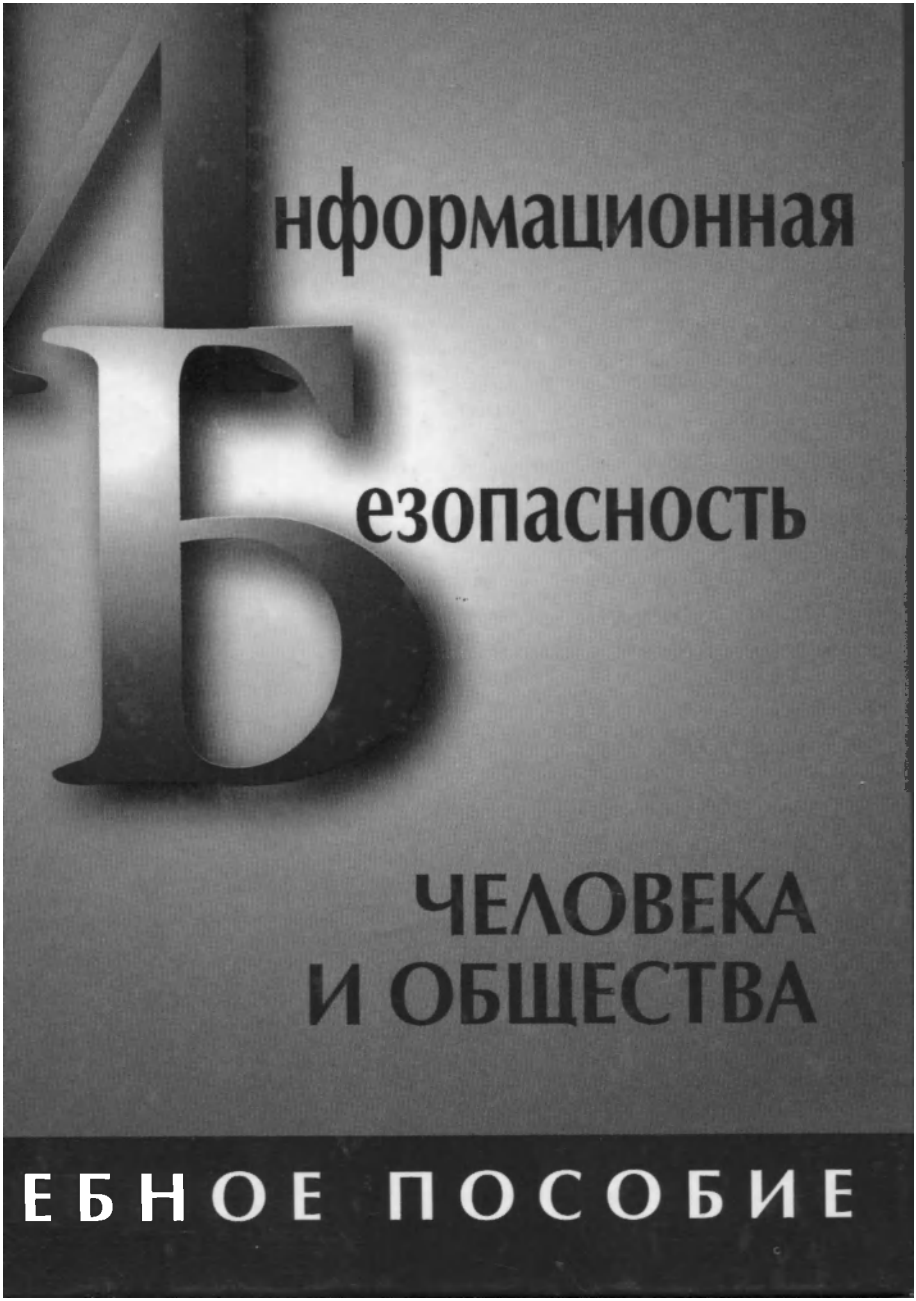
Информационная
безопасность
человека
и общества
учебное пособие

В. П. Петров
С. В. Петров

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЧЕЛОВЕКА И ОБЩЕСТВА

Учебное пособие

Рекомендовано УМО Министерства образования и науки РФ
по специальностям педагогического образования
в качестве учебного пособия для студентов
высших учебных заведений, обучающихся
по специальности 050104(033300) «Безопасность жизнедеятельности»

TATU Samarqand filiali
Axborot-resurs
markazi
№ 12787

Москва
ЭНАС
2007

УДК 614.8
ББК 68.9
П30

Издано при финансовой поддержке Федерального агентства по печати и массовым коммуникациям в рамках Федеральной целевой программы «Культура России».

Петров В. П., Петров С. В. Информационная безопасность
П30 человека и общества : учебное пособие / В. П. Петров, С. В. Петров. – М. : ЭНАС, 2007. – 336 с.

ISBN 978-5-93196-814-8

В учебном пособии рассмотрены основные понятия, история, проблемы и угрозы информационной безопасности, наиболее важные направления ее обеспечения, включая основы защиты информации в экономике, внутренней и внешней политике, науке и технике.

Обсуждаются вопросы правового и организационного обеспечения информационной безопасности, информационного обеспечения оборонных мероприятий и боевых действий. Особое внимание уделяется обеспечению информационной безопасности в правоохранительной сфере, а также при возникновении чрезвычайных ситуаций.

Рассматриваются сущность и методы информационного воздействия на человека, информационная безопасность в сфере духовной жизни человека и общества, в повседневной жизни.

Пособие соответствует требованиям образовательного стандарта и предназначено для студентов педагогических вузов специальности 033300/050104 «Безопасность жизнедеятельности». Может быть рекомендовано руководителям и работникам образовательных учреждений, слушателям курсов переподготовки и повышения квалификации работников образования, специалистам по обеспечению безопасности.

УДК 614.8
ББК 68.9

© В. П. Петров, 2007
© С. В. Петров, 2007
© ЗАО «Издательство НЦ ЭНАС», 2007

ISBN 978-5-93196-814-8

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ **5**

Глава 1. **ОСНОВНЫЕ ПОНЯТИЯ И ИСТОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** **8**

1.1. Основные понятия **8**
1.2. Информационные противостояния от древности до Нового времени **18**
1.3. Информационные войны XX века **25**

Глава 2. **ПРОБЛЕМЫ И УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** **36**

2.1. Основные проблемы информационной безопасности и пути их решения **36**
2.2. Виды и источники угроз информационной безопасности **44**
2.3. Место информационной безопасности в системе национальной безопасности России **48**
2.4. Защита сведений, составляющих государственную и коммерческую тайну, конфиденциальную информацию и интеллектуальную собственность **51**

Глава 3. **ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** **65**

3.1. Защита информации в экономике, внутренней и внешней политике, науке и технике **65**
3.2. Информационное обеспечение оборонных мероприятий и боевых действий **72**
3.3. Обеспечение информационной безопасности в правоохранительной сфере и при возникновении чрезвычайных ситуаций **80**
3.4. Основные направления и мероприятия по защите электронной информации **87**
3.5. Безопасность в сфере духовной жизни человека и общества **99**

Глава 4. **ПРАВОВОЕ И ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** **106**

4.1. Конституция РФ и Доктрина информационной безопасности РФ о правовом обеспечении информационной сферы **106**

4.2. Федеральное законодательство в сфере информационной безопасности 112
4.3. Указы Президента РФ и иные нормативно-правовые акты по вопросам информационной безопасности 122
4.4. Организационное обеспечение информационной безопасности 126
4.5. Международное сотрудничество России в области обеспечения информационной безопасности 133

Глава 5. **СУЩНОСТЬ И МЕТОДЫ ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ НА ЧЕЛОВЕКА** 138

5.1. Сущность и современное состояние манипуляции сознанием и поведением людей 138
5.2. Основные методы и средства информационного воздействия на человека 152
5.3. Мифы как инструмент воздействия на людей 170
5.4. Манипулятивные технологии в избирательных кампаниях 182
5.5. Методы тоталитарных сект и способы защиты от них 190

Глава 6. **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ПОВСЕДНЕВНОЙ ЖИЗНИ** 220

6.1. Рыночные отношения – социально-экономическая основа манипуляции людьми 220
6.2. Влияние средств массовой информации на мировоззрение людей и духовно-нравственное становление подрастающих поколений 227
6.3. Роль рекламы в манипуляции сознанием людей 240
6.4. Повседневно-бытовой уровень манипуляции сознанием 251
6.5. Защита русского языка – важное условие информационной безопасности России 265
6.6. Средства информационного воздействия и защита здоровья 281

Глава 7. **«ГЛОБАЛЬНОЕ ОБЩЕСТВО» И ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** 304

7.1. Объективные и субъективные предпосылки создания глобального общества 304
7.2. Роль Интернета в мировом информационном пространстве 310
7.3. Глобальные ожидания и опасения человечества 317

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ 329

ВВЕДЕНИЕ

Современный этап общемирового развития характеризуется возрастающей ролью информационной сферы. Превращаясь в системообразующий фактор жизни общества, она все более активно влияет на состояние политической, экономической, оборонной, личной, имущественной и других составляющих безопасности.

Сотрудничество и соперничество государств и организаций из традиционной материальной сферы все более отчетливо смещаются в ***информационную область***.

Россия стоит перед необходимостью осознания и принятия вызова, связанного с вступлением человечества в эпоху формирования мирового информационного сообщества. Современные информационные технологии существенно меняют не только структуру отношений, но и образ жизни людей, их мышление, механизмы функционирования семьи, общественных институтов, органов власти. Они становятся действенным фактором развития личности и общества. В то же время широкое распространение некоторых информационных технологий сопровождается появлением ряда новых угроз конституционным правам и свободам граждан, формированию здоровья, полноценной духовной жизни. Эти технологии уже используются для целей экономики, торговли, рекламы, политической борьбы, оказывая порой разрушительное воздействие на психику людей, в особенности подростков.

Информационное воздействие становится главным рычагом управления людьми, все больше заменяя физическое воздействие, тысячелетиями считавшееся непременным средством управления.

Вот почему одним из основных элементов национальной, общественной и личной безопасности становится информационная безопасность. В современном мире информационная безопасность – жизненно необходимое условие обеспечения интересов человека, общества и государства.

Целью дисциплины «Информационная безопасность» в гуманитарных вузах является обучение студентов принципам и средствам

обеспечения информационной безопасности личности, конкретных объектов и учреждений, общества и государства. Данная дисциплина способствует получению студентами фундаментального образования, формированию научного мировоззрения, развитию системного мышления, интеграции полученных ранее знаний.

Задачи дисциплины – дать основные знания, умения и навыки по вопросам обеспечения информационной безопасности личности, семьи, дома, образовательного учреждения, производственного объекта.

В результате изучения дисциплины студенты (слушатели) должны:

иметь представление:

о целях, задачах, принципах и основных направлениях обеспечения информационной безопасности;

о методологии создания систем защиты информации;

о средствах и методах защиты человека от противоправного информационного воздействия;

знать:

роль и место информационной безопасности в системе национальной безопасности страны;

угрозы информационной безопасности государства и общества;

содержание информационной войны, методы и средства ее ведения;

правовые основы обеспечения информационной безопасности;

информационные средства и технологии, негативно влияющие на здоровье;

способы и системы защиты информации;

средства обеспечения информационной безопасности при обработке информации, составляющей государственную, служебную или коммерческую тайну;

уметь:

выбирать и применять методы и средства защиты информации;

пользоваться современными средствами защиты информационной безопасности;

применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в иных сферах своей деятельности;

выявлять попытки противоправного информационного воздействия, манирулирования и противодействовать им;

соблюдать правила информационной безопасности в быту и в служебной обстановке;

обращаться за консультацией и помощью к специалистам при возникновении угроз информационной безопасности в любой сфере жизнедеятельности.

Учебное пособие подготовлено в соответствии с Государственным образовательным стандартом высшего профессионального образования по специальности 0333000/050104 «Безопасность жизнедеятельности».

Дисциплина «Информационная безопасность» в гуманитарных вузах тесно связана с дисциплинами, изучающими проблемы психологии, педагогики, информатики, программно-аппаратные и организационно-правовые методы обеспечения безопасности человека, общества и государства.

При подготовке учебного пособия авторы использовали публикации таких известных специалистов, как В. Т. Ганжин, М. И. Горбачев, Г. В. Грачев, А. А. Зиновьев, С. Г. Кара-Мурза, И. К. Мельник, И. Н. Панарин, Ю. И. Полищук, В. П. Пугачев, М. А. Родионов, Л. И. Шершнев.

Глава 1

ОСНОВНЫЕ ПОНЯТИЯ И ИСТОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационные процессы пронизывают все акты функционирования живой материи.
Информация пронизывает все поры жизни людей и общества.

Академик *А. И. Берг*

1.1. Основные понятия

***Информация** – это сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством для нужд человека.* Информация необходима каждому как условие и как средство существования человека в обществе. И поэтому так же нуждается в защите, как среда обитания, пища и все остальные элементы жизнедеятельности.

Стремительное нарастание возможностей оперативного обмена экономической, научно-технической, культурной, политической, военной и другой информацией является несомненным благом, великим достижением цивилизации.

В третьем тысячелетии, на фоне перехода человечества от индустриальной цивилизации к цивилизации информационной, информация стала одним из главных факторов исторического прогресса. Она имеет ключевое значение для успешного функционирования всех общественных и государственных институтов, адекватного поведения каждого отдельного человека. Без интенсивного обмена информацией, постоянной информационной связи с окружающим миром в принципе невозможна нормальная жизнедеятельность людей.

Однако, как известно, любое благо в определенных условиях или при неправильном использовании может перерасти в беду.

Например, прекращение информационных контактов с социальной средой, как правило, ведет к личностной деградации человека, становится источником различных отклонений — вплоть до психических расстройств.

Прогресс в любой сфере является позитивным и полезным до определенного предела, за которым его результаты могут оказаться вредными. Так, развитие информационных технологий вызвало одновременно расширение возможностей массовой ***дезинформации*** *— введения в заблуждение огромных масс людей путем сообщения неверных сведений, подтасовки фактов, подделки доказательств.*

В итоге современное общество образуют не только *информированные*, то есть *хорошо осведомленные о чем-либо*, люди, но и *дезинформированные — введенные в заблуждение ложной информацией.* Каких из них больше – неизвестно. Наряду с информированием людей постоянная дезинформация (а проще — обман, ложь) также стала нормой жизни во многих сообществах и странах. Она широко используется как информационное и психологическое оружие в международной политике, в идеологической обработке людей, в интересах экономической экспансии, для ослабления национально-государственного самосознания граждан, разрушения семей, корпораций и государств.

О роли влияния информационных факторов на жизнедеятельность современного общества говорит тот факт, что созданный человечеством в природной среде «искусственный мир» образует уже не только ***техносфера*** (мир техники, технологий, сооружений и т. п.), но и информационная сфера, значимость которой для жизни каждого из нас непрерывно возрастает.

Доктрина информационной безопасности РФ определяет ***информационную сферу*** как *совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.*

В наиболее общем виде информационную сферу (или информационную среду) образуют:

субъекты информационного взаимодействия или воздействия (люди, организации, системы);

собственно информация, предназначенная для использования субъектами информационной сферы;

информационные технологии и технические средства;

информационная инфраструктура, обеспечивающая возможность осуществления обмена информацией между субъектами;

общественные отношения, складывающиеся в связи с формированием, передачей, распространением и хранением информации, и система их регулирования.

Согласно Доктрине информационной безопасности РФ, ***под информационной безопасностью*** *Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.*

В специальной литературе используется более широкое определение: ***информационная безопасность*** *– это такое состояние социума, при котором обеспечена надежная и всесторонняя защита личности, общества и государства от воздействия на них особого вида угроз, выступающих в форме организованных информационных потоков и направленных на деформацию общественного и индивидуального сознания.*

Понятие «информационная безопасность» сегодня трактуется как в широком, так и в узком смысле. *В широком смысле* – это информационная безопасность человека, общества и государства. *В узком смысле* – это безопасность самой информации и каналов ее приема (передачи), а также организация защиты от применения противником информационного оружия в ходе боевых действий.

Понимание безопасности в контексте соотношения интересов личности, общества и государства предполагает рассмотрение ***информационно-психологической безопасности*** как аспекта общей проблемы.

Информационно-психологическую безопасность в общем виде можно определить как *состояние защищенности индивидуальной, групповой и общественной психологии социальных субъектов различных уровней общности от разрушительного воздействия на сознание негативных информационных факторов.*

Применительно к конкретному человеку информационно-психологическая безопасность – *это состояние защищенности*

сознания и психического здоровья человека, обеспечивающее его целостность как социального субъекта, возможность адекватного поведения и личностного развития в условиях неблагоприятных информационных воздействий.

***Информационное противоборство** – это комплексное взаимное информационное воздействие сторон друг на друга, которое способно привести к принятию благоприятных для инициатора воздействия решений либо парализовать информационную инфраструктуру противника.* Методы воздействия: радиоэлектронная борьба, компьютерные конфликты, действия на психологическом и мировоззренческом уровнях, вброс ложной или компрометирующей информации, внушение, навязывание и т. п.

Более острая стадия противоборства – ***информационная война** – согласованная деятельность по использованию информации как оружия для разрушающего воздействия на противника в различных сферах: экономической, политической, социальной и на поле боя.* Информационная война – война нового типа, ее основным объектом являются не только информационные системы, но, прежде всего, сознание людей, их поведение и здоровье.

В информационной войне для разрешения межгосударственных противоречий и конфликтов используются методы и средства силового воздействия на сознание общества и информационную сферу государств. Информационные войны могут происходить и внутри страны, например, при столкновении политических и экономических противников, в ситуациях обострения борьбы за власть, при проведении избирательных кампаний, судебных процессов и т. п.

Термин «информационная война» известен давно, но стал широко употребляться американскими специалистами после завершения войны с Ираком (1991–1992 гг.), где информационное оружие показало свою высокую эффективность. В 1992 г. Пентагон уже издал директиву «Информационная война» (TS 3600.1), в которой намечались основные задачи по подготовке к такого рода войнам, их методы и средства.

Основные цели и задачи информационной войны:

подавление и уничтожение систем управления противоборствующей стороны;

информационное обеспечение боевых действий, политики, экономики;

подавление электронных систем противника;

психологическое воздействие на личный состав и население;

хакерское проникновение в информационные системы противника.

Информационная угроза *– опасность, содержание которой составляют различная информация или ее комбинации, которые могут быть использованы против социального или социально-технического объекта (системы) с целью изменения его интересов, потребностей, ориентаций в соответствии с целями субъекта информации.*

Информационный риск *– вероятность информационной угрозы и реальных действий противника, мера измерения успешности или опасности возможных воздействий.* Риск зависит от характера воздействий и объекта воздействий, от условий их осуществления, а также от возможностей защиты.

Составным элементом информационных войн является ***информационная операция***. В зависимости от характера объектов и средств воздействия информационные операции подразделяются на *информационно-технические* и *информационно-психологические.*

Наступательная информационная операция *реализуется посредством наступательных информационных действий.* Она может включать следующие мероприятия:

стратегическая маскировка;

дезинформация противника;

психологические операции;

радиоэлектронное противоборство;

физическое уничтожение объектов информационной инфраструктуры;

атаки на компьютерные сети противника.

Наступательную информационную операцию, *осуществляемую вероломно и преследующую корыстные и даже преступные цели в отношении человека или общества* можно определить как ***информационную агрессию.***

Оборонительная информационная операция включает мероприятия по обеспечению безопасности собственных информационных ресурсов:

оперативную и стратегическую маскировку;
сохранение секретов;
контрразведку;
физическую защиту объектов информационной инфраструктуры;
глушение, блокирование СМИ противника;
контрпропаганду;
психотерапию;
контрдезинформацию;
радиоэлектронную борьбу.

Ведение информационных войн предполагает наличие и использование определенных средств борьбы, то есть оружия.

Под ***информационным оружием*** понимается *совокупность специально организованной информации, а также информационных технологий, применяемая для деструктивных воздействий на поведение и сознание населения, персонал эргасистем*, военнослужащих и информационно-технические инфраструктуры государства и общества* (информационно-технические системы, средства работы с информацией, подразделения, коллективы и социальные системы).

Информационное оружие, воздействующее непосредственно на человека, специалисты делят на два вида.

Информационно-психологическое оружие обращено прежде всего на сознание человека и уже через него *воздействует на поведение, убеждения, мотивы и потребности, нравственные установки, отношение к тому, что происходит в обществе.* В качестве такого оружия могут использоваться все средства массовой информации, Интернет, публичные выступления, беседы, внушение, гипноз и т. п.

Энергоинформационное оружие *воздействует на физиологию и психофизиологию человека, минуя его сознание.* Человек не осознает факта воздействия, но в зависимости от его вида начинает ощущать либо бодрость, уверенность в себе, либо подавленность, тревогу, страх, агрессивность на фоне утраты способности конт-

---

*Эргатическая система (эргасистема) – сложная система управления, составной элемент которой – человек-оператор (или группа операторов), например, система управления самолетом, диспетчерская служба вокзала, аэропорта.

ролировать свои действия. В природе подобное психофизическое воздействие могут оказывать, например, солнечные вспышки, влияющие на биоэлектрическую активность мозга и общее состояние человека.

В качестве источников энергоинформационного воздействия могут применяться радиолокационные системы, космические аппараты, низкочастотные и высокочастотные генераторы, биолокационные установки, химические и биологические средства и другие устройства.

С помощью энергоинформационного оружия можно изменить поведение людей, например, снизить или «разжечь» накал демонстраций, беспорядков и этим повлиять на текущие социальные процессы. Ухудшая психофизическое состояние личного состава противника или террористов, можно существенно снижать их боеспособность и даже побуждать к сдаче в плен. Важнейшим результатом применения такого оружия является необъяснимый, «животный», страх. А страх способен изменять человека коренным образом.

> Существует стариная притча о страхе. «Куда ты идешь?» – спросил странник, повстречавшись с Чумой. – «Иду в Багдад. Мне нужно уморить там пять тысяч человек». Через некоторое время тот же человек снова встретил Чуму. «Ты сказала, что уморишь пять тысяч, а уморила пятьдесят», – упрекнул он ее. «Нет, – возразила она, – я погубила только пять тысяч, остальные умерли от страха».

Цели информационных войн и применения информационного оружия – завоевание превосходства над противником и нанесение ему поражения как в конкретном акте противостояния или отдельной боевой операции, так и во внешней и внутренней политике, экономике, обороноспособности страны в целом.

Задачи применения информационного оружия:

подрыв международного авторитета государства, его сотрудничества с другими странами;

манипулирование общественным сознанием внутри страны, создание атмосферы бездуховности и безнравственности, негативного отношения к национальному наследию;

провоцирование политической напряженности и хаоса внутри страны, инициирование этнических и религиозных столкно-

вений, забастовок, массовых беспорядков и других акций протеста;

дезинформация населения об истории страны, о работе государственных органов, подрыв их авторитета, дискредитация всей системы управления;

нарушение системы управления войсками, вооружением и военной техникой, объектами повышенной опасности;

нанесение серьезного ущерба жизненно важным интересам государства в политической, экономической, социальной и других сферах деятельности.

В общей системе информационных средств особое значение имеет *социальная информация* – как наиболее сильное оружие и массовое средство воздействия. Именно эта информация определяет функционирование общественных образований, профессиональных, возрастных и этнических групп людей, государственных и общественных институтов, а также конкретных людей, их помыслы и поступки.

Под ***социальной информацией*** понимаются *сведения, неразрывно связанные с процессом усвоения человеком знаний, жизненных норм и ценностей, побуждающих его определенным образом функционировать в обществе.* К числу *сущностных признаков* социальной информации можно отнести следующие ее особенности:

социальная информация всегда обращена к личности, социальным группам, классам, социуму в целом. Она является средством прямого воздействия на развитие человеческой психики, сознание человека и общества;

социальная информация (через воздействие на общественное и индивидуальное сознание) в наибольшей степени определяет социально-экономические и политические ориентации людей во внутренней жизни государства и в отношениях с другими странами;

социальная информация определяет эффективность передачи социального опыта от поколения к поколению, сохранение и упрочение национальных традиций и обычаев;

социальная информация в значительной мере определяет практическое поведение людей.

Эти ресурсы социальной информации можно использовать как в прогрессивных целях, так и для корыстного давления одного государства (партии, социальной группы, личности и т. д.) на другое.

Главным объектом применения социальной информации как оружия является сфера общественного сознания индивидуума и различных общностей людей, национальный менталитет, духовно-нравственные и социально-психологические качества личности и общества в целом. Определенным образом структурированная и подготовленная информация такого рода может быть исключительно сильным *средством деформации индивидуального сознания*, вплоть до изменения психики, доведения ее до болезненного состояния. Более того, она способна стать побудительным мотивом к суицидальным действиям, может вызвать широкомасштабные протестные действия, экстремистские выступления, террористические акты, крупные вооруженные столкновения и т. д.

При ведении информационной войны в общественное сознание народа страны, ставшей жертвой агрессии, целенаправленно внедряются такие ложные представления об окружающем мире, которые позволяют агрессору в дальнейшем свободно манипулировать как правительством, так и населением этой страны и осуществлять захват необходимых ресурсов, практически не встречая сопротивления, без применения оружия обычного типа.

Агрессивное (по целям) использование социальной информации может прикрываться лозунгами о «социально-экономической помощи», «культурном сотрудничестве» и осуществляться через управляющую «элиту» страны – жертвы агрессии, которая в меру сформированных у нее установок способна нередко искренне верить, что работает во благо своего народа.

Преимущества информационных средств противоборства в сравнении с обычным оружием:

относительно невысокие затраты;

лучшая возможность скрытого применения;

размытость традиционных границ воздействия;

отсутствие выраженного отличия мероприятий информационной войны от других видов деятельности;

меньший риск собственного поражения;

отсутствие экологического ущерба;

возможность сохранения материально-экономической инфраструктуры.

Нередко информационное оружие называют «умным», «несмертоносным», более «гуманным». Это очень серьезное и крайне опасное по своим последствиям заблуждение. Данное оружие губительнее для людей, чем обычное средство поражения. Оно направлено против самого трудновосполнимого в человеке – его психики. И поэтому калечит людей глубже пулевого или осколочного ранения, искажая и опустошая их внутренний мир. Длительное воздействие целенаправленной дезинформацией, спланированной ложью неизбежно подавляет способность к подлинной жизни и порождает преступное поведение, наркоманию, психические расстройства, суициды.

После обычных войн рождаются здоровые, полноценные дети; общечеловеческий потенциал восстанавливается достаточно быстро. Пораженные информационным оружием не способны сформировать психически здоровое следующее поколение. По законам социальной наследственности они могут воспитать только себе подобных. Рядом с нервозным, закомплексованным, а то и просто «зомбированным» человеком, как правило, вырастает такой же невротик или зомби. В итоге после информационных войн проигравшее государство не способно восстанавливаться. А эти войны часто не имеют окончания.

Информационное оружие – это новый, страшный и пока еще не запрещенный вид оружия массового поражения. При нарастающей интенсивности и изощренности его применения у человечества нет будущего. Информационное оружие ***и смертоносно, и негуманно***: оно разрушает душевную сущность человека, лишая его главной основы жизнеспособности.

Масштабность и мощность воздействия информационных факторов на психику людей выдвигают обеспечение информационно-психологической безопасности в современных условиях на уровень общенациональной проблемы. Поэтому способность защитить себя от информационной агрессии, обеспечить информационную безопасность населения становится важнейшей задачей любого государства.

TATU Samarqand filiali
Axborot-resurs
markazi
№ 12787

1.2. Информационные противостояния от древности до Нового времени

Чтобы понять современное состояние мысли, важнейший путь – вспомнить, как человечество дошло до него...

А. И. Герцен

Отыщи всему начало, и ты многое поймешь.

Козьма Прутков

Примеры информационного противостояния можно найти в древнейших сказаниях. В частности, первой известной человечеству из Библии «информационной операцией» можно считать искушение Евы, а через нее и Адама. Искуситель сумел убедить их, что если они вкусят запретный плод с Древа познания добра и зла, то обретут способность к познанию и, в итоге, не только сравняются с Богом, но и превзойдут его по своим возможностям.

Новый Завет дает еще одно описание «информационной акции» Искусителя, направленной уже против Иисуса. Пытаясь ввести в искушение постившегося в пустыне Иисуса, дьявол, в частности, поднимается с Ним на гору, «показывает все царства мира» и говорит: «Все это дам Тебе, если падши поклонишься мне». Но эта акция Искусителю не удалась.

Христос проповедовал: «Положите себе на сердце не обдумывать заранее, что отвечать» (Лука, 21, 14), то есть сразу говорите то, что подсказывает внутренний голос, наитие, сердце, и тогда не солжете. Через восемнадцать столетий знаменитый европейский дипломат Талейран убежден уже в обратном: «Слова даны для того, чтобы скрывать свои мысли». И поэтому учил молодых коллег: «Не поддавайтесь никогда первому впечатлению, ибо оно самое искреннее». Он понимал суть рациональной цивилизации и предостерегал не от обмана, а от случайного прорыва в действительность истины.

В итоге, выражаясь языком современной психотерапии, Христос учил технике искренности в общении людей, а один из политических лидеров Нового времени – технике обмана своих

собеседников. Он уже был убежден, что такого рода умение важнее людям. На фоне нарастания подобных убеждений и осуществлялся переход человечества к информационному обществу.

В этом обществе появились и вошли в обиход понятия «святая ложь», «ложь во благо», «ложь из сострадания». Чем выше человек по уровню образования, социальному положению, тем чаще от него можно ждать «разумного лицемерия», осознанной и «обоснованной» лжи. Соответственно, чаще такие явления заметны в условиях рациональной цивилизации. Обычно их расценивают как необходимую информационную операцию.

В итоге в настоящее время политика, бизнес, реклама, избирательные кампании, социология, отношения между супругами, детьми и родителями, учениками и учителями, начальниками и подчиненными, правовые отношения, мораль оказались в большой степени выстроенными на стремлении одних манипулировать сознанием и поведением других. Манипуляция стала обычной, незамечаемой, даже как бы естественной частью нашей жизни.

Как следствие, возникла необходимость *научного анализа* информационных отношений, в том числе специфики наступательных и оборонительных действий в них, путей обеспечения информационной безопасности.

Информационное противоборство имеет глубокие исторические корни и велось практически на всех этапах человеческой истории и во всех видах военного и политического противостояния.

Устрашение и сила, с одной стороны, хитрость и коварство – с другой, – вот основные составляющие успешных действий всех известных истории правителей и полководцев. Сочетанием ***устрашения и хитрости*** побеждали древнегреческие полководцы Фемистокл, Лисандр, Александр Македонский, карфагенянин Ганнибал, римский император Юлий Цезарь, русские полководцы Суворов и Кутузов, вожди Нового времени Наполеон, Черчилль, Сталин.

Еще 2500 лет назад древнекитайский философ, государственный деятель и полководец ***Сунь Цзы*** изложил ряд формализованных правил ведения военных действий, многие из которых до сих пор сохранили свое значение. В области военного искусства не-

которые из них больше известны как приемы военной хитрости, составляющие методический базис информационно-интеллектуального обеспечения боевых действий.

На двадцати страницах своей небольшой (по нынешним меркам) книги Сунь Цзы дает ряд рекомендаций и советов полководцам, отстаивающим интересы своего государства. Эти рекомендации он называет «предварительными расчетами»:

если ты и можешь что-нибудь, показывай противнику, будто не можешь;

если ты и пользуешься чем-нибудь, показывай ему, будто ты этим не пользуешься;

хотя ты и был близко, показывай, будто ты далеко;

хотя ты и был далеко, показывай, будто ты близко;

заманивай его выгодой;

приведи его в расстройство и бери его;

если у него все полно, будь наготове;

если он силен, уклоняйся от него;

вызови в нем гнев, приведи его в состояние расстройства;

приняв смиренный вид, вызови в нем самомнение;

если его силы свежи, утоми его;

если они дружны, разъедини;

нападай на него, когда он не готов;

выступай, когда он не ожидает...

Обосновывая ***принцип экономии сил***, Сунь Цзы пишет: «По правилам войны наилучшее – сохранить государство противника в целости, на втором месте – сокрушить это государство. Наилучшее – сохранить армию противника в целости, на втором месте – разбить ее... Поэтому самая лучшая война – разбить замыслы противника; на следующем месте – разбить его союзы; на следующем месте – разбить его войска...» Один из афоризмов Сунь Цзы звучит так: «Верх искусства – это не выигрывать сто битв, напротив, покорить армию врага без сражения».

Наиболее общие и важные рекомендации (или *стратагемы*) в книге Сунь Цзы пронумерованы. Приведем некоторые из них, непосредственно подчеркивающие важность владения приемами дезинформации противника для манипулирования его состоянием и действиями.

№ 10. Добивайся доверия противника и внушай ему спокойствие. Только тогда осуществляй свои скрытые планы. Подготовь все, как подобает, нападай без колебаний и не дай врагу опомниться.

№ 21. Всегда сохраняй уверенный вид. Не допускай изъянов в своей позиции. Так можно не позволить союзнику поддаться страхам и не дать противнику повода предпринять нападение.

№ 27. Лучше сделай вид, что ничего не знаешь и не хочешь ничего делать, чем делать вид, что владеешь знанием, и не будешь действовать безрассудно.

№ 36. Сохраняй свои силы, избегая открытого противостояния.

О роли и влиянии идей Сунь Цзы на развитие военного искусства свидетельствует, в частности, тот факт, что в течение двух с половиной тысяч лет после выхода трактата в свет к нему было написано и опубликовано несколько сотен комментариев. Эта небольшая работа породила на протяжении веков незатухающую информационную волну и стала особым феноменом восточной культуры, проявлением национальной психологии ряда стран и важнейшим достоянием мировой цивилизации.

Многие из общих положений этой книги легко переносились из области войны в область политики и дипломатии. Бывший директор Центрального разведывательного управления США Ален Даллес, один из основателей и идеологов американской разведки, видел заслугу Сунь Цзы в том, что он первым обосновал рекомендации по организации разведывательной деятельности, включая искусство контрразведывательных операций, заложил основы теории и практики психологической войны, в которой основополагающим положением стало *умение управлять состоянием и действиями противника.*

В творческом наследии известного военного теоретика Нового времени ***К. Клаузевица*** имеется ряд интересных положений, относящихся к вопросам информационного противоборства и, по сути, перекликающихся с рекомендациями Сунь Цзы. Подчеркивая особую роль морально-психологического фактора в любой войне, Клаузевиц писал: «Физические явления подобны деревянной рукоятке, в то время как моральные представляют подлинный отточенный клинок... Слабой сто-

роне хитрость предлагает свои услуги как единственный якорь спасения».

С глубокой древности известна так называемая «транспортная теорема», определяющая центробежные и центростремительные механизмы взаимоотношений провинций и метрополии в любой стране. Рекомендации по использованию информационно-психологических механизмов этой «теоремы» с целью дезорганизации отношений внутри противостоящего государства разрабатывались веками и применяются с давних пор. Они сохранили свою актуальность и сегодня. Анализ и обобщение рекомендаций того времени позволяют представить суть некоторых из них в следующих кратких положениях:

пытайтесь внести разложение во все ценное, вовлекайте людей в преступные дела;

подрывайте положение авторитетов и их репутацию, навлекайте на них позор в глазах соотечественников;

используйте даже самых низких и отвратительных людей;

мешайте деятельности правительств;

сейте разногласия и раздоры;

восстанавливайте молодежь против стариков;

сокрушайте старые традиции;

не жалейте ни подарков, ни денег, ни обещаний – все окупится.

В начале шестнадцатого века своего рода информационно-психологическую концепцию государственной власти выдвинул и обосновал итальянский историк и мыслитель ***Никколо Макиавелли*** (1469–1527 гг.). В популярной до сих пор книге «Государь» Макиавелли впервые сформулировал основные принципы ведения информационного противоборства в политической сфере. Он выдвинул знаменитый тезис о том, что политик должен сочетать в себе черты льва и лисицы. Обладая качествами этих животных, он будет способен, с одной стороны, действовать решительно, с применением силы, с другой – манипулировать массами при помощи хитрости, изворотливости, обмана. Ложь во благо общества признавалась допустимой и даже необходимой.

По убеждению Макиавелли, разумный правитель «не может и не должен оставаться верным своему обещанию», если это вредит его интересам и если отпали причины, побудившие

его дать обещание. А благовидный предлог нарушить обещание всегда найдется.

Показателен еще один принцип государственности, сформулированный Макиавелли. Он требует использовать в работе с подданными «насилие для тела и ложь для души». Позднее этот принцип широко использовался орденом иезуитов, уделявшим первостепенное внимание контролю над поведением и мыслями своих членов.

В начале семнадцатого века, в годы ***Великой смуты***, против России была проведена масштабная агрессия с использованием грандиозной информационно-пропагандистской акции. С целью дестабилизации внутреннего положения в России, а затем и ее покорения другой, чуждой по вере и жизненному укладу страной в 1601 г. в Речи Посполитой объявляется самозванец, назвавший себя царевичем Дмитрием, якобы спасшимся от убийц, подосланных Борисом Годуновым. В начавшейся информационной войне для обмана населения широко использовались так называемые «подметные» письма, манифесты, подписанные самозванцем, выступления наемных провокаторов. Ставка делалась на слепую веру народа в законного царя, а также на недовольство действиями бояр и некоторыми реформами Годунова. Отчасти успеху информационной агрессии способствовали объективные трудности, связанные с двумя неурожаями подряд и сильнейшим голодом в стране. В итоге Лжедмитрий I оказался на престоле Рюриковичей в Кремле (1605 г.). Позднее при таком же информационном сопровождении в Кремль вошел Лжедмитрий II (1608 г.), а затем состоялось и воцарение в России польского королевича Владислава (1610 г.). О роли и месте этой аферы в истории нашей страны говорит тот факт, что день освобождения от покоривших в тот период народ лжецов и дезинформаторов является сегодня государственным праздником (4 ноября).

Во многом на информационной основе возник и знаменитый ***церковный раскол*** семнадцатого века, приведший к глубокому раздвоению в русской жизни и русской истории. Вспомним, как он начинался. В середине XVII столетия патриарх Никон, пытаясь упорядочить культ святых в православии и добиться единообразия в их почитании, начинает реформу богослужения. Однако его новшества, вводимые без должной пропагандистско-разъяс-

нительной работы и учета душевно-психологического состояния россиян, вызвали больше сомнений, чем доверия. В итоге более эффективными оказались слухи о том, что они не отвечают духу православия, а сам Никон – антихрист. Его прямой оппонент Аввакум сумел внушить значительной части русского народа, что за новшествами Никона неизбежно последует гибель Московского царства и наступит царство антихриста. Возникло ***движение староверов***, людей, которые не хотели принимать реформу и продолжали жить и верить в Бога на старый лад. Не желая подчиняться Никону, крестьянство целыми деревнями уходило в леса. По России прокатилась волна самосожжений. Сейчас даже трудно представить масштаб и ужас трагедии, лишившей русский народ единства. В России образовались две православные церкви – официальная и старообрядческая.

Уже в восемнадцатом веке по информационной схеме самозванцев из Речи Посполитой действовал ***Емельян Пугачев***, путем откровенной дезинформации навязав народу представление о себе как о законном российском императоре Петре III. Действовал достаточно долго и небезуспешно, при поддержке населения многих губерний России.

Еще один классический вариант дезинформации народа продемонстрировала российской истории в 1917 г. ***партия большевиков под руководством В. И. Ленина***. В сложнейшей, критической для страны ситуации она сумела убедить россиян, что только победа революции под ее руководством обеспечит, во-первых, единственно возможный выход из ненавистной для всех кровопролитной мировой войны, во-вторых, передачу земли крестьянам, в-третьих, возможность управления государством со стороны рабочих. Итог этой информационной операции тоже почти классический. Победная революция состоялась, но война тут же переросла из мировой в еще более кровавую гражданскую, а крестьяне от владения землей, как и рабочие от управления страной, оказались еще дальше, чем были до этого.

1.3. Информационные войны XX века

Наиболее ярко информационный компонент борьбы проявился в войнах XX в. Появление на вооружении воюющих сторон

средств радиосвязи привело к созданию новых способов воздействия на противника. Наряду с традиционной разведдеятельностью в области добывания информации и мерами по дезинформации противника стали применяться средства подавления радиосвязи радиопомехами. Впервые они были использованы в русско-японской войне 1904 г. В последующем эти мероприятия сыграли важную роль в обеспечении успеха операций Первой и Второй мировых войн.

Накануне Первой мировой войны психологами западных стран (Англии, США, Франции, Германии и др.) проводились многочисленные специальные исследования психологической готовности военнослужащих к адекватным и надежным действиям в боевой обстановке, изучалась их способность противостоять панике, страху, выдерживать длительные нервно-психологические нагрузки. В ходе войны во многих странах были созданы специальные подразделения для ведения пропаганды в направлении вооруженных сил и населения противника.

Долгое время основным каналом идеологического воздействия одной страны на другую были распространение печатных материалов и устная пропаганда. Прогресс радиовещания отодвинул эти каналы на второй план. Международное радиовещание и радиовойна превратились в острейшее оружие агрессивной внешней политики и идеологии многих стран еще в 20–30-е годы XX в.

Значительное развитие информационное оружие получило в период Второй мировой войны. Причем быстрее всего важность информационного воздействия осознали в Германии. Сразу после прихода к власти Гитлер впервые предпринял попытку ***глобального информационно-психологического воздействия*** (экспансии) на население других стран. Впоследствии в целях достижения внезапности нападения военно-политическим руководством Германии разрабатывались общегосударственные планы обмана правительств стран – жертв агрессии и их союзников (почти по рекомендациям Сунь Цзы). Вероломное нападение без объявления войны на СССР в июне 1941 г. – наиболее яркое проявление такого рода действий. В планы дезинформации включались объединенные единым замыслом и согласованные между собой политические, дипломатические, экономические и военные ме-

роприятия. Скрытность подготовки и внезапность нападения рассматривались как основа любой кампании. Аналогичные меры предпринимались руководством Германии при создании запрещенных Версальским договором отраслей оборонной промышленности, воздушного флота, бронетанковых войск, а также при проведении экономических, дипломатических и других акций.

В Нормандской десантной операции (1944 г.) США и их союзники успешно провели полномасштабную операцию по завоеванию информационного превосходства. В результате огромная армада кораблей союзников пересекла пролив Ла-Манш практически без помех, побережье было захвачено значительно легче, чем ожидалось. Успешно применялись мероприятия по скрытию и дезинформации противника во многих операциях советских войск.

Значительное развитие получила информационная война с появлением радиоэлектронных средств. Например, радиоразведка ВМС Германии в 1940 г. вскрыла систему радиосвязи и расшифровала около 50 % радиограмм британских ВМС. В 1943 г. радиоэлектронное подавление германской ПВО снизило ее эффективность на Западном фронте примерно на 75 %.

Одной из главных задач информационно-психологических операций была ***деморализация войск и населения противника с помощью пропаганды***. Для этого противоборствующие стороны использовали массированную радиопропаганду и разбрасывание авиацией листовок. Аппараты психологической войны многих стран стали разветвленной самостоятельной службой.

Во время войн в ***Корее*** и на ***Ближнем Востоке*** уже велись настоящие «информационные сражения» в эфире. При этом основные усилия направлялись на срыв радиосвязи противника с помощью радиопомех, дезорганизацию оперативного управления войсками, систем ПВО. Применялось также навязывание ложных распоряжений и команд войскам противника путем вхождения в его радиосети.

Например, в ***арабо-израильской войне*** 6 июня 1967 г. путем вхождения в радиосеть арабских войск был полностью сорван удар 4-й танковой дивизии Египта. Командиру дивизии израильскими дезинформаторами был передан по радио приказ о выходе из боя и отходе за Суэцкий канал. Комплексное использование Из-

раилем всех видов разведки, согласованные действия по уничтожению и подавлению систем оповещения и управления ПВО противника явились основными элементами, позволившими дезорганизовать всю его систему управления.

В захвате десантом англичан ***Фолклендских островов*** элементы информационной войны явились одной из важнейших частей подготовки и проведения операции. В частности, благодаря полученной с разведывательных спутников США информации английской подводной лодке удалось потопить крейсер «Генерал Белграно» и дезорганизовать действия аргентинского флота в целом.

В ходе ***операции «Эльдорадо Каньон» в Ливии*** (1986 г.) для достижения внезапности массированных авиационных ударов эффективно использовались меры оперативной маскировки: дезинформация, режим радиомолчания, обход зон обзора кораблей, радиомаскировка и др. Для дезорганизации системы ПВО Ливии была задействована агентура, подававшая ложные команды на выключение средств разведки.

Вторая половина XX в. стала переломным этапом и в сфере информационно-психологической борьбы. В вооруженных силах ряда стран были созданы специальные органы, силы и средства для осуществления морально-психологического воздействия на противника и на свои войска. Во всех военных конфликтах одновременно с подготовкой вторжения начиналось целенаправленное, носящее глобальный характер информационно-психологическое воздействие на общественное мнение. Лидером в разработке информационных средств и методов борьбы с противником стали Соединенные Штаты Америки.

Опыт США в организации информационных войн

США как наиболее часто воюющая держава во второй половине XX в. неуклонно, от одной акции к другой, наращивала информационно-психологическое обеспечение боевых действий своих войск, а также психологическую обработку населения собственной страны и международной общественности.

Война во Вьетнаме явилась для США поводом для пересмотра теоретических взглядов на роль общественного мнения в вооруженных конфликтах. Тогда американцы недооценили его значение и во многом из-за этого потерпели поражение. Война

показала, что для успешного ведения боевых действий против более слабого противника, применяющего партизанские методы борьбы, чисто военного и технологического преимущества недостаточно. Необходимо *информационно-психологическое превосходство*, достигаемое не только средствами вооруженных сил, но и на государственном уровне. Недостаточный учет этого фактора привел к так называемому «вьетнамскому синдрому» в армии США и в стране.

Уже в ходе вторжения на ***Гренаду*** (1983 г.), а затем и в ***Панаму*** (операция «Джаст Коз», 1989 г.) политическое и военное руководство США, учтя опыт Вьетнама, приложило немало усилий и для обработки общественного мнения, и для информационного обеспечения непосредственных боевых действий. На всех этапах операций первоочередное внимание уделялось поддержанию самых тесных контактов с печатью и телевидением. Так, уже с февраля 1988 г. начались регулярные публикации в американской печати о дискриминации американских военнослужащих и их семей в Панаме со стороны местных властей, об атмосфере страха, неуверенности и террора, в которой приходится жить американцам.

Заранее были созданы специально подобранные и проинструктированные группы журналистов и фоторепортеров, которые к началу боевых действий уже были переброшены на соответствующие объекты в Панаму. Было сделано все, чтобы ограничить доступ в зону боевых действий нежелательных журналистов. В итоге появилась единая и хорошо управляемая система информационно-психологического обеспечения военной политики и боевых действий войск США. Одновременно проводились мероприятия по дезорганизации системы государственного и военного управления Панамы, осуществлялась спецпропаганда среди личного состава сил Национальной обороны и гражданского населения Панамы. Накопленный в Панаме опыт был позднее использован при подготовке и проведении операций «***Щит пустыни***» и «***Буря в пустыне***», а также в ходе боевых действий против *Югославии*.

Войны в районе Персидского залива. Первая операция США против Ирака (1991–1992) представляет собой показательный пример битвы *за позитивное общественное мнение* в мировой ин-

формационной среде и демонстрацию возросшей роли информационного компонента *непосредственно в ходе боевых действий.* Например, за пять месяцев, предшествующих началу боевых действий, благодаря активной обработке населения, число американцев, одобряющих войну в Персидском заливе, выросло с 10 до 80 %. Информационное обеспечение самих боевых действий было также предельно контролируемым. Интервью давали лишь специально отобранные военнослужащие. Особо подчеркивалась необходимость сведения к минимуму информации о погибших и раненых. Была введена жесткая цензура на распространение информации о ходе боевых действий. Ограничивалось эфирное время, предоставляемое противникам войны.

Необходимо отметить эффективность дезинформации на государственном и военном уровне, позволившей скрыть время начала операции и сделать ее неожиданной для руководства России и Совета Безопасности ООН. С началом военных действий была сделана решительная ставка на подавление систем государственного и военного управления Ирака. Исследования информационно-психологической борьбы во время войны в Персидском заливе показали, что умелое использование ее средств позволило более эффективно реализовать боевые возможности войск США и значительно снизить боевые возможности противника.

Информационное обеспечение ***второй войны с Ираком*** и устранения Саддама Хусейна оказалось для США менее удачным. Не удалось скрыть большие потери американцев и нарастающий негативизм в отношениях между населением Ирака и оккупантами. И главное – ложью оказалась та информационная «утка», на которой строилось обоснование вторжения в Ирак. В стране не было обнаружено оружие массового поражения, значит, и не было возможности его применения против других стран. После этого оправдать оккупацию Ирака не могла никакая дезинформация, что существенно ослабило позиции президента США.

Агрессия против Югославии. НАТО во главе с США весьма успешно осуществляло информационное обеспечение агрессии против Югославии в марте–июне 1999 г. (воздушная наступательная операция «Решительная сила»). Боевым дей-

ствиям предшествовала мощная пропагандистская кампания, имевшая цель дискредитировать политический курс руководства Союзной Республики Югославии (СРЮ), сформировать среди населения западных стран «образ врага» и обеспечить моральную поддержку агрессии. В интересах навязывания единого мнения о действиях натовских войск в этой стране все сведения о боевых действиях исходили только из одного источника – пресс-службы НАТО в Брюсселе. Сотни аккредитованных журналистов за отсутствием другой информации были вынуждены тиражировать тенденциозные натовские версии. Одновременно американская авиация беспощадно уничтожала югославские средства информационного вещания. Более 40 % радио- и телевизионных передатчиков, ретрансляторов в Югославии было выведено из строя или повреждено. В итоге американцам удалось создать выгодную для себя информационно-психологическую среду вокруг войны в Югославии. После окончания военных действий мощное информационное воздействие и экономическое давление Запада достигло своих целей: к власти в СРЮ пришло прозападное руководство, а Милошевич был выдан Гаагскому трибуналу как военный преступник. Таким образом, «несмертельные» информационные средства борьбы нанесли Милошевичу тот решающий удар, который не удалось осуществить в 1999 г. даже с помощью 30 тысяч боевых самолето-вылетов.

Борьба с терроризмом. Важное место отводится информационным средствам борьбы с терроризмом, который может оказывать значительное влияние на развитие событий в мире. Способность отдельных лиц и групп людей наносить большой ущерб возрастает с повышением эффективности информационных технологий.

После взрыва в Центре мировой торговли (1994 г.) США провели успешную операцию по поимке главного организатора этой акции Рамзи Юсефа с помощью размещения информации о нем не только в СМИ, но даже внутри пакетиков со спичками. В конечном счете именно последний вариант информации стал сильнейшим соблазном для человека, выдавшего Юсефа и получившего награду.

Варварские террористические акты 11 сентября 2001 г. положили начало самой масштабной и дорогостоящей антитеррористической операции за всю историю человечества. Она еще требует своего детального анализа, но уже сейчас можно говорить об огромном удельном весе в ней мероприятий информационного характера.

Появление высокоэффективных средств и методов информационно-психологического воздействия привело к пересмотру традиционных представлений об агрессии и войнах. К концу XX столетия СМИ и информационно-компьютерные системы стали уже рассматриваться в качестве главного поражающего средства современной войны. За последнее десятилетие прошлого века общая доля расходов США на информатику и подготовку к информационным войнам возросла в три раза и достигла 20 % военного бюджета. Как считают специалисты, по мере развития информационной техники и коммуникационных технологий «горячие войны» постепенно будут вытесняться «холодными», решающую роль в которых играет информационное оружие. Считается, что в XXI в. информационное превосходство будет столь же важным условием победы, каким в первой половине XX в. было превосходство в авиации и бронетанковой технике.

Показательно высказывание бывшего президента США Р. Никсона о том, что гораздо выгоднее вложить доллар в средства массовой информации, в информационное обеспечение операций, чем десять долларов в создание новых видов оружия: вероятность использования оружия в современном мире невелика, а информационная пропаганда работает непрерывно 24 часа в сутки.

Россия и информационные войны во второй половине XX века

Почти сразу после победы в Великой Отечественной войне наша страна стала объектом информационной войны.

Сущность и направленность комплекса психологических операций против России (тогда – СССР), объединенных долговременным стратегическим замыслом, хорошо иллюстрирует выдержка из директивы основателя и первого руководителя политической разведки США в послевоенный период ***А. Даллеса***:

«Окончится война, все как-то утрясется, устроится. И мы бросим все, что имеем, – все золото, всю материальную мощь на оболванивание и одурачивание людей!

Человеческий мозг, сознание людей способны к изменению: посеяв там хаос, мы незаметно подменим их ценности на фальшивые и заставим их в эти фальшивые ценности верить. Как? Мы найдем своих единомышленников, своих союзников и помощников в самой России. Эпизод за эпизодом будет разыгрываться грандиозная по своему масштабу трагедия гибели самого непокорного на земле народа, окончательного, необратимого угасания его самосознания...

Литература, театры и кино – все будут изображать и прославлять самые низменные человеческие чувства. Мы будем всячески поддерживать и поднимать так называемых «художников», которые станут насаждать и вдалбливать в человеческое сознание культ секса, насилия, садизма, предательства – словом, всякой безнравственности. В управлении государством мы создадим хаос и неразбериху...

Мы будем незаметно, но активно и постоянно способствовать самодурству чиновников, взяточников; беспринципность, бюрократизм и волокита будут возводиться в добродетель. Честность и порядочность будут осмеиваться и никому не станут нужны, превратятся в пережиток прошлого.

Хамство и наглость, ложь и обман, пьянство и наркоманию, животный страх друг перед другом и беззастенчивость, предательство, национализм и вражду народов, прежде всего, вражду и ненависть к русскому народу, – все это мы будем ловко и незаметно культивировать, все это расцветет махровым цветом.

И лишь немногие, очень немногие будут догадываться или понимать, что происходит. Но таких людей мы поставим в беспомощное положение, превратим в посмешище, найдем способ их оболгать и объявить отбросами общества. Будем вырывать духовные корни, опошлять и уничтожать основы народной нравственности. Мы будем расшатывать таким образом поколение за поколением. Будем браться за людей с детских, юношеских лет, главную ставку всегда будем делать на молодежь, станем разлагать, развращать, растлевать ее. Мы сделаем из них циников, пошляков, космополитов».

В стратегии американского идеолога информационно-психологических войн XX века нетрудно увидеть те же рекомендации и методы, что предлагали еще древнекитайские мудрецы. Пытайтесь внести разложение во все ценное для данного народа; вовлекайте людей в безнравственные и преступные дела; подрывайте репутацию авторитетов, навлекайте на них позор в глазах соотечественников; сейте разногласия и раздоры; восстанавливайте молодежь против стариков и сокрушайте старые традиции; не жалейте ни денег, ни обещаний – все окупится. Однако трудно найти в этих рекомендациях что-либо хотя бы отдаленно соответствующее духу Священного Писания.

Информационно-психологическая война США против нашей страны продолжалась десятилетиями и оказалась, как свидетельствуют события 90-х годов, весьма успешной. Но эта работа не прекращается и сегодня. По-прежнему в России действуют радиостанции «Свобода» и «Голос Америки». При посольстве и консульствах имеются специальные информационно-ресурсные центры, каждый из которых обслуживает информационным влиянием свой «округ» территории России от Москвы до Владивостока. Помимо них на ниве дезинформации «трудятся» многочисленные фонды, филиалы Национального института прессы, отдел прессы Агентства международного развития. У американцев есть четкое представление о том, какой имидж Америки нужно формировать у российского народа и какие жизненные ценности внедрять в его сознание.

К сожалению, Россия чаще оставалась лишь пассивным объектом этого агрессивного информационного воздействия. Обеспечение информационной безопасности велось в типичном для закрытой системы стиле – через наращивание тотальной секретности и ограничение доступа к информации. Недооценка роли информационно-психологической составляющей в политическом противостоянии, отсутствие навыков наступательных действий стали причиной многих поражений в последние десятилетия. Пока еще нас мало чему научила глобальная неудача в так называемой «холодной», а по сути – информационной войне с Западом. Вслед за ней было фактически проиграно информационное противоборство в ходе первой Чеченской кампании (1994 г.), а также в отношениях со странами Прибалтики, с Украиной (осо-

бенно в ходе выборов 2004 г.), Грузией и даже с большинством русскоязычного населения стран СНГ. Наши информационные действия и в отношениях со странами так называемого «дальнего зарубежья» также невнятны и большей частью носят оборонительный характер.

Чтобы успешно противостоять новым вызовам времени в области информационной безопасности, России еще предстоит стать активным и умелым *субъектом информационных отношений.* Некоторые объективные предпосылки к этому уже есть. Они связаны с заметным оживлением экономической жизни, появлением первых практических и теоретических разработок в информационной сфере, наиболее важной из которых является Доктрина информационной безопасности Российской Федерации.

Эта же задача стоит и перед Вооруженными силами РФ. Сейчас акцент все более смещается от традиционных подходов к ведению вооруженной борьбы в информационно-интеллектуальную область. Теория и практика военного искусства России стоят перед необходимостью разработки и практической реализации системы контрмер против «информационных войн». Нужно осваивать искусство ведения информационных войн, уметь эффективно управлять действиями не только своих войск (сил), но и действиями противника, его общественных институтов.

При современном геополитическом положении России, когда проблема обеспечения военной безопасности страны решается в условиях ограничения состава и возможностей группировок наших войск, применение стратегии «непрямых действий», включая ее информационную составляющую, становится одним из немногих способов повышения обороноспособности страны.

Однако противостояние западной концепции «информационной войны» (особенно в политике и социальной сфере) должно быть связано, видимо, не с расширением масштабов использования заветов Сунь Цзы и Макиавелли (в этом уже преуспели и Гитлер, и Сталин, и Даллес...), а все большей открытостью и честностью информационных отношений. ***Необходимо противопоставить агрессии лжи и дезинформации наступательные действия с использованием честной информации.*** Ибо, как утверждал один из великих россиян, князь Александр Невский, «не в силе Бог, а в правде».

Вопросы для обсуждения

1. По каким признакам можно отличить полезную информацию от информации, являющейся средством агрессии?

2. Каковы цели и задачи информационных войн?

3. Почему «душевное общение» во многом теряет свою подлинность при общении по каналам информационных технологий?

4. К чему может привести наращивание масштабов и эффективности информационного оружия? Не лучше ли бороться за его запрещение, как это происходит с ядерным оружием?

5. Что такое «непрямые действия» и «мягкие» методы поражения? Чем они опасны для человека?

6. Почему США оказались мировым лидером в разработке и использовании информационных средств поражения?

7. Как можно использовать принципы и средства информационного противостояния для защиты национальных интересов нашей страны?

Глава 2

ПРОБЛЕМЫ И УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

Доктрина информационной безопасности Российской Федерации

2.1. Основные проблемы информационной безопасности и пути их решения

Нынешнее ***состояние информационной безопасности России*** – это состояние нового, только оформляющегося с учетом веления времени государственно-общественного института. Многое на пути его становления уже сделано, но еще больше здесь проблем, требующих самого оперативного решения. За последние годы в РФ реализован ряд мер по совершенствованию информационной безопасности. Назовем самые важные из них.

Во-первых, начато формирование базы ***правового обеспечения*** информационной безопасности. Принят ряд законов, регламентирующих общественные отношения в этой сфере, развернута работа по созданию механизмов их реализации. Этапным результатом и нормативно-правовой основой дальнейшего решения проблем в этой сфере стало утверждение Президентом РФ в сентябре 2001 г. ***Доктрины информационной безопасности Российской Федерации*** (далее – Доктрина). Она представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности России. В Доктрине рассматриваются:

объекты, угрозы и источники угроз информационной безопасности;

возможные последствия угроз информационной безопасности;

методы и средства предотвращения и нейтрализации угроз информационной безопасности;

особенности обеспечения информационной безопасности в различных сферах жизнедеятельности общества и государства;

основные положения государственной политики по обеспечению информационной безопасности в РФ.

На основе Доктрины осуществляются:

формирование государственной политики в области обеспечения информационной безопасности;

подготовка предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности;

разработка целевых программ обеспечения информационной безопасности.

Во-вторых, к настоящему времени проведены первоочередные мероприятия по обеспечению информационной безопасности в федеральных органах государственной власти, органах власти субъектов РФ, на предприятиях, в учреждениях и организациях независимо от форм собственности. Развернута работа по созданию защищенной информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти.

В-третьих, обеспечению информационной безопасности способствуют созданные:

государственная система защиты информации;

система лицензирования деятельности в области защиты государственной тайны;

система сертификации средств защиты информации.

Вместе с тем анализ состояния информационной безопасности показывает, что ее уровень *не в полной мере соответствует требованиям времени*. Все еще существует ряд проблем, серьезно препятствующих полноценному обеспечению информационной безопасности человека, общества и государства. Доктрина называет следующие основные проблемы данной сферы.

1. Современные условия политического и социально-экономического развития страны все еще сохраняют острые противо-

речия между потребностями общества в расширении свободного обмена информацией и необходимостью действия отдельных регламентированных ограничений на ее распространение.

2. Противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере существенно затрудняет поддержание необходимого баланса интересов личности, общества и государства в этой области. Несовершенное нормативное правовое регулирование не позволяет завершить формирование на территории РФ конкурентоспособных российских информационных агентств и средств массовой информации.

3. Необеспеченность прав граждан на доступ к информации, манипулирование информацией вызывают негативную реакцию населения, что в ряде случаев ведет к дестабилизации социально-политической обстановки в обществе.

4. Закрепленные в Конституции РФ права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки практически не имеют достаточного правового, организационного и технического обеспечения. Неудовлетворительно организована защита собираемых федеральными органами государственной власти, органами власти субъектов РФ, органами местного самоуправления данных о физических лицах (персональных данных).

5. Нет четкости при проведении государственной политики в области формирования российского информационного пространства, а также организации международного информационного обмена и интеграции информационного пространства России в мировое информационное пространство, что создает условия для вытеснения российских информационных агентств, средств массовой информации с внутреннего информационного рынка, ведет к деформации структуры международного обмена.

6. Недостаточна государственная поддержка деятельности российских информационных агентств по продвижению их продукции на зарубежный информационный рынок.

7. Не улучшается ситуация с обеспечением сохранности сведений, составляющих государственную тайну.

8. Серьезный урон нанесен кадровому потенциалу научных и производственных коллективов, действующих в области создания средств информатизации, телекоммуникации и связи,

в результате массового ухода из этих коллективов наиболее квалифицированных специалистов.

9. Отставание отечественных информационных технологий вынуждает федеральные органы государственной власти, органы власти субъектов РФ и органы местного самоуправления при создании информационных систем идти по пути закупок импортной техники и привлечения иностранных фирм. Из-за этого повышается вероятность несанкционированного доступа к обрабатываемой информации и возрастает зависимость России от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения.

10. В связи с интенсивным внедрением зарубежных информационных технологий в сферы деятельности личности, общества и государства, а также с широким применением открытых информационно-телекоммуникационных систем, интеграцией отечественных и международных информационных систем возросли угрозы применения информационного оружия против соответствующей инфраструктуры России. Работы по адекватному противодействию этим угрозам ведутся в условиях недостаточной координации и слабого бюджетного финансирования. Не уделяется необходимое внимание развитию средств космической разведки и радиоэлектронной борьбы.

Обеспечение информационной безопасности требует решения целого комплекса задач. Доктрина перечисляет *наиболее важные из них*:

разработка основных направлений государственной политики в области обеспечения информационной безопасности, а также мероприятий и механизмов, связанных с реализацией этой политики;

развитие и совершенствование системы обеспечения информационной безопасности, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности, а также системы противодействия этим угрозам;

разработка федеральных целевых программ обеспечения информационной безопасности;

разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности, а также их сертификации;

совершенствование нормативно-правовой базы обеспечения информационной безопасности;

установление ответственности должностных лиц федеральных органов власти и местного самоуправления, юридических лиц и граждан за соблюдение требований информационной безопасности;

координация деятельности органов государственной власти, предприятий, учреждений и организаций независимо от форм собственности в области обеспечения информационной безопасности;

развитие научно-практических основ обеспечения информационной безопасности с учетом современной геополитической ситуации, условий политического и социально-экономического развития России и реальности угроз применения информационного оружия;

создание механизмов формирования и реализации государственной информационной политики России;

повышение эффективности участия государства в формировании информационной политики государственных телерадиовещательных организаций, других государственных средств массовой информации;

обеспечение технологической независимости Российской Федерации в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность, в первую очередь в области создания специализированной вычислительной техники для образцов вооружения и военной техники;

разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, прежде всего в системах управления войсками и оружием, экологически опасными и экономически важными производствами;

развитие и совершенствование систем защиты информации и государственной тайны;

создание защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях и в военное время;

расширение взаимодействия с международными и зарубежными органами и организациями для обеспечения безопасности информации, передаваемой с помощью международных телекоммуникационных систем и систем связи;

обеспечение условий для активного развития российской информационной инфраструктуры, участия России в процессах создания и использования глобальных информационных сетей и систем;

создание системы подготовки кадров в области информационной безопасности и информационных технологий.

Важнейшая задача в деле обеспечения информационной безопасности России – осуществление ***комплексного учета интересов личности, общества и государства*** в данной сфере. Доктрина эти интересы определяет следующим образом:

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 общества в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России;

интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, реализации конституционных прав и свобод человека (гражданина) в области получения информации. Одновременно требуется использование этой сферы только 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.

Соблюдение принципа ***баланса интересов граждан, общества и государства*** в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование различных форм общественного контроля над деятельностью федеральных органов государственной власти и органов государственной власти субъектов РФ. Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в ин-

формационной сфере, является важнейшей задачей государства в области информационной безопасности.

Общие методы решения ключевых задач в деле обеспечения информационной безопасности Доктрина объединяет в три группы:

правовые;

организационно-технические;

экономические.

К ***правовым методам*** относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности РФ (они подробно рассматриваются в гл. 4 настоящего пособия).

Организационно-техническими методами обеспечения информационной безопасности являются:

создание и совершенствование систем обеспечения информационной безопасности;

усиление правоприменительной деятельности органов власти, включая предупреждение и пресечение правонарушений в информационной сфере;

совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности программного обеспечения;

создание систем и средств предотвращения несанкционированного доступа к информации и воздействий, вызывающих разрушение, уничтожение, искажение информации, изменение штатных режимов функционирования систем и средств информатизации и связи;

выявление технических устройств и программ, представляющих опасность для функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации, контроль за выполнением специальных требований по защите информации;

сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;

совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автомати-

зированных систем обработки информации по требованиям информационной безопасности;

контроль за действиями персонала в информационных системах, подготовка кадров в области обеспечения информационной безопасности;

формирование системы мониторинга показателей и характеристик информационной безопасности в наиболее важных сферах жизни и деятельности общества и государства.

Экономические методы обеспечения информационной безопасности включают в себя:

разработку программ обеспечения информационной безопасности и определение порядка их финансирования;

совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Согласно Доктрине, ***государство в процессе реализации своих функций по обеспечению информационной безопасности***:

проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности, разрабатывает меры по ее обеспечению;

организует работу органов власти по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности;

поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;

осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;

проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории РФ и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;

способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;

формулирует и реализует государственную информационную политику России;

организует разработку федеральной программы обеспечения информационной безопасности, объединяющей усилия государственных и негосударственных организаций в данной области;

способствует интернационализации глобальных информационных сетей и систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

При решении основных задач и выполнении первоочередных мероприятий государственной политики по обеспечению информационной безопасности в настоящее время доминирует стремление решать главным образом *нормативно-правовые и технические проблемы.* Чаще всего речь идет о «разработке и внедрении правовых норм», «повышении правовой культуры и компьютерной грамотности граждан», «создании безопасных информационных технологий», «обеспечении технологической независимости» и т. п.

Соответствующим образом планируется и развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности, то есть преобладает подготовка кадров в области средств связи, обработки информации, технических средств ее защиты. В меньшей степени осуществляется подготовка специалистов в области *информационно-аналитической деятельности, социальной информации, информационной безопасности личности.* К сожалению, многие государственные институты считают наиболее важной техническую сторону проблемы, упуская из виду социально-психологические ее аспекты.

2.2. Виды и источники угроз информационной безопасности

***Угрозы информационной безопасности** – это использование различных видов информации против того или иного социального (экономического, военного, научно-технического и т. д.) объекта с целью изменения его функциональных возможностей или полного поражения.*

С учетом общей направленности Доктрина подразделяет угрозы информационной безопасности на ***следующие виды***:

угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

угрозы информационному обеспечению государственной политики РФ;

угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

принятие органами власти правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;

создание монополий на формирование, получение и распространение информации в РФ, в том числе с использованием телекоммуникационных систем;

противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;

чрезмерное ограничение доступа к необходимой информации;

противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;

неисполнение органами государственной власти и местного самоуправления, организациями и гражданами требований законодательства, регулирующего отношения в информационной сфере;

неправомерное ограничение доступа граждан к информационным ресурсам органов государственной власти и местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;

дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;

нарушение конституционных прав и свобод человека и гражданина в области массовой информации;

вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;

девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;

снижение духовного, нравственного и творческого потенциала населения России;

манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики РФ могут быть:

монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;

блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;

низкая эффективность информационного обеспечения государственной политики РФ вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Угрозы развитию отечественной индустрии информации могут составлять:

противодействие доступу к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии

информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, создание условий для усиления технологической зависимости России в области информационных технологий;

закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов;

вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;

использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи;

отток за рубеж специалистов и правообладателей интеллектуальной собственности.

Все ***источники угроз*** информационной безопасности Доктрина подразделяет на ***внешние и внутренние***.

К ***внешним*** источникам угроз Доктрина относит:

деятельность иностранных политических, экономических, военных, разведывательных и информационных структур против интересов РФ;

стремление ряда стран к доминированию на мировом информационном пространстве, вытеснению России с информационных рынков;

деятельность международных террористических организаций;

увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;

деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;

разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран, нарушение функционирования информационных и телекоммуникационных систем, получение несанкционированного доступа к ним.

К ***внутренним*** источникам угроз, согласно Доктрине, относятся:

критическое состояние ряда отечественных отраслей промышленности;

неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;

недостаточная координация деятельности органов власти всех уровней по реализации единой государственной политики в области информационной безопасности;

недостатки нормативно-правовой базы, регулирующей отношения в информационной сфере и правоприменительной практики;

неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка в России;

недостаточное финансирование мероприятий по обеспечению информационной безопасности;

недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

недостаточная активность федеральных органов власти в информировании общества о своей деятельности, в разъяснении принимаемых решений, формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;

отставание России от ведущих стран мира по уровню информатизации органов власти и местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

2.3. Место информационной безопасности в системе национальной безопасности России

В современном мире информационная безопасность становится жизненно необходимым условием обеспечения интересов человека, общества и государства и важнейшим, стержневым, звеном всей ***системы национальной безопасности страны.***

Доктрина рассматривает всю работу в информационной сфере на основе и в интересах ***Концепции национальной безопасности РФ.***

Доктрина выделяет ***четыре основные составляющие*** национальных интересов России в информационной сфере.

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

Для ее реализации необходимо:

повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа страны;

усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала России;

обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;

обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;

укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;

гарантировать свободу массовой информации и запрет цензуры;

не допускать пропаганды и агитации, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;

обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

Вторая составляющая национальных интересов в информационной сфере включает в себя информационное обеспечение государственной политики страны, связанное с доведением до россий-

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

Для этого требуется:

укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;

интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

Третья составляющая национальных интересов в информационной сфере включает в себя развитие современных информационных технологий, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка этой продукцией и выход ее на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Для достижения результата на этом направлении необходимо:

развивать и совершенствовать инфраструктуру единого информационного пространства России;

развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов;

развивать производство в стране конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем;

обеспечить государственную поддержку фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи.

Четвертая составляющая национальных интересов в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

В этих целях требуется:

повысить безопасность информационных систем (включая сети связи), прежде всего, первичных сетей связи и информаци-

онных систем органов государственной власти, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности, систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;

интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля их эффективности;

обеспечить защиту сведений, составляющих государственную тайну;

расширять международное сотрудничество России в области безопасного использования информационных ресурсов, противодействия угрозе противоборства в информационной сфере.

2.4. Защита сведений, составляющих государственную и коммерческую тайну, конфиденциальную информацию и интеллектуальную собственность

Важной стороной противостояния угрозам информационной безопасности является надежная защита сведений, содержащих *государственную, коммерческую и иную тайну*, а также *конфиденциальную* информацию и информацию, составляющую *интеллектуальную собственность*.

Правовые основы защиты информации

За последние годы в России сформированы и продолжают формироваться правовые механизмы, способствующие созданию целостной системы ограничения доступа к информации, составляющей тайну или требующей особой защиты. Важными вехами становления правового режима в этой сфере стало принятие ряда законов и иных нормативно-правовых актов. Назовем основные из них (более подробно правовое обеспечение информационной безопасности рассмотрено в гл. 4).

Закон РФ ***«О безопасности»***, принятый 5 марта 1992 г. (с изменениями), определяет защиту государственной тайны как вопрос обеспечения безопасности государства и относит ее к задачам феде-

рального уровня, исключая появление региональных тайн и региональных законодательных актов, регламентирующих их защиту.

Закон РФ ***«О государственной тайне»***, принятый 21 июля 1993 г., регулирует порядок отнесения сведений к государственной тайне, их рассекречивания и защиты в интересах обеспечения безопасности России.

Закон РФ ***«Об авторском праве и смежных правах»***, вступивший в действие 3 августа 1993 г. (с изменениями), определяет отношения, возникающие в сфере использования авторской продукции и интеллектуальной собственности.

Федеральный закон ***«Об основах государственной службы»***, принятый 31 июля 1995 г., обязывает, в частности, государственных служащих соблюдать установленный порядок работы со служебной информацией, «хранить государственную и иную охраняемую законом тайну, не разглашать ставшие известными в связи с исполнением должностных обязанностей сведения, затрагивающие частную жизнь, честь и достоинство граждан» (ст. 10).

Уголовный кодекс РФ, введенный в действие 1 января 1997 г., содержит статьи «Разглашение государственной тайны» и «Утрата документов, содержащих государственную тайну». Он также относит к разряду преступлений нарушение тайны переписки, телефонных переговоров и т. п. (ст. 138, ч. 1), незаконное разглашение или использование сведений, составляющих коммерческую или банковскую тайну (ст. 183, ч. 2), нарушение авторских прав и права на интеллектуальную собственность (ст. 146, ч. 1 и ст. 147, ч. 2).

Указ Президента РФ № 1203 от 30.11.1995 г. ***«Об утверждении перечня сведений, отнесенных к государственной тайне»*** объявляет перечень сведений в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-разыскной деятельности государства, распространение которых может нанести ущерб безопасности России. В связи с совершенствованием структуры федеральных органов исполнительной власти указанный перечень был изложен в новой редакции на основании Указа Президента РФ № 61 от 24.01.98 г. ***«О перечне сведений, отнесенных к государственной тайне»***.

Указом Президента РФ от 8 ноября 1995 г. № 1108 образована ***Межведомственная комиссия по защите государственной тайны.*** В свою очередь, положение о данной комиссии было утверждено Указом

Президента РФ от 20 января 1996 г. Основной функцией Межведомственной комиссии определена координация деятельности органов государственной власти по защите государственной тайны.

Одним из первых решений Межведомственной комиссии (от 7 июля 1998 г. № 33) стало утверждение ***Концепции защиты государственной тайны в Российской Федерации.***

Наконец, ***Конституцией РФ*** определено, что каждый гражданин имеет *право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.* Ограничение этого права допускается только на основании судебного решения (ст. 23, п. 2). Конституция устанавливает также, что «интеллектуальная собственность охраняется законом» (ст. 44, п. 1).

Таким образом, состав и содержание законов РФ и указов Президента РФ, наличие соответствующих статей в Уголовном кодексе РФ, а также решений Межведомственной комиссии по защите государственной тайны позволяют говорить о сформированной (в целом) нормативно-правовой базе защиты государственной и иной тайны.

Классификация сведений, подлежащих защите

В настоящее время в различных нормативных документах указывается значительное количество (более 40) видов информации, требующих дополнительной защиты. Для удобства рассмотрения правового режима информационных ресурсов по признаку доступа их можно условно объединить в четыре группы:

государственная тайна;

коммерческая тайна;

сведения конфиденциального характера;

интеллектуальная собственность.

Государственная тайна. Закон РФ «О государственной тайне» дает следующее определение государственной тайны: *это защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб безопасности России* (ст. 2).

В ст. 5 данного Закона определен перечень сведений, отнесенных к государственной тайне:

сведения в военной области — о содержании стратегических и оперативных планов, о планах строительства Вооруженных сил,

разработке, технологии, производстве, об объектах производства, о хранении, об утилизации ядерных боеприпасов, о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о дислокации ракетных и особо важных объектов и др.;

сведения в области экономики, науки и техники – о содержании планов подготовки РФ и ее отдельных регионов к возможным военным действиям, об объемах производства, о планах государственного заказа, о выпуске и поставках вооружения, военной техники, о достижениях науки и техники, имеющих важное оборонное или экономическое значение, и др.;

сведения в области внешней политики и экономики – о внешнеполитической и внешнеэкономической деятельности РФ, преждевременное распространение которых может нанести ущерб безопасности государства и др.;

сведения в области разведывательной, контрразведывательной и оперативно-разыскной деятельности. Это, в частности, сведения, характеризующие:

силы и средства названной деятельности, ее источники, планы и результаты;

лиц, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими названную деятельность;

системы президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи;

шифры и информационно-аналитические системы специального назначения, методы и средства защиты секретной информации и др.

Дополнительный *перечень сведений*, включающий некоторые виды информации из области военной, внешнеэкономической, экономической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, отнесенные к государственной тайне, содержат указы Президента РФ № 1203 от 30.11.1995 г. и № 61 от 24.01.1998 г.

Кроме того, Доктрина информационной безопасности РФ требует защищать «помещения, предназначенные для ведения закрытых переговоров, а также переговоров, в ходе которых оглашаются сведения ограниченного доступа».

Согласно Уголовному кодексу РФ, защита государственной тайны и иной секретной информации возложена на сотрудников режимных служб и правоохранительных органов.

Коммерческая тайна. Коммерческую тайну может составлять *любая информация, полезная в бизнесе и дающая преимущество над конкурентами, которые такой информацией не обладают.* Во многих случаях коммерческая тайна является формой интеллектуальной собственности.

Согласно ст. 139 ч. 1 Гражданского кодекса РФ к числу сведений, составляющих коммерческую тайну, относится информация, которая *имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам и к которой нет свободного доступа на законном основании.* Она может включать в себя различные идеи, изобретения и другую деловую информацию.

Примерно такое же определение коммерческой тайны дает Американская Ассоциация юристов. В ее формулировке – это информация, которая:

во-первых, имеет самостоятельную экономическую стоимость (используемую или потенциальную) благодаря тому, что не является общеизвестной или доступной людям, желающим использовать ее в коммерческих целях;

во-вторых, является объектом разумных для данной ситуации усилий по ее защите.

Прежде чем предпринимать меры для защиты определенной информации как коммерческой тайны, необходимо ответить на следующие вопросы.

Какие сведения нельзя скрывать?

Какие сведения невыгодно скрывать?

Какие сведения необходимо охранять?

Ответ на первый вопрос дает постановление Правительства РФ от 5.12.1991 г. № 35 «*О перечне сведений, которые не могут составлять коммерческую тайну*». К таким сведениям относятся:

организационные сведения (устав и учредительные документы предприятия, регистрационные удостоверения, лицензии, патенты);

финансовые сведения (документы об исчислении и уплате налогов, других платежей, предусмотренных законом, документы о состоянии платежеспособности);

сведения о штате и условиях деятельности (число и состав работающих, их заработная плата, наличие свободных мест, влияние производства на природную среду, реализация продукции, причиняющей вред здоровью населения, участие должностных лиц в предпринимательской деятельности, нарушение антимонопольного законодательства);

сведения о собственности (размерах имущества, денежных средствах, вложениях платежей в ценные бумаги, облигации, займы, уставные фонды совместных предприятий).

Указанные сведения не являются предметом защиты от ознакомления с ними третьих лиц, но это не исключает их охраны от преступных посягательств. В связи с этим остается вопрос: кому предприниматель обязан предъявлять (по требованию) перечисленные сведения?

Претендовать на ознакомление с такими сведениями в пределах своей компетенции могут:

прокурор в порядке надзора и в других случаях, предоставленных ему законом;

правоохранительные органы по возбужденному уголовному делу;

налоговые службы (управления);

аудиторские фирмы (по просьбе самого владельца);

профсоюзы;

государственные предприятия (учреждения);

санитарно-эпидемиологические станции;

экологические организации;

организации и частные лица, вступающие в сделку с предпринимателем.

К сведениям, которые невыгодно скрывать, относится, в частности, рекламная информация. Без рекламы в хозяйственной деятельности трудно добиться эффективного результата, особенно в условиях жесткой конкуренции. Вместе с тем рекламная информация может стать достоянием не только законопослушных граждан, но и преступных элементов. Поэтому и в данном случае предприниматель, рекламирующий свою продукцию или деятельность, должен быть готов как к возможным посягательствам, так и к собственным ответным действиям.

Какие сведения необходимо охранять? Для ответа на этот вопрос необходимо определить круг сведений, составляющих коммер-

ческую тайну, а также их возможное распределение по категориям важности в зависимости от их ценности для предприятия, характера и размера ущерба, который может быть нанесен предприятию при разглашении этих сведений. К решению указанной проблемы следует подходить особенно тщательно. Если какие-либо данные, прямые или косвенные, будут упущены, то все принимаемые меры могут оказаться неэффективными. С другой стороны, излишние меры по ограничению доступа к информации осложнят работу и приведут к неоправданным экономическим издержкам.

Для подготовки *перечня сведений, относящихся к коммерческой тайне предприятия*, целесообразно привлечь специалистов, знакомых как с деятельностью предприятия в целом, так и с работой его отдельных подразделений. Создается группа в составе не более 4–5 человек, в которую желательно включить:

специалиста, владеющего финансовыми вопросами, конъюнктурой рынка и данными в отношении конкурирующих фирм;

специалиста, полностью представляющего систему организации работы предприятия, ее особенности;

специалиста по связям с другими предприятиями, а также по вопросам заключения контрактов, договоров;

специалиста, обладающего сведениями о выпускаемой продукции, технологическом цикле ее производства, о прохождении всех видов информации на предприятии.

Итогом работы такой группы должен стать перечень сведений, составляющих коммерческую тайну предприятия, утвержденный руководителем предприятия. При разработке перечня необходимо учитывать требования указанного выше постановления Правительства РФ от 5.12.1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».

В перечень сведений, составляющих коммерческую тайну организации, могут входить:

Сведения научного характера:

идеи, изобретения, открытия;

отдельные формулы;

новые технические проекты;

новые методы организации труда и производства;

программное обеспечение ЭВМ;

результаты научных исследований.

Сведения технологического характера:

конструкторская документация, чертежи, схемы, записи;

описания технологических испытаний;

конструкционные характеристики создаваемых изделий и оптимальные параметры разрабатываемых технологических процессов (размеры, объемы, конфигурация, процентное содержание компонентов, температура, давление, время и т. д.);

сведения о материалах, из которых изготовлены отдельные детали, условиях экспериментов и об оборудовании, на котором они проводились, и т. д.;

используемые предприятием отдельные новые либо уникальные измерительные комплексы и приборы, станки, оборудование.

Сведения делового характера:

сведения о заключенных или планируемых контрактах;

данные о поставщиках и клиентах;

обзоры рынка, маркетинговые исследования;

информация о конфиденциальных переговорах;

калькуляция издержек производства предприятия, структуры цен, уровень прибыли;

планы развития предприятия и инвестиций.

Перечень сведений, отнесенных к коммерческой тайне, определяется спецификой деятельности каждого конкретного предприятия и в каждом случае может быть сугубо специфическим.

Так, крупнейшие в мире производители прохладительных напитков фирмы «Кока-Кола» и «Пепси-Кола» выделяют в качестве главных секретов специальные добавки в концентрат, из которого изготавливаются напитки. Американские машиностроительные и приборостроительные фирмы, рекламируя качественные характеристики своей продукции, держат в глубоком секрете технологические особенности изготовления основных узлов, определяющих такие характеристики.

По мере необходимости этот перечень изменяется и дополняется; по возможности должен указываться конкретный срок, на который те или иные сведения отнесены к коммерческой тайне.

Сведения конфиденциального характера. Конфиденциальность информации – *характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации.* Конфиденциальность предполагает сохране-

ние прав на информацию, ее неразглашение (секретность) и неизменность во всех случаях, кроме правомочного использования.

Указом Президента РФ от 6 марта 1997 г. № 188 утвержден *перечень сведений конфиденциального характера.* В этот перечень вошли:

сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные);

сведения, составляющие тайну следствия и судопроизводства;

служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна);

сведения о профессиональной деятельности (врачебная, нотариальная, адвокатская тайна, тайна переписки и т. д.);

сведения о сущности изобретения или промышленных образцах до официальной публикации информации о них.

Перечень сведений конфиденциального характера дополняют другие нормативно-правовые акты: Основы законодательства РФ «Об охране здоровья граждан», законы РФ «О психиатрической помощи и гарантиях прав граждан при ее оказании», «О нотариате», «Об адвокатуре», «Об основных гарантиях избирательных прав граждан РФ», «О банках и банковской деятельности», а также Налоговый кодекс РФ, Семейный кодекс РФ и др.

В итоге можно выделить несколько групп сведений конфиденциального характера, образующих определенные «тайны»:

врачебная (медицинская) тайна;

банковская тайна;

налоговая тайна;

нотариальная тайна;

тайна страхования;

адвокатская тайна;

тайна отношения к религии и тайна исповеди;

тайна голосования;

служебная тайна и др.

К информации, определяемой понятием ***интеллектуальная собственность***, можно отнести большую часть перечисленных выше сведений научного и технологического характера, а также произведения литературы и искусства, продукцию изобретательской и рационализаторской деятельности, других видов твор-

чества. В соответствии с Законом РФ «О правовой охране программ для электронно-вычислительных машин и баз данных» от 23.09.1992 г. программы для ЭВМ и базы данных также являются объектами авторского права, нарушение которого влечет гражданскую, уголовную и административную ответственность в соответствии с законодательством РФ.

Под определение интеллектуальной собственности попадает и определенная часть сведений, отнесенных к государственной и коммерческой тайне.

Организация защиты информации

Хранить свой секрет – мудро, но ждать,
что его будут хранить другие, – глупо.

С. Джонсон

Наиболее разумными усилиями в этом направлении большинство специалистов считает проведение следующих *«защитных» мероприятий*:

адекватное определение перечня сведений, подлежащих защите;

выявление уровней доступности и прогнозирование возможных уязвимых мест в доступе к информации;

принятие мер по ограничению доступа к информации или объекту;

организация охраны помещения и постоянного контроля за сохранностью информации (в частности, необходимость наличия закрывающихся шкафов, сейфов, кабинетов, телевизионных камер слежения и т. п.);

наличие четких правил обращения с документами и их размножения. Как известно, изобретение множительной техники буквально вызвало всплеск промышленного шпионажа;

наличие на документах надписей «Секретно», «Для служебного пользования», а на дверях – «Посторонним вход воспрещен». Каждый носитель информации (документ, диск и др.) должен иметь соответствующее обозначение и место хранения (помещение, сейф, металлический ящик);

подписание с сотрудниками организации, фирмы договора о неразглашении тайны.

Основным средством защиты информации остаются в настоящее время режимные меры, направленные на предотвраще-

ние утечки конкретных сведений. Принятие этих мер зависит, прежде всего, от владельцев информации, складывающейся в их сфере деятельности конкурентной обстановки, ценности, которую представляет для них производственная или коммерческая информация, других факторов.

В числе мер защиты информации можно выделить ***внешние и внутренние.***

К ***внешним*** мероприятиям относятся: изучение партнеров, клиентов, с которыми приходится вести коммерческую деятельность, сбор информации об их надежности, платежеспособности и других данных, а также прогнозирование ожидаемых действий конкурентов и преступных элементов. По возможности выясняются лица, проявляющие интерес к деятельности организации (фирмы), к персоналу, работающему в организации.

Внутренние мероприятия по обеспечению безопасности включают вопросы подбора и проверки лиц, поступающих на работу: изучаются их анкетные данные, поведение по месту жительства и на прежней работе, личные и деловые качества, психологическая совместимость с сотрудниками; выясняются причины ухода с прежнего места работы, наличие судимостей и пр. В процессе работы продолжается изучение и анализ поступков сотрудника, затрагивающих интересы организации, проводится анализ его внешних связей.

Сотрудники – важнейший элемент системы безопасности. Они могут сыграть значительную роль в защите коммерческой тайны, но в то же время могут быть и основной причиной ее утечки. Часто это случается по причине невнимательности, неграмотности. Поэтому регулярное и доходчивое обучение персонала вопросам секретности является важнейшим условием сохранения тайны. Однако нельзя исключать случаи умышленной передачи (продажи) работником секретов фирмы. Мотивационную основу таких поступков составляют либо корысть, либо месть, например, со стороны уволенного работника. Практика подобных действий уходит своими корнями в глубокую древность.

Известно, что еще в Римской империи, когда основную часть работающего населения составляли рабы, обычной практикой было принуждение чужих рабов выдавать секреты хозяина. В Риме был даже принят специальный закон, предусматривающий наказание за подобные действия в виде штрафа размером в двойную стоимость причиненных убытков.

Для обеспечения защиты информации на предприятиях вводится определенный *режим, порядок доступа и работы с информацией*. Эффективность такого порядка возможна только при выполнении следующих условий:

единства в решении производственных, коммерческих, финансовых и режимных вопросов;

координации мер безопасности между всеми заинтересованными подразделениями;

экспертной оценки информации и объектов, подлежащих защите;

персональной ответственности руководителей и исполнителей, участвующих в закрытых работах, за обеспечение сохранности тайны и поддержание на должном уроне режима охраны проводимых работ;

организации специального делопроизводства, надежного хранения и перевозки носителей коммерческой тайны, маркировки документации и пр.;

формирования списка лиц, уполномоченных классифицировать информацию, содержащую коммерческую тайну;

ограничения круга лиц, имеющих допуск к информации;

наличия единого порядка доступа и организации пропускного режима;

организации взаимодействия с органами власти, осуществляющими контроль за определенными видами деятельности предприятий;

наличия охраны, пропускного и внутреннего режима;

планового осуществления мер по защите и контролю за коммерческой тайной;

создания системы обучения исполнителей правилам обеспечения сохранности интеллектуальной собственности.

Защита информации предполагает использование ***специальных технических средств***, электронных устройств, что позволяет не только сдерживать их утечку, но и останавливать такой вид деятельности, как промышленный (коммерческий) шпионаж. Большую их часть составляют технические средства обнаружения и средства противодействия устройствам прослушивания:

телефонный нейтрализатор (для подавления работы минипередатчика и нейтрализации снятия аудиоинформации);

телефонный подавитель устройств прослушивания;

профессиональный детектор (используется для «грубого» определения местонахождения радиозакладок);

мини-детектор передатчиков (используется для точного определения местонахождения радиозакладок);

генератор шума.

Организации, располагающие ценной информацией, должны хранить ее в специальных несгораемых шкафах или сейфах, не допускать утери ключей от них или передачи на хранение другим лицам, даже из числа особо доверенных.

> Некоторые фирмы, например, используют для хранения секретной информации сейфы (шкафы), открываемые с помощью специальной магнитной карты или других сложных сигнальных электронных устройств. Следует отметить, что эта мера значительно затрудняет доступ к информации, особенно при наличии комплекса защитных (физических и технических) мер у здания, где расположен сейф, иное хранилище. Некоторые фирмы тратят на защиту информации до 15 % своих доходов.

Одним из распространенных методов защиты интеллектуальной собственности является ***патент***, то есть *свидетельство, выдаваемое изобретателю или его правопреемнику на право исключительного пользования сделанным им изобретением.* Патент призван защитить изобретателя (автора) от воспроизводства, продажи и использования его изобретения другими лицами.

Для защиты публикуемых работ автору рекомендуется воспроизводить на каждой копии следующую информацию: имя владельца авторского права; год издания работы; символ авторского права ©. Наконец, всем авторам при борьбе с посягательствами на их интеллектуальную собственность необходимо тесное ***сотрудничество с правоохранительными органами*** и общественностью. К сожалению, существующая практика борьбы с плагиатом и пиратством показывает, что такое сотрудничество тоже далеко не всегда дает ожидаемые результаты.

Осуществление специальных внутренних и внешних мер защиты ценных информационных систем должно возлагаться на специально подготовленных лиц. С этой целью предприниматель может обращаться за помощью к частным детективным фирмам,

специализирующимся на сыске и охране собственности. Могут создаваться и собственные службы безопасности. Так как защитные мероприятия требуют значительных затрат, предприниматель сам должен решить, что ему выгоднее: мириться с утечкой информации или привлекать специализированные службы для ее защиты.

Вопросы для обсуждения

1. Какие угрозы – внешние или внутренние – оказываются более существенными для информационной безопасности нашего общества и вас лично? Почему?

2. Ощущаете ли вы в своей повседневной жизни отставание России в разработке и внедрении информационных систем разного уровня? Приведите примеры.

3. Решаются ли все проблемы информационной безопасности человека и общества созданием соответствующей нормативно-правовой базы и внедрением современных информационных технологий?

4. Ощущаете ли вы лично ограничения в праве на доступ к информации?

5. Происшедшая в мире информационная революция, на ваш взгляд, усилила или ослабила национальную безопасность России? Обоснуйте свой вариант ответа.

6. Что вы знаете об усилиях государства по защите интеллектуальной собственности и, в частности, борьбе с контрафактной продукцией? Поддерживаете ли вы эту борьбу личными действиями?

7. Есть ли в вашей деятельности и частной жизни сведения, требующие защиты от посторонних лиц? К какой группе секретности вы отнесли бы эти сведения?

Глава 3

ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации.

Доктрина информационной безопасности Российской Федерации

3.1. Защита информации в экономике, внутренней и внешней политике, науке и технике

К числу важнейших направлений жизнедеятельности общества и государства, информационная безопасность которых обеспечивает национальные интересы, Доктрина информационной безопасности РФ относит:

сферу экономики;

внутреннюю и внешнюю политику;

науку и технику;

оборону;

правоохранительную сферу и действия в условиях чрезвычайных ситуаций;

функционирование информационных и телекоммуникационных систем;

сферу духовной жизни человека и общества.

Новое в концепции бизнеса – зависимость от информационных войн, идущих по всему миру.

Э. Тоффлер

Воздействию угроз информационной безопасности ***в сфере экономики*** наиболее подвержены:

система государственной статистики;

кредитно-финансовая система;

информационные и учетные автоматизированные системы подразделений федеральных органов исполнительной власти, обеспечивающих деятельность общества и государства в сфере экономики;

системы бухгалтерского учета предприятий, учреждений и организаций независимо от формы собственности;

системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации и информации о внешнеэкономической деятельности государства, а также предприятий, учреждений и организаций независимо от формы собственности.

Переход к рыночным отношениям в экономике вызвал появление на внутреннем российском рынке товаров и услуг множества отечественных и зарубежных коммерческих структур, в том числе производителей и потребителей информации, средств информатизации и защиты информации. Бесконтрольная деятельность этих структур по созданию и защите систем сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации создает реальную угрозу безопасности России в экономической сфере. Аналогичные угрозы возникают при бесконтрольном привлечении иностранных фирм к созданию подобных систем, поскольку при этом складываются благоприятные условия для несанкционированного доступа к конфиденциальной экономической информации и для контроля за процессами ее передачи и обработки со стороны иностранных спецслужб.

Широкое использование импортных средств информатизации, телекоммуникации, связи и защиты информации создает угрозу возникновения технологической зависимости России в этой сфере от иностранных государств.

Недостаточность нормативной правовой базы, определяющей ответственность хозяйствующих субъектов за недостовер-

ность или сокрытие сведений об их коммерческой деятельности, о потребительских свойствах производимых ими товаров и услуг, о результатах их хозяйственной деятельности, об инвестициях и т. п. препятствует нормальному функционированию экономики страны в целом.

С другой стороны, существенный экономический ущерб хозяйствующим субъектам может быть нанесен вследствие разглашения информации, содержащей коммерческую тайну. В системах сбора, обработки, хранения и передачи финансовой, налоговой, таможенной информации наиболее опасны противоправное копирование информации или ее искажение вследствие преднамеренных нарушений технологии работы с информацией и несанкционированного доступа к ней. Это касается и федеральных органов исполнительной власти, занятых формированием и распространением информации о внешнеэкономической деятельности РФ.

Основными мерами по обеспечению информационной безопасности РФ в сфере экономики являются:

организация и осуществление государственного контроля за созданием, развитием и защитой систем и средств сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

коренная перестройка системы государственной статистической отчетности в целях обеспечения достоверности, полноты и защищенности информации, осуществляемая путем введения строгой юридической ответственности должностных лиц за подготовку первичной информации, организацию контроля за деятельностью этих лиц и служб обработки и анализа статистической информации, а также путем ограничения коммерциализации такой информации;

разработка национальных сертифицированных средств защиты информации и внедрение их в системы и средства сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации;

разработка и внедрение национальных защищенных систем электронных платежей на базе интеллектуальных карт, систем электронных денег и электронной торговли, стандартизация

этих систем, а также разработка нормативной правовой базы, регламентирующей их использование;

совершенствование нормативной правовой базы, регулирующей информационные отношения в сфере экономики;

совершенствование методов отбора и подготовки персонала для работы в системах сбора, обработки, хранения и передачи экономической информации.

К наиболее важным объектам обеспечения информационной безопасности ***в сфере внутренней политики*** Доктрина информационной безопасности относит:

конституционные права и свободы человека и гражданина;

конституционный строй, национальное согласие, стабильность государственной власти, суверенитет и территориальную целостность РФ;

открытые информационные ресурсы федеральных органов исполнительной власти и средств массовой информации.

Наибольшую опасность в сфере внутренней политики представляют следующие угрозы:

нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере;

недостаточное правовое регулирование отношений в области прав различных политических сил на использование средств массовой информации для пропаганды своих идей;

распространение дезинформации о политике РФ, деятельности федеральных органов государственной власти, событиях, происходящих в стране и за рубежом;

деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности РФ, разжигание социальной, расовой, национальной и религиозной вражды, на распространение этих идей в средствах массовой информации.

Основными мероприятиями по обеспечению информационной безопасности в сфере внутренней политики являются:

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

активизация контрпропагандистской деятельности, направленной на предотвращение негативных последствий распространения дезинформации о внутренней политике России.

> Чтобы защитить политическую безопасность страны, нужно научиться вести информационную войну с использованием различных средств массовой информации.
>
> *Шэнь Вэйгуан*

В сфере внешней политики к наиболее важным объектам обеспечения информационной безопасности Доктрина относит:

информационные ресурсы федеральных органов исполнительной власти, реализующих внешнюю политику РФ, российских представительств и организаций за рубежом, представительств РФ при международных организациях;

информационные ресурсы представительств федеральных органов исполнительной власти, реализующих внешнюю политику РФ, на территориях субъектов РФ;

информационные ресурсы российских предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, реализующим внешнюю политику РФ.

Из *внешних угроз* информационной безопасности в сфере внешней политики, согласно Доктрине, наибольшую опасность представляют:

информационное воздействие иностранных политических, экономических, военных и информационных структур на разработку и реализацию стратегии внешней политики РФ;

распространение за рубежом дезинформации о внешней политике РФ;

блокирование деятельности российских средств массовой информации по разъяснению зарубежной аудитории целей и основных направлений государственной политики РФ, ее мнения по социально значимым событиям российской и международной жизни;

нарушение прав российских граждан и юридических лиц в информационной сфере за рубежом;

попытки несанкционированного доступа к информации и воздействия на информационные ресурсы, информационную

инфраструктуру федеральных органов исполнительной власти, реализующих внешнюю политику РФ, российских представительств и организаций за рубежом, представительств РФ при международных организациях.

К числу *внутренних угроз* информационной безопасности в сфере внешней политики Доктрина относит:

нарушение установленного порядка сбора, обработки, хранения и передачи информации в федеральных органах исполнительной власти, реализующих внешнюю политику РФ, и на подведомственных им предприятиях, в учреждениях и организациях;

информационно-пропагандистскую деятельность политических сил, общественных объединений, средств массовой информации и отдельных лиц, искажающую стратегию и тактику внешнеполитической деятельности РФ;

недостаточную информированность населения о внешнеполитической деятельности РФ.

Основными мероприятиями по обеспечению информационной безопасности в сфере внешней политики являются:

разработка основных направлений государственной политики в области информационного обеспечения внешнеполитического курса РФ;

разработка и реализация комплекса мер по усилению информационной безопасности информационной инфраструктуры федеральных органов исполнительной власти, реализующих внешнюю политику РФ, российских представительств и организаций за рубежом, представительств РФ при международных организациях;

создание российским представительствам и организациям за рубежом условий для работы по нейтрализации распространяемой там дезинформации о внешней политике РФ;

совершенствование информационного обеспечения работы по противодействию нарушениям прав и свобод российских граждан и юридических лиц за рубежом;

совершенствование информационного обеспечения субъектов РФ по вопросам внешнеполитической деятельности, которые входят в их компетенцию.

К числу наиболее важных объектов обеспечения информационной безопасности *в области науки и техники* Доктрина относит:

результаты фундаментальных, поисковых и прикладных научных исследований, потенциально важные для научно-технического, технологического и социально-экономического развития страны, включая сведения, утрата которых может нанести ущерб национальным интересам и престижу РФ;

открытия, незапатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование;

научно-технические кадры и систему их подготовки;

системы управления сложными исследовательскими комплексами (ядерными реакторами, ускорителями элементарных частиц, плазменными генераторами и др.).

Основными *внешними угрозами* информационной безопасности в области науки и техники являются:

стремление развитых иностранных государств получить противоправный доступ к научно-техническим ресурсам России для использования полученных российскими учеными результатов в собственных интересах;

создание льготных условий на российском рынке для иностранной научно-технической продукции и стремление развитых стран в то же время ограничить развитие научно-технического потенциала России (скупка акций передовых предприятий с их последующим перепрофилированием, сохранение экспортно-импортных ограничений и т. п.);

политика западных стран, направленная на дальнейшее разрушение унаследованного от СССР единого научно-технического пространства государств – участников Содружества Независимых Государств за счет переориентации на западные страны их научно-технических связей, а также отдельных наиболее перспективных научных коллективов;

активизация деятельности иностранных государственных и коммерческих предприятий, учреждений и организаций в области промышленного шпионажа с привлечением к ней разведывательных и специальных служб.

К основным *внутренним угрозам* информационной безопасности в области науки и техники Доктрина относит:

недостаточное финансирование научно-технической деятельности, временное падение престижа научно-технической сферы, утечку за рубеж идей и передовых разработок;

недостаточную способность предприятий национальных отраслей электронной промышленности производить на базе новейших достижений микроэлектроники, передовых информационных технологий конкурентоспособную наукоемкую продукцию, позволяющую обеспечить достаточный уровень технологической независимости России от зарубежных стран, что приводит к вынужденному широкому использованию импортных программно-аппаратных средств при создании и развитии в России информационной инфраструктуры;

проблемы в области патентной защиты результатов научно-технической деятельности российских ученых;

сложности реализации мероприятий по защите информации, особенно на акционированных предприятиях, в научно-технических учреждениях и организациях.

Реальный путь противодействия угрозам информационной безопасности в области науки и техники – это *совершенствование законодательства РФ,* регулирующего отношения в данной области. Государство должно способствовать созданию системы оценки возможного ущерба наиболее важным объектам науки и техники, в том числе с помощью общественных научных советов и независимой экспертизы. Такой анализ должен заканчиваться выработкой рекомендаций для органов власти по предотвращению противоправного или неэффективного использования интеллектуального потенциала России.

3.2. Информационное обеспечение оборонных мероприятий и боевых действий

Согласно Доктрине, к объектам обеспечения информационной безопасности ***в сфере обороны*** относятся:

информационная инфраструктура центральных органов военного управления и органов военного управления видов Вооруженных сил РФ и родов войск, объединений, соединений, воинских частей и организаций, входящих в состав Вооруженных сил РФ, научно-исследовательских учреждений Министерства обороны РФ;

информационные ресурсы предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих

государственные оборонные заказы либо занимающихся оборонной проблематикой;

программно-технические средства автоматизированных и автоматических систем управления войсками и оружием, вооружения и военной техники, оснащенных средствами информатизации;

информационные ресурсы, системы связи и информационная инфраструктура родов войск, воинских формирований и органов.

К числу *внешних угроз* информационной безопасности в сфере обороны Доктрина относит:

все виды разведывательной деятельности зарубежных государств;

информационно-технические воздействия (в том числе радиоэлектронную борьбу, проникновение в компьютерные сети) со стороны вероятных противников;

диверсионно-подрывную деятельность специальных служб иностранных государств, осуществляемую методами информационно-психологического воздействия;

деятельность иностранных политических, экономических и военных структур, направленную против интересов РФ в сфере обороны.

Внутренними угрозами, представляющими наибольшую опасность в данной сфере, являются:

нарушение установленного регламента сбора, обработки, хранения и передачи информации, находящейся в штабах и учреждениях Министерства обороны РФ, 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 Вооруженных сил РФ и их боеготовность;

нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов;

нерешенность вопросов социальной защиты военнослужащих и членов их семей.

Перечисленные внутренние угрозы будут представлять особую опасность в условиях обострения военно-политической обстановки.

Главными направлениями совершенствования системы обеспечения информационной безопасности в сфере обороны считаются:

систематическое выявление угроз и их источников, структуризация целей обеспечения информационной безопасности в сфере обороны 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 военного назначения и системах связи, имеющих в своем составе элементы вычислительной техники;

постоянное совершенствование средств защиты информации от несанкционированного доступа, развитие защищенных систем связи и управления войсками и оружием, повышение надежности специального программного обеспечения;

совершенствование структуры функциональных органов обеспечения информационной безопасности в сфере обороны и координация их взаимодействия;

совершенствование приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника;

подготовка специалистов по обеспечению информационной безопасности в сфере обороны.

При современном геополитическом положении России, когда перед Вооруженными силами РФ встает проблема обеспечения военной безопасности страны в условиях резкого ограничения состава и возможностей группировок наших войск, применение *принципов стратегии «непрямых» действий*, включая ее информационную составляющую, становится особенно актуальным.

Основу достижения победы в военных действиях в XXI в. все в большей степени будут определять не технические средства, а информация. Эти изменения вытекают из содержания осуществляемого человечеством в настоящее время перехода от постиндустриального общества к обществу информационному. Уже сегодня, когда с традиционных подходов к ведению вооруженной

борьбы акцент все более смещается в информационно-интеллектуальную область, теория и практика военного искусства России стоят перед необходимостью разработать и практически реализовать *систему контрмер* западной концепции «информационной войны» и создать собственную систему наступательных и оборонительных действий нового типа.

Информационное превосходство будет главной составляющей военной стратегии нынешнего столетия подобно тому, как в XX веке такими составляющими являлись господство в воздухе и массированное применение бронетанковой техники.

Среди факторов, определяющих успех вооруженной борьбы, всегда важнейшим был и остается *человеческий фактор*. Наряду с огневым поражением личного состава все чаще планируется использование информационно-психологического воздействия. Общая тенденция состоит в переходе от истребления противника средствами обычных войн к попыткам деморализовать его, парализовать его активность, не уничтожая физически. Воздействие информационного оружия на человека связано, прежде всего, с дезорганизацией его сознания и поведения, подавлением воли к сопротивлению, изменением отношения к противнику и установок на ведение боевых действий.

Для решения этой задачи могут использоваться:

так называемые *«мягкие» методы* информационного поражения, воздействующие на сознание человека, в частности, пропаганда, дезинформация, внушение и т. п.;

так называемые *«жесткие» методы* информационного поражения, способные дезорганизовать поведение воина на глубинном, подсознательным уровне. Уже известны факты создания для этих целей генераторов частотной кодировки мозга, биолокационных установок, высокочастотных и низкочастотных генераторов, химических и биологических средств.

В обоих случаях делается попытка реализовать древний идеал враждующих сторон: победить, не вступая в бой. При этом необходимость перехода к силовому достижению целей операции считается стратегической неудачей и его использование допускается только в крайнем случае.

Командир — главное звено в системе подготовки и ведения боевых действий. Поэтому попытки воздействовать на его эмоциональную

сферу, дезорганизовать мышление и поведение всегда будет важнейшей задачей информационно-психологического воздействия.

По мнению экспертов, такие операции будут начинаться заблаговременно, еще на стадии разработки планов вооруженного конфликта, и на его начальных стадиях. Обычные боевые действия могут даже не планироваться. Достижение целей противоборства в идеальном варианте должно обеспечиваться только средствами информационной войны.

Полностью силы и средства информационной войны могут быть задействованы и в ходе самих боевых операций. В этом случае будет решаться задача уничтожения систем боевого управления, информационных систем получения, хранения и переработки информации военного и государственного значения, а также морально-психологического подавления противника.

Информационная война представляет собой сложную многоярусную структуру действий и операций, направленных одновременно на решение наступательных и оборонительных задач. Примерный перечень разнонаправленных усилий в ходе информационного противостояния представлен в табл. 3.1.

Таблица 3.1.

Информационное обеспечение наступательных и оборонительных действий

Наступательные действия	Оборонительные действия
1. Разведка, имеющая целью вскрыть ***замысел противника***, его материальные возможности и морально-психологическое состояние, ресурсы оборонного комплекса и информационного обеспечения реальных действий	Контрразведка. Маскировка своих целей, действий, объектов. Проведение дезинформации
2. Дезорганизация ***систем связи и управления*** войсками противника, разрушение его баз данных	Обеспечение собственной помехоустойчивости, защита своих баз данных, систем связи, средств обработки и передачи информации
3. Информационно-психологическое воздействие на ***руководство*** страны и Вооруженных сил, а в ходе конкретных боевых операций – на ***командиров и штабы*** противника (борьба с его «головой и шеей»)	Организация информационной защиты и психологической поддержки руководящего состава своих войск (и страны)

Наступательные действия	Оборонительные действия
4. Информационно-психологическое воздействие на ***личный состав*** подразделений и частей противника – подавление патриотических установок, внушение чувства страха и неизбежности поражения, дезорганизация мышления и приобретенных навыков действий на поле боя	Защита своих войск от информационно-психологического воздействия противника, формирование и поддержание на высоком уровне морально-волевых качеств личного состава
5. Проведение агитационно-пропагандистских мероприятий и других информационно-психологических акций среди ***населения*** противостоящей страны с целью снижения уровня национального самосознания, формирования недоверия правящей элите, нежелания поддерживать ее планы и действия. Создание (по возможности) своего рода ***«пятой колонны»*** внутри государства. Провоцирование национальных и религиозных конфликтов	Осуществление заблаговременной и активной контрпропаганды внутри страны, достижение реального единства между всеми слоями общества, между народом и армией, открытое и честное информирование населения по всему кругу вопросов

«Мы приближаемся к такой ступени развития, когда уже никто не является солдатом, но все являются участниками боевых действий. Задача теперь состоит не в уничтожении живой силы, но в подрыве целей, взглядов и мировоззрения населения, в разрушении социума» (из выступления представителя руководства Пентагона).

По мнению военных экспертов, ***в оборонной сфере наиболее уязвимыми*** считаются:

информационные ресурсы аппарата Министерства обороны, Генерального штаба, главных штабов видов Вооруженных сил и родов войск, научно-исследовательских учреждений, содержащих сведения о планах подготовки и ведения действий, о составе и дислокации войск;

информационные ресурсы предприятий оборонного комплекса, содержащих сведения об объемах создаваемой военной техники и ее боевых возможностях;

системы связи и управления войсками и оружием, их информационное обеспечение;

морально-психологическое состояние войск и населения.

Информационно-психологическое воздействие противника на личный состав армии и флота станет значительно менее эффективным, если заблаговременно (и постоянно) будет осуществляться информационное обеспечение задачи, связанной с реальным повышением статуса человека в погонах, созданием благоприятного в общественном восприятии имиджа военной службы и Вооруженных сил. Недостаточность такого обеспечения в современной России существенно облегчает работу наших соперников в информационной войне.

При современных возможностях доведения информации до объекта воздействия *информационные войны не знают границ* – ни пространственных, ни временных. Достижения в техническом оснащении средств массовой информации и коммуникации, а также в способах их применения позволяют сегодня оказывать воздействие практически на каждого человека и почти в любой точке Земли. Современная информационная война – прямой продукт глобализации мира. И она будет носить действительно глобальный характер. В число сфер ведения боевых действий войдет не только физическое пространство (суша, море, воздух, космос), но и *информационная сфера,* включающая, в частности, *виртуальное пространство Интернета, а также социальное, психологическое, идеологическое и духовное пространства,* в рамках которых и будет наноситься основное поражение противнику. В отличие от прошлых войн, понятие «театр военных действий» оказывается весьма условным.

Поле боя XXI века – это информационная сфера, в которой разворачиваются наступательные и оборонительные операции.

К характерным особенностям *глобальной информационной войны*, которая нередко определяется как очередная «мировая война», военные специалисты относят следующие:

война будет основана, прежде всего, на возможности управления и манипулирования общественным сознанием, подчинения воли человека. Основным объектом воздействия станут люди;

главные потери ожидаются не в традиционном, физическом, смысле, а в духовном, психологическом, политическом, социальном. Считается, что такие потери способны в большей степени, чем физические, стать определяющими для исхода войны;

важную роль будет играть манипулирование настроением и установками *населения страны в целом*, а также использование техноло-

гий подготовки *внутренней оппозиции* в странах – жертвах агрессии. Что из себя могут представлять такие процессы, хорошо показали прокатившиеся по странам Восточной Европы и части Азии – при поддержке США – так называемые «цветные» революции;

одновременно будет проводиться активная работа по подрыву авторитета государства, его сотрудничества с другими странами. Это тоже можно было видеть в последних акциях США (например, в Югославии, Ираке, Сомали, Белоруссии);

возрастет роль «невоенных» средств борьбы и «непрямых действий», то есть действий бесконтактным способом;

эффективность информационного оружия будет определяться тем, насколько оно поражает сущностную основу человека, его волю, нравственность, ментальность. И это поражение по своим последствиям будет более губительным для человека и человечества, чем огневое;

в отличие от всех предшествующих войн информационная война будет перманентной, непрерывно расширяющейся во времени и пространстве и, следовательно, более продолжительной, растянутой на многие годы и даже десятилетия.

Как известно, информационное оружие уже прошло успешную «обкатку» в «холодной войне» 1945–1991 гг. И мир убедился, что невоенные, нетрадиционные средства, способы и методы борьбы во много раз эффективнее традиционных военных. Масштаб демографических, территориальных, политических, экономических, психологических потерь Советского Союза после поражения в этой войне оказался неизмеримо большим и труднее восполнимым, чем ущерб Германии и Японии, проигравших Вторую мировую войну.

В настоящее время невозможно предположить, кто станет победителем в войне, где *основным объектом воздействия является психика человека.* И, главное, невозможно определить, каким будет послевоенный психологический облик и победителей, и побежденных. Вполне вероятно, что стратегическим итогом такой войны окажется принципиально деформированная психика людей. Следовательно, сегодня более важно думать не о том, как выиграть информационную войну, а о том, как ее остановить, как наложить вселенский запрет на *информационное оружие как оружие массового поражения.*

Однако пока такого запрета нет, необходимо по крайней мере заботиться о защите от информационного оружия, об обеспечении информационной безопасности человека, общества, государства. В ходе «холодной войны» 1945–1991 гг. (по своей сути уже тогда главным образом информационной) советское руководство – гражданское и военное – оказалось не готово к новым, отличным от войны 1941–1945 гг., формам противостояния. В итоге самая могучая в мире Советская армия, не вступая в битву, проиграла войну. История может повториться еще раз, в очередной войне, которая, видимо, уже ведется «неочевидными», «негорячими» средствами. Готовимся ли мы к комплексному использованию современных сил и средств (среди которых главные – информационные) или все еще надеемся лишь на мощь стратегических ракет, танковых армад и массовых армий? По мнению военных экспертов, в стратегии Российского государства понятие «война» по-прежнему рассматривается, главным образом, через призму вооруженной борьбы между государствами. Поэтому сохраняющиеся в армии, обществе, институтах власти традиционные представления о войне и мире могут с большой вероятностью сыграть такую же роковую роль в судьбе постсоветской России, как и в судьбе СССР.

3.3. Обеспечение информационной безопасности в правоохранительной сфере и при возникновении чрезвычайных ситуаций

Доктрина информационной безопасности РФ в ***правоохранительной (и судебной) сфере*** к наиболее важным объектам обеспечения информационной безопасности относит:

информационные ресурсы органов власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;

информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;

информационную инфраструктуру (информационно-вычислительные сети, пункты управления, узлы и линии связи).

На информационную безопасность в правоохранительной (и судебной) сфере могут влиять следующие ***внешние угрозы***:

разведывательная деятельность специальных служб иностранных государств, международных преступных сообществ, организаций и групп, сбор сведений, раскрывающих задачи, планы деятельности, техническое оснащение, методы работы и места дислокации специальных подразделений и органов внутренних дел РФ;

деятельность иностранных государственных и частных коммерческих структур, стремящихся получить несанкционированный доступ к информационным ресурсам правоохранительных и судебных органов.

Внутренними угрозами, представляющими опасность для данной сферы, являются:

нарушение установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в картотеках и автоматизированных банках данных и использующейся для расследования преступлений;

недостатки законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;

отсутствие единой методологии сбора, обработки и хранения информации оперативно-разыскного, справочного, криминалистического и статистического характера;

отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

преднамеренные действия, а также ошибки персонала, непосредственно занятого формированием и ведением картотек и автоматизированных банков данных.

В правоохранительной (и судебной) сфере наряду с общими приемами защиты информации применяется также ряд *специфических методов и средств* обеспечения информационной безопасности:

создание защищенной многоуровневой системы интегрированных банков данных оперативно-разыскного, справочного, криминалистического и статистического характера на базе специализированных информационно-телекоммуникационных систем;

повышение уровня профессиональной и специальной подготовки пользователей информационных систем.

В современных условиях особое значение имеет осуществление эффективной информационной политики при ***чрезвычайных ситуациях*** техногенного, социального и природного характера.

Наиболее уязвимыми *объектами* обеспечения информационной безопасности в условиях чрезвычайных ситуаций Доктрина информационной безопасности называет:

систему сбора и обработки информации о возможном возникновении чрезвычайных ситуаций;

систему принятия решений по оперативным действиям (реакциям), связанным с развитием таких ситуаций и ходом ликвидации их последствий.

Особое значение для нормального функционирования указанных объектов имеет:

обеспечение безопасности информационной инфраструктуры страны при авариях, катастрофах и стихийных бедствиях;

отсутствие сокрытия, задержки поступления, искажения и разрушения оперативной информации;

исключение несанкционированного доступа к ней отдельных лиц или групп лиц.

Несоблюдение этих условий может привести как к человеческим жертвам, так и к возникновению разного рода сложностей при ликвидации последствий чрезвычайной ситуации, связанных с особенностями информационного воздействия в экстремальных условиях:

к приведению в движение больших масс людей, испытывающих психический стресс;

к быстрому возникновению и распространению паники и беспорядков на основе слухов, ложной или недостоверной информации.

К специфическим для данных условий *направлениям обеспечения информационной безопасности* относятся:

разработка эффективной системы мониторинга объектов повышенной опасности, нарушение функционирования которых может привести к возникновению чрезвычайных ситуаций, и прогнозирования чрезвычайных ситуаций;

совершенствование системы информирования населения об угрозах возникновения чрезвычайных ситуаций, об условиях их возникновения и развития;

повышение надежности систем обработки и передачи информации, обеспечивающих деятельность федеральных органов исполнительной власти;

прогнозирование поведения населения под воздействием ложной или недостоверной информации о возможных чрезвычайных ситуациях и выработка мер по оказанию помощи большим массам людей в условиях этих ситуаций;

разработка специальных мер по защите информационных систем, обеспечивающих управление экологически опасными и экономически важными производства ми.

Исследования, проведенные сотрудниками МЧС России, показывают, что в начальный период чрезвычайных ситуаций общественное настроение, как правило, больше негативное, нежели конструктивное. У такого положения много причин. Но его доминантой является *неготовность населения к адекватному восприятию происходящего.* Корни такой неготовности – в системе информационного обеспечения населения. Эту неготовность предопределяют:

отсутствие прогностической информации и оповещения людей о времени возможного начала чрезвычайной ситуации (например, подземных толчков и сейсмических волн, их силе, характере и продолжительности). Отсюда – неожиданность и уникальность большинства чрезвычайных ситуаций для населения;

отсутствие у большей части людей информации о том, как действовать в той или иной критической обстановке, ведущее к растерянности при возникновении чрезвычайной ситуации;

недостаточная информированность населения об особенностях действий на разных этапах чрезвычайной ситуации и при разных сценариях ее развития;

повышенное повседневное *стрессовое состояние массового сознания* как фоновая характеристика нашего времени и скрытая предпосылка быстрого и резкого эмоционально-психологического срыва людей в критической обстановке;

слабая отработанность алгоритмов управления населением в условиях чрезвычайной ситуации и, как следствие, отсутствие доступной информации о действиях местных органов власти, сил МЧС, порядке аварийно-спасательных работ и эвакуации населения;

отсутствие у большинства людей знаний об особенностях развития различных видов техногенных и природных чрезвычайных ситуаций.

Формирование адекватных мнений и настроений, особенно в экстремальных условиях – сложный и трудный процесс. Спе-

циалисты отмечают, что он тем эффективнее, чем лучше этот процесс организован, чем яснее руководители представляют его элементы, структуру, прямые и обратные связи с населением на разных его этапах.

Снизить негативное влияние чрезвычайных ситуаций на общественное мнение могут только хорошо поставленное, в том числе упреждающее, информирование и быстрые, четкие и грамотные действия как местных руководителей, так и сил МЧС. Очень важно *избежать вакуума в информационном поле*, взять информационную инициативу в свои руки. В противном случае, и это характерно как для регионального, так и для федерального уровня, начинают работать домыслы, распаленные эмоциями фантазии и процесс управления информационной средой значительно усложняется. Информационное обеспечение чрезвычайных ситуаций необходимо готовить заблаговременно и на регулярной основе.

По мнению специалистов, целесообразно улучшить *обучение населения действиям при техногенных и природных катастрофах.* Неоценимый вклад в подготовку граждан к действиям в условиях чрезвычайных ситуаций могут и должны внести местные и региональные СМИ. В массовой печати, на радио и телевидении полезно в игровой форме моделировать различные чрезвычайные ситуации и правильные действия людей, попавших в бедственную природную или социальную стихию. Все комментарии специалистов должны носить четкий, ясный и однозначный характер. Не следует забывать и о такой форме, как выпускаемые массовым тиражом красочные памятки для населения о поведении в условиях чрезвычайных ситуаций.

Слухи, сплетни, паника

Явлением, противодействующим обеспечению безопасности в условиях чрезвычайной ситуации, часто оказываются ***слухи*** как *особая форма массового обмена недостоверной или искаженной информацией в устном виде.* Слухи обычно возникают при отсутствии полной и достоверной информации по актуальной для людей в данный момент проблеме. Информация, передаваемая в форме слухов, возникает, как правило, стихийно и имеет несанкционированный, неконтролируемый и неуправляемый характер. Необходимым и достаточным условием возникновения слухов чаще всего оказывается наличие неудовлетворенной актуальной по-

требности людей или угрозы безопасности их жизнедеятельности. В этих ситуациях даже самые невероятные сообщения, передаваемые неформально, как бы «по секрету», могут вызывать интерес и получить широкое распространение в виде слухов. Следовательно, главной причиной появления и распространения слухов является неудовлетворенная информационная потребность людей, своего рода «информационный голод», особенно в чрезвычайных жизненных ситуациях. Впрочем, «информационный голод» всегда чреват появлением слухов.

> Роль такого «голода» образно подмечена Н. В. Гоголем в «Мертвых душах»: «В другое время и при других обстоятельствах подобные слухи, может быть, не обратили бы на себя никакого внимания; но город N уже давно не получал никаких совершенно вестей... что, как известно, для города то же, что своевременный подвоз съестных припасов».

На появление слухов влияют также недостаточная оперативность и объективность информации, ее ангажированность, излишняя закрытость (секретность), стремление сгладить в ходе информирования населения остроту происходящего. Как раз в ответ на такие действия слухи начинают представлять ситуацию в преувеличенно драматическом варианте. Они всегда являются эмоционально-компенсирующим следствием недостаточно полной или необъективной информации, предоставляемой официальными службами.

> Характерный пример действия слухов – массовая скупка в начале 2006 г. населением Москвы и других городов России обычной поваренной соли. Неизвестные по своему источнику слухи о грядущем дефиците этого продукта за считанные дни привели к пустым прилавкам и десятикратному росту цен на соль. Никакие доводы руководителей торговли об отсутствии объективных предпосылок к нехватке соли на народ не действовали. Нормализовать ситуацию удалось только через несколько недель.

Задача профилактики слухов и купирования их в случае возникновения становится неотъемлемой частью всей программы действий в опасных для людей условиях, в частности, при различных природных и социальных бедствиях, техногенных катастрофах, во всех местах большого скопления людей. В таких условиях (как, впрочем, и в повседневной жизни) людям, прежде всего, нужна четкая и понятная информация, не только объясняющая причину слухов, но, главное, дающая объективный анализ

складывающейся ситуации и снижающая тем самым меру эмоциональной напряженности при ее восприятии. Важно не просто опровергнуть тот или иной слух, но заполнить образовавшийся информационный вакуум максимально подробной и убедительной информацией. Кроме того, в условиях чрезвычайных ситуаций необходимо также выявлять распространителей слухов и добиваться снижения их влияния на толпу.

Одной из разновидностей слухов являются ***сплетни***. В словаре С. И. Ожегова сплетня определена как *слух о ком-нибудь или о чем-нибудь, основанный на неточных или заведомо неверных сведениях*. Обычно сплетню составляет ложная или искаженная и неполная, но всегда пристрастная информация о личной жизни и поступках людей, известных и интересных значительной части населения.

Сплетни, как и слухи, тоже удовлетворяют определенную информационную потребность масс, не всегда социально добротную и пристойную. Нередко они муссируют интимные стороны жизни своих «героев» и даже носят откровенно неприличный характер. В итоге сплетня может не только выполнять некую информационно-познавательную функцию, но и быть средством борьбы за достижение определенных целей и в этом качестве представлять немалую социальную опасность. Она может использоваться для нечестной дискредитации своего противника, возбуждения против него негативных эмоций в обществе. Поэтому в процессе воспитания школьников требуется целенаправленное раскрытие сущности и роли сплетен, формирования у подростков внутренней готовности к отказу от передачи сплетен и осуждению сплетников.

Одна из задач информационного обеспечения действий в чрезвычайных ситуациях состоит в том, чтобы не допустить перерастания слухов в панику. ***Паника*** – очень *опасное психологическое состояние толпы*, требующее решительных, в том числе информационных, действий по предотвращению его нагнетания и распространения.

По мнению психологов, есть два основных обстоятельства, определяющих возникновение паники.

Первое связано с внезапностью появления угрозы для жизни, здоровья, безопасности (например, при пожаре, взрыве, аварии и т. п.).

Второе можно объяснить накоплением так называемого «психологического горючего» и, затем, срабатыванием, как «реле», того или иного психического катализатора. Длительные переживания, опа-

ение тревоги, неопределенность ситуации, предпо-
ности и невзгоды – все это создает благоприятный
икновения паники, а катализатором в этом случае
юбое событие. Вызвать панику может не только
т, страх, но и отдельные слова, чье-то поведение,
алы, даже не имеющие отношения к ожидаемым

паники может быть значительная деформация оце-
щего, снижение готовности к адекватным действи-
е страха, повышенная подверженность внешним
А в более выраженной форме это состояние может
ной невменяемости и утрате контроля над своим по-
овек может бежать, куда попало (иногда прямо в очаг
ссмысленно метаться, совершать самые нелепые,
ействия и поступки. Есть немало примеров такого
время землетрясений, ураганов, пожаров и т. д.
причинами паники в большинстве случаев опять же
информационные факторы:
онно-психологическая неготовность людей к адек-
риятию случившегося, недостаток конкретной ин-
акследствие, наличие своего рода «информационной

сть каждой экстремальной ситуации, создающая
напряжение при столкновении с ней;
готовка большинства людей к рациональным дей-
ае опасности;
толпе людей эмоционально неустойчивых, оказы-
итической ситуации катализаторами негативных
и.

сновные направления и мероприятия защите электронной информации

ению Доктрины, основными объектами обеспече-
ционной безопасности в ***общегосударственных информ-
лекоммуникационных системах*** являются:
ионные ресурсы, содержащие сведения, отнесенные
ной тайне, и конфиденциальную информацию;

средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации ограниченного доступа, их информативные физические поля;

технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается информация ограниченного доступа, а также сами помещения, предназначенные для обработки такой информации.

К *основным угрозам* информационной безопасности в общегосударственных информационных и телекоммуникационных системах Доктрина относит:

деятельность специальных служб иностранных государств, преступных сообществ, противозаконную деятельность отдельных лиц (организаций и групп), направленную на получение несанкционированного доступа к информации и осуществление контроля над функционированием информационных телекоммуникационных систем;

вынужденное в силу объективного отставания отечественной промышленности использование при создании и развитии информационных и телекоммуникационных систем импортных программно-аппаратных средств;

нарушение установленного регламента сбора, обработки и передачи информации, преднамеренные действия и ошибки персонала информационных и телекоммуникационных систем, отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

использование не сертифицированных в соответствии с требованиями безопасности средств и систем информатизации и связи, а также средств защиты информации и контроля их эффективности;

привлечение к работам по созданию, развитию и защите информационных и телекоммуникационных систем организаций и фирм, не имеющих государственных лицензий на осуществление этих видов деятельности.

Используемые в этой сфере *средства информационного воздействия* могут быть направлены на решение следующих задач:

уничтожение, искажение или хищение информационных массивов;

добывание из них необходимой информации после преодоления систем защиты;

дезорганизацию работы технических средств;

вывод из строя телекоммуникационных систем и сетей, компьютерных систем, энергетических систем, систем государственного управления, то есть всего высокотехнологичного обеспечения жизни общества и функционирования государства.

Атакующие средства информационного воздействия

Идеи и материальные основы информационного оружия формировались одновременно с развитием информационной среды. Компьютеризация различных сфер общественной жизни, новейшие информационные технологии, превращение программирования в престижную и массовую специальность создали базовые предпосылки для возникновения новых типов информационного оружия и в то же время сделали объекты управления и связи, энергетики и транспорта, банковскую систему весьма уязвимыми по отношению к информационному воздействию.

1. ***Компьютерные вирусы*** *– программные средства, способные размножаться, прикрепляться к программам, передаваться по линиям связи и сетям передачи данных, проникать в электронные телефонные станции и системы управления и выводить их из строя.*

Распространение компьютерного вируса основывается на его способности использовать любой носитель передаваемых данных в качестве «средства передвижения». В итоге любая дискета или иной магнитный накопитель, перенесенные на другие компьютеры, способны заразить их. И наоборот, когда «здоровый» носитель подключается к зараженному компьютеру, он может стать носителем вируса. Удобными для распространения обширных эпидемий оказываются телекоммуникационные сети. Достаточно одного контакта, чтобы персональный компьютер был заражен или заразил тот, с которым контактировал. Однако самый частый способ заражения – это копирование программ и данных, что является обычной практикой у пользователей персональных ЭВМ: копируемые объекты могут оказаться зараженными.

В печати часто проводится параллель между компьютерными вирусами и вирусом AIDS (СПИД). Только упорядоченная половая жизнь способна уберечь от этого вируса. Беспорядочные связи персонального компьютера со многими другими с большой вероятностью могут привести к заражению.

Поэтому специалисты предостерегают от копирования «ворованных» программ. Однако пожелание ограничить использование непроверенного программного обеспечения пока еще остается практически невыполнимым. Фирменные программы на «стерильных» носителях стоят немалых денег, поэтому избежать их неконтролируемого копирования и распространения почти невозможно.

По оценке специалистов, в настоящее время «в обращении» находятся сотни типов вирусов. По-видимому, в будущем будут появляться принципиально новые их виды. Пока речь идет только о заражении компьютеров, но в перспективе, как считают специалисты, будет возможным и заражение микросхем, информационная мощность которых стремительно развивается.

2. *«Логические бомбы»* — такое название получили *программные закладные устройства, заранее внедряемые в информационно-управляющие центры военной и гражданской инфраструктуры,* которые по сигналу или в установленное время приводятся в действие, уничтожая или искажая информацию и дезорганизуя работу программно-технических средств.

Одна из разновидностей такой бомбы — «троянский конь» — программа, позволяющая осуществлять скрытный несанкционированный доступ к информационным ресурсам противника для добывания разведывательной информации.

3. ***Средства подавления*** (или фальсификации) информационного обмена в телекоммуникационных сетях, передача по каналам государственного и военного управления, а также по каналам массовой информации нужной (с позиций противодействующей стороны) информации.

4. ***Средства внедрения*** компьютерных вирусов и «логических бомб» в государственные и корпоративные информационные сети и системы и управления ими на расстоянии.

Применение информационного оружия в информационных и телекоммуникационных системах носит скрытый и обезличен-

ный характер, легко маскируется под меры защиты авторских и коммерческих прав на программные продукты и не связывается с объявлением войны или введением периода особых действий в локальных конфликтах. Наиболее уязвимыми для нападения являются те системы, которые должны сохранять непрерывную работоспособность в реальном масштабе времени.

Специалисты выделяют три основные *формы воздействия на киберпространство*:

информационный криминал;

информационный терроризм;

операции, проводимые в рамках масштабных информационных войн.

По данным зарубежной печати, мотивы совершаемых в настоящее время компьютерных преступлений распределяются следующим образом: корыстные побуждения – 66 %, шпионаж и диверсия – 17 %, исследовательский интерес – 7 %, хулиганство – 5 %, месть – 5 %. Рассмотрим криминальные и террористические варианты действий.

Информационный криминал

Этим термином обозначают действия отдельных лиц или группы лиц, *направленные на взлом систем защиты и хищение или разрушение информации в корыстных или хулиганских целях.* Они представляют собой, как правило, разовые преступления против конкретного объекта киберпространства. Такой вид преступлений получил также название «компьютерные преступления». Стремительное развитие компьютерных технологий и сетей, в том числе международных, как неотъемлемой части различных видов общественной деятельности создало широкий простор для совершения преступных действий подобного типа. В то же время преступления, связанные с использованием современного информационного оружия, выходят за рамки обычных преступлений и нередко ставят перед правоохранительными органами трудноразрешимые задачи.

Компьютерные преступления могут быть связаны с осуществлением следующих действий:

несанкционированным проникновением в информационно-вычислительные сети или массивы информации;

хищением прикладного и системного программного обеспечения;

несанкционированным копированием, изменением или уничтожением информации;

передачей компьютерной информации лицам, не имеющим к ней доступа;

подделкой, модификацией или фальсификацией компьютерной информации. К подделке информации можно отнести также подтасовку результатов выборов, голосований, референдумов, осуществляемых с помощью электронных технологий;

разработкой и распространением компьютерных вирусов;

несанкционированным просмотром или хищением информационных баз;

механическими, электрическими, электромагнитными и другими видами воздействия на информационно-вычислительные сети, вызывающими их повреждения.

Наиболее опасны в сфере компьютерной преступности ***хакеры*** – «одержимые программисты», «электронные корсары», «компьютерные пираты». Так называют людей, осуществляющих несанкционированный доступ в чужие информационные сети. Они, как правило, хорошо подготовлены технически и профессионально, отлично разбираются в вычислительной технике и программировании. Их деятельность направлена на несанкционированное проникновение в компьютерные системы и кражу, модификацию или уничтожение имеющихся там данных. Результаты зарубежных исследований показывают, что 62 % хакеров действуют в составе преступных групп.

Однако еще более высокий уровень подготовки имеют лица, занимающиеся ***компьютерным шпионажем***. Их целью является получение из компьютерных сетей противника стратегически важных данных военного, технического и иного содержания.

По прогнозам отечественных и зарубежных специалистов, основной сферой компьютерных преступлений становится *область финансовой и банковской деятельности*. В настоящее время ущерб, наносимый только одним компьютерным преступлением, в среднем составляет 340 тыс. долларов США, тогда как средний ущерб от «традиционных» преступлений против банковских структур – ограблений – примерно 9 тыс. долларов. По оценкам специалистов

США, убытки от проникновения хакеров в автоматизированные комплексы, обслуживающие эти учреждения, оцениваются в десятки миллионов долларов. При этом число зарегистрированных компьютерных преступлений имеет тенденцию к *ежегодному удвоению*. С каждым годом расширяется и «география» компьютерных преступлений, распространяясь на все новые и новые страны.

> С приходом в нашу страну глобальной сети Интернет участились случаи взлома информационной защиты зарубежных банков и хищений с помощью компьютеров крупных денежных средств. Широко известно дело Владимира Левина, хакера из Санкт-Петербурга, похитившего из американского Сити-банка около 4 млн долларов США. В Южном округе столицы 11 марта 1998 г. был задержан гражданин Шейко П. В., который, используя номера международных кредитных карт, полученных обманным путем, через Интернет за четыре месяца совершил хищение 18 тыс. долларов США. В этом же году во Внешэкономбанке было выведено из-под учета ЭВМ и подготовлено к хищению около 300 тыс. долларов (из них 125 тыс. долларов было похищено). С использованием способов несанкционированного доступа была осуществлена попытка хищения 68 млрд 309 млн рублей из Центрального банка РФ.

Как видно из перечисленных примеров (а это только малая часть всех подобных деяний), круг преступных интересов в кредитно-финансовой сфере весьма разнообразен. Кроме того, отмечается рост преступлений, связанных с денежными хищениями на транспорте при реализации железнодорожных и авиабилетов, продажей фальшивых зарубежных путевок и т. д.

По мере развития технологий «безбумажного» документооборота, в том числе электронных платежей, серьезный сбой локальных сетей может парализовать работу банков и целых корпораций, что приведет к ощутимым материальным потерям. Не случайно защита данных в компьютерных сетях становится одной из самых острых проблем в современной информатике.

Информационный терроризм

Процессы глобальной информатизации привели к тому, что современное общество постепенно приобретает практически полную зависимость от состояния информационной инфраструктуры, включающей в себя объединение различных систем связи, телекоммуникационных средств, баз данных и информа-

ционных систем, принадлежащих государству, негосударственному сектору экономики, организациям, гражданам.

В этих условиях ***информационный терроризм*** – *терроризм с использованием информационного оружия* – представляет собой наиболее реальную угрозу как для отдельных развитых стран, так и для всего мирового сообщества.

В тактике информационного терроризма, как и любого другого, главное состоит в том, чтобы террористический акт имел опасные последствия и получил большой общественный резонанс. Как правило, действия информационных террористов сопровождаются угрозой повторения террористического акта без указания конкретного объекта.

В киберпространстве могут быть использованы различные *приемы достижения террористических целей*:

нанесение ущерба отдельным физическим элементам киберпространства, разрушение сетей электропитания, наведение помех, использование специальных программ, стимулирующих разрушение аппаратных средств, разрушение элементной базы с помощью биологических и химических средств и т. д.;

кража или уничтожение программного и технического ресурсов киберпространства, имеющих общественную значимость, внедрение вирусов, программных закладок и т. п.;

угроза опубликования или опубликование информации государственного значения о функционировании различных элементов информационной инфраструктуры государства, принципов работы систем шифрования, конфиденциальных сведений персонально-общественного характера и др.;

захват каналов средств массовой информации с целью распространения дезинформации, слухов, демонстрации мощи террористической организации и объявления своих требований;

уничтожение или подавление каналов связи, искажение адресации, искусственная перегрузка узлов коммутации и др.;

воздействие на операторов информационных и телекоммуникационных систем путем насилия, шантажа, подкупа, введения наркотических средств, использования нейролингвистического программирования, гипноза и других методов информационного воздействия.

Сегодня даже администрация США вынуждена признать, что информационное пространство Америки слабо защищено от не-

санкционированного проникновения в его пределы. Так, даже ситуационная комната Белого дома может подвергнуться информационному воздействию через сеть Интернет.

Защитные действия

Основными направлениями обеспечения информационной безопасности в общегосударственных информационных и телекоммуникационных системах, согласно Доктрине, являются:

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

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

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

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

обеспечение информационной безопасности при подключении общегосударственных информационных и телекоммуникационных систем к внешним, в том числе международным, информационным сетям;

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

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

Основными организационно-техническими мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах считаются:

лицензирование деятельности организаций в области защиты информации;

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

сертификация средств защиты информации и контроля эффективности их использования, а также защищенности инфор-

мации от утечки по техническим каналам систем и средств информатизации и связи;

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

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

В настоящее время в области борьбы с компьютерной преступностью имеется немало нерешенных проблем.

Во-первых, в нашей стране недостаточно развито специальное законодательство, затрагивающее различные аспекты компьютерной преступности, опасность подобных преступлений все еще слабо осознается законодателями, тогда как этот вид преступлений быстро прогрессирует.

Во-вторых, ввиду особой сложности компьютерных систем создание для них безошибочных программ практически невозможно.

В-третьих, распространена практика приобретения информации, в том числе нелицензированного программного обеспечения, путем несанкционированного копирования. Программное обеспечение распространяется практически повсеместно путем краж и обмена краденым.

В-четвертых, неудовлетворительно финансовое положение научно-технической интеллигенции, связанной с созданием информационных систем, что создает предпосылки для «утечки мозгов» и осуществления разного рода «информационных диверсий».

В-пятых, обеспечение информационной безопасности — дорогостоящее дело, и не столько из-за затрат на установку необходимых для этого средств, сколько из-за того, что весьма сложно определять границы разумной безопасности и поддерживать системы в работоспособном состоянии.

Используемые в настоящее время меры предупреждения компьютерных преступлений можно объединить в три группы:

технические;

организационные;

правовые.

Технические меры защиты от несанкционированного доступа к компьютерным системам предполагают:

использование средств физической защиты, включая средства защиты кабельной системы, системы электропитания, средства архивации и копирования информации на внешние носители и т. д.

организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев;

разработку программных средств защиты, в том числе антивирусных программ, систем разграничения полномочий, программных средств контроля доступа;

принятие конструктивных мер защиты от хищений и диверсий;

установку резервных систем электропитания;

оснащение помещений замками, установку сигнализации и многое другое.

К *организационным мерам* можно отнести:

организацию охраны вычислительного центра;

тщательный подбор персонала;

исключение случаев ведения особо важных работ только одним человеком;

шифрование данных для обеспечения конфиденциальности информации;

меры защиты, включающие контроль доступа в помещения, разработку стратегии безопасности фирмы, планов действий в чрезвычайных ситуациях и т. д.

организацию надежной и эффективной системы архивации и дублирования наиболее ценных данных;

защиту информации от несанкционированного доступа, включая использование различных устройств для идентификации личности по *биометрической информации* – радужной оболочке глаза, отпечаткам пальцев, голосу, размерам кисти руки и т. д.;

возложение персональной ответственности на конкретных лиц, призванных обеспечить безопасность центра, введение в штат специалистов в области безопасности информации;

универсальность средств защиты от всех пользователей (включая высшее руководство);

наличие плана восстановления работоспособности центра после выхода его из строя и т. п.

К ***правовым мерам*** относятся:

ужесточение норм, устанавливающих ответственность за компьютерные преступления;

защита авторских прав программистов;

совершенствование уголовного и гражданского законодательства в этой сфере.

К правовым мерам относятся также вопросы общественного контроля за разработчиками компьютерных систем и принятие международных договоров об ограничениях в их деятельности.

К числу основных мер ***противодействия информационному терроризму*** можно отнести:

создание единой стратегии борьбы с информационным терроризмом, в соответствии с которой функции силовых ведомств четко распределены и координируются государством;

создание общего центра для мониторинга угроз информационного терроризма и разработки мер быстрого реагирования;

организацию качественной защиты материально-технических объектов, составляющих физическую основу информационной инфраструктуры;

развитие технологий обнаружения воздействий на информацию и ее защиты от несанкционированного доступа, искажения или уничтожения;

непрерывную подготовку персонала информационных систем к эффективному противостоянию различным вариантам действий террористов;

развитие межгосударственного сотрудничества в борьбе с информационным терроризмом.

Россия вступила на путь формирования информационного общества и вхождения в мировое информационное пространство. Мы должны осознавать неизбежность появления на этом пути новых угроз, требующих создания адекватных программ и проектов для защиты национальных информационных ресурсов.

Следует осознавать, что любые мероприятия по борьбе с информационным терроризмом могут существенно ограничивать свободу всех видов информационной деятельности в обществе и государстве, права граждан и организаций на свободное производство, получение, распространение и использование информации. Поэтому государственная стратегия борьбы с инфор-

мационным терроризмом должна строиться на основе поиска приемлемого для общества компромисса – быть защищенным, но открытым, не допускающим монополизма отдельных ведомств.

Несомненно, что в начале нового столетия, когда масштабы применения все более совершенных компьютерных технологий стремительно расширяются, задача защиты компьютерных систем от преступных посягательств не только переходит в ранг задач государственной политики, но и является делом каждого.

3.5. Безопасность в сфере духовной жизни человека и общества

Информационная агрессия в любой сфере общественной жизни – в экономике, внутренней и внешней политике, науке и технике, в ходе военных действий или при организации действий правоохранительных структур и подразделений МЧС – есть, прежде всего, агрессия *психологическая*. Ее главный объект – человек в различных ситуациях современной жизнедеятельности и коллизиях общественных отношений.

Нынешнее информационное пространство до предела заполнено дискуссиями о политике, экономике, социальных реформах. Споры очень жесткие, мнения о состоянии общества и его перспективах прямо противоположные. Только идея необходимости экономического процветания – вне сомнений и критики. Она – своего рода «священная корова» современного мира. Результатом прогресса в экономике видится и возможность создания высокообразованного, культурного общества, и внутреннее, психологическое благополучие каждого отдельного человека. Но все ли здесь так однозначно?

Экономическое положение населения в стране год от года улучшается, но ощущение кризисности в сознании людей и в жизни общества не исчезает. Видимо, корни проблем современной цивилизации глубже той плоскости, на которой мы их ищем, перебирая сценарии социально-экономического развития. Мо-

жет быть, они – *внутри человека* и в его отношении к окружающему миру?

Определяется ли душевное состояние людей эффективностью экономики? И происходит ли духовное и нравственное развитие людей параллельно с их материальными достижениями? Однозначных ответов на эти вопросы нет ни у политиков, ни у педагогов. Однако сама жизнь заставляет нас все чаще увязывать проблемы информационной (и национальной) безопасности с тем, что происходит сегодня в духовной сфере человека и общества.

Согласно Доктрине информационной безопасности РФ, обеспечение безопасности ***в сфере духовной жизни*** имеет целью защиту конституционных прав и свобод человека и гражданина и связано с широким спектром действий по различным направлениям жизнедеятельности общества:

развитием, формированием и совершенствованием поведения личности;

свободой массового информирования;

использованием культурного, духовно-нравственного наследия, исторических традиций и норм общественной жизни;

сохранением культурного достояния всех народов России;

реализацией конституционных ограничений прав и свобод человека и гражданина в интересах сохранения и укрепления нравственных ценностей общества;

укреплением традиций патриотизма и гуманизма, здоровья граждан, расширением культурного и научного потенциала РФ;

обеспечением обороноспособности и безопасности государства.

К числу *основных объектов* обеспечения информационной безопасности в сфере духовной жизни Доктрина относит:

достоинство личности;

свободу совести, включая право свободно выбирать, иметь и распространять религиозные и иные убеждения и действовать в соответствии с ними;

свободу мысли и слова (за исключением пропаганды или агитации, возбуждающих социальную, расовую, национальную или религиозную ненависть и вражду);

свободу литературного, художественного, научного, технического и других видов творчества, преподавания;

свободу массовой информации;

неприкосновенность частной жизни, личную и семейную тайну;

русский язык как фактор духовного единения народов многонациональной России, язык межгосударственного общения народов СНГ;

языки, нравственные ценности и культурное наследие народов и народностей РФ;

объекты интеллектуальной собственности.

Наибольшую опасность представляют следующие угрозы информационной безопасности в сфере духовной жизни:

деформация системы массового информирования как за счет монополизации средств массовой информации, так и за счет неконтролируемого расширения сектора зарубежных СМИ в отечественном информационном пространстве;

ухудшение состояния и постепенный упадок объектов российского культурного наследия, включая архивы, музейные фонды, библиотеки, памятники архитектуры, ввиду недостаточного финансирования соответствующих программ и мероприятий;

возможность нарушения общественной стабильности, нанесение вреда здоровью и жизни граждан вследствие деятельности религиозных объединений, проповедующих религиозный фундаментализм, а также тоталитарных религиозных сект;

использование зарубежными специальными службами СМИ для нанесения ущерба обороноспособности и безопасности РФ, распространения дезинформации;

недостаточная способность гражданского общества России обеспечить формирование у подрастающего поколения общественно необходимых нравственных ценностей, патриотизма и ответственности за судьбу страны.

Основными направлениями обеспечения информационной безопасности в сфере духовной жизни, согласно Доктрине, являются:

развитие в России основ гражданского общества;

создание социально-экономических условий для осуществления творческой деятельности и функционирования учреждений культуры;

выработка цивилизованных форм и способов общественного контроля за формированием в обществе духовных ценностей,

отвечающих национальным интересам страны, воспитанию патриотизма и гражданской ответственности за ее судьбу;

совершенствование законодательства РФ, регулирующего отношения в области конституционных ограничений прав и свобод человека и гражданина;

государственная поддержка мероприятий по сохранению и возрождению культурного наследия народов и народностей РФ;

формирование правовых и организационных механизмов обеспечения конституционных прав и свобод граждан, повышения их правовой культуры в интересах противодействия сознательному или непреднамеренному нарушению этих конституционных прав и свобод в сфере духовной жизни;

разработка действенных организационно-правовых механизмов доступа средств массовой информации и граждан к открытой информации о деятельности органов власти и общественных объединений, обеспечение достоверности сведений о социально значимых событиях общественной жизни, распространяемых через средства массовой информации;

разработка специальных правовых и организационных механизмов недопущения противоправных информационно-психологических воздействий на массовое сознание общества, неконтролируемой коммерциализации культуры и науки, а также обеспечивающих сохранение культурных и исторических ценностей народов и народностей РФ, рациональное использование накопленных обществом информационных ресурсов, составляющих национальное достояние в сфере духовной жизни;

введение запрета на использование эфирного времени в электронных средствах массовой информации для проката программ, пропагандирующих насилие и жестокость, антиобщественное поведение;

противодействие негативному влиянию иностранных религиозных организаций и миссионеров.

Правительство Москвы о психологических угрозах безопасности города и защите от них

Постановлением Правительства Москвы от 22 августа 2000 г. № 654 принята ***Концепция безопасности Москвы***. В ней указывается, что значительные нагрузки на психику и сознание людей,

вызываемые социальными, политическими, экономическими, информационными, криминальными опасностями, а также особенности жизни и быта в условиях мегаполиса требуют выделить угрозы психологического характера в самостоятельный фактор опасности для личности, социальных групп и города в целом.

К угрозам психологического характера Концепция относит:

повышение психологической напряженности у населения вследствие усиления ощущения социальной незащищенности:

у детей – от невозможности понимания происходящего в мире;

у пожилых ветеранов войны и труда – от ощущения бессмысленности прожитых лет и борьбы за попранные идеалы;

противопоставление поколений на базе различия в условиях жизни и мотиваций;

информационное навязывание и финансовое подкрепление «западных» стереотипов восприятия, мышления, поведения, внедряемых в сознание жителей города без учета особенностей российского менталитета;

«зомбирование» сознания людей рекламным бизнесом и психотропными методами воздействия;

потребительское отношение к Москве, как к «пространству», где можно обрести финансовую независимость и иные материальные блага, особенно у приезжих и у некоторых некоренных жителей Москвы;

изменение жизненных ценностей в сторону потребительской и индивидуалистической (эгоцентрической) психологии;

формирование культа богатства (за счет приобретения материального благополучия любыми средствами), агрессии и насилия как жизненных ценностей и, как следствие этого, потеря ориентации на нравственные, духовные и культурные ценности.

Основными предпосылками возникновения угроз психологического характера Концепция называет:

нестабильность экономической и финансовой ситуации в городе, ухудшение криминогенной обстановки, увеличение стрессогенных и психогенных факторов в семье, в учебных заведениях, на работе, на улице и т. д.;

разрушение способов формирования духовно-нравственных, культурных, экономических оснований для объединения жите-

лей Москвы в единую социальную общность с достойным уважения менталитетом «москвича – жителя столицы»;

отсутствие психологической культуры у представителей органов власти и у населения в целом;

социальную и психологическую оторванность детей и подростков от взрослых;

нарушение преемственности социально-культурных, национальных традиций и, как следствие, усвоение чуждых российскому менталитету нормативов и образцов (российский менталитет – соборность, западный – индивидуализм);

недостаточность пространственных (ландшафтных), жилищных, культурных, спортивных и иных условий для психологической разгрузки и комфорта жителей (парки, клубы по интересам, бесплатные спортивные площадки, недорогие кафе и т. д.);

уменьшение возможностей для соответствующей моральным нормам реализации активности подростков, из-за чего она реализуется в противоправных и аморальных формах (от вандализма до криминала);

агрессивность информационной видеосреды.

Реализация угроз психологического характера может привести:

к нарушению психического здоровья определенной части жителей Москвы;

к увеличению количества психических заболеваний, самоубийств и преступлений.

Угрозы информационного характера в Концепции безопасности Москвы соответствуют общероссийской Доктрине. Дополнительно в качестве информационных угроз названы:

провоцирование социальной, межнациональной, религиозной напряженности;

искажение исторического опыта и национальных традиций народа;

низкая информационная культура жителей города;

манипулирование массовым сознанием.

Реализация указанных угроз может привести:

к подрыву авторитета города;

созданию атмосферы нестабильности;

дискредитации органов управления и провоцированию конфликтов;

нанесению значительного экономического ущерба.

Вопросы для обсуждения

1. Почему СССР, имея самую мощную армию, проиграл «холодную войну»?
2. Что такое «театр военных действий» в условиях информационной войны?
3. Как могут повлиять на психику человека информационные операции? Не следует ли запретить информационное оружие?
4. Информационная война и «цветные революции» последних лет – какие признаки позволяют говорить о наличии связи между этими явлениями?
5. Что представляет собой состояние «информационной анархии» в условиях чрезвычайных ситуаций? Знакомо ли вам такое явление? Как его избежать?
6. Почему трудно гарантировать абсолютную сохранность информации и безопасность данных в компьютерных сетях?
7. Влияет ли повышение возможностей информационных средств и систем на духовно-нравственное развитие молодежи?
8. Герой рассказа В. Шукшина сетует: «Я знаю, к кому обратиться, когда болит зуб или спина, – но что делать, когда болит душа?» – Что бы вы посоветовали этому герою?

Глава 4

ПРАВОВОЕ И ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности.

Доктрина информационной безопасности Российской Федерации

4.1. Конституция РФ и Доктрина информационной безопасности РФ о правовом обеспечении информационной сферы

Проблема правового регулирования отношений в сфере обеспечения информационной безопасности является для России одной из важнейших. От ее решения во многом зависит сохранение, приумножение и защита информационных ресурсов, становление международного авторитета и снижение криминальной напряженности в стране, защита прав, свобод и безопасности человека в системе информационных отношений.

Конституционные нормы о защите информационной сферы

Одной из важнейших задач государственной политики по обеспечению информационной безопасности граждан является реализация ***конституционных норм*** в сфере информации. Конституция РФ предусматривает право каждого гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ст. 29, п. 4). Конституция гарантирует свободу массовой информации и запрещает ее цензуру (ст. 29, п. 5).

Она же наделяет каждого гражданина правом на неприкосновенность частной жизни, сохранность личной и семейной тайны (ст. 23, п. 1). Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (ст. 24, п. 1). Согласно Конституции, каждому гарантируется свобода мысли и слова (ст. 29, п. 1), а также свобода литературного, художественного, научного, технического и других видов творчества (ст. 44, п. 1).

Положения Конституции РФ прямо или косвенно обязывают органы государственной власти и местного самоуправления, соответствующих должностных лиц обеспечить каждому гражданину РФ возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Однако декларация информационных прав и свобод не означает отказ государства от защиты информационных ресурсов. Правовое обеспечение информационной безопасности формируется на основе поддержания ***баланса интересов граждан, общества, государства***, что особенно важно в условиях существования различных форм собственности. Поэтому Конституцией определены и основания для ограничения информационных прав и свобод граждан. К их числу относятся: защита основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечение обороны страны и безопасности государства (ст. 17, п. 3, ст. 55, п. 3). Основным законом предусмотрена также возможность ограничения прав и свобод в условиях чрезвычайного положения с указанием пределов и сроков их действия (ст. 56).

Соответствующие статьи Конституции РФ направлены на пресечение распространения следующих видов информации:

информации, рассчитанной на разжигание ненависти, вражды и насилия в отношениях между людьми и народами;

непристойной и ложной информации, включая заведомо ложную рекламу;

информации, посягающей на честь и достоинство граждан, оказывающей негативное воздействие на здоровье людей и их духовно-нравственное состояние;

информации, изменяющей память о прошлом, фальсифицирующей историю страны, нарушающей связь поколений и подрывающей единство российского народа;

информации, способной инициировать процессы разрушительного свойства – от техногенных и природных катастроф до всевозможных социальных, демографических, экономических потрясений, кризисов, конфликтов.

Вместе с тем, как указывается в Доктрине информационной безопасности РФ, закрепленные Конституцией РФ права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки в практическом отношении не имеют достаточного правового, организационного и технического обеспечения. Неудовлетворительно организована зашита собираемых федеральными органами государственной власти, органами государственной власти субъектов РФ, органами местного самоуправления данных о физических лицах (персональных данных).

В итоге необеспеченность прав граждан на доступ к информации, манипулирование информацией вызывают негативную реакцию населения, что в ряде случаев ведет к дестабилизации социально-политической обстановки в обществе.

Доктрина информационной безопасности РФ о состоянии и совершенствовании правовых отношений в информационной сфере

Напомним (см. гл. 2), что Доктрина представляет собой документ, содержащий *официально принятую в России систему взглядов на проблемы обеспечения информационной безопасности, методы и средства защиты жизненно важных интересов личности, общества, государства в информационной сфере.*

Доктрина указывает на наличие ряда недостатков, связанных с противоречивостью и неразвитостью ***правового регулирования*** отношений в информационной сфере и приводящих к серьезным негативным последствиям в деле обеспечения информационной безопасности. Они рассмотрены выше, в гл. 2.

Согласно Доктрине, ***совершенствование правовых механизмов*** регулирования общественных отношений, возникающих в информационной сфере, является приоритетным направлением государственной политики в области обеспечения информационной безопасности РФ.

Работа в этом направлении предполагает:

оценку эффективности применения действующих законодательных и иных нормативных правовых актов в информационной сфере и выработку программы их совершенствования;

создание организационно-правовых механизмов обеспечения информационной безопасности;

определение правового статуса всех субъектов отношений в информационной сфере, включая пользователей информационных и телекоммуникационных систем, и установление их ответственности за соблюдение законодательства РФ в данной сфере;

создание системы сбора и анализа данных об источниках угроз информационной безопасности РФ, а также о последствиях их осуществления;

разработку нормативных правовых актов, определяющих организацию следствия и процедуру судебного разбирательства по фактам противоправных действий в информационной сфере, а также порядок ликвидации последствий этих противоправных действий;

разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности и включение соответствующих правовых норм в уголовный, гражданский, административный и трудовой кодексы, в законодательство РФ о государственной службе;

совершенствование системы подготовки кадров, используемых в области обеспечения информационной безопасности РФ.

Государственная политика в деле обеспечения информационной безопасности РФ, согласно Доктрине, основывается на следующих ***основных принципах***:

соблюдение Конституции РФ, законодательства РФ, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности *(принцип законности);*

обеспечение правового равенства всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса, основывающееся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом *(принцип баланса интересов граждан, общества и государства).*

Принцип законности требует от федеральных органов государственной власти и органов государственной власти субъектов РФ при решении возникающих в информационной сфере конфликтов неукоснительно руководствоваться законодательными и иными нормативными правовыми актами, регулирующими отношения в этой сфере.

Принцип баланса интересов граждан, общества и государства в информационной сфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование форм общественного контроля за деятельностью федеральных органов государственной власти и органов государственной власти субъектов РФ. Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности.

К ***правовым методам*** обеспечения информационной безопасности Доктриной относится разработка и неуклонная реализация требований нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности РФ.

Наиболее важными ***направлениями деятельности*** по совершенствованию системы правового обеспечения информационной безопасности в Доктрине названы:

внесение изменений и дополнений в законодательство РФ, регулирующее отношения в области обеспечения информационной безопасности, конкретизация правовых норм, устанавливающих ответственность за правонарушения в области информационной безопасности РФ;

законодательное разграничение полномочий в области обеспечения информационной безопасности, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;

совершенствование правовых актов, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну;

уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России;

Рис. 4.1. Правовое обеспечение информационной безопасности

законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи;

определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории РФ, и правовое регулирование деятельности этих организаций;

создание правовой базы для формирования в РФ региональных структур обеспечения информационной безопасности;

разработка ***механизмов правового обеспечения*** информационной безопасности России.

4.2. Федеральное законодательство в сфере информационной безопасности

Последовательное развитие законодательства в сфере информационной безопасности определяется необходимостью комплексного подхода к формированию и разработке единой концепции ее правового обеспечения, соотносимой со всей системой законодательства РФ. По мнению специалистов, при создании правовой основы информационной безопасности необходимо учитывать:

состояние и состав международных норм в области информатизации;

состояние отечественного законодательства в указанной и смежных областях;

формирование системы законодательства с охватом всех ее уровней, обеспечением преемственности и совместимости норм в законах разного уровня – конституционных, общих, специальных;

последовательный выход на развитие ведомственных и местных нормативных актов с опорой на законодательную основу;

создание механизмов, обеспечивающих организацию, применение, действенность законодательной базы в сфере информационной безопасности.

Общая ***структура правовой базы*** должна затрагивать все уровни законодательства РФ:

конституционное законодательство;

основные общие законы;

законы по организации государственной системы управления;

специальные законы.

Кроме федерального законодательства вопросы информатизации и информационной безопасности должны быть учтены в законодательстве всех субъектов РФ.

Важное место в правовом обеспечении информационной безопасности должны занимать ***подзаконные нормативные акты*** (см. п.4.3).

Завершить эту иерархическую систему законодательства должно правоохранительное законодательство, включающее нормы ответственности за правонарушения при работе с информацией (рис. 4.1).

Основные законы в сфере информационной безопасности

Базовыми актами информационного законодательства Российской Федерации являются Законы «Об информации, информационных технологиях и о защите информации», «О безопасности», «О средствах массовой информации». В них законодательно закрепляется право граждан, организаций и государства на информацию, устанавливаются их основные права и обязанности, правовой режим обработки и использования информации, порядок обеспечения информационной безопасности и гарантии реализации прав и ответственности субъектов информационных отношений.

Федеральный закон ***«Об информации, информационных технологиях и о защите информации»*** принят 27 июля 2006 г. Основная цель закона состоит в совершенствовании правовой основы отношений в области формирования и использования информационных ресурсов, в области информатизации с учетом возрастающей роли информации в обновлении производственного, научного, организационного и управленческого потенциалов страны, в решении вопроса о включении России в мировое сообщество. Сфера действия Закона охватывает отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий, обеспечении защиты информации (ст. 1).

Согласно закону «Об информации, информационных технологиях и о защите информации» (ст. 3), правовое регулирование отношений в данной сфере основывается на следующих принципах:

свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

установление ограничений доступа к информации только федеральными законами;

открытость информации о деятельности государственных органов и органов местного самоуправления;

равноправие языков народов Российской Федерации при создании информационных систем;

достоверность информации и своевременность ее предоставления;

неприкасаемость частной жизни;

недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими.

Законом «Об информации, информационных технологиях и о защите информации» (ст. 5) вся информация в зависимости от порядка ее предоставления и распространения подразделяется на следующие группы:

информация, свободно распространяемая;

информация, предоставляемая по соглашению лиц, участвующих в соответствующих отношениях;

информация, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

информация, распространение которой в Российской Федерации ограничивается или запрещается.

Согласно Закону, обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование (ст. 6). Обладатель информации обязан соблюдать права и законные интересы иных лиц, принимать меры по защите информации, ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Закон определяет порядок государственного регулирования в сфере применения информационных технологий (ст. 12), использования информационно-телекоммуникационных сетей (ст. 15) и защиты информации (ст.16), а также ответственность за правонарушения в сфере информации, информационных технологий и защиты информации (ст. 17).

Со дня вступления в силу данного Федерального закона признаны утратившими силу Федеральный закон от 20 февраля 1995 г. «Об информации, информатизации и защите информации» и ряд других законодательных актов (ст. 18).

Закон РФ «*О безопасности*» принят 5 марта 1992 г. (с изменениями от 25 декабря 1992 г.). Закон является базовым в области

защиты жизненно важных интересов государства. Он юридически закрепляет понятия информационной безопасности, ее объектов и субъектов, определяет систему безопасности и ее функции.

В ст. 13 Закона «О безопасности» указывается, что *Совет безопасности РФ*, являющийся *конституционным органом*, осуществляющим подготовку решений Президента РФ в соответствующей области, осуществляет свою деятельность в сфере государственной, экономической, общественной, оборонной, информационной, экологической и иных видов безопасности. В Законе имеется положение о том, что в функции Совета, в частности, входит рассмотрение вопросов информационной безопасности, обеспечения стабильности и правопорядка. Таким образом, Совет безопасности является ответственным за состояние защищенности жизненно важных интересов личности, общества и государства от внешних и внутренних угроз.

Национальное законодательство, призванное регулировать отношения в сфере информатизации и обеспечения информационной безопасности, включает в себя ряд других действующих законодательных актов. Перечислим и кратко охарактеризуем наиболее важные из них.

Закон РФ «*О средствах массовой информации*» принят 27 декабря 1991 г. (в редакции от 2 марта 1998 г.). В ст. 1 закона записано, что свобода массовой информации в РФ не подлежит ограничениям, за исключением случаев, предусмотренных законодательством о средствах массовой информации. Не подлежат также ограничениям поиск, получение, производство и распространение массовой информации, учреждение средств массовой информации, владение, пользование и распоряжение ими, изготовление, приобретение, хранение и эксплуатация технических устройств и оборудования, сырья и материалов, предназначенных для производства и распространения продукции средств массовой информации.

В законе прямо указывается, что цензура массовой информации, а также создание и финансирование организаций, учреждений, органов или должностей, в задачи или функции которых входит осуществление цензуры массовой информации, не допускается. В ст. 4 Закона говорится о недопустимости злоупотребления средствами массовой информации в целях совершения *уголовно наказуемых деяний*:

разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну;

призыва к захвату власти, насильственному изменению конституционного строя и целостности государства;

разжигания национальной, классовой, социальной, религиозной нетерпимости или розни, пропаганды войны;

распространения передач, пропагандирующих порнографию, культ насилия и жестокости.

В этой же статье *запрещается использование* в теле-, видео- и кинопрограммах, документальных и художественных фильмах, а также в информационных компьютерных файлах и программах обработки информационных текстов, относящихся к специальным средствам массовой информации, скрытых вставок, *воздействующих на подсознание людей* и (или) оказывающих вредное влияние на их здоровье.

Определенное отношение к сфере информационной безопасности имеет Федеральный закон ***«О государственной поддержке средств массовой информации и книгоиздания в РФ»***, принятый 1 декабря 1995 г. Этот закон регулирует порядок государственной поддержки средств массовой информации и книгоиздания, приватизации предприятий, обеспечивающих их функционирование, и направлен на обеспечение конституционного права граждан на получение полной и объективной информации.

Закон РФ ***«О государственной тайне»***, принятый 21 июля 1993 г., регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их рассекречиванием и защитой в интересах обеспечения безопасности России. Положения закона отражают практическую деятельность по защите сведений, составляющих государственную тайну. Законом сохранена преемственность по вопросам защиты большинства сведений нормативного характера, позволяющая в определенной степени сохранить существующие подходы к защите информации на всех стадиях ее существования. В основу концепции Закона «О государственной тайне» положена идея переориентации существующей системы защиты информации на достижение баланса интересов человека, общества и государства, ее адаптации к происходящим изменениям в системе управления в экономической, политической, военной и других сферах жизни общества, создания механизмов реализации правоотношений, способных развиваться в новых условиях.

Закон РФ «*О связи*» принят 20 января 1995 г. Сфера действия этого закона распространяется на отношения, связанные с деятельностью по предоставлению услуг и выполнению работ в области связи, в осуществлении которых участвуют органы государственной власти, операторы связи, отдельные должностные лица, а также пользователи связи. Закон устанавливает правовую основу деятельности в области связи, осуществляемой под юрисдикцией РФ (федеральная связь), определяет полномочия органов государственной власти по регулированию указанной деятельности, а также права и обязанности физических и юридических лиц, участвующих в указанной деятельности или пользующихся услугами связи. Отдельная глава Закона посвящена регулированию отношений в области управления связью, регулированию использования радиочастотного спектра и орбитальных позиций спутников связи, управлению сетями связи при чрезвычайных ситуациях и в условиях чрезвычайного положения. Законом определено, что к федеральной связи относятся все сети и сооружения электрической и почтовой связи на территории РФ (за исключением внутрипроизводственных и технологических сетей связи).

Закон «*О федеральных органах правительственной связи и информации*» принят 19 февраля 1993 г. Законом, в частности, определяются обязанности государства в сфере формирования информационных ресурсов, их использования и защиты. В ст. 3 Закона указывается, что государственная политика в этой сфере направлена на создание условий для эффективного и качественного информационного обеспечения стратегических и оперативных задач развития России.

В Законе сформулированы основные *направления государственной политики* в сфере информатизации и информационной безопасности, к которым относятся:

обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы;

формирование и защита государственных информационных ресурсов;

создание и развитие федеральных и региональных информационных систем и сетей, обеспечение их совместимости и взаимодействия в едином информационном пространстве России;

создание условий для качественного и эффективного информационного обеспечения граждан, органов государственной власти, орга-

нов местного самоуправления, организаций и общественных объединений на основе государственных информационных ресурсов;

обеспечение национальной безопасности в сфере информатизации, а также обеспечение реализации прав граждан, организаций в условиях информатизации;

создание и совершенствование системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов информатизации;

развитие законодательства в сфере информационных процессов, информатизации и защиты информации.

Закон ***«Об органах федеральной службы безопасности РФ»***, принятый 10 апреля 1995 г., и Закон ***«О внешней разведке»*** от 10 января 1996 г. в части, касающейся добывания, обработки разведывательной информации и защиты государственной тайны, имеют много общего.

Для достижения целей разведывательной деятельности и получения специальной информации органы Федеральной службы безопасности (ФСБ) и органы внешней разведки используют методы и средства в соответствии с федеральными законами. В ст. 20 Закона «Об органах федеральной службы безопасности Российской Федерации» указано, что хранение в информационных системах ***сведений о физических и юридических лицах*** не является основанием для принятия мер, ограничивающих права названных лиц. Законом «О внешней разведке» регламентируется деятельность подразделений и частей радиоразведки Федерального агентства правительственной связи и информации (ФАПСИ), которые обеспечивают и ведут разведывательную деятельность в сфере шифрованной, засекреченной и иных видов специальной связи.

В федеральных законах ***«О государственной охране»*** и ***«О Федеральной фельдъегерской связи»*** определены права и обязанности соответствующих служб в сфере сбора, получения, охраны, защиты и доставки информации.

Юридическое закрепление информационных отношений, возникающих в сфере деятельности органов внутренних дел, регулируются Законом «О милиции» и Федеральным законом «Об оперативно-разыскной деятельности».

Российской милиции в соответствии с Законом РСФСР ***«О милиции»***, принятым 18 апреля 1991 г., предоставлен широкий спектр полномочий в информационной сфере. Так, она обязана «принимать

регистрировать заявления, сообщения и иную поступающую информацию о преступлениях, административных правонарушениях и событиях, угрожающих личной или общественной безопасности» (ст. 10, п. 3).

В соответствии со ст. 11 Закона о милиции предоставлено право «получать от граждан и должностных лиц необходимые объяснения, сведения, справки, документы и копии к ним» (п. 4), а также «производить регистрацию, фотографирование, звукозапись, кино- и видеосъемку, дактилоскопирование лиц, заключенных под стражу, задержанных по подозрению в совершении преступлений или занятии бродяжничеством, обвиняемых в совершении умышленных преступлений, подвергнутых административному аресту, а также лиц, подозреваемых в совершении административного правонарушения при невозможности установления их личности...» (п. 15).

Органы внутренних дел России выполняют функции формирования и ведения общегосударственных справочно-информационных фондов (разд. 1.1). Эти функции возложены на информационные центры и экспертно-криминалистические подразделения во взаимодействии с другими подразделениями органов внутренних дел, а также с организациями и службами других правоохранительных органов, в том числе зарубежных.

Федеральный закон ***«Об оперативно-разыскной деятельности»*** принят 12 августа 1995 г. В соответствии с Законом оперативные подразделения органов внутренних дел получили широкие возможности по сбору информации «о событиях или действиях, создающих угрозу государственной, военной, экономической или экологической безопасности РФ» (ст. 2). В ст. 6 Закона приведен перечень оперативно-разыскных мероприятий, в ходе проведения которых для получения необходимых сведений «используются информационные системы, видео- и аудиозаписи, кино- и фотосъемки, а также другие технические и иные средства, не наносящие ущерб жизни и здоровью людей и не причиняющие вред окружающей среде».

Федеральный закон «Об оперативно-разыскной деятельности» допускает ограничения конституционных прав граждан при проведении оперативно-разыскных мероприятий только с разрешения суда на основании мотивированного постановления одного из руководителей органа — субъекта оперативно-разыскной деятельности.

Закон РФ ***«Об авторском праве и смежных правах»*** вступил в силу 3 августа 1993 г. (в настоящее время Закон действует в редакции

2004 г.). Предметом регулирования Закона, в частности, являются отношения, возникающие в связи с созданием и использованием произведений науки, литературы (включая программы для ЭВМ), которые являются результатом творческой деятельности, независимо от назначения и достоинства произведения, а также способа его выражения. Источниками регулирования являются не только законы РФ и принимаемые на их основе законодательные акты субъектов РФ, но и международные договоры, в которых участвует Россия. Если международным договором, в котором участвует РФ, установлены иные правила, чем те, которые содержатся в Законе, то применяются правила международного договора. К основным понятиям Закона относятся, в числе прочих, понятия программы для ЭВМ и базы данных, записи программы в память ЭВМ, а также понятие контрафактных экземпляров произведений. Законом определено, что программы для ЭВМ являются объектами авторского права, нарушение которого влечет гражданскую, уголовную и административную ответственность в соответствии с законодательством РФ.

Федеральный закон ***«Об основах государственной службы»*** принят 31 июля 1995 г. В Законе определены права, обязанности и ограничения, накладываемые на государственных служащих, в том числе и в области информационного обмена. Так, ст. 11 Закона запрещает государственным служащим использовать в неслужебных целях средства информационного обеспечения и служебную информацию.

В ***Гражданском кодексе РФ*** (ч. 1 и ч. 2) информация рассматривается как объект гражданского права наряду с интеллектуальной собственностью и имуществом (ст. 128). В Кодексе также определяется информация, составляющая служебную и коммерческую тайну. В ст. 139 определен состав особых формальностей, которые позволяют применять какие-либо санкции в случае нарушения конфиденциальности информации.

Конституция РФ и Гражданский кодекс РФ прямо или косвенно касаются таких важных тем информатизации, как право на информацию, гарантии, ограничения и создание условий для информационной безопасности, разграничение сфер ведения на важнейшие составные элементы информатизации: информацию и связь.

Уголовный кодекс РФ принят 24 мая 1996 г. и введен в действие 1 января 1997 г. Новый Уголовный кодекс (с последующими изме-

нениями и дополнениями) закрепляет принципиально новые
отечественного законодательства подходы к некоторым
мам уголовного права. Отдельные нормы в российской
мительной практике используются впервые. В частности, гл.
«Преступления в сфере компьютерной информации» определяет
щественно опасные и преступные деяния в сфере компьютерной
информации.

К разряду преступлений против конституционных прав и свобод человека и гражданина, носящих информационный характер, в Уголовном кодексе отнесены следующие преступления:

нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан (ст. 138, ч. 1);

незаконное производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации (с. 138, ч. 3);

предоставление гражданину должностным лицом неполной или заведомо ложной информации, если этим причинен вред правам и законным интересам граждан (ст. 140, ч. 3);

незаконное использование объектов авторского права и смежных прав, присвоение авторства (ст. 146, ч. 1);

нарушение авторских прав группой лиц (ст. 146, ч. 2);

незаконное использование изобретения, полезной модели, промышленного образца, разглашение их сущности без согласия автора или заявителя до официальной публикации сведений о них, присвоение авторства или принуждение к соавторству (ст. 147, ч. 2);

использование в рекламе заведомо ложной информации относительно товаров, работ или услуг, а также их изготовителей, исполнителей, продавцов (ст. 182, ч. 1);

собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа или угроз а также иным незаконным способом (ст. 183, ч. 1);

незаконное разглашение или использование сведений, составляющих коммерческую или банковскую тайну, без согласия их владельца (ст. 183, ч. 2);

незаконный экспорт технологий, научно-технической информации и услуг в сфере вооружения и военной техники (ст. 189, ч. 2).

Законодательное регулирование прав граждан на благоприятную окружающую среду и достоверную информацию о ее состоянии нашло отражение в Федеральном законе *«О радиационной*

опасности населения», принятом 9 января 1996 г. В соответствии со ст. 23 Закона граждане и общественные организации получили право на объективную информацию о радиационной обстановке и принимаемых мерах безопасности от тех организаций, которые осуществляют деятельность с применением источников ионизирующего излучения. Кроме того, согласно ст. 6 Закона, субъекты РФ уполномочены информировать граждан о радиационной обстановке на соответствующей территории.

4.3. Указы Президента РФ и иные нормативно-правовые акты по вопросам информационной безопасности

Подзаконные нормативно-правовые акты *– это правотворческие акты компетентных органов, которые основаны на законе и не противоречат ему.* Подзаконные акты обладают меньшей юридической силой, чем законы, они базируются на юридической силе законов и не могут противостоять им. Эффективное регулирование общественных отношений имеет место тогда, когда общие интересы согласуются с частными. Подзаконные акты как раз и призваны конкретизировать основные, принципиальные положения законов применительно к своеобразию конкретных ситуаций.

По своему содержанию подзаконные акты, как правило, являются актами различных органов исполнительной власти. По субъектам издания и сфере распространения они подразделяются *на общие, местные, ведомственные и внутриорганизационные акты.* В системе подзаконных актов высшей юридической силой обладают нормативные ***указы Президента РФ***, издаваемые на основе и в развитие федеральных законов. ***Постановления Правительства РФ*** – это нормативные акты, принимаемые в контексте с указами Президента РФ и призванные, при необходимости, регулировать более мелкие вопросы, в данном случае связанные с обеспечением информационной безопасности. ***Местные подзаконные акты*** издаются органами представительной власти на местах и органами местного самоуправления. Действие этих актов ограничено подвластной им территорией. ***Ведомственные и внутриорганизационные нормативные акты*** – приказы, инструкции и т. п. – издаются структурными подразделениями правительственных органов и, соответственно, различными органи-

ствами для регламентации своих внутренних вопросов, в частности, по обеспечению информационной безопасности. Их действие обязательно для членов этих организаций.

Указы Президента РФ по вопросам информатизации и обеспечения информационной безопасности

Указ Президента РФ от 17 декабря 1997 г. № 1300 «*Об утверждении Концепции национальной безопасности Российской Федерации*». Концепция представляет собой политический документ, отражающий совокупность официально принятых взглядов на цели и государственную стратегию в области обеспечения безопасности личности, общества и государства от внешних и внутренних угроз политического, экономического, военного, информационного и иного характера с учетом имеющихся ресурсов и возможностей.

В Концепции указывается, что национальные интересы России в ***информационной сфере*** обуславливают необходимость сосредоточения усилий общества и государства на решении задач соблюдения конституционных прав и свобод граждан в области получения информации и обмена ею, защиты национальных духовных ценностей, пропаганды национального культурного наследия, обеспечения права граждан на получение достоверной информации.

Концепцией определены ***важнейшие задачи*** по обеспечению национальной безопасности ***в информационной сфере***. К ним относятся:

установление необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения;

совершенствование информационной структуры, ускорение развития новых информационных технологий и их широкое распространение, унификация средств поиска, сбора, хранения, обработки и анализа информации с учетом вхождения России в глобальную информационную инфраструктуру;

разработка и координация соответствующей нормативной правовой базы при участии всех органов, решающих задачи обеспечения информационной безопасности;

развитие отечественной индустрии телекоммуникационных и информационных средств;

защита государственного информационного ресурса.

Указ Президента РФ от 20 января 1994 г. № 170 ***«Об основах государственной политики в сфере информатизации»*** (с изменениями и дополнениями от 9 июля 1997 г.). Указом установлено, что основными направлениями государственной политики в сфере информатизации являются:

создание и развитие федеральных и региональных систем и сетей информатизации с обеспечением их совместимости и взаимодействия в едином информационном пространстве России;

формирование и защита информационных ресурсов государства как национального достояния;

обеспечение интересов национальной безопасности в сфере информатизации;

обеспечение единства государственных стандартов в сфере информатизации, их соответствие международным рекомендациям и требованиям;

формирование и осуществление единой государственной научно-технической и промышленной политики в сфере информатизации, отвечающей современному мировому уровню;

поддержка проектов информатизации, обеспечивающих развитие информационных сетей и систем;

создание и совершенствование системы привлечения иностранных инвестиций и механизма стимулирования негосударственных структур в разработке и реализации проектов информатизации.

Указом закрепляется понятие ***«единое информационное пространство России»***.

В соответствии с Указом, на базе ликвидированного Комитета РФ по информатизации образован Комитет при Президенте РФ по политике информатизации, основными задачами которого, в частности, являются участие в разработке и проведении государственной политики в сфере информатизации, а также разработка проектов законодательных и иных нормативных актов по указанным вопросам.

Указ Президента РФ от 28 июня 1993 г. № 966 ***«О Концепции правовой информатизации России»***. В основных положениях Концепции зафиксировано, что под правовой информатизацией России понимается «процесс создания оптимальных условий максимально полного удовлетворения информационно-правовых потребностей государственных и общественных структур, предприятий, организаций, учреждений и граждан на основе эффективной организации и использования информационных ресурсов с применением прогрессивных технологий».

В соответствии с Концепцией, правовая информатизация должна осуществляться по следующим направлениям:

информатизация правотворческой деятельности;

информатизация правореализационной деятельности;

правовое обеспечение процессов информатизации.

В Концепции определены *главные цели правовой информатизации*:

информационно-правовое обеспечение внутренней деятельности органов государства;

информационно-правовое обеспечение внешних по отношению к государственным органам субъектов, в том числе юридических лиц;

сохранение и структурирование информационного правового поля.

Указ Президента РФ от 31 декабря 1993 г. № 2334 ***«О дополнительных гарантиях прав граждан на информацию»*** (с изменениями и дополнениями от 17 января 1997 г.). В Указе декларируется, что право на информацию является одним из фундаментальных прав человека. Деятельность государственных органов, организаций и предприятий, общественных объединений, должностных лиц осуществляется на *принципах информационной открытости*, что выражается:

в доступности для граждан информации, представляющей общественный интерес или затрагивающей личные интересы граждан;

в систематическом информировании граждан о предполагаемых или принятых решениях;

в осуществлении гражданами контроля над деятельностью государственных органов, организаций и предприятий, общественных объединений, должностных лиц и принимаемыми ими решениями, связанными с соблюдением, охраной и защитой прав и законных интересов граждан;

в создании условий для обеспечения граждан России зарубежными информационными продуктами и оказания им информационных услуг, имеющих зарубежное происхождение.

В 1993 г. введены в действие ***«Основы законодательства РФ об Архивном фонде РФ и архивах»***. В развитие этого документа были подписаны Указ Президента РФ от 17 марта 1994 г. № 552 ***«Об утверждении Положения об Архивном фонде РФ и Положения о Государственной архивной службе России»***, а также Указ Президента РФ от 25 марта 1994 г. № 151-рп ***«Об Архиве Президента РФ»***. В Указе Президента РФ № 151-рп определено, что Архив является

специализированным подразделением Администрации Президента, в котором осуществляется постоянное хранение и использование документов, образовавшихся в результате деятельности Президента и структурных подразделений его Администрации.

Указ Президента РФ от 4 августа 1995 г. № 808 ***«О президентских программах по правовой информатизации»***. Этим указом утвержден Президентская программа «Правовая информатизация органов государственной власти РФ». Программой предусматриваются разработка и реализация проектов и мероприятий по следующим направлениям:

правовая информатизация правотворческой деятельности органов государственной власти РФ;

правовое обеспечение процессов правовой информатизации;

создание единого информационно-правового пространства органов государственной власти РФ;

формирование государственной политики правовой информатизации.

Примером ***правовых актов местных органов власти*** может служить постановление Правительства Москвы от 22 августа 2000 г. № 654 ***«Об утверждении Концепции безопасности Москвы»*** (с изменениями от 2 декабря 2003 г.), рассмотренная выше, в гл. 3, Концепция рассматривает основные угрозы безопасности Москвы, в том числе ***угрозы психологического характера,*** а также основные направления обеспечения безопасности и организацию системы обеспечения безопасности города.

В целом анализ отечественной нормативно-правовой базы, направленной на регулирование отношений в сфере обеспечения информационной безопасности, позволяет сделать вывод о том, что она все еще находится ***в процессе становления***. В настоящее время ряд нормативных актов по вопросам обеспечения информационной безопасности проходит стадию разработки или утверждения.

4.4. Организационное обеспечение информационной безопасности

Согласно Доктрине, ***основными функциями системы организационного обеспечения*** информационной безопасности являются:

разработка нормативной правовой базы в области обеспечения информационной безопасности РФ;

создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;

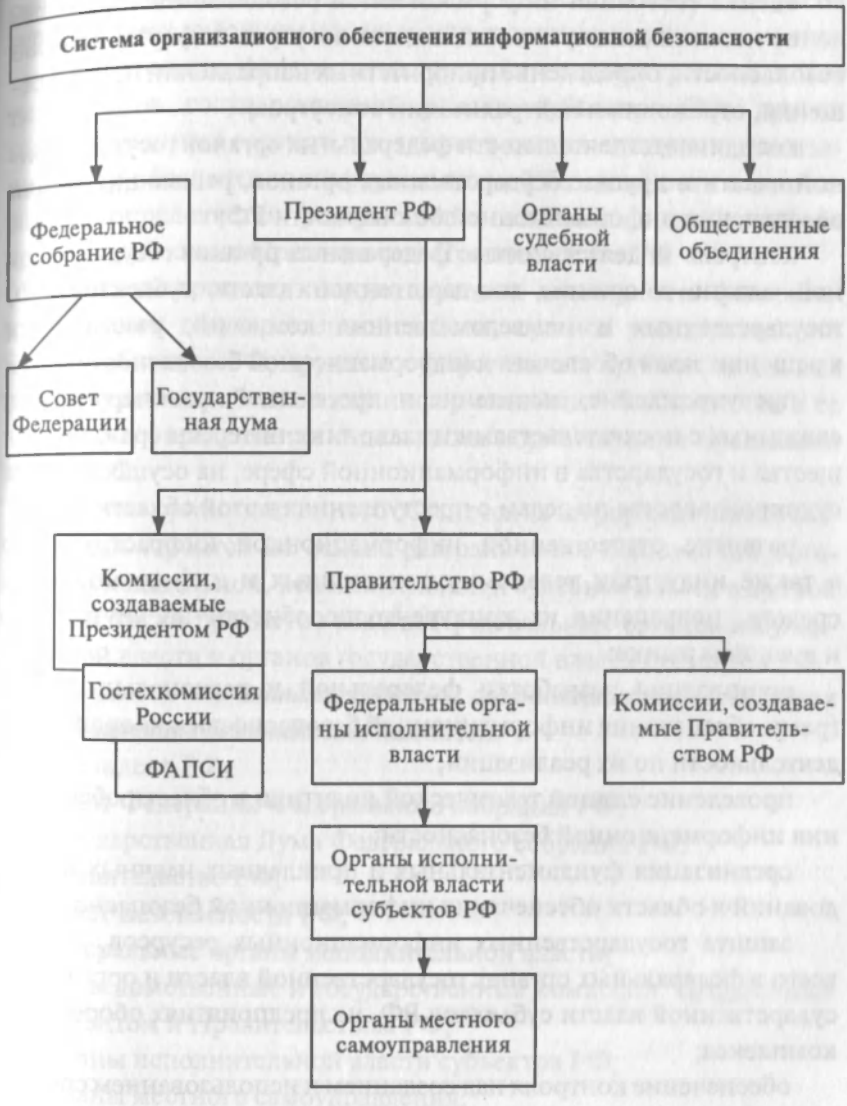

Рис. 4.2. **Система организационного обеспечения информационной безопасности**

определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;

оценка состояния информационной безопасности РФ, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;

координация деятельности федеральных органов государственной власти и других государственных органов, решающих задачи обеспечения информационной безопасности РФ;

контроль за деятельностью федеральных органов государственной власти и органов государственной власти субъектов РФ, государственных и межведомственных комиссий, участвующих в решении задач обеспечения информационной безопасности;

предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере, на осуществление судопроизводства по делам о преступлениях в этой области;

развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств, повышение их конкурентоспособности на внутреннем и внешнем рынке;

организация разработки федеральной и региональных программ обеспечения информационной безопасности и координация деятельности по их реализации;

проведение единой технической политики в области обеспечения информационной безопасности;

организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности;

защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти и органах государственной власти субъектов РФ, на предприятиях оборонного комплекса;

обеспечение контроля над созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации;

совершенствование и развитие единой системы подготовки кадров, используемых в области информационной безопасности;

осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов РФ в соответствующих международных организациях.

Компетенция федеральных органов государственной власти, органов государственной власти субъектов РФ, других государственных органов, входящих в состав системы организационного обеспечения информационной безопасности и ее подсистем, определяется федеральными законами, нормативными правовыми актами Президента и Правительства РФ.

Функции органов, координирующих деятельность федеральных органов государственной власти, органов государственной власти субъектов РФ, других государственных органов, входящих в состав системы обеспечения информационной безопасности и ее подсистем, определяются отдельными нормативными правовыми актами РФ.

Система организационного обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере, а также предметов ведения федеральных органов государственной власти и органов государственной власти субъектов РФ.

Основными элементами системы организационного обеспечения информационной безопасности являются:

Президент РФ;

Совет Федерации Федерального собрания РФ;

Государственная Дума Федерального собрания РФ;

Правительство РФ;

Совет Безопасности РФ;

федеральные органы исполнительной власти;

межведомственные и государственные комиссии, создаваемые Президентом и Правительством РФ;

органы исполнительной власти субъектов РФ;

органы местного самоуправления;

органы судебной власти;

общественные объединения;

граждане, принимающие в соответствии с законодательством РФ участие в решении задач обеспечения информационной безопасности (рис. 4.2).

Президент РФ:

руководит в пределах своих конституционных полномочий Советом Безопасности РФ, другими органами и силами по обеспечению информационной безопасности РФ;

санкционирует действия по обеспечению информационной безопасности РФ;

в соответствии с законодательством РФ формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению информационной безопасности РФ;

определяет в своих ежегодных посланиях Федеральному собранию приоритетные направления государственной политики в области обеспечения информационной безопасности РФ, а также меры по реализации Доктрины информационной безопасности РФ.

Палаты Федерального собрания РФ на основе Конституции РФ по представлению Президента и Правительства РФ формируют законодательную базу в области обеспечения информационной безопасности России.

Правительство РФ в пределах своих полномочий и с учетом сформулированных в ежегодных посланиях Президента Федеральному собранию РФ приоритетных направлений в области обеспечения информационной безопасности:

координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов РФ;

предусматривает при формировании в установленном порядке проектов федерального бюджета на соответствующие годы выделение средств, необходимых для реализации федеральных программ в этой области.

Совет Безопасности РФ:

проводит работу по выявлению и оценке угроз информационной безопасности РФ;

оперативно подготавливает проекты решений Президента РФ по предотвращению таких угроз;

разрабатывает предложения в области обеспечения информационной безопасности, а также предложения по уточнению

отдельных положений Доктрины информационной безопасности РФ;

координирует деятельность органов и сил по обеспечению информационной безопасности РФ;

контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов РФ решений Президента РФ в этой области.

Федеральные органы исполнительной власти обеспечивают исполнение законодательства РФ, решений Президента и Правительства РФ в области обеспечения информационной безопасности РФ; в пределах своей компетенции разрабатывают нормативные правовые акты в этой области и представляют их в установленном порядке Президенту РФ и в Правительство РФ.

Межведомственные и государственные комиссии, создаваемые Президентом РФ и Правительством РФ, решают в соответствии с предоставленными им полномочиями задачи обеспечения информационной безопасности.

К числу таких органов относятся Государственная техническая комиссия при Президенте РФ (Гостехкомиссия России) и Федеральное агентство правительственной связи и информации при Президенте РФ (ФАПСИ).

Гостехкомиссия России, созданная Указом Президента РФ от 19 февраля 1999 г. № 212, осуществляет межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственную или служебную тайну. Она организует деятельность государственной системы защиты информации от технических разведок на территории России и от ее утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию в целях ее уничтожения, искажения и блокирования. Гостехкомиссия России проводит единую государственную научно-техническую политику в области защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств.

Гостехкомиссия России осуществляет широкий спектр функций:

утверждает нормативно-методические документы по технической защите информации;

разрабатывает и согласовывает программу стандартизации и проекты государственных стандартов в области технической защиты информации;

проводит работу по прогнозированию развития сил, средств и возможностей технических разведок, по оценке их осведомленности об информации, составляющей государственную тайну;

осуществляет лицензирование деятельности, связанной с оказанием услуг в области технической защиты информации, созданием средств технической защиты информации, а также средств технического контроля эффективности защиты информации;

участвует совместно с ФСБ в проведении на договорной основе специальных экспертиз по допуску предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну;

осуществляет работы по сертификации средств технической защиты информации;

организует проведение радиоконтроля за соблюдением установленного порядка передачи служебных сообщений должностными лицами предприятий, учреждений и организаций, выполняющими работы, связанные со сведениями, составляющими государственную или служебную тайну, и др.

Гостехкомиссия России наделена полномочиями представлять руководству страны предложения по нормативно-правовому регулированию в области технической защиты информации, а также осуществлять контроль за соблюдением федерального законодательства в этой области и требований руководящих и нормативно-методических документов.

Подразделения правительственной связи и информации (бывшее ФАПСИ) в составе ФСБ России обеспечивают специальными видами связи и информации органы государственной власти. Они осуществляют криптографическую и инженерно-техническую безопасность шифрованной связи в РФ. Регламентация этой деятельности осуществляется Законом РФ «О федеральных органах правительственной связи и информации».

Органы исполнительной власти субъектов Российской Федерации взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства РФ, решений Президента и Правительства РФ в области обеспечения информа-

ционной безопасности, а также по вопросам реализации федеральных программ в этой области;

совместно с органами местного самоуправления осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения информационной безопасности;

вносят в федеральные органы исполнительной власти предложения по совершенствованию системы обеспечения информационной безопасности РФ.

Органы местного самоуправления обеспечивают соблюдение законодательства РФ в области обеспечения информационной безопасности.

Органы судебной власти осуществляют правосудие по делам о преступлениях, связанных с посягательствами на законные интересы личности, общества и государства в информационной сфере, и обеспечивают судебную защиту граждан и общественных объединений, чьи права были нарушены в связи с деятельностью по обеспечению информационной безопасности РФ.

В состав системы обеспечения информационной безопасности РФ могут входить и другие подсистемы, ориентированные на решение различных задач в данной сфере.

4.5. Международное сотрудничество России в области обеспечения информационной безопасности

Международное сотрудничество РФ в области обеспечения информационной безопасности – неотъемлемая составляющая политического, военного, экономического, культурного и других видов взаимодействия стран, входящих в мировое сообщество. Такое сотрудничество должно способствовать повышению информационной безопасности всех членов мирового сообщества, включая Россию.

Особенностью международного сотрудничества РФ в области обеспечения информационной безопасности является то, что оно осуществляется в условиях:

обострения международной конкуренции за обладание информационными ресурсами, за доминирование на рынках сбыта, в условиях продолжения попыток создания структуры меж-

дународных отношений, основанной на односторонних решениях ключевых проблем мировой политики;

противодействия укреплению роли России как одного из влиятельных центров формирующегося многополярного мира;

усиления технологического отрыва ведущих держав мира и наращивания их возможностей для создания «информационного оружия».

Все это может привести к новому этапу развертывания гонки вооружений в информационной сфере, нарастанию угрозы агентурного и оперативно-технического проникновения в Россию иностранных разведок, в том числе с использованием глобальной информационной инфраструктуры.

Основными направлениями международного сотрудничества РФ в области обеспечения информационной безопасности являются:

запрещение разработки, распространения и применения «информационного оружия»;

обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;

координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;

предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также с торговлей людьми.

Для осуществления международного сотрудничества по указанным основным направлениям необходимо обеспечить активное участие России во всех международных организациях, осуществляющих деятельность в области информационной безопасности, в том числе в сфере стандартизации и сертификации средств информатизации и защиты информации.

В соответствии с международными договоренностями России ***основными правовыми источниками*** в сфере информационных от-

ношений и защиты объектов и субъектов информационных технологий являются:

Всеобщая декларация прав человека, утвержденная и провозглашенная Генеральной Ассамблеей ООН (1948 г.);

Европейская конвенция о защите прав человека и основных свобод (1950 г.);

Международный пакт о гражданских и политических правах (1976 г.);

Европейская конвенция от 28 января 1981 г. об охране личности в отношении автоматизированной обработки персональных данных;

директивы Европейского парламента и Совета Европейского союза 95.46.ЕС и 97.66.ЕС, касающиеся обработки персональных данных, другие международные договоры, заключенные Российской Федерацией.

Российская Федерация, являясь членом ***Европейского совета***, участвует в международных конвенциях в области информатизации общества. В частности, Россия и Европейский союз имеют специальную статью в Соглашении о партнерстве и сотрудничестве по соблюдению требований *в области интеллектуальной собственности*. В 1973 г. СССР (правопреемник – РФ) присоединился к Всемирной конвенции об авторском праве (Женева, 1953 г., с изменениями 1971 г.). В 1990 году СССР был принят в члены Международной организации уголовной полиции – Интерпол. Впоследствии РФ стала правопреемником в этой организации, осуществляющей, в том числе, борьбу с международными компьютерными преступлениями.

Государственной Думой РФ 5 июня 1996 г. принят Федеральный закон «***Об участии в международном информационном обмене***». Этот Закон устанавливает (во взаимодействии с другими федеральными законами и нормативно-правовыми актами) порядок международного обмена как конфиденциальной, так и массовой информацией (но не затрагивает отношений, регулируемых Законом «Об авторском праве и смежных правах»).

Целью данного Закона является создание условий для эффективного участия России в международном информационном обмене в рамках единого мирового информационного пространства, обеспечение защиты интересов РФ, субъектов и муниципальных обра-

зований, а также интересов, прав и свобод физических и юридических лиц при международном информационном обмене.

В Законе указываются *объекты* международного информационного обмена:

документированная информация;

информационные ресурсы;

информационные услуги;

средства международного информационного обмена.

Законом сформулированы *обязанности* органов государственной власти РФ и власти субъектов РФ разного уровня. В частности, они должны:

создавать условия для обеспечения, своевременного и достаточного пополнения государственных информационных ресурсов РФ иностранными информационными продуктами и услугами;

содействовать внедрению современных информационных технологий для участия в международном информационном обмене;

обеспечивать защиту государственных информационных ресурсов и соблюдение правового режима информации;

стимулировать расширение взаимовыгодного международного информационного обмена документированной информацией;

создавать условия для защиты от некачественной и недостоверной иностранной информации, недобросовестной конкуренции со стороны физических и юридических лиц иностранных государств в информационной сфере;

способствовать развитию товарных отношений при международном информационном обмене.

В ст. 8 Закона введены *ограничения* на перемещение из РФ документальной информации, отнесенной к государственной тайне, или иной конфиденциальной информации, общероссийскому национальному достоянию, архивному фонду, иным категориям документированной информации, вывоз которой может быть ограничен законодательством РФ.

При осуществлении международного сотрудничества РФ в области обеспечения информационной безопасности особое внимание уделяется проблемам взаимодействия с государствами — участниками ***Содружества Независимых Государств***.

Непосредственно этому взаимодействию посвящены два указа Президента РФ:

Указ от 19 октября 1993 г. № 1665 «***Об информационно-правовом сотрудничестве РФ с государствами – членами Содружества Независимых Государств***». Указом намечалось подготовить с участием заинтересованных министерств и ведомств проект межгосударственного соглашения по вопросу информационно-правового сотрудничества. Соглашение было подготовлено и принято 21 октября 1994 г.;

Указ от 27 декабря 1993 г. № 2293 «***Вопросы формирования единого информационно-правового пространства Содружества Независимых Государств***». Указом, в частности, закрепляется понятие «единое информационно-правовое пространство СНГ» как элемент категории «единое информационное пространство».

Вопросы для обсуждения

1. Как вы оцениваете значимость для обеспечения информационной безопасности правовых актов разного уровня?
2. В какой мере обеспечивается сегодня баланс интересов человека, общества и государства в информационной сфере?
3. Как вы относитесь к сбору и хранению в информационных системах сведений о физических лицах, в том числе о вас лично?
4. Что необходимо расширить сегодня в сфере информирования населения средствами массовой информации: свободу или систему ограничений?
5. Что преобладает сегодня в международном информационном обмене: открытость или осторожность и недоверие? Что такое принцип «двойных стандартов»?
6. Нуждается ли в улучшении защита от передачи за границу документальной и художественной информации, отнесенной к общероссийскому национальному достоянию?
7. Из каких основных элементов состоит система правового и организационного обеспечения информационной безопасности?

Глава 5

СУЩНОСТЬ И МЕТОДЫ ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ НА ЧЕЛОВЕКА

Лучшие обманы – те, при которых вы как бы предоставляете другому человеку выбор: у ваших жертв возникает иллюзия свободы выбора, а на самом деле они лишь марионетки.

Роберт Грин

5.1. Сущность и современное состояние манипуляции сознанием и поведением людей

Термин ***манипулирование*** происходит от латинского ***manipulare*** и означает в буквальном переводе ***управление***. Первоначально он употреблялся в положительном смысле, означал сложные виды действий, выполняемых руками, – управление рычагами, обращение с предметами, требующими сноровки и мастерства, а затем и как управление людьми, осуществляемое со знанием дела и пользой для него. В социальном контексте это понятие стало употребляться с негативным оттенком. В обыденной речи оно используется для обозначения действий, содержащих скрытый умысел и наносящих ущерб тем, против кого они направлены.

Родственный термин ***манипуляция*** Оксфордский словарь английского языка трактует с некоторым пренебрежительным подтекстом как акт влияния на людей или управления ими с определенной ловкостью, скрытой их обработкой. Считается, что изначально этим понятием обозначались действия фокусников, работающих только руками, без использования сложных приспособлений (фокусник-манипулятор). Своих эффектов фокусник-манипулятор добивается, используя психологические стереотипы зрителей, отвлекая, перемещая и концентрируя их внимание, действуя на воображение, создавая иллюзии восприятия. Искусство этих артистов основано, прежде всего, на знании психологии человека.

В русском языке в социальном (не техническом) контексте смысл терминов *манипулирование и манипуляция* обычно считается аналогичным тому, что мы вкладываем в слова обман, обольщение, одурачивание и т. п.

Определения, предлагаемые разными авторами, в главном имеют несомненное сходство.

«Вид управления, при котором манипулятор относится к другим как к вещам, применяя при этом маску и различные изощренные трюки» (Э. Шостром).

«Вид воздействия, при котором прибегают не к средствам принуждения, а к убеждению, основанному на предумышленном обмане» (Л. Войтасик).

«Отношение к другому как к средству, объекту, орудию» (В. Сагатовский).

«Стремление приспособить сознание людей к интересам господствующей элиты» (Б. Бессонов).

«Управление мышлением и чувствами, исключающее осмысленную жизнь. Полная унификация духа, превращающая человека в управляемый извне объект» (Б. Бессонов).

«Вид психологического воздействия, используемый для достижения одностороннего выигрыша посредством скрытого побуждения другого к совершению определенных действий» (Е. Доценко).

«Господство над духовным состоянием, управление изменением внутреннего мира человека» (Д. Волкогонов).

«Система способов ... духовно-идеологического воздействия с целью подчинения людей определенным ценностям и образу жизни...» (Энциклопедический словарь).

Анализ приведенных определений позволяет выделить ***специфические признаки манипуляции***. Для нее, прежде всего, характерно:

направленное воздействие на психику человека – его мышление, чувства, волю, сознание в целом;

отношение манипулятора к другому человеку (группе людей) как к средству достижения собственных целей;

скрытый характер воздействия (как самого факта воздействия, так и его направленности);

стремление выработать у человека нужные манипулятору потребности, побудить к принятию определенных жизненных ценностей и к определенным практическим действиям;

наличие возможности последующего управления внутренним миром и поведением человека;

воздействие на человека вопреки существующему у него в данный момент желанию.

Манипуляция – это процесс, имеющий определенную временную протяженность и отдельные этапы. *Подготовительный этап* связан с определением цели и объекта манипуляции, изучением психологических особенностей объекта и выбор наиболее действенных для него стимулов и приманок, выстраивание общего сценария (технологии) манипуляции. *Этап практической реализации* предполагает установление контакта с адресатом и применение стимулов (методов, средств, уловок), побуждающих его к нужным действиям. Для определения действий на этом этапе применяется термин «программирование», или ***психологическое программирование*** человека. Оно может быть позитивным, конструктивным и негативным.

Цель ***программирования психики*** – сознательное и планомерное формирование определенных индивидуальных качеств человека, предопределяющих его поведение в тех или иных ситуациях. И в этом смысле оно стоит в одном ряду не только с манипулированием, но и с обучением, воспитанием, социализацией индивида. Его можно рассматривать как составную часть всего процесса формирования личности.

Специфическими признаками программирования, отличающими его от традиционных воспитательных приемов, являются высокий уровень осознанности и целенаправленности воздействия на психику, а также его оснащенность новейшими методами и технологиями.

Осознанное применение искаженной информации, ее препарирование «в интересах дела», а также скрытность воздействия и его обращенность не только к сознанию, но и, главным образом, к бессознательным уровням психики ставят программирование в один ряд с манипуляцией, политическим обманом. Однако манипуляция – более узкий вид воздействия. Она оперирует уже имеющимися у человека потребностями, ценностными ориентировками, привычками и, особенно, его слабостями. Процедура программирования психики здесь не требуется и не входит в процесс управления человеком.

Пример такой манипуляции образно показан И. Крыловым в басне «Ворона и Лисица». Лиса-плутовка использует уже имеющееся у вороны честолюбие и лишь разжигает это чувство с помощью лести: «Голубушка, как хороша! Ну что за шейка, что за глазки! ...Какие перышки! Какой носок!» В ответ на лестные слова вороне надлежит выполнить безобидную просьбу – спеть. Как тут устоять честолюбивой вороне!

Примерно по такому же сценарию происходит манипуляция сознанием в многочисленных случаях на улицах городов, когда мошенник путем обольщения, иногда с добавлением элементов внушения принуждает людей (в основном, женщин и детей) добровольно отдавать деньги, ценности, имеющиеся не только при себе, но и в квартирах. Для достижения целей манипуляции формирования новых личностных качеств у ее объекта здесь не требуется.

Уровни манипуляции. С учетом *масштаба и целей* можно выделить два вида манипулирования человеком: *простое* (тактическое) и *сложное* (стратегическое).

Первое из них носит ситуативный характер и реализуется посредством одной-двух операций в ограниченном временном интервале. Такое воздействие непосредственно направлено на получение конкретного результата.

Сложное манипулирование осуществляется через систему операций, последовательных ходов, объединенных в рамках тщательно разработанной и подчиненной единой цели программы. Оно опирается на глубокое изучение и, как правило, длительную обработку объекта манипуляции различными средствами и методами манипулятивной технологии.

По ***используемым методам*** манипуляция может быть *мягкой* и *жесткой*.

При мягкой обработке в основном применяются методы вербального характера: логические доводы, убеждение, апелляция к опыту других людей, лесть, обман, особым образом спланированная подача информации, специальные игры и беседы, внушение и т. п.

Методы жесткого воздействия обращены к глубинным уровням психики человека, его психофизиологии. В этом случае используются нейролингвистическое программирование (НЛП), дианетические приемы кодирования психики, наркотические средства и химические препараты, энергоинформационные (психотронные) средства, принуждающий тренинг бихевиористского (поведенче-

ского: от англ. *behaviour* – поведение) толка с его требованием действовать только по принципу «стимул–реакция». Значительную часть таких методов принято считать «грязными», то есть выходящими не только за рамки морали, но и закона. Результатом жесткого воздействия может стать так называемое *зомбирование*, ведущее к серьезным нарушениям в эмоционально-волевой сфере человека, его мышлении, способности к самоконтролю.

По итогам анализа манипуляцию можно определить как *процесс воздействия на психику с использованием различных специфических методов и средств, осуществляемый скрытно и имеющий своей задачей изменить мнение, намерение, цель действий, внутреннее состояние или практическое поведение человека (или группы людей) в нужном манипулятору направлении.*

Практика манипулирования сознанием и поведением людей восходит к глубокой древности и сопровождает человечество на всех этапах его истории, составляя фактически главную, сущностную, особенность отношения цивилизации, в том числе современной, к человеку. В настоящее время хорошо известны древние методы зомбирования людей, применяемые *культом Вуду* и *гаитянскими колдунами*. Этнологи, изучавшие эти методы, пришли к выводу, что процесс модификации психики осуществляется с использованием сильных токсических веществ, образующих так называемый *«порошок зомби»*. В его состав входит высушенная и истертая рыба фугу, а также активные вещества, получаемые от жабы *Bufo marinus*, желчный пузырь мертвого мула или человека, некоторые растения. Главным действующим компонентом *«порошка зомби»* является яд тетрадотоксин.

После применения порошка возникает чувство эйфории, покалывание в конечностях, затем наступает паралич, дыхание перестает определяться, сердце почти останавливается, и человек переходит в состояние, подобное клинической смерти (способное обмануть даже опытного врача). Однако если доза порошка выверена точно, человек не умирает, но в его мозгу происходят необратимые изменения – он теряет волю, разум и становится послушным орудием.

В практике Вуду есть *два уровня зомбирования*:

низшая, грубая, степень зомбирования – это существование тела с практически «мертвым» мозгом. Такие зомби могут только тупо выполнять команды и не способны к осмысленным действиям;

более тонкая степень зомбирования отличается тем, что зомби выглядит вполне по-человечески, может реагировать на боль, контролирует поведение и мысли, но лишен эмоциональной сферы. Он тоже ориентируется лишь на приказы хозяина, однако, в отличие от *глубоких зомби*, способен самостоятельно планировать свои действия для наилучшего достижения цели.

В своем развитии мир прошел через практику обращения человека в раба, феодальное закабаление людей, их церковную унификацию, в том числе с помощью методов инквизиции. Но только в XX веке человечество узнало, что такое тотальное насилие над сознанием и поведением людей. Этот век (на фоне научно-технического прогресса и нарастания демократических преобразований в общественной жизни) превзошел все другие эпохи человеческой истории в своем стремлении поставить под полный контроль мысли, потребности и практические действия человека.

Задачу «улучшения» человека через манипуляцию его сознанием пытались практически решить марксисты всех разновидностей, национал-социалисты, многочисленные диктаторские режимы, тоталитарные секты, религиозные фундаменталисты. Именно в этом столетии мир узнал, что такое японские камикадзе, исламские шахиды, готовые к самопожертвованию солдаты, фанатики всех мастей – идеологические, религиозные, националистические, классовые и даже футбольные.

XX век по разнообразию методов, использованных для манипулирования внутренней жизнью человека, стал, безусловно, наиболее заметным в истории человечества, значительно обойдя в этом отношении средние века и эпоху «святой инквизиции». Апробацию прошли самые различные приемы и средства приведения людей к «единому знаменателю» – от социальной демагогии до концентрационных лагерей, от психотерапии до психотропных препаратов.

Наиболее показательным примером использования тотального насилия ради установления нужного порядка во внутреннем мире человека оказался ***метод концентрационных лагерей***. Здесь имеет место совсем не то, что было при крепостном праве или рабстве. Обе эти системы насилия сложились стихийно и были вполне естественными для своего времени. Концлагерь же есть искусственно созданная, спланированная по целям и методам *система подавления человеческого в человеке*, его перерождения в нечто механическое. Этот эксперимент чрезвычайно показателен в своей завершен-

ности. У него нет внешних, словесных прикрас в виде призывов к свободе, равенству, братству, соблюдению прав человека, здесь в полной наготе видится то, что, по сути, заложено в любой идее овладения душевной жизнью человека, создания из него идеального члена той или иной социальной системы.

Что представляет собой «идеальный заключенный»? Автор многих публикаций по вопросам психологии лагерной жизни М. Максимов описывает вложенный в это понятие замысел следующим образом. Когда человеку дают команду, то между ее получением и началом исполнения есть хотя бы небольшой временной зазор – время на обработку команды внутри человека. Так вот, у «идеального заключенного» этого зазора нет. Команда мгновенно проваливается в исполнительные органы. Обработки внутри не происходит, потому что «нутра» – нет. У этого существа (назвать его человеком уже трудно) нет внутреннего содержания – разума, души и всего того, что призвано принимать решения. Оно похоже на модель, управляемую по радио: один человек переключает кнопки на пульте управления – и тысячи, миллионы «идеальных заключенных» выполняют нужные действия. Задачей гитлеровских концлагерей поначалу и было научиться превращать за три года нормального здорового человека в «идеального заключенного», а затем этот опыт использовать для формирования миллионов «идеальных людей».

Какими методами решалась задача? В их основе – тотальный страх, боль, неопределенность, бессмысленность, доведенные до неукоснительной, абсолютной системы. Заключенным не позволялось ни о чем думать, они не должны были понимать смысл происходящего. Например, при загрузке песком вагона, им вдруг приказывали оставить лопаты и бросать песок только руками или выполнять бессмысленные упражнения: «Встать! Лечь! Встать! Лечь!». «Идеальный заключенный» не должен иметь возможности планировать свое поведение хотя бы на час вперед, распределять силы, самостоятельно оценивать ситуацию. Он должен быть окончательно и бесповоротно убежден: от меня ничего не зависит. Все осмысленные действия заменяются реакциями на приказ. В предельном варианте реализуется бихевиористская идея манипулированного поведения по принципу «стимул–реакция».

Концлагерь, прежде всего, направлен против духа человека, его внутреннего мира, он имеет целью сломать и подавить в человеке все то, что не поддается другим методам, довести его до животного состояния и даже до состояния вещи, добиться, чтобы не духовная, а материальная сущность управляла его поведением. По мнению французского философа А. Камю, система концлагерей позволяла осуществлять на практике «диалектический переход от управления личностями к управлению вещами, поставив личность на место вещи».

Однако идея, заложенная в концлагерях, тоже не состоялась. Некоторую часть заключенных удалось довести до «идеального» состояния. Но все они очень быстро погибали – получалось нежизнеспособное существо, лишенное внутреннего содержания, ходячий труп. Как пишет Максимов, к 1942 г. стало ясно, что программа перевоспитания в лагерях не дает результата, и с этого времени рабочие лагеря в Германии стали постепенно превращаться в лагеря уничтожения. А новые уже сразу строились как лагеря смерти.

И пусть не кажется происходившее в концлагерях чем-то бесконечно далеким от реальной жизни. Бывшие узники в один голос говорят: концлагерь – «микрокосмическое отражение мира людей вообще» (В. Франкл); «лагерь – не противопоставление, а слепок нашей жизни, сгусток тех же ее законов» (В. Шаламов). В обычной жизни происходит все то же самое, только методическое оснащение работы иное – преобладают экономические, идеологические, националистические или религиозные формы воздействия на людей. Педагогика концентрационных лагерей – апофеоз общей тенденции XX века по созданию *полностью манипулируемого человека*.

Эта же задача настойчиво решается и сегодня. Так называемое *гражданское общество западных стран* несравнимо глубже влияет на формирование психики человека, чем любая тоталитарная система. Шаблоны поведения, обусловленные мнением элиты и волей окружающего большинства, быстрее приобретают внутреннюю обязательность, заставляют неукоснительно следовать предлагаемой системе отношений. А в этой системе тоже все строго предопределено гласными и негласными правилами, требованиями имиджа, принадлежностью к тому или иному слою населения. Человек постоянно находится под давлением страха отстать от своего круга, выбиться из колеи, опуститься до автомобиля или магазина другого класса, до журнала, собеседника или клуба иного уровня.

> Критикуя американского психолога-бихевиориста Б. Скиннера, основного теоретика превращения человеческого поведения в полностью манипулируемое, один из крупнейших мыслителей XX века Л. Берталанфи писал: «Расширяющаяся экономика «общества изобилия» не может существовать без подобной манипуляции. Только при все большем манипулятивном превращении людей в скиннеровских крыс, роботов, торгующих автоматов... может это великое общество прогрессировать к все возрастающему национальному продукту».

В течение века менялись формы воздействия, их словесное прикрытие, но цель переделки человека под вещь (или робота) оставалась неизменной.

Принято считать, что разные социальные системы стремятся создать разные типы людей, каждая «строит» человека под себя, видит собственный идеал. Но в своей сути идеал везде видится одинаковым. Это – послушное, управляемое существо, знающее общие правила поведения и действующее, в том числе инициативно, лишь в их пределах; кроме того, имеющее потребность славословить хозяина, благодарить его за счастливую жизнь. На практике любое общество стремится «держать человека в выгодном для себя состоянии безликости» (А. Швейцер). Различается только «метафизическое обоснование рабства» (Н. А. Бердяев). И всегда такого рода усилия прикрываются обращениями к «достоинству» человека, словами об «интересах самого человека», о стремлении сделать его жизнь более благополучной.

Вступление человечества к концу XX века в *информационную стадию развития* существенно расширило возможности получения нужных результатов в деле управления индивидуальной психикой и психологией больших масс людей. В работу по программированию психики включились новые науки (кибернетика, информатика, генетика) и технологии (электронные СМИ, глобальные информационные сети, в первую очередь Интернет как «мировая паутина» – для человека – в буквальном смысле).

Установки манипуляторов те же: сделать поведение людей более стабильным, неконфликтным, хорошо поддающимся контролю и управлению. Переход к глобальному обществу позволил только придать информационно-психологическому воздействию и использованию психологических манипуляций всеобщий, почти вселенский характер.

Особенно преуспели в этом ***средства массовой информации.*** Сегодня по их шаблонам люди высказывают «свое» мнение, спорят друг с другом. По их рецептам определяют отношение к политическим партиям и общественным лидерам, воспитывают детей, одеваются, лечатся, худеют, выбирают покупки и «идолов» для подражания, влюбляются, занимаются сексом. Заметна программирующая роль СМИ и во время выборов, когда, главным образом, они подводят наивного избирателя к мысли, что только предлагаемый кандидат лучше всего защитит его права. При этом избиратель остается в святом убеждении, что выбор он сделал самостоятельно.

Во все времена каждый, кто пытался переделать человека, приспособить к своим требованиям, искал пути к овладению его душой. К душе рвутся, хотят заполучить власть над нею все – от гаитянских колдунов (или Мефистофеля у Гёте) до современных последователей Рона Хаббарда.

Известно, что Сталин активно поощрял работу так называемых «инженеров человеческих душ». Уже в те времена говорили о возможности создания новой отрасли науки – ***«душевной инженерии»***. С этой же целью в секретных лабораториях Гитлера изучались возможности языческих ритуалов, буддийских мантр, опыта оккультных сект, особых руничесих табличек, на которых якобы рукой дьявола было начертано некое знание. Философ Мераб Мамардашвили назвал идею модификации человека «одной из самых трагических и глупых идей XX века».

Вроде бы нынче нет того, что проделывали с людьми маги и гаитянские колдуны. Однако с младенчества и до самой смерти мы тоже подвергаемся разным типам зомбирования. Этот процесс принято называть ***социальным программированием,*** или социализацией, социальной адаптацией. Цель же любого социального программирования не отличается от цели магов Вуду: создать послушный человеческий экземпляр, которым легко управлять. Причем, в отличие от гаитянского, наш зомби убежден, что действует по собственной воле и все мысли принадлежат ему самому. Именно такой тип манипуляции человеческим сознанием заложен в современной системе воспитания и обучения, деятельности различных коллективов, фирм, общественных организаций и государственных образований в целом, независимо от степени их цивилизованности. В любой структуре зомбированный под ее требования человек делает не то, что ему выгодно или приятно, а то, что выгодно фирме, коллективу, партии, государству.

Уже не кажется преувеличением описанный известным американским публицистом и психотерапевтом Э. Шостромом в книге «Анти-Карнеги, или человек-манипулятор» инструктаж опытным мексиканцем своих земляков, впервые выезжающих в США: «Американцы – прекраснейшие люди, но есть один момент, который их задевает. Вы не должны говорить им, что они трупы». По мнению Э. Шострома, здесь – предельно точное определение «болезни» современного человека (не только американца). Он – мертв; он – кукла, и его поведение действительно очень похоже на «поведение» зомбированного трупа. У него серьезные трудности с эмоциями, сменой переживаний, способностью жить и реагировать на происходящее по принципу «здесь и теперь», менять решения и вдруг, неожиданно даже для себя, без всякого расчета, ставить свое «хотение» превыше всего. «Мертвым душам» (отнюдь не по Гоголю) не знакомы искренние переживания. Рыночные отношения требуют: никаких чувств, только дело.

Процесс манипулирования начинается с первых шагов ребенка, его наставляют, «вводят в рамки», призывают к повиновению, контролируют, наказывают, требуют: «ты должен», «ты обязан». Даже *знание* оказывается в этом процессе обоюдоострым оружием. С одной стороны, оно помогает человеку приспособиться к определенному виду деятельности и образу жизни; с другой – делает его привязанным к этому знанию и даже подчиненным ему. *Иногда не столько человек овладевает знанием, сколько знание овладевает человеком.* Хорошо воспитанный и обученный ребенок – это уже социально управляемый индивид. Дальше с ним работать намного проще, он прошел первый и самый важный этап в деле снижения уровня внушаемости. Так что подготовку к будущим манипуляциям проводят сами родители, заинтересованные в благополучии своего чада.

Такого рода манипулирование не связано с неблаговидными целями. Более того, оно исходит из добрых побуждений. Однако и у добрых побуждений есть второе дно. Не случайно говорят, что благими намерениями вымощена дорога в ад. И в данном случае, помогая ребенку адаптироваться к условиям жизни, родители и учителя, не желая того, одновременно снижают порог его внушаемости, делают более подверженным любой манипуляции в будущем.

С таким манипулированием мы сталкиваемся в жизни постоянно. И уже как бы смирились с ним. Гораздо хуже, когда бытовое манипулирование перерастает в целенаправленное зомбирование с использованием *более жестких средств и методов,* например,

психотропных препаратов и специальных технологий. Их цель – выключить самоконтроль и способность к сопротивлению и, следовательно, открыть путь к овладению психикой человека. Это облегчает ее последующее программирование любыми, специально подобранными для конкретного человека или группы людей, методами – от убеждения и внушения до нейролингвистического программирования. Сегодня все чаще появляются сообщения о людях с полностью утраченной памятью («человек без прошлого») и как бы выключенным сознанием. Внутренняя пустота делает их идеальными исполнителями команд любого «хозяина».

Конечная цель интенсивного манипулирования психикой людей в современном мире состоит в том, чтобы незаметно подвести человечество к новому обществу, в котором есть *управляющее меньшинство и управляемое большинство*. Люди, в одинаковой степени самостоятельные в своих решениях, для нового миропорядка не пригодны. Меньшинство – это «золотой миллиард», «интернациональное братство богатых и очень богатых людей» (П. И. Одинцов), которым необходима только стабильность. Задача большинства – быть управляемым и не омрачать своими действиями жизнь тех, кто принадлежит к «золотому миллиарду». Взгляд управляющего меньшинства на большинство людей определил еще Наполеон: у народа есть единственная обязанность – быть управляемым. Популярные слова о демократии как власти народа, власти большинства – красивая легенда, часто весьма далекая от того, что происходит в реальной жизни.

Защитные действия

Учащимся, подросткам необходимо вновь и вновь показывать, что манипуляция их сознанием может осуществляться не только через реализацию глобальных проектов, специальных научных методов и технических средств, перед которыми человек беззащитен. В значительно большей степени она оказывается результатом того, что происходит с ними ежедневно, и что мы не расцениваем как манипуляцию. Программирование и зомбирование начинается и в обычных жизненных ситуациях. И особенно эффективно оно осуществляется в детстве и подростковом возрасте, на фоне формирования человеческой психики и ее высокой пластичности.

Чтобы, по возможности, избежать манипулирования (зомбирования), подростку необходимо знать и уметь выявлять ***основные***

признаки внушенного извне (значит, утратившего естественность) поведения, уметь оценивать по ним свои действия. Вот некоторые явные признаки того, что молодой человек подвергся информационной манипуляции или запрограммирован и находится на пути к состоянию ***социального зомби***:

он бесповоротно одержим каким-либо желанием, связанным, например, с приобретением престижной веши, стремлением всеми доступными средствами «делать деньги», добиваться лидерства в коллективе или выглядеть эффектнее других внешне;

почти полно-

круг основных интересов его узок, неоригинален;

стью подобен общепринятым в данной среде шаблонам;

он готов бездумно повторять в кругу друзей как «последнюю истину» то, что услышал в телепередаче, от знакомых или прочитал на рекламном щите;

того, не пред-

он верит рекламе, живет от одного телешоу до другого, от сериалов; составляет свое времяпрепровождение без телевизора и

почти утрачена способность переживать за других людей, сострадать им, а понятия «душевность», «сердечность», «справедливость» стали для него пустыми звуками;

действия и го-

налицо боязнь ответственности за свои решения и

товность обвинять всех и каждого в совершенных ошибках, утрачена способность сомневаться, чувствовать свою вину в случившемся;

защищая свое мнение, он готов лгать, изворачиваться, извращать факты или, напротив, бездумно, не приводя аргументов, при первых возражениях оппонентов отказаться от собственного утверждения;

потеряло остроту чувство любви к близким, способность получать наслаждение от общения с природой, искусства, людьми, осталось желание, например, часами сидеть у компьютера или игрового автомата;

непримиримости

в его суждениях и убеждениях много фанатизма и

к другим мнениям, растет желание активно участвовать в деятельности объединений «фанатов» того или иного толка;

к жизни –

проявляется феномен «туннельного» отношения

он видит и слышит в ней лишь то, что хочет видеть и слышать.

Что можно рекомендовать подросткам для повседневной защиты от постепенного превращения в зомбированное существо, для сохранения собственного лица, независимости и яркой индивидуальности?

Во-первых, нужно знать и уметь распознавать цели, методы и средства манипулирования сознанием и уметь контролировать степень своей зависимости от внешних воздействий (например, по указанным выше признакам) каждый день и в каждой из жизненных ситуаций. Это достигается тренингом и обсуждением примеров и ситуативных задач.

Во-вторых, в любой пламенной речи, тексте, рекламе лучше «пропускать мимо ушей» красивые фразы, обороты, сравнения и стараться ухватить только главный довод. Что же вам предлагают и куда настойчиво зовут? Нет ли более адекватной, безопасной или интересной альтернативы этой идее? Стоит включить здравый смысл, и окажется, что альтернатива всегда есть. Хотя и здравый смысл надо уметь ставить под сомнение. Ведь он – тоже хорошо усвоенная программа.

В-третьих, освобождению сознания от однобокой зависимости. его раскрепощению могут способствовать творческое отношение к жизни, участие в делах, требующих нестандартного мышления и оригинальных решений, наконец, постоянный интерес ко всему новому, неожиданному, приобщенность и любовь к искусству, природе, науке.

В-четвертых, надо поменьше бывать в зоне контакта с теми субъектами, которые способны вами манипулировать. Не следует уповать на свою устойчивость – речи нынешних манипуляторов очень убедительны. Для противостояния им хорош «метод Одиссея». Помните? Чтобы не попасть под чары пения сирен, он членам команды своего корабля залепил уши воском, а себя приказал привязать к мачте. Только поэтому путешественники избежали зомбирования пением сирен и не погибли. Можно использовать один из этих приемов. если не хватает силы воли для того, чтобы ограничить, например, время сидения перед телевизором или компьютером.

В-пятых, можно использовать такой простой прием, как временный уход из зоны действия внушения. Оцените ситуацию со стороны, подумайте, успокойтесь. Возникшее вначале очарование пропадет, и дальнейшие стадии манипуляции могут показаться даже странными. С этой же целью, если есть возможность, полезно прервать словоизлияния манипулятора вопросами, нарушающими его спенарий. Перерыв или хотя бы временная смена стиля отношений всегда действуют отрезвляюще. Еще более полезен прием

защиты, сформулированный народной мудростью: «Утро вечера мудренее». Отложите окончательный вывод об услышанном или увиденном до утра, и подумайте о нем «на свежую голову».

Государство нередко является участником процесса манипуляции сознанием и поведением своих граждан в контексте общих задач и принципов. Однако нынче и оно стремится защитить людей от нарастающего использования «жестких» методов и средств информационного воздействия на их психику. В связи с этим 26 июня 2001 г. Государственной Думой РФ была принята поправка в Федеральный закон «Об оружии»; 26 июля того же года Президент РФ В. В. Путин подписал эту поправку. Вот что она гласит: «На территории РФ запрещается оборот в качестве гражданского и служебного оружия: оружия и иных предметов, поражающее действие которых основано на использовании радиоактивного излучения, электромагнитного излучения, инфразвукового излучения, ультразвукового излучения и биологических факторов».

Вопросы для обсуждения

1. По мере развития цивилизации человек становится более (или менее) податливым к влиянию различных видов манипуляции? А что происходит с возрастом?

2. В какой мере каждый из присутствующих считает свое поведение манипулируемым? Не зомби ли вы?

3. Есть ли у вас опыт манипулирования другими людьми? В какой ситуации и какими методами оно осуществлялось?

4. Что отличает гаитянского зомби от манипулируемого (зомбированного) человека наших дней?

5. Назовите примеры и признаки манипулирования в подростковой среде.

5.2. Основные методы и средства информационного воздействия на человека

В конце XX века активно формировались все новые факторы, расширяющие возможности информационного воздействия на человека и более полного управления его поведением. Наряду с появлением принципиально новых технических средств массо-

вого информирования людей и глобализацией информационных потоков к числу таких факторов следует отнести бурное развитие *поведенческих (бихевиористских) наук*, используемых для разработки эффективных методов и технологий манипуляции сознанием граждан, их отношением к происходящему в окружающем мире.

В настоящее время существуют целые научные дисциплины о том, как управлять поведением человека, коллектива, общества. К ним относятся современные варианты психотерапии, теория рекламы, суггестология, нейролингвистическое программирование, дианетика и т. п. Получил свое теоретическое обоснование гипноз, и были сделаны попытки перенесения методов гипнотического воздействия с отдельного индивидуума на коллективы и целые человеческие сообщества. Все это было невозможно 40–50 лет назад из-за отсутствия эффективных средств массовой информации и научно обоснованных алгоритмов управления социумом.

> «Там, где манипуляция является основным средством социального контроля, как, например, в Соединенных Штатах, разработка и усовершенствование методов манипулирования ценятся гораздо больше, чем другие виды интеллектуальной деятельности». Г. Шиллер, американский политолог.

Нейролингвистическое программирование

В основе концепции нейролингвистического программирования (НЛП) лежит убеждение, что нашу *психику можно уподобить компьютеру*, в котором восприятие и обработка информации осуществляется по определенным, заданным, программам. Первичная информация в ней воспринимается, структурируется, осмысливается и оценивается на основе внутреннего опыта, состоящего из мыслей, убеждений, ценностей, эмоциональных переживаний, памяти. Один из принципов НЛП: *сознание и тело – части одной управляемой системы.*

Вторым основанием НЛП является убеждение, что можно соединить в единое целое две системы: *первую сигнальную систему* (система условно-рефлекторных связей, формирующихся в коре больших полушарий головного мозга животных и человека при воздействии конкретных раздражителей: свет, звук, боль) и *вторую сигнальную систему* (обычная человеческая речь).

Поэтому словосочетание «нейролингвистическое программирование» включает в себя три понятия:

«нейро» – то, что происходит в мозге и центральной нервной системе;

«лингвистическое» – то, какими словами мы пользуемся, и как это влияет на наше восприятие внешнего мира и взаимодействие с ним;

«программирование» – процесс, который позволяет самому человеку (или тому, кто его программирует) решить, как он будет мыслить, чувствовать и говорить.

Специалисты по НЛП работают с так называемыми словесными «якорями», то есть программами, которые незаметно для пациента вводятся в его мозг в виде слов и вызывают проявление того или иного типа поведения. НЛП – это современный вариант *кодирования (или перекодирования) психики*.

Территория и карты. Один из базовых постулатов НЛП гласит: у человека есть индивидуальный образ мира, ***его карта***. Этот образ всегда субъективен и не тождествен реальности. Он формируется за счет фильтрации внешней информации с помощью языка, личного опыта (персональной истории), особенностей перцептивной системы (специфики работы органов чувств, анализаторов) и, в конечном счете, образует *ментальную карту* (или психологическую «карту мира») человека.

Территория – это громадный мир вокруг нас, все события и вещи в нем; тогда как *карта* («ментальная карта») – наша модель, наше представление об этом мире.

Ментальная карта *– это символическое представление (не обязательно адекватное) в нашей психике реальности, всего внешнего и внутреннего мира, это присущая каждому человеку субъективная модель реальности, тех или иных ее фрагментов.* Мы воспринимаем мир в ходе повседневного опыта с помощью органов чувств, мозга и языковых систем, посредством которых осмысливается реальность. Первичный материал всегда богаче, чем отображающая его ментальная карта. Поэтому результаты нашего восприятия подобны карте, которая представляет мир, но не копирует его. У всех людей свои, специфические карты, или субъективные модели мира. И они в большей степени, чем сама действительность, определяют то, как мы интерпретируем окружающий мир, реагируем на его сигналы, какой смысл придаем своему поведению.

Нейролингвистические программы определяют, что и как мы воспринимаем и интерпретируем. От их характера и совершенства

непосредственно зависят восприятие и обработка информации, образ мышления, ощущения, действия и жизнь вообще. Программы, имеющиеся у разных людей, существенно отличаются не только с точки зрения субъективных ощущений, но и с точки зрения эффективности решения жизненных проблем. Поэтому разные люди неодинаково воспринимают одни и те же события и даже слова и по-разному реагируют на них.

Столь важная роль ментальных карт (программ) в восприятии и отборе стимулов делает их одним из ключевых звеньев в управлении психикой. Они как бы предопределяют и программируют наше общее восприятие и общую реакцию на мир. На протяжении многих тысячелетий ментальные карты формировались преимущественно стихийно с помощью традиционных институтов социализации: семьи, церкви, школы и т. д. В конце XX века стало возможным, как считают создатели НЛП, целенаправленно в сравнительно короткий промежуток времени формировать или по крайней мере существенно изменять наши «программы». Этим, собственно, и занимается нейролингвистическое программирование. Следовательно, НЛП можно рассматривать как *процесс анализа и преобразования структуры субъективного опыта человека, обучения его новым формам реагирования на внешние и внутренние стимулы путем модификации старых «программ» или замены их на новые.*

Фильтры восприятия – еще одно понятие НЛП. Способности человеческого восприятия ограничены, и нам приходится выбирать наиболее важное, а все остальное – отсеивать. Поэтому в определенном смысле НЛП – это также *наука о фильтрах нашего восприятия*, о том, что для конкретного человека важно, а что он отсеивает. Мы не можем видеть или слышать абсолютно все, что нас окружает, мы выбираем то, что нам кажется более важным и интересным, или то, что нам ближе и роднее. Как говорится, что ищем, то и находим.

Все техники НЛП построены на реорганизации информационных процессов человека, создании новых психологических «карт» и фильтров восприятия и, как следствие, изменении в нужную сторону его взаимодействия с реальным миром. Причем изменению подлежит не только поведение индивида, но и внутренние установки, оценочные критерии, весь процесс мышления и принятия жизненных решений.

НЛП стремится манипулировать человеческим сознанием путем *подбора кодовых фраз, слов, звукосочетаний, изображений* и прочей

атрибутики. Цель – пробраться к потаенным инстинктам, чувствам и желаниям ни о чем не подозревающей «жертвы» в обход разума и заставить ее совершать поступки под диктовку навязанных установок.

В ходе программирования учитывается эффект, который раздельно производят на человека:

слова и их смысловое содержание;

голос, его интонация и тембр;

поза, мимика и жесты говорящего.

Пропорции их воздействия, как показывает анализ, выглядят следующим образом: 55 % этого воздействия занимает *«язык тела»* (позы, движения, мимика), около 38 % – *голос* (тон, интонации, ритм, тембр) и только 7 % – собственно слова, их смысл. Когда они не согласованы (в НЛП это называется неконгруэнтностью), собеседник получает по трем каналам три разных или даже противоречащих друг другу сообщения, причем в соответствующей пропорции. Цифры показывают, что мы должны быть в курсе возможностей вербального и невербального управления нашим поведением, уметь распознавать и адекватно реагировать на различные формы воздействия. Примеры воздействия на человека известны со времен Одиссея. Немало их и в современных источниках.

> ...Вдруг зазвучал другой голос, негромкий и мелодичный. В нем было непередаваемое очарование. Слышавшие этот голос редко потом вспоминали сами слова, а если все же вспоминали, то удивлялись, ибо в словах этих не было никакой силы. Но голос доставлял наслаждение. Все произносимое им казалось мудрым, со всем хотелось согласиться. ...Одного звучания этого голоса было достаточно, чтобы стать его рабом, и это колдовство жило в слушателях, даже когда они были уже далеко. Голос все шептал, приказывал, и они повиновались. Никто не мог слушать его без волнения, никто не мог противостоять его чарам. Устоять могла только твердейшая воля и устремленная мысль.
>
> *Дж. Р. Р. Толкиен.* «Властелин колец»

Есть еще одно, очень важное правило НЛП. Если сознание говорит одно, а подсознание совершенно другое – *обычно побеждает подсознание*. Этим как раз и пользуются профессиональные мошенники. Им могут доверить посторожить вещи самые бдительные люди, а потом будут сильно удивляться тому, что пропал не только новый приятный знакомый, но и чемоданы. А сознание находит логичное объяснение уже совершенному поступку.

Ожидаемые результаты. Считается, что НЛП в состоянии помочь людям избавиться от навязчивых страхов, восстановить их правильную ориентацию в мире, выстроить более комфортную модель поведения.

Однако НЛП, как и другие методы программирования психики, можно использовать для внедрения в подсознание людей различных по своей политической и социальной значимости программ, как «продуктивных», так и «непродуктивных». Приспособление к весьма негуманному миру потребительства, эгоизма и жесткой борьбы за существование стало сегодня парадигмой большинства прикладных направлений в психологии и поведенческих науках. Поэтому формируемые в массовых масштабах одномерные «психические линзы» чаще всего не позволяют людям видеть альтернативные, более человечные варианты отношений с миром. Фильтры восприятия их не пропускают, а сформированные опытом или навязанные в ходе сеансов НЛП ментальные карты не видят в них ценности.

Цель последователей НЛП стара как мир: они желают манипулировать другими людьми, как куклами на веревочках. В старину для этой цели использовались различные приворотные и отворотные зелья, заговоренные гребешки и булавки, потом настала пора массового увлечения гипнозом.

Разумеется, в соответствии с традициями колдовства НЛП обещает своим последователям научить их пробуждать в себе физические и интеллектуальные *сверхвозможности*, дать способность управлять временем и пространством. Вместе с тем существует и немало сомнений в возможностях данного метода. По утверждению ряда врачей-психиатров, посещавших курсы НЛП из профессионального интереса, эта «наука» представляет собой смесь из элементарных психологических приемов, мистицизма, ссылок на некие авторитеты и большого количества словесной шелухи.

Однако многое зависит от квалификации специалистов НЛП и качества проводимых тренировок по данной методике. На определенном этапе подготовки даже подбор слов и их порядок, длина и интонация предложений, другие лингвистические особенности речи могут оказывать значительное влияние на психику человека. И тогда НЛП позволяет *эффективно управлять человеческим сознанием* через приказы, заложенные в словах, интонациях, позах тела. Это может быть чрезвычайно опасным. Не случайно в США раз-

работки в области нейролингвистической психологии запрещены законодательствами всех пятидесяти штатов.

Дианетика как метод и технология манипулирования человеком

Создатель дианетики – американский писатель-фантаст Р. Хаббард (1911–1986). Начало новому методу было положено изданной им в 1950 г. книгой «Дианетика» (подзаголовок – «Современная наука душевного здоровья»), ставшей позднее руководством по применению технологии очищения и рационализации психики человека.

Последователи Хаббарда утверждают, что их методика позволяет проникнуть сквозь плотную завесу времени и выяснить, какие события прошлого явились причиной сегодняшних бед человека. Суть дианетической терапии заключается в том, чтобы провести индивида через сохранившиеся в подсознании *«критические точки»* и путем их повторного переживания излечиться от связанных с ними недугов.

В этом и состоит технология данной терапии, процесс которой называют *одитингом*, а того, кто его проводит, – *одитором*. Пациент с помощью одитора как бы «проживает», находясь в особом состоянии, всю свою жизнь с момента зачатия, натыкается на «болевые точки» и неоднократно их переживает – до тех пор, пока накопленная в них негативная энергия не разрядится полностью. В итоге человек получает свободный от былых кошмаров и комплексов, *«чистый»*, разум. И только разум! Все иное – чувства, эмоции, переживания, влечения и т. п. – ему теперь не нужны.

Дианетика – это наука о Разуме и мышлении. Для нее человеческий ум – «превосходная вычислительная машина», «отлично построенный компьютер». В освобождении от всех других волнительных для человека особенностей психики эта наука видит залог вечно счастливой жизни. Р. Хаббард был убежден: «В сегодняшнем мире нет ни одной проблемы, которая не могла бы быть разрешена одним только разумом».

С точки зрения инженерно-компьютерного понимания человека дианетика перекликается с НЛП. Видимо, в условиях победного шествия технического прогресса заманчивой стала перспектива переноса его идей и методов на извечно провальный процесс формирования «нового человека» в тех или иных вариантах. Новейшие методики призваны обеспечить возможность *работать с человеком как с машиной*. Но для этого необходимо избавить его от всего собствен-

но человеческого – способности и потребности переживать, любить, сострадать, поступать «по совести». Оставить только очищенный разум. Тогда человек станет прекрасным природным компьютером, и им можно будет без каких-либо проблем управлять (манипулировать), вводя программы и нажимая на клавиши (или меняя интонации голоса). Таков в своей глубине замысел и дианетики, и НЛП.

Конечный продукт дианетической терапии – *клир*, полностью разумное (и только разумное!) существо, внутри которого все «неправильное» вычислено и вычищено. Оно способно лишь на хорошо просчитанные решения и действия в строгом соответствии с вводимой информацией. Его ум – превосходная вычислительная машина, а сама дианетика – уже «инженерная наука». «Мы сейчас стоим на мосту между двумя состояниями человека, – провозгласил Р. Хаббард, – впереди – клир». Позади, видимо, – человек Сервантеса, Шекспира, Гёте, Достоевского...

> Л. Н. Толстой в одном из писем писал: «Чтобы жить честно, надо рваться, путаться, биться, ошибаться, начинать и бросать, и опять начинать и опять бросать, и вечно бороться и лишаться... А спокойствие – душевная подлость. От этого-то дурная сторона нашей души и желает спокойствия, не предчувствуя, что достижение его сопряжено с потерей всего, что есть в нас прекрасного, не человеческого, а оттуда».

К «душевной подлости» и ведет нас дианетика, видя в ней залог «здоровья». Предельная рационализация человека и его обездушивание неизбежно идут нога в ногу.

Сайентология. Идеологической вершиной дианетики стала созданная Хаббардом на ее основе прикладная, фактически религиозная, философия – сайентология.

Руководствуясь своей философией, последователи дианетики готовы переделать внутренний мир миллионов людей, структуры власти и государства. Сайентологи почти открыто действуют, собирая любую информацию, связанную с исполнительными органами власти, структурами правопорядка, средствами массовой информации, с деятельностью основных религиозных конфессий, а также иными организациями, имеющими влияние в обществе или оказывающими какое-либо воздействие на принятие государственных решений – например, банки, профсоюзы, крупные предприятия.

В соответствии с заветами Хаббарда сайентологи стремятся продвинуть на ключевые посты любых структур и организаций своих

людей или добиться сочувствия своим идеям от лиц, нужные посты уже занимающих. При необходимости сайентологи прибегают к подкупу, шантажу, прямым угрозам.

Технологии дианетики в рамках ее философии направлены на реанимацию хорошо известной из истории *пирамидальной системы управления* с четким вертикальным подчинением и полным контролем меньшинства над большинством. Р. Хаббард всегда мечтал о тотальной власти над людьми: «Сайентология дает полную свободу, но она должна нести и установление тотальной власти и авторитета для достижения тотальной дисциплины».

Такого рода цели хаббардистов нередко привлекают к себе внимание психически неполноценных маньяков и даже некоторых общественных структур. Но в то же время эти цели и деятельность их последователей привели к запрету сайентологических центров, подобных религиозным сектам, во многих развитых странах мира.

Внушение и гипноз

Внушение – один из наиболее распространенных и важнейших методов манипулирования сознанием человека. Оно представляет собой *преимущественно скрытое воздействие на подсознание и отчасти сознание индивида с целью изменения его общего состояния и отдельных характеристик психики – установок, ценностей, убеждений и т. п.*

Внушение осуществляется с помощью слов, взглядов, жестов, образов и других средств передачи информации. В зависимости от средств воздействия выделяются два основных вида внушения:

вербальное – с помощью речи;

невербальное – посредством жестов, определенных форм поведения, создаваемых образов и т. п.

При внушении с помощью речи главное воздействие на внушаемого чаще всего оказывает не значение слов и предложений, не логическая аргументация, а построение речи, ее форма, источник и сопутствующая ей паравербальная информация: интонация, громкость, темп, дикция, образность и т. п.

Внушение может быть *прямым* и *косвенным*. Прямое внушение характеризуется открытостью влияния, четкой формулировкой требований, непосредственной направленностью на конкретного индивида.

Косвенное внушение в большей мере относится к методам манипулирования и обычно является составной частью манипуляционных акций. Оно осуществляется без прямых требований, с помощью опосредованного воздействия, путем намеков, незаконченных фраз. В этом случае более широко используется паравербальная информация.

Внушение *неодинаково действует на разных людей*. Это действие зависит также от состояния, в котором находится человек, и его возраста. Наиболее восприимчивы к внушению люди эмоционально неустойчивые, впечатлительные, имеющие неуравновешенную нервную систему, а также находящиеся в ослабленном, переутомленном или встревоженном, растерянном состоянии, неоформившиеся в возрастном и личностном отношениях.

По мнению ряда авторов, многовековое воздействие цивилизационной культуры стабилизирует нервную систему человека и снижает влияние внушения на его психику. Поэтому более восприимчивы к внушению, в частности, представители традиционных сообществ и народов стран «третьего мира», не прошедших длительную цивилизационную эволюцию.

> Внушение основано на некритичности восприятия и предполагает, как правило, неспособность внушаемого сознательно контролировать поток поступающей информации. Необходимым условием внушающего воздействия является авторитетность источника информации.
>
> *Б. Д. Парыгин*, социальный психолог.

Факторы эффективности внушения. В современной литературе к числу таких факторов чаще всего относят:

личные качества субъекта внушения (суггестора), наличие у него соответствующих способностей, личное обаяние, уверенность в себе, чувство внутреннего превосходства, авторитетность, а также знание техник внушения и умение их использовать;

личные качества и состояние объекта внушения. Более внушаемым человека делают тревожность, неуверенность, робость, низкая самооценка, впечатлительность, повышенная эмоциональность, ограниченный жизненный опыт и конкретное состояние, определяющее восприимчивость к внушению;

отношения между субъектом и объектом внушения. Успеху способствуют взаимное доверие и уважение, а также способности первого подстроиться (подключиться) к внутреннему миру объекта общения и «вести» его в нужном направлении;

ситуация, уровень личностной значимости происходящего для объекта внушения, дефицит времени, неожиданность;

конструкция сообщений в ходе процесса внушения. Наиболее эффективны сообщения, имеющие образную форму и даже кажущиеся бессмысленными, но способные непосредственно обращаться к подсознательному уровню человеческой психики.

Как показывает практика, за счет сочетания ярких, красочных образов, эмоциональных комментариев и т. п. сообщения суггестора способны достигать бессознательных уровней психики без какого-либо адекватного рационального осмысления, вызывая при этом определенные чувства и поведенческие реакции. Для усиления возможностей внушающего воздействия речевые сообщения могут сопровождаться видеозаписями, движениями, музыкой и т. п.

Гипноз. Внушение может проводиться в состоянии бодрствования или гипнотического сна. Гипноз – *это внушаемый сон.* Существуют различные стадии гипноза, различающиеся по тонусу коры головного мозга, ее активности, глубине транса.

Само слово «гипноз» появилось в середине XIX века, но состояния, которые оно обозначает, наблюдались еще у истоков цивилизации. Уже в те времена использование данного состояния было связано как с лечебным эффектом и появлением, в частности, *«чудесных исцелений»*, так и с попытками поставить его на службу личным и кастовым интересам отдельных групп людей, особенно служителей религиозных культов.

> В одном древнем папирусе, который египтологи рассматривают как копию с еще более раннего утерянного текста, есть следующая запись: «Принеси опрятную и очищенную лампу, наполни ее лучшим ароматным маслом и повесь ее на клин из куска лаврового дерева на стене, расположенной с внутренней стороны. Затем поставь перед ней мальчика. Погрузи его в сон твоей рукой и зажги лампу. Произнеси над ним слова заклинаний до семи раз. Снова разбуди его и спроси так: «Что видел ты?» Ответит он: «Да! Я видел богов вокруг лампы». Тогда будут говорить ему боги все, о чем их будут спрашивать».

Налицо описание одного из вариантов гипнотического навязывания человеку определенных представлений и попытки управления его мыслями через эти представления.

В современной практике гипноз широко используется в медицине, педагогике, спорте, промышленности, искусстве и других сферах человеческой деятельности:

как *метод лечения*, прежде всего психических расстройств;

как *метод извлечения* «забытой» информации;

как *метод программирования психики и управления человеком* через скрытое навязывание ему определенных представлений, намерений, моделей поведения.

Не менее вероятно его использование в преступных целях, а также для решения определенных задач в ходе любого *информационного противостояния*. Гипноз особенно привлекателен для разного рода манипуляторов и мошенников. Он позволяет отключить разум и критическое мышление, быстро, без использования каких-либо аргументов записывать в мозг человека определенную информацию, закладывать те или иные эмоционально-поведенческие установки и таким образом предопределять его будущее поведение.

Эффективность гипноза, как и любого внушения, прежде всего зависит от психологических особенностей пациента, его состояния в данный момент, а также от личных возможностей и умения гипнотизера.

В современной психотерапии различают две группы *методов введения в гипноз* как в особое состояние сознания:

методы многократно повторяющегося воздействия монотонными раздражителями на различные анализаторы (органы чувств);

шоковые методы, при которых особое состояние сознания вызывается внезапным действием сильного раздражителя (вспышка света, сильный звук, слабый удар электрического тока), сопровождаемого категорическим приказом (например, «Спать!»).

Издавна для введения людей в *транс* (слабая форма гипноза) используется *музыка*. Звукоритмическое воздействие лежит в основе любой религиозно-мистической системы. У древних и современных народов бой барабанов, ритмичные танцы и песнопения являются средством введения людей в транс и повышения эффективности сопутствующего словесного внушения.

Многие специалисты причисляют ритмичную музыку, телевизионные передачи, чтение «массовой» литературы к числу приемов, обеспечивающих в определенной степени гипнотизацию населения.

По словам профессора МГУ В. П. Пугачева, наиболее простая технология телевизионного программирования может выглядеть примерно так. Человек удобно устраивается в кресле и расслабляется. Расслаблению способствуют специальные яркие мерцающие точки или другие фигуры на экране, притягивающие внима-

ние. Сосредоточение внимания на них способствует вхождению индивида в транс. Затем привлекательную точку сменяет быстрое мелькание различных сюжетов и картинок. Человек не может ухватить их смысл, поэтому левое полушарие и связанное с ним сознание на какое-то время отключаются. В результате открывается прямой путь к воздействию на подсознание. Обработанный таким образом человек может внезапно почувствовать (вопреки привычным рациональным оценкам) симпатию или даже любовь к одним людям и презрение к другим. Вложив в подсознание нужное представление, телезрителя тотчас серией новых ярких вспышек выводят из состояния полузабытья. На пробужденное сознание снова воздействуют более крупной дозой информации, которая почти беспрепятственно проникает в человеческий мозг и память, находящиеся еще в постгипнотическом состоянии.

В современном информационном обществе в связи с расширением возможностей средств массовой информации и активизацией манипуляционных тенденций массовый гипноз в легких и средних формах буквально пронизывает нашу повседневную жизнь. Сегодня все мы – как бы в полузабытьи. И порою нам очень трудно, спустя время, логически объяснить свои действия, например, при совершении покупок в магазине, голосовании в ходе выборов, или «свои» суждения по тем или иным событиям в стране и мире.

Опасной тенденцией XX века стала практика массового гипнотизирования людей в больших аудиториях и даже на стадионах. Как оказалось, внутреннее состояние человека, обусловленное неопределенностями и тревогами жизни, делает его не менее восприимчивым к внушению и гипнозу, чем пациента специальной клиники.

Средства манипуляции человеком

К числу средств, используемых при реализации вышерассмотренных методов манипуляции человеческим сознанием, можно отнести:

средства массовой информации (радио, пресса, телевидение, Интернет);

агитационно-пропагандистские и учебные материалы (видеокассеты, электронные и печатные учебники, энциклопедии, наглядные пособия, рекламную продукцию и др.);

произведения литературы (художественной, научно-технической, общественно-политической, публицистической, специальной) и искусства (в том числе различных направлений массовой культуры);

энергоинформационные средства (специальные генераторы, передающие устройства и излучатели электромагнитных волн и импульсов, радиоэлектронные приборы и др.);

лингвистические средства (языковые единицы, «специальную» терминологию, обороты речи, имеющие семантическую неоднозначность при переводе на другие языки и др.);

психотропные средства (особым образом структурированные лекарства, психофармакологические и психодислептические препараты, транквилизаторы, антидепрессанты, галлюциногены, наркотики, алкоголь и др.);

личное индивидуальное и групповое общение (учебное, профессиональное, деловое, семейное, повседневное и др.).

Рассмотрим, к примеру, ***литературу***. В России она всегда была важнейшим средством духовно го и нравственного воспитания подрастающих поколений, приобщения молодежи к возвышенным мыслям и романтике. Увы, и литература не избежала пагубных тенденций и используется разными силами как средство манипуляции сознанием людей. Немало сюжетов используется для скрытой атаки на историю и самосознание народов России. Не случайно В. В. Путин на встрече с преподавателями истории в июне 2007 г. сказал, что у нас великая и успешная история и нельзя навязывать народу чувство вины.

Содержание некоторых изданий больше определяется поговоркой: «Бумага все стерпит». Книжный рынок заполнен произведениями, кодирующими читателя на либерально-потребительский, свободный от социальных обязанностей стиль жизни. За яркими обложками можно найти скрытую пропаганду наркотического «расширения» сознания, изобилие неформальной лексики, порнографические сцены, смакование актов насилия, рекламу товарных брендов, алкоголя и табака. Прямо или косвенно такой информацией наполнены многие романы, детективы, новомодные исторические творения, утратившая элементы научности фантастика. Детские книжки, издаваемые по мотивам известных романов и сказок, содержат картинки из иностранных мультипликационных фильмов, искажающие сами произведения.

Широко рекламируемые так называемые бестселлеры о жизни Гарри Поттера и других популярных «героев» полны элементов мистики, сатанизма, ксенофобии, жестокости, отрыва от реально-

сти, искаженных представлений о подлинных ценностях. Мы считаем, что так готовится искусственная почва для программируемого дельцами массового сбыта товаров (мантий, «волшебных палочек», колпачков, мечей и прочей магической атрибутики на миллиарды долларов), которые никогда не попали бы на прилавок без подобных произведений. Чем не НЛП и зомбирование наивных ребятишек и их родителей на тотальное приобретение изделий из дешевой бумаги, тканей и прочих материалов по сверхценам?

Ряд наиболее действенных манипуляционных средств, в частности, средства массовой информации, энергоинформационные, психотропные и лингвистические средства, рассмотрены ниже в отдельных разделах.

Некоторые защитные приемы и методы

Для защиты от манипулирования необходимо знать не только его методы и средства, но и ряд общих условий, расширяющих возможности воздействия на психику человека.

Обработка человека всегда начинается с ослабления или отключения его способности сопротивляться. Это – первый этап и главнейшая задача для любого манипуляционного метода: и для НЛП, и для дианетики, и для гипноза. Выведи из состояния равновесия, выключи привычные формы внутреннего контроля – и ты можешь делать с психикой человека все, что пожелаешь. На данном этапе могут использоваться самые разные приемы и эффекты, помогающие удивить, поразить, «сбить с толку» человека. Вполне годится здесь и скрытое энергоинформационное воздействие или легкое наркотическое опьянение, маскируемое обрядовыми напитками, благовониями. Главное – заморочить человеку голову настолько, чтобы он разрешил себе измениться.

Этот принцип далеко не нов. Его знали еще христианские миссионеры средних веков. Огромные храмы, органная музыка, изобилие цветов. Первая цель состояла в том, чтобы нарушить душевное равновесие и внутренний покой человека, обеспокоить его, ослабить существующие стереотипы и шаблоны представлений. В таком состоянии человек теряет привычную ориентацию внутри себя и в окружающем мире, после чего готов прислушаться к любому мнению, принять любую, кажущуюся спасительной установку.

И сегодня человек, находящийся в состоянии удивления, восхищения, внутреннего распутья или возмущения – самая удобная жертва не только для гипнотизеров, специалистов НЛП и дианетики, но и для религиозных сектантов и политических демагогов.

Еще одно важное условие, на которое следует обращать внимание, связано с *речью манипулятора*. Мы, разумные, привыкли в любой речи прежде всего улавливать ее логику и смысл. Однако в большинстве методов на нас скрытно воздействуют интонации, жесты, позы, мимика, движения рук и выражения глаз, эмоциональные переходы и т. п. Именно эти эффекты адресованы нашему подсознанию, которое, как известно, обычно побеждает сознание. И устоять против такого воздействия (вспомним автора «Властелина колец») может «только твердейшая воля и устремленная мысль», разумная установка на «спасительное недоверие» к обещаниям счастья и богатства.

Метод самовнушения. Если манипуляции подвержен психологически издерганный человек, то защитой от нее будет своевременное улучшение и, по возможности, постоянное поддержание хорошего психического самочувствия. Сегодня самовнушение, медитация является одним из основных методов внутренней саморегуляции и восстановления психического равновесия. Человек, использующий данный метод, должен сформировать индивидуальное словесное утверждение, направленное на регуляцию собственного состояния. Формулировки должны быть простыми, утвердительными, позитивно окрашенными: «Мой страх (моя наивность) полностью исчезает»; «Я спокоен, уравновешен, способен анализировать ситуацию»; «Мой организм способен вырабатывать вещества, которые помогут сохранить спокойствие и увидеть ложь, нечестные помыслы мошенника» и т. п. Словесные формулировки наиболее эффективны при мысленном проговаривании в ходе воздействия манипулятора.

Формулы самовнушения должны быть краткими, уверенными и иметь по возможности позитивный характер. Мысленное проговаривание слов осуществляется в медленном темпе, в такт дыханию. Делать это лучше на естественном выдохе. Если формула состоит из двух слов, то при выдохе произносится одно слово, а при вдохе другое. Словесные формулировки необходимо хорошо запомнить, тогда во время психорегулирующих тренировок не придется отвлекаться и задумываться об их последовательности. Если в процессе

упражнений самовнушения возникают какие-то помехи (например, шум), то формулы рекомендуется проговаривать скороговоркой. Это повышает концентрацию, хотя эффективность самовнушения при этом несколько снижается. Рекомендуется проводить самовнушение в одинаковой позе – это способствует усилению его эффекта. Установлено также, что рифмованные, ритмические словесные формулы (даже если они не блещут оригинальностью) приводят к их быстрому запоминанию и усваиваются легче. Словесные формулы самовнушения каждый может составить для себя самостоятельно.

Аутогенная тренировка. Методика аутогенной тренировки (АТ) разработана немецким психотерапевтом И. Г. Шультцем в начале XX века. Он поставил перед собой задачу – соединить в одной методике эффективность лечебного действия гипноза с возможностью его самостоятельного использования пациентом.

К настоящему времени выявлены два главных эффекта, которые дает АТ или ее модификации: снятие эмоционального напряжения (успокоение) и ускорение восстановительных процессов различных уровней (восстановление). Эти эффекты обусловливают целесообразность использования АТ в широком спектре жизненных ситуаций: переутомление, неврастенические расстройства, эмоциональная напряженность и т. д. На физиологическом уровне АТ является профилактикой сердечно-сосудистых заболеваний и дисфункции пищеварительного тракта.

Успокоение и восстановление обеспечиваются постепенным формированием способности произвольно вызывать у себя *релаксационное действие*. Релаксация вызывается путем формирования установки на покой и отдых: проговариванием определенных словесных формул, управлением вниманием и образными представлениями. У большинства после сеансов АТ улучшается самочувствие и повышается работоспособность, появляются уверенность в себе и чувство безопасности. Для полного овладения АТ желательно пройти обучение.

Отказ от контактов. Лучше всего избегать гипнотизеров, быстро уходить от учителей НЛП и дианетики. Они – специалисты в своей области, и трудно даже решительному человеку их переговорить и тем более переубедить. А они между тем очень привязчивы и настойчивы в общении. Авторам известно немало случаев, когда

самоуверенные молодые офицеры, самонадеянно считавшие, что не попадутся на «крючок» цыганкам, каталам, лохотронщикам, – оставались без денег.

Не раз случалось и такое: идет девушка или юноша по улице, видит книжный прилавок, на котором выставлены книги с крупными заголовками: «Дианетика» или «Л. Р. Хаббард»; от прилавка отделяется молодой человек или девушка, улыбается и приветливо здоровается:

«Добрый день! Как ваше настроение?» – продолжает улыбаться собеседник.

«Вот вы пробегаете мимо, – мягко укоряет хаббардист, – а между прочим, в нашем центре работают бесплатные психотерапевты, социологи, медики, которые с удовольствием помогут вам добиться успехов в жизни, чтобы настроение всегда было не просто «нормальным», а прекрасным». Как тут устоять?

Другой вариант. К руководителю предприятия приходит солидный человек, представляется высококвалифицированным менеджером и предлагает резко повысить рентабельность производства без крупных капиталовложений. Нетрудно догадаться, что для этого всем работникам необходимо пройти курс обучения по методике Хаббарда.

Добиваясь влияния на возможно большее количество сотрудников административного аппарата и бухгалтерии, пользуясь доброжелательным отношением или наивностью руководителей, манипуляторы исподволь прибирают к своим рукам право распоряжаться имуществом и деньгами фирмы, а когда хозяева наконец спохватываются, избавиться от хаббардистов становится крайне трудно.

Поэтому, лучше всего обходить стороной представителей дианетики и НЛП, уличных гипнотизеров, гадалок и прочих мошенников. Если уж общение оказалось неизбежным, то психологи советуют, прежде всего, не смотреть им в глаза. Лучше быть невежливым, чем обманутым. Можно отреагировать на попытки внушения чем-либо неожиданным – смехом, прибауткой, поговоркой. Такой реакцией любой гипнотизер будет обескуражен. В случае прямых угроз следует немедленно обращаться в правоохранительные органы, причем сразу в несколько мест: в отделение милиции, в прокуратуру, в УБОП. Учитывая опыт и образ действия хаббардистов, можно нарваться на их ставленника, но сайентологи не могут обосноваться сразу везде.