Серия «Высшее образование»

В. В. Гафнер

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Рекомендовано
Государственным образовательным учреждением
высшего профессионального образования
«Московский педагогический государственный университет»
в качестве учебного пособия для студентов
высших учебных заведений, обучающихся по специальности
050104.65 «Безопасность жизнедеятельности»
Регистрационный номер рецензии МГУП 637 от 08.12.09

Ростов-на-Дону
«ФЕНИКС»
2010

УДК 004.05(075.8)
ББК 32.973-018.2я73
КТК 216
Г24

Рецензенты:

Репин Ю. В., кандидат педагогических наук, профессор, заведующий кафедрой безопасности жизнедеятельности, декан факультета безопасности жизнедеятельности Уральского государственного педагогического университета

Сапронов В. В., кандидат технических наук, профессор Московского государственного университета культуры и искусств, директор Института безопасности жизнедеятельности (сфера образования) Фонда национальной и международной безопасности

Чеурин Г. С., научный руководитель муниципального образовательного учреждения «Центр экологического выживания и безопасности» (г. Екатеринбург), руководитель учебного центра по предотвращению социальных и природных чрезвычайных ситуаций ООО «ТМО «ИТАЛЛ», руководитель молодёжной учебно-оздоровительной экспедиции «Сибирский путь», действительный член географического общества России, почетный полярник

Гафнер В. В.

Г24 Информационная безопасность : учеб. пособие / В.В. Гафнер. — Ростов н/Д : Феникс, 2010. — 324 с. — (Высшее образование).

ISBN 978-5-222-17389-3

Учебное пособие «Информационная безопасность» предназначено для студентов педагогических ВУЗов, обучающихся по специальности 050104.65 «Безопасность жизнедеятельности». В пособии рассматриваются теоретические и практические аспекты обеспечения информационной безопасности в мирное и военное время, а также в условиях чрезвычайных ситуаций. Значительное место уделяется социальным аспектам информационной безопасности, влиянию информации на жизнь и деятельность людей.

УДК 004.05(075.8)
ББК 32.973-018.2я73

ISBN 978-5-222-17389-3

© Гафнер В.В., 2010
© Оформление: ООО «Феникс», 2010

ОГЛАВЛЕНИЕ

Введение ……..……... 8

ГЛАВА 1. Значение информации в современном мире и образовании …….. 10

1.1. Понятие информации и информационной безопасности …… 10

Понятие информации
Виды и свойства информации
Структура информационного процесса
Понятие информационной безопасности
Информационные опасности и угрозы
Принципы обеспечения информационной безопасности

1.2. Окружающая среда как источник информации …... 31

Восприятие информации человеком
Особенности восприятия окружающей среды человеком
Перенасыщенная информацией среда
Энергоинформационные свойства воды

1.3. Роль информации в развитии общества …….. 41

Информационные революции
Информационное общество
Проблема информационного неравенства
Россия в информационной эпохе

1.4. Образование в информационном обществе …… 53

Особенности обучения в информационном обществе
Компетентность педагога в информационном обществе
Информационная пассивность педагога

Вопросы для самоконтроля ……... 58

ГЛАВА 2. Основы правового обеспечения информационной безопасности ……. 60

2.1. Информация как объект правового регулирования …….. 60

Информационные правоотношения
Понятие и виды информации, защищаемой законодательством РФ

2.2. Защита государственной тайны …… 64

Государственная тайна как особый вид защищаемой информации

Ущерб от утечки сведений, составляющих государственную тайну
Система защиты государственной тайны
Способы защиты государственной тайны
Режим секретности
2.3. Конфиденциальная информация и её защита …… 82
Коммерческая тайна
Служебная тайна
Профессиональные тайны
Персональные данные
2.4. Защита интеллектуальной собственности ……..... 93
Международное право в сфере защиты информации
Защита авторских и смежных прав в законодательстве РФ
Объекты авторского права
Субъекты авторского права
Права обладателей авторских прав

Вопросы для самоконтроля ……... 107

ГЛАВА 3. Обеспечение информационной безопасности РФ …… 108
3.1. Информационная безопасность РФ ……..... 108
Доктрина информационной безопасности РФ
Национальные интересы РФ в информационной сфере
Виды угроз информационной безопасности РФ
Источники угроз информационной безопасности РФ
Основные цели и задачи обеспечения информационной безопасности РФ
Объекты информационной безопасности РФ
3.2. Правовое обеспечение информационной безопасности РФ …… 119
3.3. Государственная политика обеспечения информационной безопасности РФ ……. 123
Основные положения государственной политики обеспечения информационной безопасности РФ
Основные положения государственной политики обеспечения информационной безопасности субъектов РФ
3.4. Государственная система защиты информации РФ…... 128
Задачи системы защиты информации РФ
Структура государственной системы защиты информации РФ
3.5. Международное сотрудничество РФ в области обеспечения информационной безопасности ……. 133

3.6. Русский язык как объект национальной безопасности РФ ……..... 135

Вопросы для самоконтроля …….. 139

ГЛАВА 4. Информационная безопасность человека …... 141
4.1. Неприкосновенность частной жизни граждан …... 141
Угрозы неприкосновенности частной жизни граждан
Кодекс справедливого использования информации
4.2. Влияние средств массовой информации на человека.... 145
Методы влияния СМИ на человеческое сознание
Влияние телевидения на детей
Влияние просмотра сцен насилия по телевидению на поведение человека
4.3. Влияние рекламы на человека ……..... 164
Понятие рекламы
Влияние рекламы на детей
Особенности рекламы для детей в различных странах
Приемы рекламного воздействия
Реклама нездорового образа жизни
4.4. Интернет и безопасность детей ……..... 176
Опасности сети Интернет
Интернет-зависимость в подростковой среде
4.5. Жестокие компьютерные игры …… 180
Опасность жестоких компьютерных игр
Влияние жестоких компьютерных игр на поведение человека

Вопросы для самоконтроля ……... 185

ГЛАВА 5. Информационная безопасность человека в чрезвычайных ситуациях ……. 186
5.1. Слухи как неформальный обмен информацией…. 186
Слухи как социально-психологический феномен
Определение слуха
Классификация слухов
Причины возникновения и механизмы распространения слухов
Управление слухами
Особенности распространения слухов в чрезвычайных ситуациях
Распространение слухов через Интернет на примере теракта в США 11 сентября 2001 года

5.2. Принятие решений в чрезвычайных ситуациях…. 210
Принятие решения
Виды решений
Этапы принятия решения
Особенности индивидуального и группового принятия решений

Вопросы для самоконтроля ……... 220

ГЛАВА 6. Информационная преступность …… 221
6.1. Информационные преступления в интеллектуальной сфере ……. 221
6.2. Информационные преступления против личности …… 222
6.3. Компьютерные преступления ……... 223
Особенности компьютерных преступлений
Уголовно-правовая характеристика компьютерных преступлений
Криминалистическая характеристика компьютерных преступлений
Предотвращение и раскрытие компьютерных преступлений

Вопросы для самоконтроля …… 233

ГЛАВА 7. Методы и средства защиты информации…. 234

7.1. Технологии идентификации человека ……. 235
Технологии идентификации человека в истории
Идентификация по фотографии
Идентификация по отпечаткам пальцев
Идентификация по ДНК
Компьютерная биометрия
Уязвимость биометрических систем
7.2. Применение паролей в механизме аутентификации человека …… 241
Классификация паролей
Правила создания паролей
7.3. Информационная безопасность компании ……..... 244
Человеческий фактор в обеспечении информационной безопасности компании
Система информационной безопасности компании
Безопасное использование Интернет-ресурсов в компании

Вопросы для самоконтроля …….. 252

ГЛАВА 8. Информационные и психологические войны …… 253
8.1. Информационная война ……. 253
Понятие информационной войны
Информационное оружие
Информационная атака
Стратегическое информационное противоборство
8.2. Психологическая война …….. 265
Понятие психологической войны
Цели психологической войны
Психологическая война в истории человечества
Использование пропаганды во второй мировой войне
Психологическая операция
Виды психологического воздействия
Средства психологического воздействия
Инструментарий психологических операций
Вопросы для самоконтроля …….. 290

Список литературы …… 291

Приложения ……..... 298
Приложение 1. Видеоэкология ……..... 298
Приложение 2. Улучшение визуальной среды обитания……. 301
Приложение 3. Правила пользования Интернетом (рекомендации для родителей) …… 302
Приложение 4. Снижение телеагрессии у детей …….. 303
Приложение 5. Гигиенические требования к просмотру телепередач 304
Приложение 6. Основы грамотного восприятия средств массовой информации ребёнком…… 305
Приложение 7. Основы критического восприятия рекламы ребёнком 310
Приложение 8. Свод правил по защите персональной информации 312
Приложение 9. Видеоигры как средство информационно-психологической войны…… 314
Приложение 10. Кино как средство информационно-психологической войны…… 317

Словарь основных терминов …… 319

ВВЕДЕНИЕ

Учебная дисциплина «Информационная безопасность» включает в себя теоретические и практические аспекты обеспечения информационной безопасности в мирное и военное время, а также в условиях чрезвычайных ситуаций. Основная цель этой дисциплины заключается в формировании системы знаний об информационной безопасности личности, организации, общества, государства и основных мерах по её обеспечению. Дисциплина носит междисциплинарный характер и тесно связана с другими дисциплинами специальности «Безопасность жизнедеятельности»: теоретические основы безопасности человека, основы национальной безопасности, правовое регулирование и органы обеспечения безопасности жизнедеятельности, опасности социального характера и защита от них, криминальные опасности и защита от них, психологические основы безопасности.

Учебное пособие подготовлено в соответствии с положениями Государственного образовательного стандарта высшего профессионального образования по специальности «050104.65 – Безопасность жизнедеятельности», дисциплина ДПП. Ф16. «Информационная безопасность» (федеральный компонент).

Предполагается, что в результате изучения этой дисциплины студенты получат знания:

– о понятиях информационной безопасности;

– о видах и источниках опасностей и угроз в сфере информационных процессов и систем;

– о нормативных актах, обеспечивающих информационную безопасность;

– об основах государственной политики обеспечения информационной безопасности;

– о методах и средствах обеспечения информационной безопасности в мирное и военное время, а также в условиях чрезвычайных ситуаций;

– о методах и средствах ведения современной информационно-психологической войны.

Успешно изучившие данную дисциплину будут уметь:

– защищаться от негативного информационного воздействия;

– принимать решения на основе анализа и оценки информации;

– применять полученные знания в самостоятельной педагогической деятельности;

– формировать у учащихся знания и умения в области информационной безопасности.

Отличие настоящего учебного пособия от имеющейся учебной литературы по информационной безопасности заключается в том, что его основное содержание посвящено социальным аспектам информационной безопасности, влиянию информации на жизнь и деятельность людей.

В пособии показано значение информации в современном мире и образовании, рассматриваются основы правового обеспечения информационной безопасности, меры по обеспечению информационной безопасности РФ, вопросы обеспечения информационной безопасности человека в повседневной жизни и в чрезвычайных ситуациях, методы и средства защиты информации. Отдельными разделами представлены информационные и психологические войны, а также информационная преступность.

Текст пособия подробно структурирован. Все разделы снабжены соответствующими подзаголовками. В конце пособия приведён словарь основных терминов, содержащий их наиболее употребительные толкования.

ГЛАВА 1. ЗНАЧЕНИЕ ИНФОРМАЦИИ В СОВРЕМЕННОМ МИРЕ И ОБРАЗОВАНИИ

1.1. Понятие информации и информационной безопасности

Понятие информации. Виды и свойства информации. Структура информационного процесса. Понятие информационной безопасности. Информационные опасности и угрозы. Принципы обеспечения информационной безопасности.

Основные термины и понятия:
Данные
Доступность информации
Защита информации
Знания
Информатизация
Информационная безопасность
Информация
Конфиденциальность информации
Целостность информации

Понятие информации

Информация является одним из фундаментальных понятий современности и относится к разряду тех, которые имеют очень широкое употребление. Информационные взаимодействия – это основа существования как живой, так и неживой природы. Без информационных процессов немыслима и социальная жизнь. Информационные технологии представляют собой основу современной и особенно зарождающейся цивилизации – информационного общества.

Термин «информация» происходит от латинского слова «***informatio***», что означает *сведения, разъяснения, изложение*. Обычно под информацией понимаются знания, сведения, данные, сообщения и сигналы, с которыми мы имеем дело в повседневной жизни и проявление которых мы наблюдаем в природе и обществе.

Определение информации, которое содержится в энциклопедическом словаре, говорит о том, что «**информация** – *это общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом,*

обмен сигналами в животном и растительном мире; передачу признаков от клетки к клетке, от организма к организму».

Правовое определение «информации» ввёл Федеральный закон (ФЗ) «Об информации, информатизации и защите информации». В соответствии с ним «**информация** – *это сведения о лицах, предметах, фактах, событиях, процессах независимо от формы их представления*». Позже этот ФЗ утратил силу и его преемником стал ФЗ «Об информации, информационных технологиях и о защите информации». В новом законе интересующее нас определение было немного изменено: «**информация** – *сведения (сообщения, данные) независимо от формы их представления*».

В научной литературе можно встретить десятки попыток дать определение «информации». Многие специалисты признают, что даже достаточно полного, не говоря уж о всеобъемлющем, определения информации дать невозможно, что в каждой научно-прикладной ситуации её определение имеет «своё лицо» и выполняет свои функции.

В философских работах развиваются представления об информации как о некой фундаментальной субстанции, стоящей в одном ряду с материей и энергией, или о том, что информационные взаимодействия – это всего лишь некие формы процессов «отражения», присущих как материальному, так и духовному миру.

В естественных науках под информацией, как правило, понимаются знания об объектах и процессах окружающего нас мира ранее получателю неизвестные. В процессе познания именно информация представляет собой «нечто», что заставляет «подправлять», умножать наши знания. Естественно, что ценность её всегда весьма субъективна и во многом определяется возможностями потребителя, его целями, степенью его восприимчивости и уровнем его познаний.

В наше время существует несколько подходов к определению понятия «информация». В связи с развитием средств связи, телекоммуникаций, вычислительной техники, их использованием для обработки и передачи информации, возникла необходимость измерять её количественные характеристики. Так, в первом подходе различают разные измерения (меры) информации и понятие «информация» может наполняться новым содержанием:

– *техническая мера* – информация, которая передается по телеграфным линиям и отображается на экранах радиолокато-

ров. Количество такой информации может быть точно вычислено, и процессы, происходящие с такой информацией, подчиняются физическим законам. По сути, при таком измерении информация отождествляется с данными;

– *семантическая*, т.е. смысловая, мера – та информация, которая содержится, к примеру, в литературном произведении. По существу, при таком подходе информация отождествляется со сведениями и фактами.

Другой подход состоит в том, что информация – это характеристика, такая же, как, например, энергия или масса в физике. Определенным образом и в определенных условиях информация равным образом описывает как процессы, происходящие в естественных физических системах, так и процессы, происходящие в искусственно созданных системах.

Сторонники третьего подхода считают, что информация как объект едина, но количественные оценки могут быть разными. Отдельно следует вводить количество информации − строгую оценку, для которой можно развивать единую формальную теорию. Кроме количества информации следует оценивать ещё и качественные её показатели, которые в конечном итоге определяют ценность информации: достоверность, актуальность, надёжность.

Учитывая сказанное выше, остановимся на следующем определении:

Информация – *сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии, которые воспринимают информационные системы (живые организмы, управляющие машины и др.) в процессе жизнедеятельности и работы.*

Информация может существовать в виде текстов, рисунков, чертежей, фотографий, световых или звуковых сигналов, радиоволн, электрических и нервных импульсов, магнитных записей, жестов и мимики, запахов и вкусовых ощущений, хромосом, посредством которых передаются по наследству признаки и свойства организмов, и т.д.

На практике часто отождествляются определения таких понятий, как «информация», «данные», «знания». Однако эти понятия необходимо различать.

Данные – *фиксируемые в виде определенных сигналов воспринимаемые факты окружающего мира.*

Данные несут в себе сведения о событиях, произошедших в материальном мире, и являются регистрацией сигналов, возникших в результате этих событий. Однако данные не тождественны информации. Станут ли данные информацией – зависит от того, известен ли метод преобразования данных в известные понятия.

Например, мы можем услышать речь обращающегося к нам человека, говорящего на иностранном и незнакомом нам языке. С одной стороны, мы получили от него данные в виде звуков, но с другой – никакой информации от него мы получить не смогли, т.к. не сумели понять передаваемые нам данные. Они для нас были закодированы, а метода раскодирования мы не знали.

Знание – *форма существования и систематизации результатов человека.*

Информацию человек может получать откуда угодно, а знания приходят тогда, когда человек использует эту информацию и сочетает ее со своим собственным опытом. Информация становится знанием, когда она переработана и проанализирована человеческим мозгом. Знание существует только благодаря людям. Знание – это осознание, понимание и толкование определенной информации с учетом путей наилучшего ее использования для достижения конкретных целей. Знания должны иметь структуру, связь между собой, а не быть хаотичными. Очень важно постоянно их использовать и пополнять.

Выделяют различные виды знания: научное, обыденное (здравый смысл), интуитивное, религиозное и др. Обыденное знание служит основой ориентации человека в окружающем мире, основой его повседневного поведения и предвидения, но обычно содержит ошибки, противоречия. Научному знанию присущи логическая обоснованность, доказательность,

воспроизводимость результатов, проверяемость, стремление к устранению ошибок и преодолению противоречий.

Можно сделать вывод, что фиксируемые воспринимаемые факты окружающего мира представляют собой данные. При использовании данных в процессе решения конкретных задач – появляется информация. Результаты решения задач, истинная, проверенная информация (сведения), обобщенная в виде законов, теорий, совокупностей взглядов и понятий представляют собой знания.

Виды и свойства информации

Информацию можно упорядочить по ряду признаков, т.е. провести ее классификацию. В связи с этим, информация может быть классифицирована следующим образом:

1. По способам восприятия:

Визуальная

Аудиальная

Тактильная

Обонятельная

Вкусовая

2. По форме представления:

Буквенная

Цифровая

Графическая

Кодированная

Комбинированная

3. По форме передачи:

Вербальная (словесная, звуковая)

Невербальная (представленная на определенном носителе: бумаге, дискете и т.д.)

Письменная

Печатная

Телефонная

Электронная

Спутниковая и т.д.

4. По назначению:

Экономическая

Техническая

Социальная

Организационная и т.д.

5. По общественному значению:

5.1. Массовая

Обыденная

Общественно-политическая

Эстетическая

5.2.Личная

Знания

Интуиция

5.3. Специальная

Научная

Производственная

Техническая

Управленческая

6. По изменчивости во времени:

Условно-постоянная (например, место жительства человека)

Условно-переменная (например, последовательность календарных месяцев)

Постоянная (например, дата рождения человека)

Переменная

7. По режиму передачи от одного потребителя информации другому:

В произвольные сроки

По запросу

Принудительно в определенные сроки.

Как и всякий объект, информация обладает **свойствами**. Информация отличается от других объектов природы и общества характерной особенностью: на свойства информации влияют как свойства исходных данных, составляющих ее содержательную часть, так и свойства методов, фиксирующих эту информацию.

Можно выделить 3 группы свойств информации:

1. Атрибутивные свойства – свойства, без которых информация не существует.

2. Прагматические свойства – свойства, которые характеризуют степень полезности информации для пользователя, потребителя и практики.

3. Динамические свойства – свойства, которые характеризуют изменение информации во времени.

Рассмотрим подробнее указанные группы свойств информации.

Атрибутивные свойства информации.

Дискретность. Информацию характеризуют отдельные фактические данные, закономерности и свойства изучаемых объектов, которые распространяются в виде различных сообщений, состоящих из линии, составного цвета, буквы, цифры, символа, знака.

Неотрывность информации от физического носителя и языковая природа информации. Однако информация не связана жестко ни с конкретным языком, ни с конкретным носителем.

Непрерывность. Информация имеет свойство сливаться с уже зафиксированной и накопленной ранее, тем самым способствуя поступательному развитию и накоплению.

Передаваемость информации с помощью каналов связи (в том числе с помехами) хорошо исследована в рамках теории информации К. Шеннона. В данном случае имеется в виду несколько иной аспект: способность информации к копированию, т.е. к тому, что она может быть «запомнена» другой системой и при этом останется тождественной самой себе. Очевидно, что количество информации не должно возрастать при копировании.

Воспроизводимость информации тесно связана с ее передаваемостью и не является ее независимым базовым свойством. Если передаваемость означает, что не следует считать существенными пространственные отношения между частями системы, между которыми передается информация, то воспроизводимость характеризует неиссякаемость и неистощимость информации, т.е. при копировании информация остается тождественной самой себе.

Преобразуемость – фундаментальное свойство информации. Оно означает, что информация может менять способ и форму своего существования.

Копируемость есть разновидность преобразования информации, при котором ее количество не меняется. В общем случае количество информации в процессах преобразования меняется, но возрастать не может.

Прагматические свойства информации.

Адекватность – степень соответствия реальному объективному состоянию дела. Неадекватная информация может образовываться при создании новой информации на основе неполных

или недостоверных данных. Однако и полные, и достоверные данные могут приводить к созданию неадекватной информации в случае применения к ним неадекватных методов.

Актуальность – степень соответствия информации текущему моменту времени. Актуальность – важность для настоящего времени, злободневность, насущность. Только вовремя полученная информация может быть полезна.

Доступность – свойство информации, характеризующее возможность ее получения данным потребителем. Отсутствие доступа к данным или соответствующих методов обработки данных приводит к одинаковому результату: информация оказывается недоступной.

Достоверность. Информация достоверна, если она отражает истинное положение дел. Объективная информация всегда достоверна, но достоверная информация может быть как объективной, так и субъективной. Достоверная информация помогает принять нам правильное решение. Недостоверной информация может быть по следующим причинам:

- преднамеренное искажение (дезинформация) или непреднамеренное искажение субъективного свойства;
- искажение в результате воздействия помех («испорченный телефон») и недостаточно точных средств ее фиксации.

Защищенность – свойство, характеризующее невозможность несанкционированного использования или изменения информации.

Объективность и субъективность. Объективный – существующий вне и независимо от человеческого сознания. Информация – это отражение внешнего объективного мира. Информация объективна, если она не зависит от методов ее фиксации, чьего-либо мнения, суждения. Понятие объективности информации является относительным, т.к. методы являются субъективными. Более объективной принято считать ту информацию, в которую методы вносят меньший субъективный элемент. Объективную информацию можно получить с помощью исправных датчиков, измерительных приборов. Отражаясь в сознании конкретного человека, информация перестает быть объективной, т.к., преобразовывается (в большей или меньшей степени) в зависимости от мнения, суждения, опыта, знаний конкретного субъекта. В ходе информационного процесса степень объективности

информации всегда понижается. Это свойство учитывают, например, в правовых дисциплинах, где по-разному обрабатываются показания лиц, непосредственно наблюдавших события или получивших информацию косвенным путем (посредством умозаключений или со слов третьих лиц).

Полезность. Уменьшение неопределенности сведений об объекте. Полезность может быть оценена применительно к нуждам конкретных ее потребителей и оценивается по тем задачам, которые можно решить с ее помощью. Дезинформация расценивается как отрицательные значения полезной информации.

Полнота. Характеризует качество информации и определяет достаточность данных для принятия решений или для создания новых данных на основе имеющихся. Неполная информация может привести к ошибочному выводу или решению.

Релевантность – способность информации соответствовать нуждам (запросам) потребителя.

Смысл и новизна. Информация перемещается в социальных коммуникациях (взаимодействиях потребителей) и выделяется та ее часть, которая нова для потребителя.

Точность информации определяется степенью ее близости к реальному состоянию объекта, процесса, явления и т.п.

Ценность. Ценность информации различна для различных потребителей и пользователей. Самая ценная информация – объективная, достоверная, полная, и актуальная. При этом следует учитывать, что и необъективная, недостоверная информация (например, художественная литература), имеет большую значимость для человека.

Эргономичность – свойство, характеризующее удобство формы или объема информации с точки зрения данного потребителя.

Динамические свойства информации.

Кумулятивность (от лат. *cumulatio* – увеличение, скопление) характеризует накопление и хранение информации.

Рост информации. С течением времени количество информации растет, информация накапливается, происходит ее систематизация, оценка и обобщение.

Старение. Информация подвержена влиянию времени. Старение информации заключается в уменьшении ее ценности с течением времени. Старит информацию не само время, а появление новой информации, которая уточняет, дополняет или

отвергает полностью или частично более раннюю. Научно-техническая информация стареет быстрее, эстетическая (произведения искусства) – медленнее.

Стираемость. Это свойство связано с таким преобразованием информации (передачей), при котором ее количество уменьшается и становится равным нулю.

Запоминаемость. С запоминаемой информацией мы имеем дело в реальной практике.

Структура информационного процесса

Те предметы или устройства, от которых человек может получить информацию, называют **источниками** информации.

Те предметы или устройства, которые могут получать информацию, называют **приёмниками** информации.

При переносе информации в виде сигнала от источника к приёмнику (потребителю) она проходит последовательно следующие фазы (говорят – фазы обращения), составляющие информационный процесс:

1. Восприятие (если фаза реализуется технической системой) или сбор (если фаза реализуется человеком) – осуществляет отображение источника информации в сигнал. Здесь определяются качественные и количественные характеристики источника, существенные для решения задач потребителя информации, для чего и собирается или воспринимается информация. Совокупность этих характеристик создает образ источника, который фиксируется в виде сигнала на носителе той или иной природы (бумажном, электронном и т.п.).

2. Передача – перенос информации в виде сигнала в пространстве посредством физических сред любой природы. Включается в информационный процесс, если места выполнения других фаз информационного процесса территориально разобщены.

3. Обработка – любое преобразование информации с целью решения определенных функциональных задач (они определяются потребителем информации). Данная фаза может включать хранение информации как перенос ее во времени.

4. Представление (если потребителем информации является человек) или воздействие (если потребителем является техническая система). В первом случае выполняется подготовка информации к виду, удобному для потребителя (графики, тексты,

диаграммы, таблицы и т.д.). Во втором случае вырабатываются управляющие воздействия на технические средства.

Понятие информационной безопасности

В повседневной жизни часто информационная безопасность (ИБ) понимается лишь как необходимость борьбы с утечкой секретной и распространением ложной и враждебной информации. Однако это понимание очень узкое. Существует много разных определений информационной безопасности, в которых высвечиваются отдельные её свойства.

В утратившем силу ФЗ «Об информации, информатизации и защите информации» под **информационной безопасностью** понималось *состояние защищённости информационной среды общества, обеспечивающее её формирование и развитие в интересах граждан, организаций и государства*.

В других источниках приводятся следующие определения:

Информационная безопасность – это

1) *комплекс организационно-технических мероприятий, обеспечивающих целостность данных и конфиденциальность информации в сочетании с её доступностью для всех авторизованных пользователей*;

2) *показатель, отражающий статус защищенности информационной системы;*

3) *состояние защищённости информационной среды*;

4) *состояние, обеспечивающее защищенность информационных ресурсов и каналов, а также доступа к источникам информации.*

В. И. Ярочкин считает, что **информационная безопасность** есть *состояние защищённости информационных ресурсов, технологии их формирования и использования, а также прав субъектов информационной деятельности*.

Достаточно полное определение дают В. Бетелин и В. Галатенко, которые полагают, что

Информационная безопасность – *защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры.*

В данном пособии мы будем опираться на приведённое выше определение.

ИБ не сводится исключительно к защите информации и компьютерной безопасности. Следует различать информационную безопасность от защиты информации.

Защита информации – *деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.*

Иногда под защитой информации понимается создание в ЭВМ и вычислительных системах организованной совокупности средств, методов и мероприятий, предназначенных для предупреждения искажения, уничтожения или несанкционированного использования защищаемой информации.

Международный день защиты информации отмечается 30 ноября с 1988 года. В этот год произошла первая массовая компьютерная эпидемия – эпидемия червя Морриса.

Меры по обеспечению информационной безопасности должны осуществляться в разных сферах – политике, экономике, обороне, а также на различных уровнях – государственном, региональном, организационном и личностном. Поэтому задачи информационной безопасности на уровне государства отличаются от задач, стоящих перед информационной безопасностью на уровне организации.

Субъект информационных отношений может пострадать (понести материальные и/или моральные убытки) не только от несанкционированного доступа к информации, но и от поломки системы, вызвавшей перерыв в работе. ИБ зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал. Поддерживающая инфраструктура имеет

самостоятельную ценность, важность которой переоценить невозможно.

После событий 11 сентября 2001 года в законодательстве США в соответствии с законом «О патриотизме» было определено понятие «критическая инфраструктура», которая понимается как «совокупность физических или виртуальных систем и средств, важных для США в такой мере, что их выход из строя или уничтожение могут привести к губительным последствиям в области обороны, экономики, здравоохранения и безопасности нации». Понятие критической инфраструктуры охватывает такие ключевые области народного хозяйства и экономики США, как национальная оборона, сельское хозяйство, производство пищевых продуктов, гражданская авиация, морской транспорт, автомобильные дороги и мосты, тоннели, дамбы, трубопроводы, водоснабжение, здравоохранение, службы экстренной помощи, органы государственного управления, военное производство, информационные и телекоммуникационные системы и сети, энергетика, транспорт, банковская и финансовая системы, химическая промышленность, почтовая служба.

В социальном плане информационная безопасность предполагает борьбу с информационным «загрязнением» окружающей среды, использованием информации в противоправных и аморальных целях.

Объектом ИБ будет считаться *информация, затрагивающая государственные, служебные, коммерческие, интеллектуальные и личностные интересы, а также средства и инфраструктура её обработки и передачи.*

Также объектами информационного воздействия и, следовательно, информационной безопасности могут быть общественное или индивидуальное сознание.

Общественное сознание – *совокупность идей, взглядов, представлений, существующих в обществе в данный период, в которых отражается социальная действительность.*

На государственном уровне субъектами ИБ являются органы исполнительной, законодательной и судебной власти. В отдельных ведомствах созданы органы, специально занимающиеся информационной безопасностью.

Субъектами ИБ являются *органы и структуры, которые в той или иной мере занимаются ее обеспечением.*

Кроме этого, субъектами ИБ могут быть:

– граждане и общественные объединения;

– средства массовой информации;

– предприятия и организации независимо от формы собственности.

Интересы субъектов ИБ, связанных с использованием информационных систем, можно подразделить на следующие основные категории:

Доступность – возможность за приемлемое время получить требуемую информационную услугу. Информационные системы создаются (приобретаются) для получения определенных информационных услуг (сервисов). Если по тем или иным причинам получение этих услуг пользователями становится невозможным, это наносит ущерб всем субъектам информационных отношений. Особенно ярко ведущая роль доступности проявляется в разного рода системах управления: производством, транспортом и т.п. Поэтому, не противопоставляя доступность остальным аспектам, доступность является важнейшим элементом ИБ.

Целостность – актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения. Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)). Практически все нормативные документы и отечественные разработки относятся к статической целостности, хотя динамический аспект не менее важен. Пример области применения средств контроля динамической целостности – анализ потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Конфиденциальность – защита от несанкционированного ознакомления. На страже конфиденциальности стоят законы, нормативные акты, многолетний опыт соответствующих служб. Аппаратно-программные продукты позволяют закрыть практически все потенциальные каналы утечки информации.

Цель мероприятий в области информационной безопасности – защита интересов субъектов ИБ.

Задачи ИБ:

1. Обеспечение права личности и общества на получение информации.

2. Обеспечение объективной информацией.

3. Борьба с криминальными угрозами в сфере информационных и телекоммуникационных систем, с телефонным терроризмом, отмыванием денег и т.д.

4. Защита личности, организации, общества и государства от информационно-психологических угроз.

5. Формирование имиджа, борьба с клеветой, слухами, дезинформацией.

Роль информационной безопасности возрастает при возникновении экстремальной ситуации, когда любое недостоверное сообщение может привести к усугублению обстановки.

Критерий ИБ – гарантированная защищённость информации от утечки, искажения, утраты или иных форм обесценивания. Безопасные информационные технологии должны обладать способностью к недопущению или нейтрализации воздействия как внешних, так и внутренних угроз информации, содержать в себе адекватные методы и способы её защиты.

Информационные опасности и угрозы

Создание системы ИБ предполагает выявление **источников** информационных опасностей и угроз. Существуют **четыре** действия, производимые с информацией, которые могут содержать в себе угрозу: сбор, модификация (искажение), утечка и уничтожение информации. Эти действия являются базовыми для рассмотрения классификации источников информационных опасностей и угроз.

Рассмотрим внешние и внутренние источники информационных опасностей и угроз.

Источниками **внутренних** угроз являются:

1. Сотрудники организации.
2. Программное обеспечение.
3. Аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

– ошибки пользователей и системных администраторов;

– нарушения сотрудниками фирмы установленных регламентов сбора, обработки, передачи и уничтожения информации;

– ошибки в работе программного обеспечения;

– отказы и сбои в работе компьютерного оборудования.

К **внешним** источникам угроз относятся:

1. Компьютерные вирусы и вредоносные программы.
2. Организации и отдельные лица.
3. Стихийные бедствия.

Формами проявления внешних угроз являются:

– заражение компьютеров вирусами или вредоносными программами;

– несанкционированный доступ к корпоративной информации;

– информационный мониторинг со стороны конкурирующих структур, разведывательных и специальных служб;

– действия государственных структур и служб, сопровождающиеся сбором, модификацией, изъятием и уничтожением информации;

– аварии, пожары, техногенные катастрофы, стихийные бедствия.

Все перечисленные выше виды угроз (формы проявления) можно разделить на **умышленные** и **неумышленные**. По данным Института защиты компьютеров (CSI), свыше 50% вторжений – дело рук собственных сотрудников компаний. Что касается частоты вторжений, то 21% опрошенных указали, что они испытали рецидивы «нападений». Несанкционированное изменение данных было наиболее частой формой нападения и в основном применялось против медицинских и финансовых учреждений. Свыше 50% респондентов рассматривают конкурентов как вероятный источник «нападений». Наибольшее значение респонденты придают фактам подслушивания, проникновения в информационные системы и «нападениям», в которых «злоумышленники» фальсифицируют обратный адрес, чтобы перенацелить

поиски на непричастных лиц. Такими злоумышленниками наиболее часто являются обиженные служащие и конкуренты.

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации: информационные, программные, физические, радиоэлектронные и организационно-правовые.

К **информационным** угрозам относятся:

– несанкционированный доступ к информационным ресурсам;

– незаконное копирование данных в информационных системах;

– хищение информации из библиотек, архивов, банков и баз данных;

– нарушение технологии обработки информации;

– противозаконный сбор и использование информации;

– использование информационного оружия.

К **программным** угрозам относятся:

– использование ошибок и «дыр» в программном обеспечении;

– компьютерные вирусы и вредоносные программы;

– установка «закладных» устройств.

К **физическим** угрозам относятся:

– уничтожение или разрушение средств обработки информации и связи;

– хищение носителей информации;

– хищение программных или аппаратных ключей и средств криптографической защиты данных;

– воздействие на персонал.

К **радиоэлектронным** угрозам относятся:

– внедрение электронных устройств перехвата информации в технические средства и помещения;

– перехват, расшифровка, подмена и уничтожение информации в каналах связи.

К **организационно-правовым** угрозам относятся:

– нарушение требований законодательства и задержка в принятии необходимых нормативно-правовых решений в информационной сфере;

– закупки несовершенных или устаревших информационных технологий и средств информатизации.

Информатизация – *организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.*

Для защиты интересов субъектов информационных отношений необходимо сочетать **меры** следующих уровней:

1) **законодательный уровень** (законы, нормативные акты, стандарты и т.п.). Законодательный уровень является важнейшим для обеспечения информационной безопасности. К мерам этого уровня относится регламентация законом и нормативными актами действий с информацией и оборудованием, и наступление ответственности нарушение правильности таких действий. Подробнее этот вопрос рассматривается в других главах.

2) **административный уровень** (действия общего характера, предпринимаемые руководством организации). Главная цель мер административного уровня – сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел. Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

3) **процедурный уровень** (конкретные меры безопасности, ориентированные на людей).

Меры данного уровня включают в себя:

– мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов систем обработки данных;

– мероприятия по разработке правил доступа пользователей к ресурсам системы (разработка политики безопасности);

– мероприятия, осуществляемые при подборе и подготовке персонала, обслуживающего систему;

– организацию охраны и режима допуска к системе;

– организацию учета, хранения, использования и уничтожения документов и носителей информации;

– распределение реквизитов разграничения доступа;

– организацию явного и скрытого контроля за работой пользователей;

– мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях оборудования и программного обеспечения.

4) **программно-технический уровень** (технические меры).

Меры защиты этого уровня основаны на использовании специальных программ и аппаратуры и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты:

– идентификацию и аутентификацию пользователей;

– разграничение доступа к ресурсам;

– регистрацию событий;

– криптографические преобразования;

– проверку целостности системы;

– проверку отсутствия вредоносных программ;

– программную защиту передаваемой информации и каналов связи;

– защиту системы от наличия и появления нежелательной информации;

– создание физических препятствий на путях проникновения нарушителей;

– мониторинг и сигнализацию соблюдения правильности работы системы;

– создание резервных копий ценной информации.

Принципы обеспечения информационной безопасности

Организация информационной безопасности предполагает разработку определённых **принципов** её обеспечения. Одним из основных является принцип **баланса интересов личности, общества и государства**. Личность заинтересована в конфиденциальности информации об интимной жизни, доходах, социально значимых ошибках и т.д., а общество заинтересовано в получении сведений об антисоциальных проявлениях, коррупции, преступных доходах и т.д.

Принцип **законности и правой обеспеченности**. Рост значимости ИБ явно опережает развитие соответствующей сферы права, чем умело пользуются и политики, и преступники. Средства массовой информации (СМИ) не несут практически никакой ответственности за ложную информацию, направленную на массового потребителя этой информации (читателя, телезрителя).

Принцип **интеграции с международными системами безопасности информации**. Глобализация жизни на планете требует развития международных коммуникаций и их согласованности в обеспечении безопасности передачи информации.

Глобализация – *процесс всемирной экономической, политической и культурной интеграции и унификации.*

Принцип **экономической эффективности**. Этот принцип говорит о том, что результаты от мер ИБ должны превышать совокупные затраты на них. Если этот принцип не соблюдается, то меры по обеспечению секретности информации не только не окупаются, но даже вредят прогрессу.

Принцип **мобильности системы ИБ**. Система ИБ должна не допускать неоправданных режимных ограничений, т.к. одновременно с этим государство утрачивает возможность защищать главное богатство своей страны – способность создавать и генерировать новые знания.

Принцип **презумпции несекретности информации** означает, что строгому нормированию подлежит конфиденциальность, а не гласность.

При разработке и проведении в жизнь политики информационной безопасности в какой-либо организации целесообразно руководствоваться следующими принципами:

– Принцип **невозможности миновать защитные средства** говорит сам за себя и не требует дополнительных пояснений.

– Принцип **усиления самого слабого звена**. Надежность любой обороны определяется самым слабым звеном. Злоумышленник не будет бороться против силы, он предпочтет легкую победу над слабостью. Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения ИБ приобретает нетехнический характер.

– Принцип **невозможности перехода в небезопасное состояние** означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ.

– Принцип **минимизации привилегий** предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей. Назначение этого принципа – уменьшить ущерб от случайных или умышленных некорректных действий пользователей и администраторов.

– Принцип **разделения обязанностей** предполагает такое распределение ролей и ответственности, чтобы один человек не мог нарушить критически важный для организации процесс или создать брешь в защите по заказу злоумышленников.

– Принцип **эшелонированности обороны** предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией – управление доступом и, как последний рубеж, протоколирование и аудит. Эшелонированная оборона способна, по крайней мере, задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

– Принцип **разнообразия защитных средств** рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками (например, умением преодолевать высокую ограду и знанием слабостей нескольких операционных систем).

– Принцип **простоты и управляемости информационной системы**. Залогом информационной безопасности являются не сложность и скрытность, а, напротив, простота и апробированность. Только в простой и управляемой системе можно проверить согласованность конфигурации различных компонентов и осуществить централизованное администрирование.

– Принцип **обеспечения всеобщей поддержки мер безопасности** носит нетехнический характер. Если пользователи и/или системные администраторы считают информационную

безопасность чем-то излишним или даже враждебным, режим безопасности сформировать заведомо не удастся. Следует с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

1.2. Окружающая среда как источник информации

Восприятие информации человеком. Особенности восприятия окружающей среды человеком. Перенасыщенная информацией среда. Энергоинформационные свойства воды.

Основные термины и понятия:
Видеоэкология
Вкус
Зрение
Обоняние
Осязание
Слух
Структурная память воды
Шумовое загрязнение

Восприятие информации человеком

Анализаторы являются специальными структурами организма, служащими для ввода внешней информации в мозг для последующей ее переработки. Человек связан со средой с помощью анализаторов, которые состоят из рецепторов, проводящих нервных путей и мозгового конца в коре головного мозга. Мозговой конец состоит из ядра и рассеянных по коре головного мозга элементов, обеспечивающих нервные связи между отдельными анализаторами. Например, когда человек ест, то он чувствует вкус, запах пищи и ощущает её температуру. Основная характеристика анализаторов – чувствительность.

У человека рецепторы настроены на следующие раздражители:

– электромагнитные колебания светового диапазона – фоторецепторы в сетчатке глаза;

– изменение положения тела относительно вектора гравитации – рецепторы вестибулярного аппарата;

– механические колебания воздуха – фонорецепторы уха;

– изменение гидростатического и осмотического давления крови – баро- и осморецепторы;

– воздействие химических веществ – хеморецепторы;

– температурные изменения как внутри организма, так и в окружающей среде – терморецепторы;

Кроме перечисленных, у человека также есть тактильные и болевые рецепторы.

В ответ на изменение условий окружающей среды, чтобы внешние раздражители не вызывали повреждений и гибели организма, в нём формируются компенсаторные реакции, которые могут быть: поведенческими (изменение места пребывания, отдёргивание руки от горячего или холодного) или внутренними (изменение механизма терморегуляции в ответ на изменение параметров микроклимата).

Человек обладает рядом важных специализированных периферических образований – органами чувств, обеспечивающими восприятие воздействующих на организм внешних раздражителей. К ним относятся органы зрения, слуха, обоняния, вкуса, осязания. Нельзя путать понятия «органы чувств» и «рецептор». Например, глаз – это орган зрения, а сетчатка – фоторецептор, один из компонентов органа зрения. Органы чувств сами по себе не могут обеспечить ощущение. Для возникновения субъективного ощущения необходимо, чтобы возбуждение, возникшее в рецепторах, поступило в соответствующий отдел коры больших полушарий.

Рассмотрим отдельные пути поступления информации в организм человека и определим их относительное значение для восприятия целого окружающего пространства.

Зрение является ведущим источником информации для человека. Некоторые исследователи считают, что 90% информации об окружающей среде человек получает с помощью зрения. Мы знаем, как трудно ориентироваться в условиях абсолютной темноты. Зрительный анализатор включает в себя глаз, зрительный нерв, зрительный центр в затылочной части коры головного мозга. Глаз чувствителен к видимому диапазону спектра электромагнитных волн от 0,38 до 0,77 мкм.

Визуальная среда, с которой человек соприкасается каждый день, влияет на орган зрения человека, оказывая воздействие и на

его самочувствие. Неблагоприятная визуальная среда может вызывать у человека раздражение, приводить к тяжелым психическим расстройствам. Изучением окружающей видимой среды как экологического фактора занимается **видеоэкология**.

Большое значение в восприятии человеком окружающей среды имеет **осязание**. Осязание – сложное ощущение, возникающее при раздражении рецепторов кожи, наружных частей слизистых оболочек и мышечно-суставного аппарата. Кожный анализатор воспринимает внешние механические, температурные, химические и другие раздражители кожи. Осязание дополняет зрение в том смысле, что дает информацию об изменении осязательных аспектов окружающей среды. Путем исследований доказано, что человек может жить, потеряв зрение, но без осязания, точки которого рассеяны по всей поверхности тела, он жить не может.

Мы постоянно соприкасаемся с чем-то: с одеждой, с предметами, с которыми работаем. Осязание непосредственно позволяет чувствовать сопротивление и давление и почти не зависит от нашего воображения, чего нельзя сказать о других рецепторах. Таким образом, осязание постоянно информирует нас об особенностях окружающей среды. Материалы нас либо привлекают, либо отталкивают: мы не станем гладить забор из гофрированной жести – этого любимого сегодня строительного материала. Но мы с удовольствием прикоснемся к отполированной годами скамейке у деревенского забора, которая как бы зовет нас к отдыху и размышлениям.

Слух является пассивным органом в процессе восприятия. Слух – способность организма принимать и различать звуковые колебания слуховым анализатором в диапазоне от 16 до 20 000 Гц. Порог болевых ощущений 130–140 дБ. Человек может закрыть глаза и тем самым исключить восприятие чего-то неприятного, но в ушах у нет никакого клапана. Слух часто дает нам информацию о среде, которая находится вне нашего зрительного поля, за горизонтом, охватываемым зрением. Восприятие пространства в значительной мере зависит от функции слухового аппарата, регистрирующего приятные и неприятные звуки, например шум, который относится к типу невротического влияния окружающей среды, – это типичный продукт технически развитого общества.

Шумовое загрязнение – *форма физического (обычно антропогенного) загрязнения, возникающего в результате увеличения интенсивности и повторяемости шума сверх природного уровня. Приводит к повышению утомляемости человека, снижению умственной активности и при достижении 90–100 дБ к постепенной потере слуха.*

Обоняние – способность воспринимать запахи. Животные обладают прекрасным обонянием. Человек обладает разной степенью обоняния к различным пахучим веществам. Приятные запахи улучшают самочувствие человека, а неприятные действуют угнетающе, вызывают отрицательные реакции вплоть до тошноты, рвоты, обморока (сероводород, бензин), способны изменять температуру кожи, вызывать отвращение к пище, приводить к подавленности и раздражительности. В развитии ориентации у ребёнка обоняние играет весьма существенную роль с первых дней жизни. Грудной ребёнок, которому всего несколько дней, может четко различать одежду матери, при этом он руководствуется только обонянием.

В городской среде у человека систематически и подсознательно уменьшается чувствительность органа обоняния. Воздух здесь наполнен таким количеством отработанных газов, что людям ничего не остается, как только постепенно привыкать к ним. Современный человек проявляет все большую склонность к пренебрежению обонянием, хотя именно оно является крайне важной способностью. Пригодность среды для выполнения определенной деятельности человек оценивает, как правило, носом, который по запахам получает информацию там, где глаз не видит, и откуда не доносятся акустические сигналы. Например, легкое ощущение знакомого запаха может вызвать четкие воспоминания о чем-то давно минувшем, например в памяти всплывает живое представление определенной ситуации.

Вкус – ощущение, возникающее при воздействии определённых химических веществ, растворимых в воде, на вкусовые рецепторы, расположенные на различных участках языка. Вкус складывается из четырёх простых вкусовых ощущений: кислое, солёное, сладкое и горькое. Все остальные вариации вкуса – это

комбинации из основных ощущений. Различные участки языка имеют разную чувствительность к вкусовым веществам.

Восприятие окружающей среды происходит путем одновременного взаимодействия всех органов чувств, хотя человек все более становится рабом зрения. Это усиленно закрепляет сегодня аудиовизуальный характер культуры, где на первом месте стоит телевидение. Можно смело утверждать, что современный человек в своей оценке окружающей среды все больше полагается на зрение. Об этом свидетельствует и тот факт, что определенное пространство и возможность его использования для практической деятельности ограничиваются прежде всего визуально.

Есть ли у человека наряду с классическими пятью органами чувств и наряду с чувством, информирующим его о внутренних процессах, происходящих в организме (например, чувство равновесия), другие органы, с помощью которых он может ориентироваться в жизненной среде и получать информацию? В 1976 г. английский психолог Робин Бейкер решил провести исследование скрытых, по его мнению, способностей человека ориентироваться в незнакомой среде, где к тому же отсутствуют важные элементы, облегчающие ориентацию. В этом эксперименте приняли участие 64 студента-зоолога из университета в Манчестере. Им завязали глаза темной материей и посадили в автобус. Затем автобус отправился по очень сложному маршруту, чтобы никто не мог запомнить направление его движения. Проехав 50 км, автобус остановился, и студенты вышли с завязанными глазами. Их задачей было ответить на вопрос: в каком направлении расположен университет? Затем они должны были определить сторону света. Только после этого с них сняли повязку и попросили показать, на этот раз с открытыми глазами, где находится университет.

Согласно результатам исследования, определение направления, сторон света было более правильным, когда они отвечали с повязкой на глазах. Когда у студентов сняли повязку, то точность ответа исчезла. Таким образом, подтверждена была гипотеза, согласно которой человек также обладает органом, воспринимающим действие магнитного поля, в данном случае в ориентировании в незнакомой местности и в определении направления исходной точки.

Особенности восприятия окружающей среды человеком

Человек через доступные ему каналы получает зрительную, звуковую, осязательную, вкусовую информацию и запах. Какими бы физическими характеристиками окружающая среда ни обладала, она всегда воздействует на человека как целое, из чего следует, что импульсы, которые воспринимает человек, никогда не бывают изолированными. Однако он воспринимает не всю поступающую к нему информацию. Он слышит или видит не все звуки и не все световые сигналы, а только те, которые имеют для него определенное значение. При этом на отбор информации влияние оказывают не только физические возможности органов чувств воспринимать информацию, но и такие личностные особенности человека, как отношение к происходящему, его предыдущий опыт, его система ценностей, настроение и т.п., т.е. информация как бы проходит через определенный фильтр. Отбор позволяет отбросить неважную или ненужную информацию. Например, человек может не слышать разговор людей, стоящих рядом, в том случае, если он его не интересует. В то же время отбор информации может привести к потере важной информации, к существенному искажению реальности.

Каждая среда содержит больше информации, чем мы можем сознательно воспринять, зарегистрировать. Наряду с осознанным существует и подсознательное восприятие. Мы получаем информацию, даже не сознавая этого. Такой вид восприятия называется сублимированным. Его существование подтверждено целым рядом экспериментов, среди которых достаточно привести пример подсознательно действующей рекламы.

М. Черноушек указывает на семь видов информации, которые характеризуют ситуации восприятия окружающей среды как целого:

– среда не имеет определенных, твердо фиксированных рамок во времени и пространстве;

– среда воздействует на все чувства, и информацию о среде мы получаем из сочетания данных всех органов;

– среда дает не только главную, но и периферийную информацию;

– любая среда наряду с физическими и химическими особенностями обладает психологическими и символическими значениями;

– среда содержит всегда больше информации, чем мы способны сознательно зарегистрировать и понять;

– среда воспринимается в тесной связи с практической деятельностью, восприятие связано с действием и наоборот;

– окружающая среда воздействует как единое целое.

В результате исследований психологи пришли к выводу, что восприятие ребёнка и взрослого принципиально отличаются. Взрослые способны одновременно воспринимать запахи, звуки, зрительную и тактильную информацию. При этом мозг взрослого человека способен эту информацию суммировать и, например, недостаток звуковой информации восполнять зрительной. У детей младше 8 лет восприятие устроено иначе. Мозг ребёнка способен в один и тот же момент обрабатывать информацию только от одного органа чувств: ребёнок либо осязает, либо видит. Суммировать информацию от разных органов чувств человек учится постепенно.

Перенасыщенная информацией среда

Ускоренное развитие техники способствовало тому, что город стал многолюден, перегружен машинами, перенасыщен шумом, визуальными импульсами, другими источниками информации. Современный житель большого города подвергается чрезмерному воздействию информации и его способность воспринимать и интерпретировать сигналы, отличать полезную информацию от ненужной определенным образом изменяется. Он защищается от некоторых импульсов, чтобы воспринимать только те, в соответствии с которыми будет ориентироваться и принимать решения. Таким образом, среда предъявляет все большие требования к личности. И если мы стараемся на шумной главной улице не воспринимать все раздражители, то воздействия некоторых из них мы избежать не можем. Всевозрастающий уровень раздражителей требует новой адаптационной стратегии, заставляет индивида использовать такие источники, которые дают упрощенную информацию. Проблемы и сложности возникают в том случае, когда изменение адаптационного поведения оборачивается потерей существенных данных среды.

Если количество информации превышает средний уровень, то поведение человека может стать слишком простым, рутинным.

Понятие «перенасыщенная среда» впервые применил социолог Г. Зиммель, который уже в начале XX столетия сделал вывод, что городская среда препятствует нормальному отношению людей к новым импульсам, поскольку их энергия распыляется на решение мелких, частных проблем среды. Следовательно, богатая импульсами среда города настолько загружает нас информацией, что остается очень мало времени для восприятия новой информации. Это подтверждает и личный опыт: иногда мы даже не регистрируем изменения в слишком знакомой среде.

Американский психолог Д. Д. Миллер считает, что люди в противодействие перенасыщенной среде вырабатывают специфическую адаптационную стратегию. Они устраняют импульсы, не воспринимают и не концентрируют внимания на информации, которую они не считают для себя важной. Это может себя не оправдать, т.к. мы можем включить во второстепенный ряд и весьма важную информацию. Но часто у людей вообще не остаётся времени для оценки той или иной информации. Мы постоянно спешим, и в спешке действительно невозможно уделить должное внимание импульсам окружающей среды.

Общепризнано ослабление межчеловеческих связей и взаимной социальной ответственности, поскольку в настоящее время человеческая деятельность определяется индивидуальным стремлением к преодолению трудностей перенасыщенной среды. Социально и физически перенасыщенная среда вызывает отчуждение между людьми, ослабляет межчеловеческую солидарность, желание помочь друг другу. Дружеские межчеловеческие отношения в перенасыщенной среде исчезают, особенно по отношению к неизвестным людям.

Энергоинформационные свойства воды

Вода – это самое распространённое вещество на Земле в её приповерхностном слое. Только вода встречается в земных условиях во всех трёх состояниях: твёрдом, жидком и газообразном. С древнейших времён человечество приписывает чудесные свойства воде. При этом большинство её свойств не вписывается в общие физические принципы. Можно утверждать, что во-

да – это неизученное вещество. Только в последние годы вода стала подвергаться серьёзному научному изучению.

С. В. Зенин, доктор биологических наук, заведующий проблемной лабораторией Министерства здравоохранения РФ, в результате исследований пришел к выводу, что вода имеет особую молекулярную структуру. Эта структура меняется, если на воду воздействовать различными способами: химическим, электромагнитным, механическим, информационным и т.д. Под этими воздействиями её молекулы способны перестраиваться и таким образом запоминать любую информацию. Феномен «структурной памяти» позволяет воде впитывать в себя, хранить и обмениваться с окружающей средой данными, которые несут свет, мысль, музыка, молитвы или простое слово. Подобно тому, как каждая живая клетка хранит в себе сведения обо всём организме, каждая ячейка воды способна хранить в себе информацию обо всех изменениях в нашей планетарной системе.

Воздействуем ли мы через водную среду друг на друга своими мыслями, словами? Способны ли мы программировать сами себя и окружающих? Безусловно. Способность воды обрабатывать информацию делает её очень похожей на обычный компьютер. Таким образом, человек, состоящий на 70–80% из воды, представляет собой программируемую систему: любые внешние факторы, в том числе и общение людей друг с другом, меняют структуру и биохимический состав жидких сред организма. Это происходит на клеточном уровне, программируется даже сама молекула ДНК, вплоть до полного ее разрушения. Это означает, что нарушения в индивидуальной программе, заложенной в любом организме на молекулярном уровне в воде, – это и есть истинная причина и источник болезней, которые проявятся в будущем. Такие ощущения, как резкая усталость, беспричинная агрессия, дурное настроение и даже многие болезни могут стать последствиями негативного энергоинформационного воздействия. И наоборот, чистотой собственных мыслей человек способен поправить собственное здоровье и очистить окружающую среду.

В лаборатории С. В. Зенина исследовали воздействие людей на свойства воды. Контроль велся как по изменению физических параметров, в первую очередь по изменению электропроводности воды, так и с помощью тестовых микроорганизмов.

Исследования показали, что чувствительность информационной системы воды оказалась настолько высокой, что она способна ощущать влияние не только тех или иных полевых воздействий, но и форм окружающих предметов, воздействия человеческих эмоций и мыслей. Вода реагирует на мысли и эмоции окружающих её людей, на события, происходящие с населением и так далее. Кристаллы, образовавшиеся из только что полученной дистиллированной воды, имеют простую форму хорошо известных шестиугольных снежинок. Накопление информации меняет их строение, усложняя и делая их красивее, если информация положительная, и, напротив, искажая или даже разрушая первоначальные формы, если информация отрицательная.

Исследования японского ученого М. Эмото, который замораживал капельки воды, а затем изучал их под сильным увеличением в микроскопе, имеющим встроенную фотокамеру, наглядно подтверждают результаты работы С. В. Зенина. М. Эмото обнаружил, что загрязненная вода имела нарушенную и случайным образом сформированную структуру, а вода из горных потоков и ключей была прекрасно сформирована геометрически.

Далее ученый решил посмотреть, какой эффект оказывает музыка на структуру воды. Он поставил дистиллированную воду между двух колонок на несколько часов и потом сфотографировал её после замораживания. Так же он использовал слова, напечатанные на бумаге и наклеенные на ночь на стеклянную посуду с водой. Полученные фотографии доказывают невероятные изменения воды, как живой субстанции, реагирующей на каждую нашу эмоцию или мысль. Совершенно ясно, что вода легко меняется под воздействием вибраций энергии, независимо от того, загрязненная это или чистая среда. Работа М. Эмото наглядно продемонстрировала различие в молекулярной структуре воды при её взаимодействии с окружающей средой. Этот метод дал возможность показать, каким образом мысли и слова человека воздействуют на его молекулярную структуру.

По мнению С. В. Зенина, вода выступает не просто как жидкость, а как вещество, находящееся в информационно-фазовом состоянии. Вода хранит в себе полную информацию о любых воздействиях на неё. Смысл информационно-фазового состояния воды заключается в том, что полная информация, поступающая в водную среду, отражается в каждой ячейке. В дополнение к ме-

ханической, бактериологической и химической очистке воды уже пора всерьёз говорить об информационной очистке и последующим обогащением воды полезной информацией.

1.3. Роль информации в развитии общества

Информационные революции. Информационное общество. Проблема информационного неравенства. Россия в информационной эпохе.

Основные термины и понятия:
Информационная революция
Информационная технология
Информационное неравенство
Информационное общество
Ноосфера
Технологическая революция

Информационные революции

Ряд современных исследователей процесса цивилизационного развития человеческого общества считают, что история человечества может рассматриваться как закономерная последовательность технологических революций.

Технологическая революция – *радикальное изменение доминирующего в обществе технологического уклада, который, в свою очередь, определяется средствами и способами организации общественного производства и жизнеобеспечения общества.*

Профессор А. И. Ракитов показал, что в основе каждой технологической революции лежит информационная революция.

Информационная революция – *это преобразование общественных отношений из-за кардинальных изменений в сфере обработки информации.*

Следствием преобразований общественных отношений является приобретение человеческим обществом нового качества, переход на новый уровень технологического развития.

В настоящее время принято выделять шесть основных информационных революций.

Первая информационная революция (устная) заключается в появлении языка и членораздельной человеческой речи. Развитие языка оказало колоссальное влияние на развитие сознания людей. Язык сделал возможным развитие процессов абстрактного мышления, т.е. зарождения интеллектуальной деятельности людей. В первобытном обществе, когда выживало более организованное племя, возникла необходимость приобретения, сохранения и передачи знаний и умений. В то время использовались и распространялись только «живые знания», носителями которых являлись живые люди − старейшины, жрецы, шаманы. К пожилым людям, имеющим ценный для племени опыт, применялся принцип «не убий». Так возникла система «Учитель» (по Н. Н. Моисееву), которая способствовала развитию не столько в индивидуальной сфере, сколько в общественной.

В условиях первобытного общества процессы накопления знаний и их распространения осуществлялись чрезвычайно медленно, а сохранение уже накопленных знаний в виде легенд, мифов и сказаний было недостаточно надёжным.

Вторая революция (письменная) связана с изобретением письменности. Люди научились отчуждать знания и фиксировать их на материальных носителях в виде рисунков или условных знаков. Это изобретение позволило не только обеспечить сохранность уже накопленных человеческим обществом знаний, но и создать условия для их широкого распространения. Существенным образом изменилась и информационная среда общества, стали возможными новые виды информационных коммуникаций между людьми посредством обмена письменными сообщениями. Позже появились исторические летописи, поэзия и литература, зародились элементы того нового и своеобразного явления, которое мы сегодня называем информационной культурой. Понятие «образование» приобрело новый смысл. Теперь образованным мог считаться только тот человек, который достаточно хорошо владел навыками чтения и письма, причем не только на своём родном языке, но и на других языках.

Третья информационная революция (печатная) началась в эпоху Возрождения (середина XVI века) и была вызвана изобретением печатного станка. Книгопечатание радикально изменило

общество, культуру, организацию деятельности человека. Относительная простота процесса книгопечатания, большие тиражи печатных книг и их значительно меньшая стоимость по сравнению с рукописными книгами привели к первому информационному взрыву. Произошел взрывообразный рост количества используемых в обществе документов, началось более широкое распространение информации, научных знаний. Появились первые библиотеки печатных книг. Возникла возможность обеспечить сохранение авторства, интеллектуальной собственности (выходные данные книги).

Своего апогея третья информационная революция достигла с появлением печатных СМИ: газет, журналов, рекламных объявлений, информационных справочников и т.п. Несмотря на появление в последние годы различного рода электронных носителей информации, объёмы печатной продукции продолжают расти.

Четвертая информационная революция (электронная) началась в XIX веке и была обусловлена изобретением электричества, благодаря которому появились телеграф, телефон, радио, телевидение. Новые качества, которые принесла в информационную сферу общества эта информационная революция, заключаются не только в том, что по новым коммуникационным сетям стали передаваться невиданные ранее объёмы информации, но также и в том, что информационные коммуникации стали осуществляться с более высокой скоростью. Любое событие, которое происходит сегодня на нашей планете, в течение нескольких часов может стать известным подавляющему большинству её обитателей, где бы они ни находились.

Пятая информационная революция (компьютерная) началась в 50-е годы XX века с появлением средств цифровой вычислительной техники. Применение этих средств для обработки информации кардинальным образом изменило возможности человека по активизации и эффективному использованию информационных ресурсов: роль систематизации, хранения, переработки информации, а также передачи её на расстояние взяла на себя техника. Изобретение в 70-х годах прошлого века микропроцессорной технологии сделало компьютеры доступными для повседневного персонального использования, что во многом изменило психологию и практику научной, педагогической и производственной деятельности людей.

Шестой информационной революцией (сетевой) стало объединение компьютеров для передачи данных в сети, что привело к появлению единого глобального информационного пространства. Некоторые специалисты ставят появление Интернета по его влиянию на цивилизацию в один ряд с книгопечатанием. Интернет – открытая, саморазвивающаяся кибернетическая система, включающая в себя миллионы компьютеров, объединённых в различные локальные и глобальные сети. Использование информационных ресурсов Интернета в образовательных целях ставит ряд философских, психолого-педагогических и методических проблем.

Последняя революция знаменует возникновение безбумажного, виртуального этапа в развитии социальных коммуникаций. Бумага стала необходима только для итогового воспроизводства визуально подготовленных документов. Возникла новая отрасль – **информационная индустрия**, связанная с производством технических средств, методов, технологий для производства новых знаний.

Важнейшими составляющими информационной индустрии становятся все виды информационных технологий, особенно телекоммуникации. При применении информационных технологий достигается экономия затрат труда, энергии людских и материальных ресурсов, необходимых для реализации данного процесса.

Информационная технология – *это представленное в пригодном для практического использования виде концентрированное выражение научных знаний и практического опыта, позволяющее рациональным образом организовать тот или иной достаточно часто повторяющийся информационный процесс.*

Современная информационная технология опирается на достижения в области компьютерной техники и средств связи. Однако с другой стороны, изменения, происходящие в обществе под влиянием сетевых средств массовой коммуникации, не ограничиваются только определенными преимуществами и выгодами, что открывает самые широкие возможности для ведения информационного противоборства в социально-политической

сфере. Информационный терроризм, распространение нелегальных материалов (в том числе безнравственной, возбуждающей низменные человеческие чувства), образование в Сети неформальных молодежных объединений, деструктивное влияние новых коммуникационных технологий на личность – это «оборотная» сторона существования сетевых средств массовой коммуникации.

По расчетам, приведенным Л. Д. Рейманом, пятьдесят лет тому назад, пересылка по почте 30 страниц текста на расстояние 5 тысяч километров длилась бы примерно 10 дней и стоила бы около 30 долларов. Двадцать лет назад, используя факс, подобная пересылка заняла бы примерно 1 час, и стоимость составляла около 50 долларов. Сегодня на это требуется не более 3 секунд, а стоимость составит около 3 центов. Таким образом, стоимость упала в 1000 раз, скорость возросла в 300 тысяч раз.

Бурное развитие компьютерной техники и информационных технологий послужило толчком к развитию общества, построенного на использовании различной информации и получившего название информационного общества.

Информационное общество

По подсчётам ученых, с начала нашей эры для удвоения знаний потребовалось 1750 лет, второе удвоение произошло в 1900 году, третье – в 1950 году и так далее в геометрической прогрессии. Быстрое сокращение времени удвоения объёма накопленных научных знаний указывает на явление, получившее название «информационный взрыв» и свидетельствующее о начале века информации, возникновении информационного общества.

Информационное общество – *это ступень развития цивилизации, в которой главными продуктами производства являются информация и знания.*

В мире активное обсуждение теоретических вопросов развития информационного (постиндустриального) общества

проходило в конце 1970-х – начале 1980-х годов. Концепция информационного общества как общесоциологическая теория развития достаточно глубоко разработана западными исследователями: Д. Беллом, Дж. Гелбрейтом, Дж. Мартином, И. Масудой, Ф. Полаком, Э. Тоффлером, Ж. Фурастье и др. Именно Ж. Фурастье определил постиндустриальное общество как «цивилизацию услуг». Отечественная наука обратилась к данной проблематике значительно позже. Среди отечественных ученых, внесших значительный вклад в развитие этого направления, необходимо отметить В. М. Глушкова, Н. Н. Моисеева, А. И. Ракитова, А. В. Соколова, А. Д. Урсула и др.

Отличительными **чертами** информационного общества являются:

– увеличение роли информации и знаний в жизни и экономике общества;

– возрастание доли информационных коммуникаций, продуктов и услуг в валовом внутреннем продукте;

– быстрое сокращение времени удвоения объёма накопленных научных знаний;

– превышение материальных затрат на хранение, передачу и переработку информации аналогичных расходов на энергетику;

– превращение информации в ресурс общества наряду с природными ресурсами;

– создание глобального информационного пространства, обеспечивающего эффективное информационное взаимодействие людей, их доступ к мировым информационным ресурсам и удовлетворение их потребностей в информационных продуктах и услугах;

– сокращение числа людей, занятых в промышленном производстве и сельском хозяйстве.

Кроме положительных моментов прогнозируются и **опасные тенденции** информационного общества:

– усиливается влияние на общество средств массовой информации;

– информационные технологии могут разрушить частную жизнь людей и организаций;

– существует опасность разрыва между «информационной элитой» (людьми, занимающимися разработкой информационных технологий) и потребителями;

– существует проблема отбора качественной и достоверной информации;

– многим людям будет трудно адаптироваться к среде информационного общества.

Одним из основных **критериев** перехода общества к постиндустриальной и далее к информационной стадии развития может служить процент населения, занятого в сфере услуг:

– если в обществе более 50% населения занято в сфере услуг, наступила *постиндустриальная* фаза его развития;

– если в обществе более 50% населения занято в сфере информационных услуг, общество стало *информационным*.

Наряду с вышеуказанными, существуют и другие критерии информационного общества, в частности:

1) превращение информации в основной товар, или увеличение доли стоимости информации в стоимости товаров (в широком смысле). В соответствии с этим критерием общество может быть названо «информационным», если стоимость информации и интеллектуального труда заметным образом превышает стоимость сырьевых товаров, физического труда и т.д.; престижными и высокооплачиваемыми становятся профессии, связанные с владением, накоплением, оперированием информацией и т.д. Внешними признаками перехода общества в состояние «информационного» могут быть преобладание в экономике высокотехнологичных отраслей, престиж профессий, связанных с владением информацией, высокие цены на информационные услуги, экспорт интеллекта в различных его формах (технологий, специалистов и т.п.).

2) качественные изменения в жизненном мире, связанные с разрастанием значимого для индивидов в их повседневной жизни информационного поля.

К описанию эволюции общества применяются разные подходы. Рассмотрим процесс возникновения и развития информационного общества, используя **ритмо-информациологический подход**, предложенный отечественными учеными В. В. Нечаевым и А. В. Дарьиным.

Эволюция человеческого общества может быть охарактеризована двумя фундаментальными процессами: развитием человека и социально–технологическим развитием общества. **Биологический период** (развитие человека) отражает смену

поколений. С течением времени биологический период практически не изменился и его можно считать как среднестатистический возраст родителей при появлении их первого ребёнка, т.е. 20–25 лет.

Периоды и циклы социально-технологического развития характеризуются сменой социальных формаций, например, прогресс в области используемых технологий. Под **технологическим циклом** понимаются не только кардинальные революционные изменения технологии (каменный век, железный век), но и последовательная смена технологий и моделей, выражающаяся, например, в поколениях средств связи, средств передвижения и т.п. Абсолютно точно периодичность социального развития установить невозможно. Однако прослеживается общая тенденция: если 5–7 веков назад период социального развития составлял около 200–300 лет, то к началу XXI века он сократился до 1–2 лет.

До конца XIX века базовой характеристикой социального развития общества был технологический уровень. За один и тот же технологический период происходило несколько циклов смены поколений. Следовательно, информационно-несущими выступали периоды смены технологий, накладываемые на более высокую частоту смены поколений людей.

Совпадение периодов биологического и социального развития пришлось на первую половину XX века. При современном уровне развития человечества на время одного поколения приходится несколько технологических циклов, и текущий технологический уровень характеризует лишь сравнительно небольшой интервал жизни человека. Это означает изменение не только лежащих в основе технологий процессов и деятельности, но и всей сопутствующей системы механизмов и средств такой деятельности. Происходит **смена целевых установок**, ценностных ориентаций, системы знаний.

Таким образом, возникновение информационного общества обусловлено сменой информационной составляющей эволюции цивилизации с социального ритма на биологический. Современное общество, начиная с последней четверти XX века, перешло к информационной эре, а информационно-несущим компонентом, определяющим уровень, качество и характеристику цивилизации, стал сам человек.

В прошлом веке В. И. Вернадский писал о том, что неизбежно наступит время, когда эволюционные процессы на нашей планете будет определять человеческая жизнедеятельность. Определяющим началом при этом будет не стихия естественного развития, а разум человека. Таким образом, биосфера станет **ноосферой**, т.е. сферой господства разума человека. В ноосфере люди должны *принять на себя ответственность* за дальнейший ход эволюции на Земле. В условиях быстрых изменений индивидуальные качества человека приобретают ещё более важное значение, чем раньше.

Ноосфера (от греч. *nous* – разум и *sphaira* – шар) – *сфера взаимодействия общества и природы, в границах которой разумная человеческая деятельность становится определяющим фактором развития.*

Указанное В. И. Вернадским время наступило «наполовину». С одной стороны, изменения произошли: человеческая деятельность действительно стала заметно влиять на эволюционные процессы. С другой стороны, изменения произошли так быстро, что человечество, в основной массе даже не успело понять этого и не совершилось самого главного – господства разума человека. Наступил экологический кризис, характеризующийся разрушением многих экосистем, истощением ресурсов и загрязнением планеты.

При переходе к информационному обществу возникает новая индустрия переработки информации на базе компьютерных и телекоммуникационных информационных технологий. Ближе всех на пути к информационному обществу стоят страны с развитой информационной индустрией, к числу которых следует отнести США, Японию, Великобританию, Германию, страны Западной Европы. В ряде публикаций отмечается, что США вступили в постиндустриальный период своего развития в 1956 году, а информационным обществом США стали в 1974 году.

Признавая несомненность достижений США и других стран в области информатизации, необходимо понимать, что определенная доля «информационности» этих стран создана за счёт выноса ряда материальных, нередко экологически вредных, производств в другие страны мира, за счёт так называемого «экологического колониализма».

Проблема информационного неравенства

Анализ основных тенденций развития информатизации общества показывает, что этот процесс создает для развития цивилизации не только новые возможности, но и новые проблемы. Возникающая новая высокоавтоматизированная информационная среда оказывается в различной степени доступной для отдельных людей, организаций, регионов и стран мирового сообщества. При этом то общество, которое способно эффективно использовать возможности новой информационной среды для своего научно-технического и социально-экономического развития, получает **существенные** преимущества перед другими субъектами мирового сообщества, которые при этом вытесняются на обочину современного процесса развития цивилизации. Прогнозы специалистов свидетельствуют о том, что глобальная информатизация общества в XXI веке существенно усилит технологическую и экономическую дифференциацию между передовыми и развивающимися странами. Категория развивающихся стран будет всё быстрее размываться, т.к. многие из них перейдут в категорию отсталых стран.

Складывающаяся ситуация, признаки появления которой можно наблюдать уже сегодня, называется проблемой информационного неравенства. О путях преодоления электронно-цифрового разрыва (информационного неравенства) говорится в Окинавской хартии глобального информационного общества, которая была принята лидерами стран «большой восьмерки» 22 июля 2000 года.

В структуре проблемы информационного неравенства специалисты особо выделяют личностно-социальный аспект, который связан с проблемой социальной адаптации человека в новой, быстро изменяющейся информационной среде. Информационное неравенство можно рассматривать как новую форму социального неравенства людей. Снизить остроту этой проблемы призвана перспективная система образования, которая должна предоставить возможность всем членам общества получать необходимые знания и умения для того, чтобы правильно ориентироваться в новом информационном пространстве и эффективно использовать его возможности.

Россия в информационной эпохе

Некоторые исследователи склоняются к мнению, что информационная эра – исторически выигрышный этап для России. Многие особенности российского менталитета, которые с точки зрения индустриального развития можно было считать недостатками, в информационную эру превращаются в достоинства, в частности, отсутствие жесткой привязки к месту и времени, способность переключаться и быстро осваивать новое, беспокойство о судьбах мира и др.

Вошла ли Россия в фазу «информационного» общества или находится на пути к ней? Если рассматривать критерий превращения информации в основной товар, то Россия частично вошла в указанную стадию. Признаками этого могут служить следующие изменения:

– ускоренное развитие сферы информационных услуг: электронные СМИ, компьютеризация, Интернет; развитие сетей информационных услуг, связанных с функционированием банковской и финансовой систем, рынка ценных бумаг, рынков товаров (реклама), рынка недвижимости (риэлторские конторы); информационные юридические услуги (консультирование, нотариат, адвокатура) и т.д.;

– высокая стоимость многих информационных продуктов и услуг;

– престиж и относительно высокая доходность некоторых профессий, связанных с владением и оперированием информацией (экономисты, юристы, госслужба, PR, реклама, политтехнологи, программисты, журналисты, риэлторы и т.п.);

– заметное возрастание спроса на высшее образование и разрастание сети высших учебных заведений (в том числе платных);

– разрастание сети СМИ и формирование информационных «империй»;

– массированное проникновение информационных политтехнологий в политический процесс; возрастание роли информационного воздействия в политической жизни и протекании политических процессов;

– возрастание роли манипулирования массовым сознанием и поведением в функционировании российского общества в целом.

Однако российское общество не может в полном смысле слова быть названо «информационным обществом» ввиду следующих обстоятельств:

– упадок высокотехнологичных секторов экономики (ВПК, космическая отрасль и т.д.);

– полуколониальный характер экспорта (преобладание экспорта сырья);

– низкая стоимость умственного труда (в т. ч. научного, инженерного, преподавательского);

– инфляция и неуклонная деградация высшего образования, связанная со множеством факторов, в т. ч. устареванием материально-технической базы учебного процесса в вузах, ослаблением преподавательских кадров в условиях кризисного существования, массовым применением молодыми людьми учебы в вузах как средства ухода от призыва в армию и т.д.; получение высшего образования само по себе не дает никаких гарантий престижного и выгодного трудоустройства из-за отсутствия реального рынка труда;

– частичность «интернетизации» с точки зрения территориального и социально-пространственного охвата и специфического характера применения Интернет-ресурсов.

По другому критерию – степени изменения в жизненном мире (информационной среде) российского человека – мы, вероятно, уже в полной мере вошли в состояние «информационного общества». Наиболее очевидные признаки этого вхождения: бум рекламы, PR, информационных предложений и т.п. Это массивное изменение создало ряд новых проблем, с которыми российский человек до 90-х годов прошлого века еще не сталкивался. Многие оказались психологически и социально не готовы к произошедшему информационному взрыву и к тому колоссальному массиву информации, который на них обрушился. Кроме этого, информационная среда стала обладать гораздо большей степенью навязчивости, чем прежде. Особенно ярко это проявляется в случае торговой и политической рекламы. Человек становится все более несвободен от навязываемой ему информации.

1.4. Образование в информационном обществе

Особенности обучения в информационном обществе.
Компетентность педагога в информационном обществе.
Информационная пассивность педагога.

Основные термины и понятия:
Информационная пассивность педагога
Компетентность
Профессиональная компетентность учителя безопасности жизнедеятельности

Особенности обучения в информационном обществе

В обществе, где прошлое плавно перетекает в настоящее и повторяет себя в будущем, самым разумным способом подготовки подрастающего поколения к жизни было вооружение его навыками и умениями прошлого с целью использования их в будущем. Знание приобреталось в семье, религиозных организациях и в процессе обучения ремеслу. Прошлый опыт составлял основу содержания обучения.

Развивающейся промышленности XX века нужен был человек нового типа. Она требовала таких умений и навыков, каких сама по себе ни семья, ни церковь не в состоянии были обеспечить. Возникла система образования, которая уже самой своей структурой воспроизводила новый мир. Школьник не просто изучал факты, он знакомился с образом жизни, который ему предстояло вести. Центр внимания в образовании начал постепенно смещаться от прошлого к настоящему.

Динамизм современных общественных преобразований создает трудности в преемственности опыта поколений: детям приходится овладевать теми знаниями и специальностями, которые были недоступны их родителям. Поэтому сейчас не может идти речь о прямой передаче профессионального опыта. Молодым людям приходится действовать в условиях, когда старый опыт не только не помогает, но иногда даже мешает.

В сфере образования в настоящее время можно выделить следующие признаки информационного общества:

– расширение источников получения знаний в процессе обучения;

– получение образования в любом возрасте и в любое время;

– месторасположение учебного заведения и место проживания обучаемого не имеют особого значения;

– возможность составления программы обучения в соответствии с индивидуальными потребностями и уровнем развития обучающегося.

К сожалению, традиционное образование, которое получают дети и молодежь, должным образом не отражает тот мир, в котором им приходится жить. Динамика образования человека должна повторять, и, в определенной степени, упреждать динамику появления новых знаний. Как отмечают некоторые исследователи, на подготовку человека к будущим событиям сказывается темп изменения окружающей среды. Чем он стремительнее, тем быстрее ускользает от нас современная окружающая обстановка. Однако чем с большей скоростью водитель движется, тем дальше должен быть отодвинут знак, чтобы водитель успел его прочитать и среагировать. Точно так же и общее ускорение темпа жизни вынуждает нас усилить интерес к будущему. Первоочередная задача образования – преодолеть отставание от запросов современной жизни, а это значит, что в подготовке учеников необходимо учитывать не только проблемы и потребности сегодняшнего дня, но и те, что проявятся **в будущем**.

Современное общество в виду высокой скорости изменений в жизни выдвигает справедливое требование непрерывности образования. Современное среднее образование дает тот минимальный уровень знаний, которым должен обладать каждый член современного общества. Получив высшее образование, современный человек лишь в определенной мере достигает текущего минимально необходимого уровня знаний и технологий в какой-либо области. Далее выпускник вынужден в соответствии с появлением новых знаний повышать свой профессиональный уровень.

Для человека процесс потребления большого количества информации может представлять опасность. Новая информация может не совпадать с прошлым опытом, нормами и ценностями человека. Поэтому постиндустриальный тип общества характеризуется появлением нового вида грамотности – информационной, когда на первый план выдвигаются такие качества, как умение собрать информацию для решения задачи, способность анализировать и обобщать, умение быстро ориентироваться в глобальном информационном пространстве и др.

Компетентность педагога в информационном обществе

Частая смена технологий в современном мире означает трансформацию не только лежащих в её основе процессов и деятельности специалистов, но и всей сопутствующей системы механизмов и средств такой деятельности. Изменения в обществе требуют повышения профессиональной компетентности педагогов, а также коррекции содержания отдельных предметов и стратегии образования в целом. Можно предположить, что ориентация сознания учителя на будущее станет звеном, объединяющим его профессиональную и социальную компетентность.

Компетентность – *специфическая способность, позволяющую человеку конструктивно действовать в изменяющихся социальных и профессиональных условиях.*

Профессиональная компетентность учителя безопасности жизнедеятельности – *соответствующая определенной компетенции способность учителя осуществлять педагогическую деятельность с учетом специфики курса «Основы безопасности жизнедеятельности».*

Образование – социальный институт, формирующий потребности и облик будущего общества. Образование предопределяет личностные качества каждого человека, его знания, умения, навыки, мировоззренческие и поведенческие приоритеты, а, следовательно, в конечном итоге – экономический, интеллектуальный, нравственный и духовный потенциал общества. Необходимо формировать у учителя и у учащихся новое, обращенное в будущее, мышление, которое способно решить задачи, как развития цивилизации, так и сохранения окружающей среды.

Среди стереотипов педагогического мышления особо выделяется ориентация на конечность образования, которая понимается как подготовка к жизни, выполнение определенных социальных ролей. На практике этот стереотип приводит к стремлению научить всему и навсегда, усвоению готовых знаний, перегрузке учебных программ конкретным материалом, догматизму и формализму мышления. Преодоление этого стереотипа в условиях лавинообразного возрастания объёмов информации и её быстрого старения,

поддержание удовлетворительной компетенции педагога требует формирования у него новой установки на непрерывное образование и необходимость самообразования.

Преподаватель современной школы обязан не только информационно соответствовать сегодняшнему дню, но и знать направления дальнейшего информационного развития цивилизации с возможными опасностями этого развития. Имеющаяся у рядового педагога информационная картина мира, по большому счёту, не соответствует существующей реальности и препятствует осознанию ответственности человека за происходящие негативные изменения в современном мире. Компетентность современного педагога должна включать в себя мировоззренческую и философскую составляющие. Владея философскими категориями, научным пониманием процесса познания и методами научного познания, педагог будет готов действовать конструктивно в изменяющихся социальных и профессиональных условиях.

Образовательные учреждения находятся внутри достаточно стабильной среды, но их окружает большое число внешних элементов, которые трансформируются. Хотя изменения носят постепенный и предсказуемый характер, педагог должен следить за тем, что происходит в среде, с тем, чтобы своевременно прореагировать на происходящие изменения, а в идеальном случае – предвосхитить их. Адаптируясь, таким образом, к меняющимся потребностям общества, педагог активно влияет на его состояние, предопределяя и сами эти потребности. В условиях распространения информационных и коммуникационных технологий роль учителя как источника информации должна постепенно отойти на второй план, а главными для педагога должны стать **воспитательные** задачи.

Традиционно в общественный образ учителя вкладываются идеальные представления, связанные с его способностью «сеять разумное, доброе, вечное». В российской традиции учитель ассоциируется с духовным наставником, просветителем. Он, прежде всего, творец мировоззрения, а потом уже предметник. В настоящее время формируется иная общественная позиция: учитель – функционер, формальным предназначением которого является передача социального знания. Но учитель-функционер не может подготовить молодых людей к жизни в обществе социальных перемен с его высокими требованиями к качествам личности.

Отсюда всё в большей мере общественные ожидания связывают деятельность учителя с творческой самостоятельностью, поиском, высоким профессионализмом.

Учитель не свободен от условий, в которых он живет и работает. Но он свободен занять ту или иную позицию по отношению к ним. Поэтому, в конечном счёте, не учитель должен быть подвластен условиям, а скорее, условия подвластны ему. Сознательно или бессознательно он решает, будет ли он противостоять неблагоприятным условиям или позволит себе быть управляемым ими.

Информационная пассивность педагога

Информационная пассивность педагога как вид информационного поведения сформировалась ещё в советский период. Низкая социальная значимость информации в обществе вела к отсутствию интереса к ней, что выражалось в информационной пассивности граждан, создавая нездоровую информационную среду, феномен боязни использования и обмена информации. Жесткая регламентация школьной жизни породила исполнительного, равнодушного, лишенного инициативы педагога, сформировала пренебрежительное отношение к новаторскому поиску и опыту. Бюрократическое управление системы образования противилось внедрению в педагогическую практику нового и передового, укрепляя в педагогах состояние беспомощности. Отсутствие привычки к информационной обеспеченности привело к информационной нетребовательности и безразличию.

Информационная пассивность педагога характеризуется:

– несоответствием информационной картины мира педагога существующей реальности и требованиям информационного общества;

– прекращением своего профессионального самообразования и самовоспитания после накопления определенного количества информации и методической базы для преподавания своего предмета;

– нежеланием совершенствования навыков работы с информацией и повышения своей информационной компетентности (информационной культуры);

– неумением отобрать из огромной массы информации, в том числе при помощи компьютера, наиболее ценную и необходимую,

обработать и систематизировать, а также обеспечить хранение, которое гарантирует её сохранность, легкость и экономичность использования.

Согласно результатам исследований, только 44% учителей в возрасте до 30 лет обращаются к дополнительным информационным психолого-педагогическим источникам, у учителей в возрасте 40 лет и старше интерес к таким источникам почти исчезает. Низкий уровень готовности к повышению профессиональной компетентности подтверждаются другими данными: лишь 10–14% педагогов способны критически отнестись к собственному опыту.

Стремительный рост объёма информации тоже создает условия для возникновения информационной пассивности – возникает проблема в отслеживании новой информации даже с учётом узкой профессиональной специализации. У человека становится всё меньше времени для того, чтобы углубиться в изучение какого-либо вопроса. Избыток имеющейся информации в совокупности с неумением работать с большими объёмами информации является такой же преградой для становления профессиональной компетентности, как и отсутствие необходимых условий для её поиска и обработки.

Вопросы для самоконтроля

1. Дайте определение «информации».
2. Почему существует множество определений «информации»?
3. Дайте определение «информационной безопасности».
4. Почему существует множество определений «информационной безопасности»?
5. Перечислите виды информации.
6. Перечислите атрибутивные свойства информации.
7. Перечислите прагматические свойства информации.
8. Перечислите динамические свойства информации.
9. Перечислите фазы, составляющие информационный процесс.
10. Приведите примеры информационных процессов в природе.
11. Приведите примеры информационных процессов в технических системах.

12. Каковы цели и задачи информационной безопасности?

13. Приведите примеры опасностей и угроз в сфере информационных процессов и систем.

14. Назовите источники информационных внешних угроз.

15. В каких формах могут проявляться внутренние угрозы?

16. Назовите источники информационных внутренних угроз.

17. В каких формах могут проявляться внешние угрозы?

18. В чем суть защитных мер законодательного уровня?

19. В чем суть защитных мер административного уровня?

20. В чем суть защитных мер процедурного уровня?

21. В чем суть защитных мер программно-технического уровня?

22. Назовите несколько принципов обеспечения информационной безопасности.

23. Перечислите пути поступления информации в организм человека.

24. Какими информационными свойствами обладает вода?

25. В чём может заключаться информационная очистка воды?

26. Перечислите информационные революции и дайте их краткую характеристику.

27. Покажите на примерах значение информации в развитии общества.

28. Что такое информационное общество? Каковы его отличительные черты?

29. Что такое информационное неравенство людей в информационной среде? Каковы его причины?

30. В чём причины информационной пассивности педагога?

31. Почему в условиях распространения информационных и коммуникационных технологий главными для педагога должны стать воспитательные задачи?

ГЛАВА 2. ОСНОВЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Информация как объект правового регулирования

Информационные правоотношения.
Понятие и виды информации, защищаемой законодательством РФ.

Основные термины и понятия:
Документированная информация
Информационные правоотношения

При рассмотрении информации в качестве предмета правоотношений в правовой системе, приходится возвращаться к определению информации в его исходном смысле: под информацией понимается содержание сообщений, сведений и сигналов. В основе такого подхода (антропоцентрического) к определению понятия «информация» лежит идея, что в процессе создания, распространения, преобразования и потребления информации подавляющее большинство общественных отношений возникает именно по поводу информации в форме сведений или сообщений. Кроме понятия «информация» ФЗ «Об информации, информационных технологиях и о защите информации» вводит термин «документированная информация».

Документированная информация – *зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.*

Информационные правоотношения

Правовое обеспечение защиты информации представляет совокупность законов и других нормативно-правовых актов, а также организационных решений, которые регламентируют как общие вопросы обеспечения защиты информации, так и организацию и функционирование защиты конкретных объектов и систем.

Информационные отношения достигли такой ступени развития, на которой оказалось возможным сформировать самостоятельную отрасль законодательства, регулирующую информационные отношения. В эту отрасль, которая целиком посвящена вопросам информационного законодательства, включаются:

– законодательство об интеллектуальной собственности;

– законодательство о средствах массовой информации;

– законодательство о формировании информационных ресурсов и предоставлении информации из них;

– законодательство о реализации права на поиск, получение и использование информации;

– законодательство о создании и применении информационных технологий и средств их обеспечения.

В соответствии с действующим законодательством

Информационные правоотношения – *это отношения, возникающие при:*

– *формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации;*

– *создании и использовании информационных технологий и средств их обеспечения;*

– *защите информации, прав субъектов, участвующих в информационных процессах и информатизации.*

В отрасли права, акты которых включают информационно-правовые нормы, входят конституционное право, административное право, гражданское право, уголовное право, предпринимательское право.

Понятие и виды информации, защищаемой законодательством РФ

Статья 5 ФЗ «Об информации, информационных технологиях и о защите информации» устанавливает две группы информационных ресурсов по категориям доступа: открытые информационные ресурсы и информационные ресурсы, доступ к которым ограничен в соответствии с законом.

Все государственные информационные ресурсы РФ являются открытыми и общедоступными. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа.

В соответствии с ФЗ «Об информации, информационных технологиях и о защите информации» защите подлежат сведения ограниченного доступа, а степень защиты определяет их собственник.

Не может быть ограничен доступ к:

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Информация с ограниченным доступом, в свою очередь, подразделяется на сведения, составляющие **государственную тайну** и **конфиденциальную информацию**.

Конфиденциальная информация классифицируется следующим образом:

- коммерческая тайна;
- служебная тайна;
- профессиональная тайна;
- персональные данные;
- иные виды тайн.

В Указе Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» утвержден перечень сведений конфиденциального характера, в котором перечислены шесть видов информации:

1) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

2) сведения, составляющие тайну следствия и судопроизводства;

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

4) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

5) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами (коммерческая тайна);

6) сведения о сущности изобретения полезной модели или промышленного образца до официальной публикации информации о них.

Конфиденциальными в соответствии с законом являются, в частности, такие виды информации, как:

− содержащая государственную тайну (Закон РФ «О государственной тайне», ст. 275, 276, 283, 284 УК РФ);

− передаваемая путем переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ч. 2 ст. 23 Конституции РФ, ст. 63 ФЗ «О связи», ст. 138 Уголовного кодекса (УК) РФ); касающаяся тайны усыновления (ст. 139 Семейного кодекса (СК), ст. 155 УК РФ);

− содержащая служебную тайну (ст. 139 ГК РФ), коммерческую тайну (ст. 139 ГК РФ и ст. 183 УК РФ), банковскую тайну (ст. 183 УК РФ), личную тайну (ст. 137 УК РФ), семейную тайну (ст. 137 УК РФ), информация, являющаяся объектом авторских и смежных прав (ст. 1255 ГК РФ, ст. 146 УК РФ);

− информация, непосредственно затрагивающая права и свободы гражданина или персональные данные (ФЗ «Об информации, информационных технологиях и о защите информации», ст. 140 УК РФ) и др.

Уголовный кодекс РФ вводит нормы, объявляющие общественно опасными деяниями конкретные действия в сфере компьютерной информации и устанавливающие ответственность за их совершение. К преступлениям отнесены неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273) и нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274).

В тех случаях, когда общественно опасные действия в области информационных отношений совершаются без применения компьютерных средств, законодатель нередко относит их к другим соответствующим родовым объектам.

Клевета или оскорбление (ст. 129, 130), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138), отказ в предоставлении гражданину информации (ст. 140), нарушение авторских, смежных изобретательских и патентных прав (ст. 146, 147), разглашение тайны усыновления (удочерения) (ст. 155) находятся в разделе «Преступления против личности».

Кража, мошенничество, хищение предметов, имеющих особую ценность, умышленное уничтожение или повреждение имущества, заведомо ложная реклама, изготовление и сбыт поддельных кредитных карт, незаконный экспорт технологий, научно-технической информации (ст. 158, 159, 164, 167, 182, 187, 189) – в разделе «Преступления в сфере экономики» и т.д.

2.2. Защита государственной тайны

Государственная тайна как особый вид защищаемой информации. Ущерб от утечки сведений, составляющих государственную тайну. Система защиты государственной тайны. Способы защиты государственной тайны. Режим секретности.

Основные термины и понятия:

Государственная тайна
Защита сведений, составляющих государственную тайну, и их носителей
Сведения особой важности
Сведения секретные
Сведения совершенно секретные
Система защиты государственной тайны

Государственная тайна как особый вид защищаемой информации

В современном мире информация рассматривается как один из наиболее ценных продуктов человеческой жизнедеятельности, а информационные ресурсы и технологии, которыми располагает государство, определяют его стратегический потенциал и влияние в мире. В результате безопасность государства, его общественно-политических институтов, организаций и граждан включает в настоящее время в качестве обязательной составляющей информационную безопасность. Важным элементом информационных ресурсов является государственная тайна, отнесенная по условиям правового режима к документированной информации ограниченного распространения.

Тайны являются неотъемлемой составляющей общественной жизни, частью правовой системы и могут служить даже своеобразным мерилом для определения вида политического режима в государстве, ибо состояние защиты секретов отражает характер взаимоотношений общества и государства, демократизации государственной власти.

Государственные средства воздействия на информационные процессы − важнейшее политическое условие обеспечения прав человека и рационализации использования информационных ресурсов в обществе. Система защиты секретов − наиболее сильное звено государственного опосредования общественных отношений в информационной сфере. Сведения, составляющие государственную тайну, имеют особую важность для общества и государства.

Вследствие величины возможного ущерба от её разглашения государственная тайна занимает приоритетное место в системе социального института тайн. Режим защиты государственной тайны – важнейший элемент системы государственного управления.

Правовой институт государственной тайны − признанный всеми странами институт регулирования информационных общественных отношений. Государственная секретность в той или иной степени наличествует во всех государствах мира. Это вполне объяснимо и логично, поскольку информация, с одной стороны − объект отношений людей, а с другой − ресурс: ресурс управления, принятия решений. Поэтому в качестве реальной

угрозы своей безопасности государства рассматривают потенциально возможную утечку защищаемой информации за границу.

Правовой институт государственной тайны имеет три составляющие:

1) сведения, относимые к определенному типу тайны (а также принципы и критерии, по которым сведения классифицируются как тайна);

2) режим секретности (конфиденциальности) − механизм ограничения доступа к указанным сведениям, т.е. механизм их защиты;

3) санкции за неправомерное получение и (или) распространение этих сведений.

Понятие «государственная тайна» является одним из важнейших в системе защиты государственных секретов в любой стране. От её правильного определения зависит и политика руководства страны в области защиты секретов. Определение этого понятия дано в Законе РФ «О государственной тайне».

Государственная тайна − *защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.*

В этом определении указываются категории сведений, которые защищаются государством, и сообщается, что распространение этих сведений может нанести ущерб интересам государственной безопасности. Для сравнения приведем краткие определения понятия «государственная тайна», даваемые специалистами других стран.

В Уголовном кодексе ФРГ зафиксировано, что государственной тайной являются факты, предметы или познания, которые доступны лишь ограниченному кругу лиц и должны содержаться в тайне от иностранного правительства, чтобы предотвратить опасность наступления тяжкого ущерба для внешней безопасности ФРГ.

В Исполнительном Указе Президента США от 2.04.1982 г. говорится, что к информации по национальной безопасности

относится определенная информация по национальной обороне и международным вопросам, которая защищается от несанкционированного раскрытия.

В некоторых странах это понятие выражается в других терминах, например, в Японии – «оборонный секрет».

Модель определения государственных секретов обычно включает в себя следующие существенные признаки:

1) предметы, явления, события, области деятельности, составляющие государственную тайну;

2) противник (данный или потенциальный), от которого в основном осуществляется защита государственной тайны;

3) указание в законе, перечне или инструкции сведений, составляющих государственную тайну;

4) наносимый ущерб обороне, внешней политике, экономике, научно-техническому прогрессу страны и т.п. в случае разглашения (утечки) сведений, составляющих государственную тайну.

Важным признаком государственной тайны является степень секретности сведений, отнесенных к ней. В нашей стране принята следующая система обозначения сведений, составляющих государственную тайну: «особой важности», «совершенно секретно», «секретно». Эти грифы проставляются на документах или изделиях (их упаковках или сопроводительных документах). Содержащиеся под этими грифами сведения являются государственной тайной.

К сведениям **особой важности** (Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности, указанные в Постановлении Правительства РФ от 4 сентября 1995 г. № 870) следует относить такие сведения, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких областях.

К **совершенно секретным** сведениям следует относить такие сведения, распространение которых может нанести ущерб интересам министерства (ведомства) или отраслям экономики Российской Федерации в одной или нескольких областях.

К **секретным** сведениям следует относить все иные из числа сведений, составляющих государственную тайну. Ущерб может быть нанесен интересам предприятия, учреждения или организации.

Перечень сведений, которые могут быть отнесены к государственной тайне, содержится в ст. 5 Закона РФ «О государственной тайне».

Государственную тайну составляют:

1) **сведения в военной области:**

– о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, предусмотренных Федеральным законом «Об обороне», об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;

– о планах строительства Вооруженных Сил Российской Федерации, других войск Российской Федерации, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

– о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, о технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;

– о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

– о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;

– о дислокации, действительных наименованиях, об организационной структуре, о вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

2) **сведения в области экономики, науки и техники:**

– о содержании планов подготовки Российской Федерации и её отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, о запасах стратегических видов сырья и материалов, а также о размещении, фактических размерах и об использовании государственных материальных резервов;

– об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства;

– о силах и средствах гражданской обороны, о дислокации, предназначении и степени защищенности объектов административного управления, о степени обеспечения безопасности населения, о функционировании транспорта и связи в Российской Федерации в целях обеспечения безопасности государства;

– об объемах, о планах (заданиях) государственного оборонного заказа, о выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, о наличии и наращивании мощностей по их выпуску, о связях предприятий по кооперации, о разработчиках или об изготовителях указанного вооружения, военной техники и другой оборонной продукции;

– о достижениях науки и техники, о научно-исследовательских, об опытно-конструкторских, о проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

– об объемах запасов, добычи, передачи и потребления платины, металлов платиновой группы, природных алмазов, а также об объемах других стратегических видов полезных ископаемых Российской Федерации (по списку, определяемому Правительством Российской Федерации);

3) **сведения в области внешней политики и экономики:**

– о внешнеполитической, внешнеэкономической деятельности Российской Федерации, преждевременное распространение которых может нанести ущерб безопасности государства;

– о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной

деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;

4) **сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:**

– о силах, средствах, об источниках, о методах, планах и результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

– о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;

– об организации, о силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если эти данные раскрывают перечисленные сведения;

– о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной связи, о шифрах, о разработке, об изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения;

– о методах и средствах защиты секретной информации;

– об организации и о фактическом состоянии защиты государственной тайны;

– о защите Государственной границы Российской Федерации, исключительной экономической зоны и континентального шельфа Российской Федерации;

– о расходах федерального бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности в Российской Федерации;

– о подготовке кадров, раскрывающие мероприятия, проводимые в целях обеспечения безопасности государства.

В статье 7 Закона РФ «О государственной тайне» приведён перечень сведений, **не подлежащих** отнесению к государственной тайне и засекречиванию. Не подлежат отнесению к государственной тайне и засекречиванию сведения:

– о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

– о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

– о фактах нарушения прав и свобод человека и гражданина;

– о размерах золотого запаса и государственных валютных резервах Российской Федерации;

– о состоянии здоровья высших должностных лиц Российской Федерации;

– о фактах нарушения законности органами государственной власти и их должностными лицами.

Ущерб от утечки сведений, составляющих государственную тайну

Понятие, виды и размер ущерба разработаны пока ещё недостаточно и, видимо, будут различны для каждого конкретного объекта защиты: содержания сведений, составляющих государственную тайну, сущности отраженных в ней фактов, событий, явлений действительности. В зависимости от вида, содержания и размеров ущерба можно выделить группы некоторых видов ущерба при утечке (или возможной утечке) сведений, составляющих государственную тайну.

Политический ущерб может наступить при утечке сведений политического и внешнеполитического характера, о разведывательной деятельности спецслужб государства и др. Политический ущерб может выражаться в том, что в результате утечки информации могут произойти серьезные изменения в международной обстановке не в пользу Российской Федерации, утрата страной политических приоритетов в каких-то областях, ухудшение отношений с какой-либо страной или группой стран и т.д.

Экономический ущерб может наступить при утечке сведений любого содержания: политического, экономического, военного, научно-технического и т.д. Экономический ущерб может быть выражен прежде всего в денежном исчислении. Экономические потери от утечки информации могут быть прямые и косвенные.

Прямые потери могут наступить в результате утечки секретной информации о системах вооружения, обороны страны, которые в результате этого практически потеряли или утратили свою эффективность и требуют крупных затрат на их замену или переналадку. Косвенные потери чаще всего выражаются в виде размера упущенной выгоды: срыв переговоров с иностранными фирмами, о выгодных сделках с которыми ранее была договоренность; утрата приоритета в научном исследовании, в результате чего соперник быстрее довел свои исследования до завершения и запатентовал их и т.д.

Моральный ущерб, как правило, неимущественного характера, наступает от утечки информации, вызвавшей или инициировавшей противоправную государству пропагандистскую кампанию, подрывающую репутацию страны, приведшую к выдворению из каких-то государств наших дипломатов, разведчиков, действовавших под дипломатическим прикрытием, и т.п.

Тенденция увеличения степени открытости государства перед обществом диктует необходимость максимально возможного сокращения числа сведений, относимых к государственной тайне, открытости общего перечня относимых к ней категорий сведений, механизмов засекречивания и условий рассекречивания. Обязанность государства − взять на себя формирование взвешенного механизма защиты различных видов информации и установления рамок действия институтов тайн. Такие требования возникают из потребности современного общества быть более открытым и доступным, и диктуются необходимостью обеспечения безопасности личности, общества и государства.

Система защиты государственной тайны

В общем смысле защита информации − комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих её распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и её носителям.

Защита информации разбивается на решение двух основных групп задач:

1) своевременное и полное удовлетворение информационных потребностей, возникающих в процессе управленческой,

инженерно-технической, маркетинговой и иной деятельности, т.е. обеспечение специалистов организаций, предприятий и фирм секретной или конфиденциальной информацией;

2) ограждение засекреченной информации от несанкционированного доступа к ней соперника, других субъектов в злонамеренных целях.

При решении первой группы задач учитывается, что специалисты могут использовать как открытую, так и засекреченную информацию. Снабжение специалистов открытой информацией ничем не ограничивается, кроме её фактического наличия. При снабжении же специалиста засекреченной информацией действуют ограничения: наличие соответствующего допуска (к какой степени секретности информации он допущен) и разрешения на доступ к конкретной информации. В решении проблемы доступа специалиста к соответствующей засекреченной информации всегда существуют противоречия: необходимо, с одной стороны, максимально ограничить его доступ к засекреченной информации и тем самым уменьшить вероятность утечки этой информации, а с другой – наиболее полно удовлетворить его потребности в информации, в том числе и засекреченной, для обоснованного решения им служебных задач.

Вторая группа задач включает в себя такие условия, как:

– защита информационного суверенитета страны и расширение возможностей государства по укреплению своего могущества за счёт формирования и управления развитием своего информационного потенциала;

– обеспечение безопасности защищаемой информации: предотвращение хищения, утраты, несанкционированного уничтожения, модификации, блокирования информации и т.п., вмешательства в информацию и информационные системы;

– сохранение секретности информации в соответствии с установленными правилами её защиты, в том числе предупреждение её утечки и несанкционированного доступа к её носителям;

– сохранение полноты, достоверности, целостности информации и её массивов и программ обработки;

– недопущение безнаказанного растаскивания и незаконного использования интеллектуальной собственности, принадлежащей государству.

Вопросы защиты государственной тайны приобрели особую значимость в последние годы, в период глубоких социально-экономических преобразований в РФ, когда, с одной стороны, появились новые угрозы безопасности государства, а, с другой стороны, сложившиеся режимы защиты государственной тайны перестают срабатывать должным образом.

В ст. 2 Закона РФ «О государственной тайне» дано определение системы защиты государственной тайны.

Система защиты государственной тайны – *совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.*

Система защиты сведений, отнесенных к государственной тайне, и их носителей складывается из:

- органов защиты государственной тайны;
- средств и методов защиты государственной тайны;
- проводимых мероприятий.

Защита сведений, составляющих государственную тайну, и их носителей – *деятельность органов защиты этой тайны, направленная на обеспечение безопасности информации, отнесенной к государственной тайне, предотвращение её утечки и её максимально эффективное использование.*

Главным субъектом, осуществляющим защиту сведений, составляющих государственную тайну, является государство в лице его высших органов власти и управления, которое располагает всей полнотой властных полномочий по решению задач защиты государственной тайны. В ст. 4 Закона РФ «О государственной тайне» определены полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защите. Распоряжением Президента РФ от 11 февраля 1994 г. № 73-рп утвержден перечень должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне.

Высшие органы государственной власти и управления создают нормативно-правовую базу, регламентирующую деятельность по защите сведений, отнесенных к государственной тайне. Координация деятельности по разработке и выполнению государственных программ, по подготовке нормативных и методических документов, обеспечивающих реализацию законодательства РФ о государственной тайне, возложена на Межведомственную комиссию. Каждый орган и должностное лицо наделяются полномочиями по проведению организационно-правовых мероприятий по защите государственной тайны (Закон РФ «О государственной тайне», ст. 20).

В систему защиты государственной тайны включаются кроме мер, осуществляемых непосредственно в местах сосредоточения и обращения сведений, составляющих эту тайну, также проводимые государством мероприятия и устанавливаемые административно-правовые режимы:

- борьба со шпионажем и разглашением государственной тайны;
- охрана государственных тайн в печати;
- пограничный режим;
- режим въезда и передвижения иностранцев;
- режим выезда специалистов в служебные командировки за границу.

Они в качестве составных элементов включаются в систему защиты государственной тайны и в большинстве своём играют роль препятствия, преграды в возможных каналах утечки секретной информации.

Рассматривая проблемы деятельности по защите государственной тайны, можно назвать ряд факторов, которые предопределяют её формирование и состояние. Организация деятельности по защите государственных секретов в стране зависит от военно-политической обстановки в мире и стране. Обострение международной обстановки обычно приводит к усилению деятельности спецслужб противоборствующих сторон и соответственно к ужесточению принимаемых мер по защите своих секретов.

Уровень защиты секретной информации в определенной степени должен соответствовать важности этой информации для собственника и интенсивности действий потенциального противника по добыванию секретов о нашем государстве. Защита секретов должна носить превентивный характер: меры защиты

секретной информации должны предупреждать возможность несанкционированного доступа к засекреченной информации и возможные вредные последствия, которые могут наступить в случае утечки секретной информации.

Организация защиты государственной тайны находится в зависимости от принятой системы и критериев засекречивания информации: чем больше засекречивается информации, тем больше требуется сотрудников для её обработки, хранения и выдачи, тем выше стоимость её защиты; чем выше степень секретности информации, тем выше уровень её защиты, и т.д. После засекречивания информация начинает жить своей собственной жизнью: практически уже не имеет значения, произведено засекречивание сведений, действительно составляющих государственную тайну, или информация засекречена «на всякий случай», чтобы что-то скрыть и т.п. Секретная информация сама начинает «диктовать» условия своей защиты режимным службам и другим исполнителям.

Расширение круга засекречиваемых сведений и значительное увеличение в связи с этим количества секретной информации затрудняет её защиту, а увеличение числа лиц, допущенных к этой информации, усиливает вероятность её утечки. А это начинает противоречить одному из основных принципов защиты секретной информации – максимальному ограничению числа лиц, допускаемых к секретам.

Система защиты информации включает в себя совокупность элементов, её образующих, и их свойства. Внутренние связи системы и их свойства составляют архитектуру системы, её структуру и внутреннюю организацию. Одновременно элементы системы имеют внешние связи, которые целенаправленно воздействуют на внешнюю среду и решают поставленные перед системой задачи, это – функциональная часть системы. Вполне естественно, что обе части системы – структурная и функциональная – не отделены друг от друга: это как бы две стороны одних и тех же элементов, составляющих систему защиты информации.

Структурная часть системы защиты информации составляет её внутреннюю организацию, которая позволяет системе нормально функционировать, создает условия для обеспечения

безопасности засекреченной информации, её обращения только по каналам, контролируемым данной системой.

Структурная часть системы защиты информации включает:

1) систему законов и других нормативных актов, устанавливающих:

− порядок и правила защиты информации, а также ответственность за покушение на защищаемую информацию или на установленный порядок её защиты;

− защиту прав граждан, связанных по службе со сведениями, отнесенными к охраняемой тайне;

− права и обязанности государственных органов, предприятий и должностных лиц в области защиты информации;

2) систему засекречивания информации, в которую входят:

− законодательное определение категории сведений, которые могут быть отнесены к государственной тайне;

− законодательное и иное правовое определение категорий сведений, которые не могут быть отнесены к государственной тайне;

− наделение полномочиями органов государственной власти и должностных лиц в области отнесения сведений к охраняемой законом тайне;

− составление перечней сведений, отнесенных к государственной тайне;

3) систему режимных служб и служб безопасности с их собственной структурой, штатным расписанием, обеспечивающими функционирование всей системы защиты информации.

Структурная часть системы защиты информации является устойчивой частью данной системы, её консервативной частью. Как видно из перечисления основных элементов структурной части системы, её элементы могут изменяться только «скачкообразно», они не могут приспосабливаться быстро и непрерывно в зависимости от изменения внешней среды, а также изменения обстановки, поскольку внешняя среда может оказывать влияние на структурную часть системы защиты информации лишь через её функциональную часть, т.е. опосредованно.

Функциональная часть системы защиты информации решает задачи обеспечения засекреченной информацией деятельности вышестоящей системы, в которую данная система защиты информации «встроена». В эту деятельность вовлекается широкий

круг работников объекта: сотрудники службы безопасности, связанные с обработкой, хранением, выдачей и учётом засекреченной информации; руководители объекта и структурных подразделений; исполнители, т.е. все работники объекта, которые являются потребителями защищаемой информации.

Способы защиты государственной тайны

Основными организационными и техническими способами, используемыми в защите государственной тайны, являются: скрытие, ранжирование, дробление, учёт, дезинформация, морально-нравственные меры, кодирование и шифрование.

Скрытие как метод защиты информации является в основе своей реализацией на практике одного из основных организационных принципов защиты информации – максимального ограничения числа лиц, допускаемых к секретам. Скрытие – один из наиболее общих и широко применяемых методов защиты информации. Реализация этого метода достигается обычно путём:

– засекречивания информации, т.е. отнесения её к секретной или конфиденциальной информации различной степени секретности и ограничения в связи с этим доступа к этой информации в зависимости от её важности для собственника, что проявляется в проставляемом на носителе этой информации грифе секретности;

– устранения или ослабления технических демаскирующих признаков объектов защиты и технических каналов утечки сведений о них.

Ранжирование как метод защиты информации включает, во-первых, деление засекречиваемой информации по степени секретности и, во-вторых, регламентацию допуска и разграничение доступа к защищаемой информации: предоставление индивидуальных прав отдельным пользователям на доступ к необходимой им конкретной информации и на выполнение отдельных операций. Разграничение доступа к информации может осуществляться по тематическому признаку или по признаку секретности информации и определяется матрицей доступа. Ранжирование как метод защиты информации является частным случаем метода скрытия: пользователь не допускается к информации, которая ему не нужна для выполнения его служебных

функций, и тем самым эта информация скрывается от него и всех остальных (посторонних) лиц.

Дезинформация – метод защиты информации, заключающийся в распространении заведомо ложных сведений относительно истинного назначения каких-то объектов и изделий, действительного состояния какой-то области государственной деятельности. Дезинформация обычно проводится путем распространения ложной информации по различным каналам, имитацией или искажением признаков и свойств отдельных элементов объектов защиты, создания ложных объектов, по внешнему виду или проявлениям похожих на интересующие соперника объекты, и др.

Дробление (расчленение) информации на части с таким условием, что знание какой-то одной части информации (например, знание одной операции технологии производства какого-то продукта) не позволяет восстановить всю картину, всю технологию в целом. Этот способ применяется достаточно широко при производстве средств вооружения и военной техники, а также при производстве товаров народного потребления.

Морально-нравственные способы защиты информации можно отнести к группе тех методов, которые, исходя из расхожего выражения, что «тайну хранят не замки, а люди», играют очень важную роль в защите информации. Именно человек, сотрудник предприятия или учреждения, допущенный к секретам и накапливающий в своей памяти колоссальные объёмы информации, в том числе секретной, нередко становится источником утечки этой информации или по его вине соперник получает возможность несанкционированного доступа к носителям защищаемой информации.

Морально-нравственные методы защиты информации предполагают прежде всего воспитание сотрудника, допущенного к секретам, т.е. проведение специальной работы, направленной на формирование у него системы определенных качеств, взглядов и убеждений (патриотизма, понимания важности и полезности защиты информации и для него лично), и обучение сотрудника, осведомленного в сведениях, составляющих охраняемую тайну, правилам и методам защиты информации, привитие ему навыков работы с носителями секретной и конфиденциальной информации.

Учёт также является одним из важнейших методов защиты информации, обеспечивающим возможность получения в любое время данных о любом носителе защищаемой информации, о количестве и местонахождении всех носителей засекреченной информации, а также данные обо всех пользователях этой информации. Без учёта решать проблемы было бы невозможно, особенно когда количество носителей превысит какой-то минимальный объём.

Принципы учёта засекреченной информации:

1) обязательность регистрации всех носителей защищаемой информации;

2) однократность регистрации конкретного носителя такой информации;

3) указание в учётах адреса, где находится в данное время данный носитель засекреченной информации;

4) единоличная ответственность за сохранность каждого носителя защищаемой информации и отражение в учётах пользователя данной информации в настоящее время, а также всех предыдущих пользователей данной информации.

Кодирование – метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации и заключающийся в преобразовании с помощью кодов открытого текста в условный при передаче информации по каналам связи, направлении письменного сообщения, когда есть угроза, что оно может попасть в руки соперника, а также при обработке и хранении информации в средствах вычислительной техники.

Для кодирования используются обычно совокупность знаков (символов, цифр и др.) и система определенных правил, при помощи которых информация может быть преобразована (закодирована) таким образом, что прочесть её можно будет только если потребитель располагает соответствующим ключом (кодом) для её раскодирования. Кодирование информации может производиться с использованием технических средств или вручную.

Шифрование – метод защиты информации, используемый чаще при передаче сообщений с помощью различной радиоаппаратуры, направлении письменных сообщений и в других случаях, когда есть опасность перехвата этих сообщений соперником.

Шифрование заключается в преобразовании открытой информации в вид, исключающий понимание его содержания, если перехвативший не имеет сведений (ключа) для раскрытия шифра.

Шифрование может быть предварительным (шифруется текст документа) и линейным (шифруется разговор). Для шифрования информации может использоваться специальная аппаратура.

Знание возможностей приведенных методов позволяет активно и комплексно применять их при рассмотрении и использовании правовых, организационных и инженерно-технических мер защиты секретной информации.

Режим секретности

При рассмотрении проблем защиты информации часто затрагивается вопрос о режиме секретности или конфиденциальности (в дальнейшем – режим секретности). Понятие «режим секретности» тесно связано с понятием «защита информации», переплетается с ним, а иногда и отождествляется.

Режим секретности является частью системы защиты засекреченной информации, а точнее, это реализация системы защиты информации для конкретного объекта или одного из его структурных подразделений или конкретной работы.

Основное назначение режима секретности – обеспечить соответствующий уровень защиты информации, т.к. чем выше степень её секретности, тем более высокий уровень её защиты устанавливается, соответственно изменяется и режим секретности. Режим секретности – это не регламентация правовых норм и правил защиты сведений, а реализация на конкретном объекте действующих норм и правил защиты сведений, составляющих государственную тайну, установленных и регламентированных соответствующими законодательными и подзаконными нормативными актами.

Режим секретности включает следующие группы мер:

– разрешительную систему, определяющую порядок доступа в служебных целях конкретных сотрудников к определенной защищаемой информации и в конкретные помещения, где ведутся конфиденциальные или секретные работы;

– порядок и правила делопроизводства с секретными или конфиденциальными документами и иными носителями защищаемой информации. Возможно разделение потоков документальной

информации по степени секретности сведений, содержащихся в документах, а также разделение потоков информации, документов, содержащих государственную и коммерческую тайну;

– установление пропускного и внутри объектового режима, соответствующего степени секретности информации, имеющейся на объекте;

– воспитательно-профилактическую работу, уровень и содержание которой должны соответствовать уровню требуемой защиты информации с целью предотвратить или значительно уменьшить риск утечки засекреченной информации через сотрудников объекта, работающих с такой информацией.

В рамках установленного на объекте режима секретности проводятся все остальные мероприятия по защите сведений, составляющих государственную тайну.

2.3. Конфиденциальная информация и её защита

Коммерческая тайна. Служебная тайна. Профессиональные тайны. Персональные данные.

Основные термины и понятия:
Коммерческая (служебная) тайна
Персональные данные
Профессиональная тайна

С развитием информационного общества проблемы, связанные с защитой конфиденциальной информации, приобретают всё большее значение. В настоящее время в российском законодательстве данные вопросы полно и системно не решены. Развернутая классификация конфиденциальной информации, как уже говорилось выше, приводится в перечне сведений конфиденциального характера, установленном Указом Президента РФ от 6 марта 1997 г. № 188. Далее мы рассмотрим более подробно некоторые виды конфиденциальной информации.

Коммерческая тайна

Коммерческая деятельность организации тесно связана с получением, накоплением, хранением, обработкой и использованием разнообразной информации. Защите подлежит не вся

информация, а только та, которая представляет ценность для организации. При определении ценности коммерческой информации необходимо руководствоваться такими её свойствами, как полезность, своевременность и достоверность.

Полезность информации состоит в том, что она создает субъекту выгодные условия для принятия оперативного решения и получения эффективного результата. В свою очередь полезность информации зависит от своевременного её получения и доведения до исполнителя. Из-за несвоевременного поступления важных по своему содержанию сведений часто упускается возможность заключить выгодную торговую или иную сделку.

Критерии полезности и своевременности тесно взаимосвязаны и взаимозависимы с критерием достоверности информации. Причины возникновения недостоверных сведений различны: неправильное восприятие (в силу заблуждения, недостаточного опыта или профессиональных знаний) фактов или умышленное, предпринятое с определенной целью, их искажение. Поэтому, как правило, сведения, представляющие коммерческий интерес, а также источник их поступления должны подвергаться перепроверке.

Коммерческая (служебная) тайна негосударственной организации – *сведения, не являющиеся государственными секретами, которые связаны с производственной, управленческой, финансовой или иной деятельностью организации и распространение которых может нанести ущерб её интересам.*

Собственник коммерческой информации на основании совокупности перечисленных критериев определяет её ценность для своей хозяйственной деятельности и принимает соответствующее оперативное решение.

В зарубежной экономической литературе коммерческая информация рассматривается не в качестве средства извлечения прибыли, а, прежде всего, как условие, способствующее или препятствующее получению прибыли. Особо подчеркивается наличие стоимостного фактора коммерческой информации, т.е. возможность выступать в качестве предмета купли-продажи. Поэтому важное значение в условиях развития многообразных

форм собственности имеет вопрос об определении принадлежности информации на правах интеллектуальной собственности конкретному субъекту предпринимательства, а в итоге – о наличии у него прав на её защиту.

Определение и вопросы гражданско-правовой защиты служебной и коммерческой тайны в российском законодательстве не различаются и рассмотрены в ст. 139 части первой ГК РФ, называющейся «Служебная и коммерческая тайна»:

«Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране её конфиденциальности. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами.

Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим Кодексом и другими законами.

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору».

Обеспечение защиты государственной тайны не имеет прямого отношения к защите коммерческой тайны. Однако следует указать на некоторые возможные исключения. Под защиту государства может быть взята коммерческая информация, оцененная как особо важная не только для её собственника, но и для государства, когда не исключено, что к ней может проявить интерес иностранная спецслужба. Вопрос о подобной защите должен решаться на договорной основе между предпринимателем и органом федеральной безопасности с обозначением пределов и функций профессиональной деятельности последних. Что касается собственно коммерческой тайны, то она специальной уголовно-правовой и режимной защитой не обладает.

Действительная или потенциальная коммерческая ценность информации во многом носит субъективный характер и позволяет предпринимателю ограничивать доступ к практически любым сведениям, используемым в предпринимательской деятельности, за исключением сведений, определяемых нормативно-правовым и актами.

Какие сведения не могут составлять коммерческую тайну? В постановлении Правительства РСФСР от 5 декабря 1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну» обозначены:

– учредительные документы (решение о создании предприятия или договор учредителей) и Устав;

– документы, дающие право заниматься предпринимательской (деятельностью (регистрационные удостоверения, лицензии, патенты);

– сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему РСФСР;

– документы о платежеспособности;

- сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;

– документы об уплате налогов и обязательных платежах;

– сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения, а также других нарушениях законодательства РСФСР и размерах причиненного при этом ущерба;

– сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, товариществах, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

Этим же нормативным актом запрещено государственным и муниципальным предприятиям до и в процессе их приватизации относить к коммерческой тайне данные:

– о размерах имущества предприятия и его денежных средствах;

– о вложении средств в доходные активы (ценные бумаги) других предприятий, в процентные облигации и займы, в уставные фонды совместных предприятий;

– о кредитных, торговых и иных обязательствах предприятия, вытекающих из законодательства РСФСР и заключенных им договоров;

– о договорах с кооперативами, иными негосударственными предприятиями, творческими и временными трудовыми коллективами, а также отдельными гражданами.

Следует отметить, что ограничения, вводимые на использование сведений, составляющих коммерческую тайну, направлены на защиту интеллектуальной, материальной, финансовой собственности и других интересов, возникающих при формировании трудовой деятельности организации, персонала подразделений, а также при их сотрудничестве с работниками других организаций.

Целью таких ограничений является предотвращение разглашения, утечки или несанкционированного доступа к конфиденциальной информации. Ограничения должны быть целесообразными и обоснованными с точки зрения необходимости обеспечения информационной безопасности. Не допускается использование ограничений для сокрытия ошибок и некомпетентности руководства организации, расточительства, недобросовестной конкуренции и других негативных явлений в деятельности организации, а также для уклонения от выполнения договорных обязательств и уплаты налогов.

Служебная тайна

Если основной целью обеспечения конфиденциальности информации, составляющей коммерческую тайну, является обеспечение конкурентного превосходства, то защита конфиденциальности служебной тайны, хотя и может затрагивать коммерческие интересы организации, но главной задачей имеет обеспечение интересов клиентов либо собственных интересов, непосредственно не связанных с коммерческой деятельностью. Так, к служебной, а не к коммерческой, тайне следует отнести сведения, касающиеся мер по обеспечению безопасности сотрудников организации, охране складских и иных помещений и

др., прямо не связанные с осуществлением предметной деятельности.

В настоящее время институт служебной тайны в отечественном праве является наименее разработанным. В этой проблеме можно выделить три ряда вопросов.

Во-первых, на законодательном уровне требуют урегулирования вопросы «пограничных» и «производных» сведений. «Пограничные» сведения – это такая служебная информация в любой отрасли науки, техники, производства и управления, которая при определенном обобщении и интеграции становится государственной тайной. «Производные» сведения – служебная информация, полученная в результате дробления сведений, составляющих государственную тайну, на отдельные компоненты, каждый из которых не может быть к ней отнесен.

Во-вторых, особого правового регулирования требует защита сведений, образующихся в деятельности органов государственной власти и управления. Для формирования административно-правового института служебной тайны следует принять специальный закон, действие которого должно распространяться на все уровни системы государственного управления.

В-третьих, требует защиты определенная категория значимых сведений субъектов гражданско-правовых отношений. Здесь имеется в виду правовая защита сведений, которые в деятельности организаций не могут быть отнесены к коммерческой тайне, несмотря на то, что в ГК РФ понятие служебной тайны напрямую связано с действительной или потенциальной коммерческой ценностью информации.

Следует заметить, что в настоящее время практикуется упрощенный подход: любые сведения о предпринимательской деятельности организации, доступ к которым ограничен, относят к коммерческой тайне. Однако при таком подходе могут возникнуть трудности определения материального ущерба и упущенной выгоды при неправомерном распространении конфиденциальной информации, например сведений о режиме охраны организации или других аспектах её функционирования, напрямую не связанных с осуществлением предметной деятельности. Вместе с тем указанные сведения необходимо защищать, т.к. от ограничения доступа к ним в значительной степени зависит коммерческий успех организации.

Профессиональные тайны

В соответствии с действующим законодательством к профессиональной тайне относится информация, связанная со служебной деятельностью медицинских работников, нотариусов, адвокатов, частных детективов, священнослужителей, работников банков, ЗАГСов, учреждений страхования. В качестве субъекта профессиональной тайны может выступать как юридическое, так и физическое лицо.

Профессиональная тайна – *информация, защита которой от несанкционированного распространения является обязанностью субъекта в силу выполняемых им профессиональных функций.*

Сохранение в тайне сведений, полученных в связи с выполнением профессиональных функций, вызвано в первую очередь нормами профессиональной этики, а не собственными коммерческими интересами предпринимателя или организации. Соответствующий правовой статус рассматриваемым нормам придает их законодательное закрепление.

1) **банковская тайна**. Понятие банковской тайны, в соответствии со ст. 857 ГК РФ, охватывает сведения о банковском счёте, вкладе, операциях по счёту, а также сведения о клиентах банка.

Банковская тайна защищает конфиденциальную информацию клиента или коммерческую информацию корреспондента.

ФЗ «О банках и банковской деятельности» определяет обязанности субъектов, категории информации и основания, по которым сведения предоставляются заинтересованным органам государственной власти, организациям и лицам. Кредитная организация, Банк России гарантируют тайну об операциях, о счётах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, счётах и вкладах её клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

Банк России не вправе разглашать сведения о счетах, вкладах, а также сведения о конкретных сделках и об операциях из отчетов кредитных организаций, полученные им в результате

исполнения лицензионных, надзорных и контрольных функций, за исключением случаев, предусмотренных федеральными законами.

Таким образом, кредитная организация вправе относить к банковской тайне любые сведения, за исключением прямо указанных в Законе.

2) **нотариальная тайна**. Тайна является специфическим правилом нотариальных действий. В соответствии со ст. 5 Основ законодательства РФ о нотариате нотариусу при исполнении служебных обязанностей, а также лицам, работающим в нотариальной конторе, запрещается разглашать сведения, оглашать документы, которые стали им известны в связи с совершением нотариальных действий, в том числе и после сложения полномочий или увольнения, за исключением случаев, предусмотренных Основами. Обязанность хранить профессиональную тайну включена в текст присяги нотариуса.

3) **процессуальные тайны** обычно делят на два вида: следственную тайну и тайну совещания судей.

Следственная тайна связана с интересами законного производства предварительного расследования по уголовным делам (ст. 310 УК РФ «Разглашение данных предварительного расследования»). Сведения о ходе предварительного расследования могут быть преданы гласности только с разрешения прокурора, следователя или лица, производящего дознание. Такая информация может касаться как характера производимых следственных действий, так и доказательственной базы, перспектив расследования, круга лиц, участвующих в расследовании. Важно отметить, что законодательно не закреплен перечень сведений, составляющих следственную тайну. Это означает, что прокурор, следователь или лицо, производящее дознание, могут по своему усмотрению устанавливать, какая информация о предварительном расследовании может быть специально охраняемой, а какая – нет.

Тайна совещания судей. Для всех четырех видов существующих в отечественном судопроизводстве процессов предусмотрена определенная процедура обеспечения независимости и объективности вынесения решения по делу. Эта процедура имеет одной из целей запрет на разглашение информации о дискуссиях, суждениях, результатах голосования, которые имели место во время совещания судей. Обеспечение тайны совещания судей

устанавливается ст. 193 Гражданским Процессуальным Кодексом (ГПК) РФ, ст. 70 Федерального конституционного закона «О Конституционном суде Российской Федерации», ст. 124 Арбитражного процессуального кодекса Российской Федерации.

4) **врачебная тайна**. Согласно ст. 61 Основ законодательства РФ об охране здоровья граждан информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении, составляют врачебную тайну. Гражданину должна быть подтверждена гарантия конфиденциальности передаваемых им сведений.

5) **адвокатская тайна**. В соответствии с ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» адвокат, помощник адвоката и стажер адвоката не вправе разглашать сведения, сообщенные доверителем в связи с оказанием ему юридической помощи. Причем доверительные сведения, полученные адвокатом, могут быть как в виде документов, так и в устном виде. Законом установлены гарантии независимости адвоката. В частности, адвокат не может быть допрошен в качестве свидетеля об обстоятельствах, которые стали ему известны в связи с исполнением им обязанностей защитника или представителя (ст. 15 Закона).

6) **тайна страхования**. Институт страховой тайны во многих отношениях схож с институтом банковской тайны. Тайну страхования, в соответствии со ст. 946 ГК РФ, составляют полученные страховщиком в результате своей профессиональной деятельности сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц. За нарушение тайны страхования страховщик в зависимости от рода нарушенных прав и характера нарушения несет ответственность в соответствии с правилами, предусмотренными ст. 139 или ст. 150 ГК РФ.

Согласно ст. 8 Закона РФ «Об организации страхового дела в Российской Федерации» в качестве лица, обязанного сохранять тайну страхования, могут выступать как юридические, так и физические лица – страховые агенты и страховые брокеры. Кроме того, в соответствии со ст. 33 указанного Закона должностные лица федерального органа исполнительной власти по надзору за страховой деятельностью не вправе использовать в

корыстных целях и разглашать в какой-либо форме сведения, составляющие коммерческую тайну страховщика.

7) **тайна связи.** ФЗ «О связи» в части защиты информации регулирует общественные отношения, связанные с обеспечением невозможности противоправного ознакомления с сообщениями, передаваемыми любыми субъектами – физическими или юридическими лицами – по средствам связи. При такой постановке вопроса тайна связи становится инструментом обеспечения сохранности конфиденциальной информации.

Тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, охраняется Конституцией РФ. Обязанность обеспечения соблюдения тайны связи возлагается на оператора связи, под которым понимается физическое или юридическое лицо, имеющее право на предоставление услуг электрической или почтовой связи. Также операторы связи обязаны соблюдать конфиденциальность сведений об абонентах и оказываемых им услугах связи, ставших известными операторам в силу выполнения профессиональных обязанностей.

8) **тайна усыновления**. Институт тайны усыновления связан с интересами охраны семейной жизни и выражается в установлении гражданской и уголовной ответственности за разглашение тайны усыновления (удочерения). Согласно ст. 155 УК РФ тайна усыновления может быть двух разновидностей. Первой обладают лица, которые обязаны хранить факт усыновления как служебную или профессиональную тайну (судьи, работники местных администраций, органов опеки и попечительства и прочие лица, указанные в ч. 1 ст. 139 СК РФ). Второй – все другие лица, если установлены их корыстные или иные низменные побуждения при разглашении тайны усыновления без согласия обоих усыновителей.

9) **тайна исповеди**. Обеспечение тайны исповеди является внутренним делом священника; юридической ответственности за её разглашение он не несет. Согласно ч. 2 ст. 51 Конституции РФ и ч. 7 ст. 3 ФЗ «О свободе совести и религиозных объединениях» священнослужитель не может быть привлечен к ответственности за отказ от дачи показаний по обстоятельствам, которые стали ему известны из исповеди.

Персональные данные

В соответствии с ФЗ «О персональных данных» от 27 июля 2006 года № 152 определен круг сведений, которые могут быть отнесены к персональным данным.

Персональные данные – *любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.*

В России нормы, регулирующие вопросы защиты персональных данных, были впервые включены в Конституцию РФ 1993 г. Согласно ст. 23 и 24 Конституции РФ каждый гражданин РФ имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Конституционное положение о недопустимости сбора, хранения, использования и распространения информации о частной жизни лица является одной из гарантий закрепленного в ст. 23 Конституции РФ права на неприкосновенность частной жизни. Оно призвано защитить частную жизнь, личную и семейную тайну от какого бы то ни было проникновения в неё со стороны как государственных органов, органов местного самоуправления, так и негосударственных предприятий, учреждений, организаций, а также отдельных граждан. В соответствии с ФЗ «Об информации, информационных технологиях и о защите информации» запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина

(физического лица), если иное не предусмотрено федеральными законами.

Особое значение запрет собирать, хранить, использовать и распространять информацию о частной жизни лица приобретает в связи с созданием информационных систем на основе использования средств вычислительной техники и связи, позволяющих накапливать и определенным образом обрабатывать значительные массивы информации. Порядок доступа к персональным данным граждан (физических лиц) устанавливается ФЗ «О персональных данных». В Уголовном кодексе РФ существуют ст. 137 и 140, устанавливающие ответственность за нарушение неприкосновенности частной жизни.

2.4. Защита интеллектуальной собственности

Международное право в сфере защиты информации. Защита авторских и смежных прав в законодательстве РФ. Объекты авторского права. Субъекты авторского права. Права обладателей авторских прав.

Основные термины и понятия:
Авторские права
Интеллектуальная собственность

Международное право в сфере защиты информации

До середины XIX в. авторское право как таковое не существовало. Право собственности могло распространяться лишь на конкретные овеществленные произведения искусства (картины, скульптуры и т.п.). Начиная с середины XIX в. авторское право становится самостоятельной формой собственности – произведения интеллектуального труда стали отвечать всем признакам товара.

Бернская конвенция «Об охране литературных и художественных произведений» (1886 г.). Работа по созданию правового инструмента по охране авторского права была начата в Брюсселе в 1858 г. на состоявшемся там конгрессе авторов произведений литературы и искусства. Затем последовали конгрессы в Антверпене (1861 и 1877 г.) и Париже (1878 г.), с 1883 г. работа была продолжена в Берне, где в 1886 г. после трех дипломатических конференций было выработано международное соглашение, получившее название Бернской конвенции об охране литературных и художественных произведений. Соглашение было

подписано девятью государствами: Бельгией, Великобританией, Испанией, Италией, Либерией, Гаити, Тунисом, Францией и Швейцарией. Конвенция вступила в силу 5 декабря 1887 г.

Основные положения Конвенции подлежали обязательному включению в национальные законодательства стран-участниц в тех случаях, когда национальные законодательства обеспечивали менее благоприятный режим для обладателей авторских прав. В этом проявилось стремление создателей Конвенции к унификации основных положений авторского права.

Парижская конференция (1896 г.). 15 апреля 1896 г. в Париже состоялась первая конференция по изменению Конвенции 1886 г. В конвенцию было включено понятие «публикация», определенное как выпуск копий. Таким образом, представление и исполнение драматических, драматическо-музыкальных и музыкальных произведений, выставки произведений искусства к публикации не относились. Было также принято уточнение к ст. 3, в соответствии с которым охрана предоставлялась произведению, впервые опубликованному в стране-участнице Конвенции даже в том случае, когда автор был гражданином страны, не входящей в Бернский союз. Территориальный принцип Конвенции оставался неизменным, однако акцент был перенесен с издателя на автора произведения.

Берлинская конференция (1908 г.). Результатом работы конференции явился почти полный пересмотр всех основных положений Бернской конвенции. Новая редакция содержала 30 статей, и основные нововведения относились к следующим проблемам.

Конвенция 1886 г. ставила охрану авторского права в зависимость от условий выполнения формальностей, предусмотренных в стране первой публикации. На Берлинской конференции было решено отказаться от всех формальностей даже в том случае, если в стране первой публикации они существуют.

Берлинский вариант Конвенции более полно определил и существенно расширил круг объектов охраны, включив в него произведения хореографии и пантомимы, кинематографии, фотографии и архитектуры. Были признаны права композиторов на разрешение адаптировать их произведения для исполнения аппаратами механического воспроизведения и их публичное исполнение.

Правила, регламентирующие право перевода, были расширены. Берлинская конференция признала их действительность на протяжении всего срока действия авторского права без всяких ограничений.

Срок охраны авторского права был установлен равным 50 годам, исчисляемым со дня смерти автора. Правило не носило обязательный характер – допускались различия в сроках охраны авторских прав, определяемые законом страны, где ищется защита.

Конвенция более четко определила понятия литературного и художественного произведений и закрепила положение о том, что они должны охраняться во всех странах-участницах с обязательным отражением этого в национальных законодательствах.

Римская конференция (1928 г.). Римская конференция проходила в период бурного развития средств массовой информации и коммуникаций. Это нашло отражение в признании охраны прав авторов при трансляции по радио их произведений, в расширении числа объектов охраны, признании личных прав автора и т.п.

Уровень охраны авторского права был повышен в связи с включением в число объектов авторского права устных литературных произведений (лекций, речей, проповедей и т.п.). К числу наиболее важных нововведений следует отнести признание так называемых личных прав автора, которые сохраняются за ним и при отчуждении имущественных прав (издание, публикация, постановка и т.п.).

Брюссельская конференция (1948 г.). Бернская конвенция подверглась существенным изменениям в Брюсселе в 1948 г. Основной целью конференции было стремление добиться более полной унификации правил Конвенции и национальных законодательств, а также учесть новые условия научного и технического развития. Унификация правил применения Конвенции была достигнута путем усиления принципа её главенства над национальными законодательствами.

Всемирная конвенция об авторском праве (1952 г.). Говоря о причинах принятия Всемирной конвенции об авторском праве, следует иметь в виду прежде всего стремление к этому Соединенных Штатов Америки и ряда других стран, которые

хотели иметь соглашение с как можно меньшим количеством императивных условий и формальностей. Всемирная конвенция об авторском праве была принята на состоявшейся в Женеве в сентябре 1952 г. межправительственной конференции с участием представителей 50 стран. Конвенция вступила в силу в сентябре 1955 г.

Женевская конвенция об авторском праве содержит общую декларацию о стремлении стран-участниц конференции создать международно-правовой инструмент, приемлемый для возможно более широкого крута стран и направленный на облегчение распространения произведений интеллектуального творчества в целях лучшего международного взаимопонимания.

Стокгольмская конференция (1967 г.). К этому времени на международной арене появилось большое количество развивающихся стран с их специфическими нуждами и проблемами, которые стремились понизить уровень охраны авторских прав с целью получения свободного доступа к произведениям науки и культуры. Добившиеся высокого уровня охраны авторских прав, развитые капиталистические страны боялись наметившейся тенденции и всячески ей противились. Для сохранения прежнего уровня охраны авторского права предполагалось пойти на сужение границ Бернского союза. Россия присоединилась к Бернской конвенции лишь спустя почти 100 лет после её первого опубликования, в ноябре 1994 г.

Постановлением Правительства РФ от 3 ноября 1994 г. №1224 Российская Федерация присоединилась к Бернской конвенции об охране литературных и художественных произведений в редакции 1971 г. и Всемирной конвенции об авторском праве в редакции 1971 г.

Защита авторских и смежных прав в законодательстве РФ

В настоящее время положение с охраной и защитой прав на интеллектуальную собственность в России характеризуется как весьма тревожное.

Высокая доходность и доступность интеллектуальной собственности стала особенно привлекательной для дельцов «теневой» экономики. Преступность в данной сфере приняла устойчивые организационные формы. Налажены нелегальные каналы быстрого получения экземпляров новых программных

продуктов, их взлома в случаях, когда они защищены ключами аппаратной защиты или программными средствами, а также получения новинок аудио-видеопродукции, организованы подпольные технологические линии по тиражированию носителей программ для ЭВМ и аудио-видеокассет, установлены криминальные связи с легальными заводами-производителями компьютерных носителей (компакт-дисков) и по изготовлению крупных партий контрафактного программного обеспечения, аудио-видеопродукции и производству дополнительных (официально не учтенных) тиражей легальной продукции без ведома правообладателя, созданы и действуют оптовые и розничные сбытовые сети.

В отличие от темпов развития законодательства, защищающего авторские права на объекты интеллектуальной собственности, организованная преступность в этой сфере развивается довольно стремительно. Этому способствуют: извлечение из данной деятельности крупной прибыли при минимальных издержках; коррумпированные связи дельцов в государственных органах, в том числе и правоохранительных; несовершенство законодательства и низкий уровень правосознания общества.

Интеллектуальной собственность – *совокупность исключительных прав на результаты интеллектуальной деятельности, а также на некоторые иные приравненные к ним объекты, такие как средства индивидуализации участников гражданского оборота и производимой ими продукции (работ, услуг).*

Понятие «интеллектуальная собственность» включает в себя не только авторские права и права на промышленную собственность, но и права на средства индивидуализации товаров и услуг. Кроме этого, имеются специальные законы о специфичных объектах интеллектуальной собственности – топологии интегральных микросхем и селекционных достижениях.

В юридической литературе существуют и другие мнения о понятии «интеллектуальная собственность». Под интеллектуальной собственностью иногда понимают нематериальные объекты авторского и патентного права, иногда их ещё называют «промышленная собственность» или «литературная собственность». Однако произведение (изобретение, товарный знак,

фирменное наименование и т.д.), охраняемое авторским и патентным правом, имеет такие особенности духовного порядка, которые не позволяют отождествить его с вещью. Материальное воплощение идей и образов представляет собой «вещь» настолько условную, что по отношению к праву на объект любого творческого произведения правильнее применять термин «интеллектуальные права».

Авторское и патентное права, специфическим объектом которых как раз и является творческое произведение, регулируют данные отношения настолько своеобразно, что становится невозможным даже проведение аналогий между нормами о праве собственности и нормами об интеллектуальных правах. Однако следует отметить, что правовой режим охраны нематериальных объектов выполняет в отношении нематериальных объектов ту же функцию, что и право собственности в отношении материальных объектов (вещей), устанавливает абсолютное право, дающее возможность субъекту (обладателю права) вводить объект в хозяйственный оборот.

Понятие «право собственности» в объективном смысле представляет собой совокупность правовых норм, регулирующих отношения собственности в данном обществе и действительных для всех членов общества, а нарушение этих норм влечет за собой применение принудительных санкций государства.

Право интеллектуальной собственности не является разновидностью права собственности. Это два различных правовых института. Под интеллектуальной собственностью понимаются исключительные права на результаты интеллектуальной деятельности, т.е. на нематериальные объекты, тогда как право собственности относится к вещным правам.

В целях обеспечения защиты авторских, издательских, иных прав на интеллектуальную собственность с 1 января 2008 года вступил в силу раздел VII «Права на результаты интеллектуальной деятельности и средства индивидуализации» ГК РФ от 18 декабря 2006 г. № 230-ФЗ (часть четвертая).

Защита прав на результаты интеллектуальной деятельности осуществляется в судебном (общем) и административном (специальном, применяемом в прямо указанных законом случаях) порядке.

Конституция РФ гарантирует каждому свободу литературного, научного, технического и других видов творчества, при этом подчеркивается, что интеллектуальная собственность охраняется законом. Одной из гарантий реализации авторских и смежных прав, декларированной ст. 44 Конституции РФ, является уголовно-правовая защита этих прав, установленная ст. 146 УК РФ.

Действующий УК РФ предусматривает уголовную ответственность за преступления в сфере интеллектуальной собственности по ст. 146 «Нарушение авторских и смежных прав», ст. 147 «Нарушение изобретательских и патентных прав», ст. 180 «Незаконное использование товарного знака».

Правоприменительная практика российского законодательства, защищающего объекты интеллектуальной собственности, окончательно ещё не сложилась. Но в целом борьба с преступлениями в сфере интеллектуальной собственности в ближайшем будущем приобретет ещё большую актуальность, т.к. с каждым днем возрастает значимость объектов интеллектуальной собственности, что обусловлено требованиями научно-технического прогресса, экономическим и социальным развитием России.

Объекты авторского права

Авторское право и регулируемые им имущественные и личные неимущественные отношения связаны с созданием и использованием произведений литературы, науки и искусства. Авторское право как самостоятельный институт решает конкретные задачи, которые включают:

– всемерную охрану имущественных, личных неимущественных прав и законных интересов авторов;

– обеспечение правовыми средствами наиболее благоприятных условий для создания научных и художественных произведений;

– широкое использование их обществом.

Международное авторское право является частью международного частного права. В первоначальном тексте Бернской конвенции 1886 г. понятие «литературные и художественные произведения» было определено через перечисление различных конкретных видов произведений (книги, брошюры, картины

и т.п.). Здесь же говорилось о произведениях в области литературы, науки и искусства, которые могут быть выпущены в свет «любым способом издания или воспроизведения». На сегодняшний день круг произведений намного расширился.

Можно выделить ряд основных **объектов** авторского права.

Литературные произведения составляют значительную часть объектов авторского права. Особенность их в том, что мысли, чувства, идеи и образы выражаются посредством слова в оригинальной композиции и оригинальном изложении.

В структуре литературного произведения выделяются тема, материал, идеология, образная система, сюжет, язык, заглавие. Эти элементы литературного произведения разделяются на юридически безразличные, т.е. тема, материал, сюжет, идейное содержание, и юридически значимые – образная система и язык. Использование значимых элементов произведения в ряде случаев требует согласия автора.

Литературная обработка – особый объект авторского права. Она представляет собой музыкальную или литературную обработку произведений авторов, которые в силу некоторых причин (отсутствие навыков и др.) не в состоянии сами привести свое произведение в законченный вид. Кроме того, обработке могут подвергаться народные произведения, произведения неизвестных авторов и т.д. Записанный и обработанный литературный материал должен отвечать требованиям, предъявляемым законом к литературным и музыкальным произведениям.

Музыкальные произведения выражаются в сочетании звуков, образующих мелодию и связанных ритмом и гармонией. Они имеют форму ораторий, симфоний, песен и т.п. Кроме музыкальных произведений существуют также музыкально-драматические произведения, которые создаются на литературно-драматической основе (либретто) и исполняются на сцене в виде опер, балетов, оперетт.

Музыкальные произведения записываются композитором особыми знаками, позволяющими фиксировать его творческий замысел. Нотная запись музыкального произведения образует клавир, представляющий собой переложение музыкального произведения для фортепиано, или же партитуру, содержащую все партии многоголосного музыкального произведения. Музы-

кальное произведение может фиксироваться также на аудионосителях (кассеты, компакт-диски и т.п.).

Обработка чужих произведений, оркестровка, переложение относятся к объектам авторского права, если они содержат элемент творчества.

Хореографические произведения, или пантомимы, – произведения искусства, создаваемые при помощи пластических движений человеческого тела. В сочетании с музыкой хореографическое произведение образует музыкально-сценическое произведение. В связи с тем, что хореографические произведения довольно сложно закрепить с помощью каких-то особых знаков на бумаге, для этих целей, как правило, используют фото-, кино- и видеозапись.

Произведения изобразительного искусства – это произведения живописи, графики, скульптуры, декоративно-прикладного искусства и т.п. Художники, скульпторы создают оригинальные произведения, которые могут воспроизводиться путем изготовления копий либо самими авторами, либо иными лицами.

Архитектурные произведения (проекты) также являются объектами авторского права. Они представляют собой синтез инженерного искусства, бионики, живописи, скульптуры, науки, архитектуры. В них слиты наука, техника, искусство. Эскизный архитектурный проект, в котором воплощается замысел автора, содержит решения будущего произведения, внутреннее развитие его сочлененных пространств, их объёмы, фактуру и цвет. На основе эскизного архитектурного проекта строятся здания, сооружения, комплексы и т.п.

Аудиовизуальные произведения – достаточно широкая категория, охватывающая многообразные произведения для кино, телевидения, радио, интерактивных сетей и т.п.: сценарии, сценарные планы, тексты песен, кинофильмы, телепередачи, радиопередачи, заставки и многое другое. Данная категория произведений, как правило, закрепляется на аудио-, кино- и видеоносителях (пленка, кассеты, цифровые носители и т.п.).

Программные продукты для средств вычислительной техники могут представлять собой как отдельные прикладные программы (текстовые редакторы, компиляторы и т.п.), так и базы данных, энциклопедии, мультимедийные программы. Кро-

ме того, особенность этой категории заключается в том, что в программах для ЭВМ может иметь место использование других объектов авторского права, это могут быть произведения литературы, музыкальные произведения, произведения изобразительного искусства, кинематографии, а также многое другое. В связи со стремительным прогрессом в области использования вычислительной техники закономерно ожидать появления новых норм внутригосударственного и международного права, направленных на разрешение множества коллизий.

Все вышеперечисленные объекты авторского права можно отнести к категории оригинальных произведений, создаваемых авторами. Кроме них конвенционной охране подлежат также зависимые произведения, возникшие на основе существующих оригинальных произведений. Эти произведения появляются в результате перевода (с иностранного языка), переделки, составительства.

Зависимость перевода литературного, художественного, научного произведения от оригинала не лишает его самостоятельности. Конвенция относит переводы к объектам авторского права, сохраняя для них те же критерии охраноспособности, что и для других произведений. Если же переводчик ограничивает свою работу лишь подбором равнозначных слов к языку оригинала, то подобный перевод («подстрочник») не может быть объектом авторского права. Перевод, выполненный с согласия автора или его правопреемников одним лицом, не может препятствовать другому лицу осуществлять новый перевод этого же произведения.

К объектам авторского права относятся ***сборники произведений***. В сборники могут включаться произведения, не являющиеся предметом чьего-либо авторского труда (законы, статистика, судебные решения и т.д.), а также произведения отдельных авторов. Творческий характер труда составителя заключается в подборе и расположении материала. Авторское право составителя сборника не может мешать другому лицу самостоятельно систематизировать, обрабатывать и выпускать в свет те же произведения.

Научное произведение – это определенная система понятий. Научное произведение может быть выражено в форме учебника, монографии, статьи и т.д. Существуют и другие фор-

мы воплощения научных произведений: чертежи, планы, эскизы, модели, компьютерные программы, различного рода карты и т.п.

Основное отличие авторского права от режима правовой охраны других результатов интеллектуальной деятельности состоит в том, что произведение литературы, науки и искусства становится объектом авторского права в силу самого факта его создания автором без какой-либо регистрации, оформления или соблюдения иных формальностей.

Субъекты авторского права

Субъектами авторского права выступают лица, создавшие творческим трудом произведения литературы, науки и искусства (авторы). Возникновение субъективных авторских прав у гражданина не зависит от возраста, имущественного положения, места создания и выпуска произведения в свет и т.п. Субъектом авторских прав может стать даже человек, признанный судом недееспособным (например, по причине душевной болезни).

Иностранный гражданин может быть субъектом российского авторского права, если его произведение впервые выпушено в свет на территории страны либо не выпущено, но находится на её территории в какой-либо объективной форме. Когда произведение иностранного автора впервые выпущено в свет за границей или находится там в объективной форме, этот автор становится субъектом российского авторского права только в силу заключенных РФ соглашений и в пределах, ими установленных.

Наряду с авторами произведений к субъектам авторского права относятся лица (граждане и организации), которые не участвуют в творческом создании произведений литературы, науки и искусства. Их называют правопреемниками. К правопреемникам переходит определенный круг авторских правомочий по использованию произведений автора, основанием такого перехода служит закон, наследование или договор с автором.

Как правило, автором того или иного произведения выступает одно лицо, которое создало его творческим трудом. Однако в работе над произведением литературы, науки и искусства могут быть объединены усилия нескольких лиц – соавторов.

Особое место в международной системе охраны авторских прав занимают обладатели так называемых смежных прав. Это

новое понятие для нашего права, а в некоторых странах понятие «обладатели смежных прав» вообще не используется. К такого рода субъектам относится достаточно широкий круг лиц, таких как режиссеры, актеры, исполнители, продюсеры и т.п.

В международном праве охрана прав, примыкающих к авторским, осуществляется в соответствии с международной конвенцией об охране прав артистов, исполнителей, изготовителей фонограмм и вещательных организаций, подписанной в Риме в 1961 г. Эта Конвенция представляет собой попытку сбалансировать охрану всех категорий субъектов авторского права.

Права обладателей авторских прав

Автором произведения признается гражданин, творческим трудом которого оно создано.

Автору произведения принадлежит исключительное право на свое произведение, включающее:

– право авторства;

– право на имя;

– право на неприкосновенность произведения;

– право на опубликование произведения;

– право на использование произведения (право осуществлять или разрешать его воспроизведение любыми способами – в печати, путем публичного исполнения, передачи в эфир, в видео- и звукозаписи, по кабельному телевидению, с помощью спутников и иных технических средств; перевод, переработку произведения; распространение экземпляров воспроизведенного произведения; реализацию архитектурного и дизайнерского проекта и т.п.);

– право на вознаграждение за разрешение использовать и использование произведения.

Автор может передать право на использование своего произведения как на территории своего государства, так и за рубежом любым гражданам и юридическим лицам, в том числе и иностранным.

Авторское право на произведение, созданное совместным творческим трудом двух или более граждан, принадлежит соавторам совместно, независимо от того, образует ли такое произведение одно неразрывное целое или состоит из частей, каждая из которых имеет также самостоятельное значение.

Взаимоотношения соавторов могут определяться договором между ними. Каждый из соавторов сохраняет авторское право на созданную им часть произведения, имеющую самостоятельное значение, и вправе использовать такую часть произведения по своему усмотрению.

Составители сборников произведений, которые представляют собой по подбору и расположению материалов результат творческого труда, пользуются авторским правом на сборник при условии соблюдения прав авторов каждого из произведений, включенных в сборник.

Авторы произведений, включенных в сборник, сохраняют авторское право каждый на свое произведение и могут использовать свои произведения независимо от сборника в целом.

Организации, выпускающие в свет энциклопедии, энциклопедические словари, газеты, журналы, периодические и продолжаемые сборники научных трудов и другие периодические издания, пользуются правом на использование издания в целом, если иное не установлено в договорах с авторами, произведения которых включены в такое издание.

Авторы кино-, теле- и видеофильма по авторским договорам передают право на использование фильма его изготовителю в пределах, предусмотренных договором.

Авторы произведений, использованных в фильме, сохраняют авторское право каждый на свое произведение, передают изготовителю право на его использование и могут использовать произведение независимо от фильма в целом.

К наследникам автора переходит право охраны неприкосновенности произведения, право осуществлять или разрешать его опубликование или использование, а также право на получение вознаграждения за разрешение использовать или использование произведения.

К иным правопреемникам автора, в том числе юридическим лицам, может переходить только право на использование произведения.

Обладатели «смежных прав» имеют следующие права: исполнителям-артистам, режиссерам-постановщикам и дирижерам принадлежат право на имя, право на защиту постановки и исполнения произведения, право осуществлять или разрешать использование постановки и исполнения и право на вознаграж-

дение. Запись исполнения, трансляция и иное использование могут производиться только с согласия исполнителя.

Лицу, создавшему звуко- и видеозапись, принадлежит право осуществлять или разрешать её воспроизведение. Использование звуко- и видеозаписи допускается только с разрешения этого лица или его правопреемника (правообладателя).

Право на звуко- и видеозапись включает право её воспроизведения любыми способами, право её публичного распространения, в том числе передачи за границу, а также право на защиту от импорта и распространения экземпляров записи без разрешения правообладателя. Если право собственности на экземпляр звуко- или видеозаписи принадлежит не её создателю, то исключительное право коммерческого проката сохраняется за лицом, создавшим звуко- или видеозапись.

Организациям эфирного вещания принадлежит право разрешать другим организациям ретрансляцию, запись и воспроизведение их передач. Организациям публичного вещания принадлежит также право разрешать публичное воспроизведение телевизионных передач, если оно производится за плату в местах, доступных неопределенному кругу лиц.

Создатели звуко- и видеозаписей, организации эфирного вещания осуществляют свои права в пределах прав, полученных по договору с автором и исполнителем, а организации эфирного вещания так же, без ущерба правам создателей звукозаписи.

Исполнители осуществляют свои права с соблюдением прав авторов исполняемых ими произведений.

Чтобы защитить своё исключительное право на использование программного продукта, правообладатель может обратиться в суд, арбитражный или третейский суд и требовать возмещения причиненных убытков, в размер которых включается сумма доходов, неправомерно полученных нарушителем, или выплаты нарушителем компенсации, определяемой по усмотрению судебных органов. Помимо возмещёния убытков или выплаты компенсации по усмотрению судебного органа в доход бюджета России может быть взыскан штраф в размере 10% суммы, присужденной в пользу истца.

Судебный орган может вынести решение о конфискации контрафактных экземпляров программного продукта, а также материалов и оборудования, используемых для их воспроизве-

дения, и об их уничтожении либо о передаче их в доход бюджета Российской Федерации, либо истцу по его просьбе в счёт возмещёния убытков.

Тем не менее в настоящее время существующую судебную практику защиты прав правообладателя нельзя, к сожалению, считать совершенной; имеющиеся случаи судебной защиты авторских прав пока ещё редки, однако ситуация меняется – ещё несколько лет назад в судах подобные дела к производству практически не принимались.

Вопросы для самоконтроля

1. Перечислите отрасли права, акты которых включают информационно-правовые нормы.
2. К какой информации, в соответствии с законодательством, не может быть ограничен доступ?
3. Какая информация относится к сведениям конфиденциального характера?
4. Какие сведения относят к сведениям особой важности?
5. Какие сведения относят к совершенно секретным сведениям?
6. Какие сведения относят к секретным сведениям?
7. В сведениях какого характера может содержаться государственная тайна?
8. Какие сведения не подлежат отнесению к государственной тайне и засекречиванию?
9. Какие меры включаются в систему защиты государственной тайны?
10. Перечислите основные организационные и технические способы защиты государственной тайны.
11. Каково основное назначение режима секретности?
12. Какие группы мер включает в себя режим секретности?
13. Какие сведения не могут составлять коммерческую тайну?
14. Чем вызвано обязательство сохранения в тайне сведений, составляющих профессиональную тайну?
15. Какой нормативный документ определяет порядок доступа к персональным данным граждан?
16. Перечислите основные объекты авторского права.
17. Что включает в себя исключительное право автора на свое произведение?

ГЛАВА 3. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ

3.1. Информационная безопасность РФ

Доктрина информационной безопасности РФ. Национальные интересы РФ в информационной сфере. Виды угроз информационной безопасности РФ. Источники угроз информационной безопасности РФ. Основные цели и задачи обеспечения информационной безопасности РФ. Объекты информационной безопасности РФ.

Основные термины и понятия:
Доктрина информационной безопасности РФ
Информационная безопасность РФ
Национальные интересы РФ в информационной сфере
Объект информационной безопасности РФ
Угрозы информационной безопасности РФ

Современный этап развития общества характеризуется возрастающей ролью информационных взаимодействий инфраструктур и субъектов, осуществляющих сбор, формирование, распространение и использование информации. Информационная сфера, являясь системообразующим фактором в жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности РФ. Национальная безопасность РФ существенно зависит от обеспечения информационной безопасности.

Доктрина информационной безопасности РФ

Доктрина информационной безопасности РФ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Информационная безопасность РФ – *это состояние защищённости её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.*

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

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

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

Доктрина информационной безопасности РФ была утверждена Президентом Российской Федерации В. В. Путиным 9 сентября 2000 г. и структурно состоит из 4 разделов.

В первом разделе «Информационная безопасность Российской Федерации» приведены национальные интересы Российской Федерации в информационной сфере и пути их обеспечения, указаны виды и источники угроз информационной безопасности РФ, рассмотрено состояние информационной безопасности РФ и намечены основные задачи по ее обеспечению.

Во втором разделе «Методы обеспечения информационной безопасности Российской Федерации» рассматриваются общие методы обеспечения информационной безопасности РФ (правовые, организационно-технические и экономические). Рассмотрены вопросы международного сотрудничества РФ в области обеспечения информационной безопасности. Указаны особенности обеспечения информационной безопасности РФ в различных сферах общественной жизни:

– в сфере экономики;

– в сфере внутренней политики;

– в сфере внешней политики;

– в области науки и техники;

– в сфере духовной жизни;

– в общегосударственных информационных и телекоммуникационных системах;

– в сфере обороны;

– в правоохранительной и судебной сферах.

В третьем разделе «Основные положения государственной политики обеспечения информационной безопасности Российской Федерации и первоочередные мероприятия по её реализации» приведены основные положения государственной политики обеспечения информационной безопасности РФ и первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности РФ.

В четвёртом разделе «Организационная основа системы обеспечения информационной безопасности Российской Федерации» рассматриваются основные функции системы обеспечения информационной безопасности РФ и основные элементы её организационной основы.

Национальные интересы РФ в информационной сфере

В информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности с учётом национальных интересов РФ. Согласно Доктрине информационной безопасности РФ, выделяют **четыре** основные составляющие национальных интересов РФ в информационной сфере.

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

Вторая составляющая представляет собой информационное обеспечение государственной политики РФ, связанное с доведением до российской и международной общественности достоверной информации о самой государственной политике, её официальной позиции по социально значимым событиям

российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая предусматривает развитие современных информационных технологий, отечественной индустрии информации (средств информатизации, телекоммуникации и связи); обеспечение потребностей внутреннего рынка её продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронного и компьютерного производства.

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

Правовое обеспечение информационной безопасности РФ должно базироваться, прежде всего, на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере.

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

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 форм общественного контроля деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации. Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности.

Виды угроз информационной безопасности РФ

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие **виды**:

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

2) угрозы информационному обеспечению государственной политики Российской Федерации;

3) 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;

4) 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 федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;

– создание монополий на формирование, получение и распространение информации в Российской Федерации, 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;

– нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;

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

– неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;

– неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов 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, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;

– манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

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

– низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики;

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

Угрозами 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 могут являться:

- противодействие доступу Российской Федерации 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, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;

– закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;

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

– увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться:

– противоправные сбор и использование информации;

– нарушения технологии обработки информации;

– внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

– уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

– воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;

– разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

– компрометация ключей и средств криптографической защиты информации;

– утечка информации по техническим каналам;

– внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

– уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

– перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

– использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;

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

– нарушение законных ограничений на распространение информации.

Источники угроз информационной безопасности РФ

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние.

К **внешним** источникам относятся:

– деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;

– стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;

– обострение международной конкуренции за обладание информационными технологиями и ресурсами;

– 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 мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К **внутренним** источникам относятся:

– критическое состояние 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 федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;

– недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

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

– недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;

– недостаточная экономическая мощь государства;

– снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;

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

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

Основные цели и задачи обеспечения информационной безопасности РФ

Основные цели обеспечения информационной безопасности определяются на базе устойчивых приоритетов национальной безопасности, отвечающих долговременным интересам общественного развития, к которым относятся:

– сохранение и укрепление российской государственности и политической стабильности в обществе;

– сохранение и развитие демократических институтов общества, обеспечение прав и свобод граждан, укрепление законности и правопорядка;

– обеспечение достойной роли России в мировом сообществе;

– обеспечение территориальной целостности страны;

– обеспечение прогрессивного социально-экономического развития России;

– сохранение национальных культурных ценностей и традиций.

В соответствии с указанными приоритетами основными **целями** информационной безопасности РФ являются:

– защита национальных интересов России в условиях глобализации информационных процессов, формирования мировых

информационных сетей и стремления США и других развитых стран к информационному доминированию;

– обеспечение органов государственной власти и управления, предприятий и граждан достоверной, полной и своевременной информацией, необходимой для принятия решений, а также предотвращение нарушений целостности и незаконного использования информационных ресурсов;

– реализация прав граждан, организаций и государства на получение, распространение и использование информации.

К основным **задачам** обеспечения информационной безопасности РФ относятся:

– выявление, оценка и прогнозирование источников угроз информационной безопасности;

– разработка государственной политики обеспечения информационной безопасности, комплекса мероприятий и механизмов её реализации;

– разработка нормативно-правовой базы обеспечения информационной безопасности, координация деятельности органов государственной власти и управления и предприятий по обеспечению информационной безопасности;

– развитие системы обеспечения информационной безопасности, совершенствование её организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий её нарушения;

– обеспечение активного участия России в процессах создания и использования глобальных информационных сетей и систем.

Объекты информационной безопасности РФ

К объектам информационной безопасности РФ относятся:

– информационные ресурсы, независимо от форм хранения, содержащие информацию ограниченного доступа, информацию, составляющую государственную тайну, коммерческую тайну и другую конфиденциальную информацию, а также открытую (общедоступную) информацию и знания;

– система формирования, распространения и использования информационных ресурсов, включающая информационные системы различного класса и назначения, библиотеки, архивы,

базы и банки данных, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, научно-технический и обслуживающий персонал;

– информационная инфраструктура, включающая центры обработки и анализа информации, каналы информационного обмена и телекоммуникации, механизмы обеспечения функционирования телекоммуникационных систем и сетей, в том числе системы и средства защиты информации;

– система формирования общественного сознания (мировоззрение, политические взгляды, моральные ценности и пр.), базирующаяся на средствах массовой информации и пропаганды;

– права граждан, юридических лиц и государства на получение, распространение и использование информации, защиту конфиденциальной информации и интеллектуальной собственности.

Информационная безопасность всех вышеуказанных объектов создает условия надежного функционирования государственных и общественных институтов, а также формирования общественного сознания, отвечающего прогрессивному развитию страны.

3.2. Правовое обеспечение информационной безопасности РФ

Правовое обеспечение рассматривается как приоритетное направление формирования механизмов реализации политики обеспечения информационной безопасности в РФ и включает в себя:

1) нормотворческую деятельность по созданию законодательства, регулирующего отношения в обществе, связанные с обеспечением информационной безопасности;

2) исполнительную и правоприменительную деятельность по исполнению законодательства в области информации, информатизации и защиты информации органами государственной власти и управления, организациями (юридическими лицами), гражданами.

Нормотворческая деятельность в области обеспечения информационной безопасности предусматривает:

– оценку состояния действующего законодательства и разработку программы его совершенствования;

– создание организационно-правовых механизмов обеспечения информационной безопасности;

– формирование правового статуса всех субъектов в системе информационной безопасности, пользователей информационных и телекоммуникационных систем и определение их ответственности за обеспечение информационной безопасности;

– разработку организационно-правового механизма сбора и анализа статистических данных о воздействии угроз информационной безопасности и их последствиях с учётом всех видов (категорий) информации;

– разработку законодательных и других нормативных актов, регулирующих порядок ликвидации последствий воздействия угроз, восстановления нарушенного права и ресурсов, реализации компенсационных мер.

Исполнительная и правоприменительная деятельность предусматривает разработку процедур применения законодательства и нормативных актов к субъектам, совершившим преступления и проступки при работе с закрытой информацией и нарушившим регламент информационных взаимодействий, а также правонарушения с использованием незащищенных средств информатизации, разработку составов правонарушений с учётом специфики уголовной, гражданской, административной, дисциплинарной ответственности.

Вся деятельность по правовому обеспечению информационной безопасности должна строиться на основе трех фундаментальных положений права: соблюдение законности, обеспечение баланса интересов отдельных субъектов и государства, неотвратимость наказания.

Соблюдение законности предполагает наличие законов и иных нормативных установлений, их применение и исполнение субъектами права в области информационной безопасности. Законодательная и нормативно-правовая база в сфере информации и информационной безопасности в РФ включает в себя:

1. Законы Российской Федерации:

– Конституция РФ;

– «О банках и банковской деятельности»;

– «О безопасности»;

– «О внешней разведке»;

– «О государственной тайне»;

– «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера»;

– «О закрытом административно-территориальном образовании»;

– «О милиции»;

– «О связи»;

– «О сертификации продукции и услуг»;

– «О средствах массовой информации»;

– «О стандартизации»;

– «О федеральных органах правительственной связи и информации»;

– «Об архивном фонде Российской Федерации и архивах»;

– «Об информации, информационных технологиях и о защите информации»;

– «Об обороне»;

– «Об оперативно-розыскной деятельности»;

– «Об органах Федеральной службы безопасности в Российской Федерации»;

– «Об обязательном экземпляре документов»;

– «Об участии в международном информационном обмене»;

– «Об электронной цифровой подписи»;

2. Нормативные правовые акты Президента Российской Федерации:

– Доктрина информационной безопасности РФ;

– Военная доктрина РФ;

– Стратегия национальной безопасности Российской Федерации до 2020 года;

– «Вопросы межведомственной комиссии по защите государственной тайны»;

– «Вопросы Государственной технической комиссии при Президенте Российской Федерации»;

– «О создании Государственной технической комиссии при Президенте Российской Федерации»;

– «О Государственной технической комиссии при Президенте Российской Федерации»;

– «О некоторых вопросах межведомственной комиссии по защите государственной тайны»;

– «О перечне сведений, отнесенных к государственной тайне»;

– «Об основах государственной политики в сфере информатизации»;

– «Об утверждении перечня должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне»;

– «Об утверждении перечня сведений конфиденциального характера».

3. Нормативные правовые акты Правительства Российской Федерации:

– «О сертификации средств защиты информации»;

– «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»;

– «Об установлении порядка рассекречивания и продления сроков засекречивания архивных документов Правительства СССР»;

– «Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности»;

– «О подготовке к передаче сведений, составляющих государственную тайну, другим государствам»;

– «О лицензировании отдельных видов деятельности».

4. Руководящие документы Гостехкомиссии России:

– «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»;

– «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники»;

– «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;

– «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;

– «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;

– «Защита информации. Специальные защитные знаки. Классификация и общие требования»;

– «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».

5. Гражданский кодекс РФ (часть четвертая).

6. Уголовный кодекс Российской Федерации.

Реализация механизмов правового обеспечения информационной безопасности должна опираться на информатизацию правовой сферы в целом.

3.3. Государственная политика обеспечения информационной безопасности РФ

Основные положения государственной политики обеспечения информационной безопасности РФ. Основные положения государственной политики обеспечения информационной безопасности субъектов РФ.

Основные термины и понятия:
Государственная политика обеспечения информационной безопасности РФ

Государственная политика обеспечения информационной безопасности Российской Федерации определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей по защите интересов Российской Федерации в информационной сфере в рамках направлений их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государственная политика обеспечения информационной безопасности Российской Федерации основывается на следующих основных **принципах**:

– соблюдение Конституции Российской Федерации, законодательства Российской Федерации, общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности Российской Федерации;

– открытость в реализации функций федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и общественных объединений, предусматривающая информирование общества об их деятельности с учетом ограничений, установленных законодательством Российской Федерации;

– правовое равенство 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;

– приоритетное развитие отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов Российской Федерации.

Государственная политика является открытой и предусматривает информированность общества о деятельности государственных органов и общественных институтов в области информационной безопасности с учётом ограничений, предусмотренных действующим законодательством.

Государственная политика исходит из принципа безусловного правового равенства всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса. Она основывается на обязательном обеспечении прав граждан и организаций на свободное создание, поиск, получение и распространение информации любым законным способом. В этих целях государство

совершенствует существующее и разрабатывает новое законодательство и нормативно-правовую базу информационных отношений в обществе, а также осуществляет контроль за безусловным их исполнением.

Государство исходит из того, что информационные ресурсы являются объектом собственности, способствует введению их в хозяйственный оборот при соблюдении законных интересов собственников, владельцев и распорядителей информационных ресурсов.

Государство считает приоритетным развитие современных информационных и телекоммуникационных технологий и технических средств, способных обеспечить создание национальных телекоммуникационных сетей и включение России в глобальные информационные сети и системы мониторинга.

Исходя из принципа разделения ответственности между органами федеральной, региональной власти и местного самоуправления, государственная политика предусматривает согласованность организационных и технических решений, принимаемых этими органами для обеспечения информационной безопасности в рамках единого информационного пространства России.

Государственная политика не допускает монополизма министерств, ведомств и организаций в области обеспечения информационной безопасности.

Основные положения государственной политики обеспечения информационной безопасности РФ

Государственная политика обеспечения информационной безопасности исходит из следующих основных положений:

– ограничение доступа к информации есть исключение из общего принципа открытости информации и осуществляется только на основе законодательства;

– ответственность за сохранность информации, её засекречивание и рассекречивание персонифицируется;

– доступ к какой-либо информации, а также вводимые ограничения доступа осуществляются с учётом определяемых законом прав собственности на эту информацию;

– государство формирует нормативно-правовую базу, регламентирующую права, обязанности и ответственность всех субъектов, действующих в информационной сфере;

– юридические и физические лица, собирающие, накапливающие и обрабатывающие персональные данные и конфиденциальную информацию, несут ответственность перед законом за их сохранность и использование;

– государство законными средствами обеспечивает защиту общества отложной, искаженной и недостоверной информации, поступающей через средства массовой информации;

– государство осуществляет контроль за созданием и использованием средств защиты информации посредством их обязательной сертификации и лицензирования деятельности в области защиты информации;

– государство проводит протекционистскую политику, поддерживающую деятельность отечественных производителей средств информатизации и защиты информации и осуществляет меры по защите внутреннего рынка от проникновения на него некачественных средств информации и информационных продуктов;

– государство способствует предоставлению гражданам доступа к мировым информационным ресурсам, глобальным информационным сетям;

– государство стремится к отказу от зарубежных информационных технологий для информатизации органов государственной власти и управления по мере создания конкурентоспособных отечественных информационных технологий и средств информатизации;

– государство формирует федеральную программу информационной безопасности, объединяющую усилия государственных организаций и коммерческих структур в создании единой системы информационной безопасности России;

– государство прилагает усилия для противодействия информационной экспансии ряда развитых стран, поддерживает интернационализацию глобальных информационных сетей и систем.

На основе изложенных принципов и положений определяются общие направления формирования и реализации политики информационной безопасности в политической, военной, экономической и других сферах деятельности государства.

Государственная политика в качестве механизма согласования интересов субъектов информационных отношений и нахождения компромиссных решений предусматривает формиро-

вание и организацию эффективной работы различных советов, комитетов и комиссий с широким представительством специалистов и всех заинтересованных структур. Механизмы реализации государственной политики должны быть гибкими и своевременно отражать изменения, происходящие в политической и экономической жизни страны.

Основные положения государственной политики обеспечения информационной безопасности субъектов РФ

Информационная собственность субъектов РФ является разновидностью государственной собственности субъектов РФ и включает в себя:

– информационную собственность органов власти и управления субъектов РФ;

– информационную собственность предприятий и учреждений, созданных или приобретенных за счёт средств субъектов РФ;

– культурные ценности народов, населяющих территорию субъектов РФ.

Обязанностью органов власти и управления субъектов РФ является защита права информационной собственности, находящейся на территории субъектов РФ, объектов федеральной информационной собственности, информационной собственности органов местного самоуправления, других юридических и физических лиц.

Субъекты РФ обладают всей полнотой информационных прав, действующих в РФ. Эти права от имени субъектов РФ осуществляют их органы государственной власти и управления.

Субъектам РФ гарантируется:

– равное право доступа на российский рынок информации и средств обеспечения информационной безопасности, находящихся в любой форме собственности;

– право использования для решения региональных государственных задач федеральных информационных банков данных с соблюдением установленных правил обеспечения информационной безопасности;

– право проведения самостоятельной внутренней и внешнеэкономической деятельности в сфере информационной безопасности в рамках, определенных федеральными законами;

– право осуществлять защиту своих информационных прав и права информационной собственности как самостоятельно, так и путем обращения в федеральные и международные правозащитные органы.

Более подробная проработка основных направлений региональной политики обеспечения информационной безопасности должна быть осуществлена субъектами РФ с учётом особенностей их территорий, состояния и перспектив развития хозяйственной сферы.

3.4. Государственная система защиты информации РФ

Задачи системы защиты информации РФ.
Структура государственной системы защиты информации РФ.

Основные термины и понятия:
Государственная система защиты информации РФ

Анализ состояния информационной безопасности в стране диктует необходимость реформирования существующей организации обеспечения информационной безопасности в целях создания целостной системы обеспечения информационной безопасности РФ (далее – система).

Система является составной частью общей **системы национальной безопасности страны** и представляет собой совокупность органов государственной власти и управления и предприятий, согласованно осуществляющих деятельность по обеспечению информационной безопасности на основе единых правовых норм.

Основными **функциями** системы обеспечения информационной безопасности Российской Федерации являются:

– разработка нормативной правовой базы в области обеспечения информационной безопасности Российской Федерации;

– создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;

– определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене ин-

формацией и необходимыми ограничениями на распространение информации;

– оценка состояния информационной безопасности Российской Федерации, 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 Российской Федерации;

– контроль деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, государственных и межведомственных комиссий, участвующих в решении задач обеспечения информационной безопасности Российской Федерации;

– 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 Российской Федерации;

– организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Российской Федерации;

– защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти и органах государственной власти субъектов Российской Федерации, на предприятиях оборонного комплекса;

– обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицен-

зирования деятельности в данной сфере и сертификации средств защиты информации;

– совершенствование и развитие единой системы подготовки кадров, используемых в области информационной безопасности Российской Федерации;

– осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

Компетенция федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяется федеральными законами, нормативными правовыми актами Президента Российской Федерации и Правительства Российской Федерации.

Функции органов, координирующих деятельность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяются отдельными нормативными правовыми актами Российской Федерации.

Задачи системы защиты информации РФ

Основными задачами системы защиты информации РФ являются:

1) проведение единой технической политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности.

2) исключение или существенное затруднение добывания информации техническими средствами разведки, а также предотвращение её утечки по техническим каналам, несанкционированного доступа к ней, предупреждение преднамеренных программно-технических воздействий в целях разрушения (уничтожения) или искажения информации в процессе её обработки, передачи и хранения.

3) анализ состояния и прогнозирование возможностей технических средств разведки и способов их применения, формирование системы информационного обмена сведениями по осведомленности иностранных разведок.

4) оценка состояния информационной безопасности в стране, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, парирования и нейтрализации этих угроз.

5) контроль состояния защиты информации в органах государственной власти и на предприятиях.

6) организация фундаментальных, поисковых и прикладных научных исследований в области информационной безопасности.

7) обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в области защиты информации и сертификации средств защиты информации.

8) осуществление международного сотрудничества в сфере информационной безопасности, представление интересов РФ в соответствующих международных организациях.

Система должна обеспечивать гибкое управление процессами информационной безопасности на государственном, региональном, отраслевом, производственном и пользовательском уровнях.

Масштабность, сложность и разнообразие перечисленных функций требуют создания иерархической организационной структуры, обеспечивающей координацию деятельности всех составляющих системы информационной безопасности.

Структура государственной системы защиты информации РФ

Структуру государственной системы защиты информации составляют:

– органы государственной власти и управления РФ и субъектов РФ, решающие задачи обеспечения информационной безопасности в пределах своей компетенции;

– государственные и межведомственные комиссии и советы, специализирующиеся на проблемах информационной безопасности;

– Государственная техническая комиссия при Президенте РФ;

– Федеральная служба безопасности РФ;

– Министерство внутренних дел РФ;

– Министерство обороны РФ;

– Федеральное агентство правительственной связи и информации при Президенте РФ;

– Служба внешней разведки РФ;

– структурные и межотраслевые подразделения по защите информации органов государственной власти;

– головные и ведущие научно-исследовательские, научно-технические, проектные и конструкторские организации по защите информации органов государственной власти;

– предприятия, проводящие работы по оборонной тематике и другие работы с использованием сведений, отнесенных к государственной или служебной тайне, их подразделения по защите информации;

– учебные заведения, осуществляющие подготовку и переподготовку кадров для работы в системе обеспечения информационной безопасности.

В соответствии с Указом Президента РФ от 5 января 1992 г. № 9 создана Государственная техническая комиссия при Президенте РФ в целях обеспечения национальной безопасности народов и территорий Российской Федерации в части приоритетов и защиты информации в области обороны, политики, экономики, науки, экологии, ресурсов и противодействия иностранным техническим разведкам.

Гостехкомиссия России, являясь органом государственного управления, осуществляет проведение единой технической политики и координацию работ в области защиты информации, возглавляет Государственную систему защиты информации от технических разведок, несет ответственность за обеспечение защиты информации от иностранных технических разведок и от её утечки по техническим каналам на территории РФ, осуществление контроля эффективности принимаемых мер защиты. Гостехкомиссия России подчиняется непосредственно Президенту РФ.

Особое место в системе информационной безопасности занимают государственные и общественные организации, осуществляющие законный контроль за деятельностью государственных и негосударственных средств массовой информации.

Построение системы осуществляется на основе разграничения предметов ведения и полномочий федеральных и региональных органов государственной власти, с учётом согласованности деятельности территориальных органов федеральной исполнительной власти и органов власти субъектов РФ.

3.5. Международное сотрудничество РФ в области обеспечения информационной безопасности

Международное сотрудничество 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 РФ.

Особенность международного сотрудничества РФ в области обеспечения информационной безопасности заключается в том, что оно осуществляется в условиях обострения международной конкуренции за обладание технологическими и информационными ресурсами, за доминирование на рынках сбыта, в условиях продолжения попыток создания структуры международных 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». 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.

Международное сотрудничество в области защиты информации опирается на нормативно-правовую базу:

– Соглашение с Республикой Казахстан от 13.01.1995 г., г. Москва (Постановление Правительства РФ от 15.05.94 г. № 679);

– Соглашение с Украиной от 14.06.1996 г., г. Киев (Постановление Правительства РФ от 7.06.96 г. № 655);

– Соглашение с Республикой Беларусь (Проект);

– Выдача сертификатов и лицензий при международном информационном обмене (Федеральный закон от 4.07.96 г. № 85-ФЗ).

Основными направлениями международного сотрудничества, отвечающими интересам РФ, являются:

– предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских сетях и в каналах информационного обеспечения мировой торговли, к конфиденциальной информации в международных политических, экономических и военных союзах, блоках и организациях, к информации в международных правоохранительных организациях, ведущих борьбу с международной организованной преступностью, международным терроризмом, распространением наркотиков и незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми;

– запрещение разработки, распространения и применения «информационного оружия»;

– обеспечение безопасности международного информационного обмена, в том числе сохранности информации при её передаче по национальным телекоммуникационным сетям и каналам связи;

– координация деятельности правоохранительных органов государств — участников международного сотрудничества по предотвращению компьютерных преступлений;

– участие в проведении международных конференций и выставок по проблеме безопасности информации;

– контроль обеспечения безопасности информации в ходе международного военно-технического сотрудничества, при проведении международных выставок (салонов) вооружения и военной техники.

Особое внимание в ходе сотрудничества должно быть уделено проблемам взаимодействия со странами СНГ с учётом перспектив создания единого информационного пространства на территории бывшего СССР, в пределах которого используются практически единые телекоммуникационные системы и линии связи.

Для реализации указанных направлений сотрудничества необходимо:

– активное участие России во всех международных организациях, действующих в области информационной безопасности, в том числе в сфере стандартизации и сертификации средств информатизации и защиты процессов переработки информации;

– расширение применения обмена опытом в области обеспечения информационной безопасности, в том числе через международные и отечественные печатные издания;

– расширение участия российских специалистов в международных конференциях, семинарах, выставках.

Для разработки методологических и научно-технических проблем обеспечения международной информационной безопасности целесообразно создание под эгидой ООН международного научно-исследовательского центра.

3.6. Русский язык как объект национальной безопасности РФ

Основные термины и понятия:
Манипулирование социально-политическое

Русский язык является национально-культурной ценностью и представляет собой объект системы национальной безопасности. Сегодня существует ряд угроз сохранности русского языка, к которым относятся:

1) засорение русского языка терминами и словесными оборотами иностранного происхождения, не свойственными традициям русской словесности;

2) вытеснение русского языка из зоны «дальнего зарубежья» и всё большее ограничение его использования в качестве одного из мировых языков международного общения;

3) широкое использование в русской речи слов и оборотов жаргонного характера;

4) активное сокращение русскоязычного информационного пространства в «ближнем зарубежье», т.е. в государствах СНГ.

Сохранять родной язык необходимо в виду следующих обстоятельств:

– В любом языке содержится больше исторической и культурной информации о его носителе, чем в самом народе, если «вживую» изучать его нравы, традиции, обычаи.

– Поняв язык, можно осознать нормы культуры, конкретные особенности взаимоотношений человека и социальной общности, в которую он включен, проследить изменения в отношении к чему-либо.

– Вместе с гибелью языка рушится жизненный мир: традиции, обычаи, культурная самобытность народа.

Мышление взрослого, нормального человека неразрывно связано с речью. В речи мысль не только формулируется, но и формируется, развивается. Мы мыслим словами, которые произносим вслух или проговариваем про себя, т.е. мышление происходит в речевой форме. Психологи утверждают, что развитие у человека способностей к абстрактному логическому мышлению существенным образом зависит от богатства того языка, на котором он мыслит.

В сознании каждого человека существует нормативная система, которая представляет собой модель мира, задающая программу деятельности и состоящую из неявных и явных норм. Неявные нормы запрограммированы в языке, который отражает сложную структуру бытия, систему отношений и связи между людьми. Слова действуют на сознание человека через ассоциации, порождая поток образов и чувств. Другими словами, «образ мира», который формируется в нашем сознании, определяется не только уровнем наших знаний и идеологическими установками, но также и теми языковыми средствами, с помощью которых он формируется в процессе мышления.

Слова в естественном языке отражают становление национального характера, тип человеческих отношений и отношения человека к миру. Специфика языка определяет специфику осмысления мира. При усвоении родного языка у каждого ребёнка формируется «фильтрующая сетка», заставляющая воспринимать мир в определенных категориях. Именно в этом смысле надо понимать слова Уорфа: «…мир предстает перед нами как калейдоскопический поток впечатлений, который должен быть организован нашим сознанием, а это значит, в основном – языковой системой, хранящейся в нашем сознании. Мы расчленяем мир, организуем его в понятия и распределяем значения так, а не

иначе, в основном, потому, что мы – участники соглашения, предписывающего подобную систематизацию. Это соглашение имеет силу для определенного речевого коллектива и закреплено в системе моделей нашего языка».

Искажения языка происходили всегда и во всех странах, но в наше время это явление приняло угрожающие размеры (процесс стал неуправляемым или, наоборот, очень хорошо спланированным). История показывает, что введение жесткой «языковой цензуры» не приносит ощутимого эффекта, но из этого не следует, что нам нужно пассивно смотреть на происходящее, надеясь, что «язык переживал ещё и не такое, он справится». Во времена Петра I, когда заимствования насаждались в приказном порядке, этот процесс происходил осознанно. В настоящее время ситуация принципиально иная: люди добровольно употребляют заимствованные слова, порой не считаясь ни с какими смыслами (как в случае с употреблением нецензурных слов, которое, как показывают последние научные исследования, негативно отражается даже на физическом здоровье человека).

Методичную и тщательную замену слов русского языка чуждыми нам словами следует рассматривать как манипуляцию сознанием, а не просто «засорение» языка или признак бескультурья. Постепенно происходит искажение модели мира, заложенной структурой родного языка, и навязывание чуждой модели мира, которая призвана обеспечить желаемые (кому-то) типы поведения. Эти действия в специальной литературе называются информационно-психологическими операциями. Ещё в XIX веке Президент Российской Академии наук, государственный секретарь, министр просвещения А. С. Шишков писал, что «не одно оружие и сила одного народа опасна бывает другому; тайное покушение прельстить умы, очаровать сердца, поколебать любовь к земле своей и гордость к имени своему, есть средство надежнее мечей и пушек. Средство медленное, но верное, и, рано или поздно, но цели своей достигает. Мало-помалу налагает оно нравственные узы, дабы потом наложить и настоящие цепи, зная, что пленник в оковах может разорвать их, может ещё быть горд и страшен победителю, но пленник умом и сердцем остается всегда пленником».

В современном обществе естественный язык стал заменяться искусственным, специально создаваемым. Слова стано-

вятся рациональными, они «очищаются» от множества уходящих в глубь веков смыслов. С. Г. Кара-Мурза полагает, что, когда вместо силы главным средством власти стала **манипуляция** общественным сознанием, власть имущим понадобилась полная свобода слова − превращение слова в безличный, неодухотворённый инструмент. «Освобождение» слова означало, прежде всего, устранение из него святости, искры божьей − десакрализацию. Означало и отделение слова от мира (от вещи). Слово, имя, переставало тайно выражать заключенную в вещи первопричину. Отрыв слова (имени) от вещи и скрытого в вещи смысла был важным шагом в разрушении всего упорядоченного Космоса, в котором жил и прочно стоял на ногах человек Средневековья и древности. Начав говорить «словами без корня», человек стал жить в разделенном мире, и в мире слов ему стало не на что опереться.

Манипулирование социально-политическое − *целенаправленное воздействие на общественное мнение и социально-политическое поведение людей с помощью средств массовой коммуникации с целью изменения их сознания, позиции и действий вопреки их интересам.*

По мнению С. Г. Кара-Мурзы, создание «бескорневых» слов (слов-«амёб») стало важнейшим способом разрушения национальных языков и средством атомизации общества. Слова-«амёбы», прозрачные, не связанные с контекстом реальной жизни, перешли в огромном количестве из науки в идеологию, а затем и в наш обыденный язык. «Они настолько не связаны с конкретной реальностью, что могут быть вставлены практически в любой контекст, сфера их применимости исключительно широка (например, слово «прогресс»). Это слова, как бы не имеющие корней, не связанные с вещами (миром). Они делятся и размножаются, не привлекая к себе внимания − и пожирают старые слова. Они кажутся никак не связанными между собой, но это обманчивое впечатление. Они связаны, как поплавки рыболовной сети − связи и сети не видно, но она ловит, запутывает наше представление о мире».

Важный признак слов-«амёб» − их кажущаяся «научность». Сказав «коммуникация» вместо слова «общение», «мемуары»

вместо «воспоминания» или «электорат» вместо «избиратели» начинаешь думать, что мысли якобы подкрепляются авторитетом науки. Здесь уместно привести мнение языковеда и собирателя сказок А. Н. Афанасьева, который подчеркивал значение корня в слове: «забвение корня в сознании народном отнимает у образовавшихся от него слов их естественную основу, лишает их почвы, а без этого память уже бессильна удержать все обилие словозначений; вместе с тем связь отдельных представлений, державшаяся на родстве корней, становится недоступной».

Процесс криминализации нашего общества оказывает влияние и на его язык. Широко употребляемые такие слова как «наезд», «зачистка», «разборка» и т.п. – это прямые заимствования из словаря представителей преступного мира. Криминальное «заражение» речи происходит в основном через СМИ, литературу, кино и музыку. «Жертвами» криминального жанра (боевики, триллеры, фильмы ужасов и т.д.) чаще оказывается молодежь с традиционно высокой степенью внушаемости, психически больные, лица с неустойчивой психикой и отсутствующей сформированной профессиональной мотивацией. Они начинают употреблять слова из криминального словаря, не понимая заложенного в них смысла. Современное «криминальное чтиво» для некоторых категорий людей представляет собой учебники, руководство к действию.

Вопросы для самоконтроля

1. В чём заключаются интересы государства в информационной сфере?
2. В чём заключаются интересы общества в информационной сфере?
3. В чём заключаются интересы личности в информационной сфере?
4. В чём заключаются национальные интересы РФ в информационной сфере?
5. Какие существуют виды угроз информационной безопасности РФ?
6. Перечислите внешние источники угроз информационной безопасности РФ.

7. Перечислите внутренние источники угроз информационной безопасности РФ.

8. Покажите на примерах значение информационной безопасности в обеспечении национальной безопасности государства.

9. Какие нормативные акты обеспечивают информационную безопасность на территории РФ?

10. Какие международные нормативные акты в сфере защиты информации вы знаете?

11. В чём заключается суть государственной политики обеспечения информационной безопасности?

12. Назовите основные функции системы обеспечения информационной безопасности.

13. Из каких элементов состоит Государственная система защиты информации?

14. Почему русский язык рассматривается как объект национальной информационной безопасности?

15. Какие существуют угрозы русскому языку?

16. Как связана речь человека с его мышлением?

ГЛАВА 4. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЧЕЛОВЕКА

4.1. Неприкосновенность частной жизни граждан

Угрозы неприкосновенности частной жизни граждан.
Кодекс справедливого использования информации.

Сегодня деловая и частная жизнь многих миллионов людей оставляет «электронный след» в различного рода информационных системах (базах данных). Фиксируются телефонные звонки, оплата счетов, поездки, таможенные декларации, а также покупки в магазинах, если они оплачиваются с помощью кредитных карточек. В современном обществе граждане должны заботиться об обеспечении некоторой степени приватности, защите персональных данных. Выше были разобраны некоторые вопросы правовой защиты персональных данных. Рассмотрим социальные аспекты неприкосновенности частной жизни граждан, частным вопросом которой и является защита персональных данных.

Значительная часть персональных данных о личности накапливается в государственных и муниципальных информационных системах, что уже вызывает определенную тревогу в обществе. Возможность доступа к этим данным бюрократического аппарата и их свободного использования нарушает баланс между интересами личности и государства, создает угрозы личной свободе граждан и гражданскому обществу в целом. Так, например, информация о прописке граждан, хранящаяся в паспортных столах служб коммунального городского хозяйства России, в последнее время всё более часто становится источником махинаций и преступлений с недвижимостью. Интерес для преступников имеют и данные о суммах вкладов граждан, хранящихся на их счетах в сберегательных банках.

В крупных городах видеокамеры устанавливаются в магазинах, жилых массивах, автомобильных парковках и общественных местах (на аллеях, на улицах), офисных зданиях, внутри домов. Использование камер видеонаблюдения в районах с высоким уровнем преступности снижает этот уровень примерно на

13%. Но камеры видеонаблюдения фиксируют также события личной жизни, компьютеры хранят личные данные, а сети телекоммуникаций дают возможность получить доступ к персональной информации по всему миру.

Угрозы неприкосновенности частной жизни граждан

Рассмотрим некоторые основные угрозы личной свободе граждан, которые принимают в последнее время опасные масштабы.

1. Потеря контроля над процессом. Правительства многих стран и деловые круги, делая ставку на компьютерные технологии, заменили миллиарды бумажных папок электронными системами обработки данных. В результате возник мир, в котором ничтожная ошибка, сделанная чиновником, может повлечь разрушительные последствия для чьей-то личной жизни. Это мир, в котором не человек, а компьютер всегда прав.

2. Систематическая фиксация всего происходящего. Мы находимся на пороге нового мира, в котором каждое сделанное нами приобретение, каждое посещённое нами место, каждое сказанное или прочитанное нами слово будут записываться для последующего анализа. Но, располагая такой технологией, мы должны также и обладать достаточной мудростью, чтобы правильно и справедливо распорядиться накопленной информацией, ведь в результате мы получаем не виданное доселе количество данных наблюдения, потенциальный эффект от использования которых мы только начинаем осознавать.

3. Тотальное прослушивание окружающего мира. Серьезную угрозу свободе представляет постоянный мониторинг общественных мест при помощи микрофонов, видеокамер, систем спутникового наблюдения и других устройств дистанционного контроля в сочетании с новейшими достижениями в области обработки информации. Вскоре в больших городах большинство людей просто не сможет найти себе места, чтобы уединиться.

4. Нецелевое использование медицинских записей. Медицинские записи традиционно считаются видом конфиденциальной информации. Обязательство хранить врачебную тайну всегда рассматривалось как одно из ключевых требований к медицинскому работнику. Но обеспечение конфиденциальности пациента может идти вразрез с интересами индустрии медицинского страхования.

5. Бесконтрольная реклама. Рекламные буклеты в почте, рекламные сообщения в электронной почте, реклама по факсу и телефону, представляют собой широкомасштабную и бесконтрольную рекламную кампанию. Маркетологи всё чаще используют персональную информацию для навязчивых рекламных предложений, которые трудно отделить от подборок новостей, личных писем и другой некоммерческой корреспонденции.

6. Персональная информация как товар. Идентифицирующая личность информация: имя, профессия, хобби и другие мелочи, делающие человека уникальным – всё это превратилось в ценный объект владения, которым обладают бизнесмены, постоянно использующие его для получения прибыли и захвата рынка.

7. Микроуправление интеллектуальной собственностью. Корпорации очень бдительно следят за правомерностью использования своей интеллектуальной собственности. Но с пиратством чрезвычайно сложно бороться, когда технология позволяет любому потребителю стать распространителем интеллектуальной собственности. Чтобы предотвратить её хищение, правообладатели задействуют самые изощренные технологии слежки за клиентами. А поскольку технология уже существует, маловероятно, что её применение будет ограничено лишь защитой от пиратства.

Этот перечень не охватывает всех проблем, которые могут ожидать нас в будущем. Многие из бурно развивающихся технологий могут неожиданно оказать серьезное влияние на приватность и продемонстрировать недопустимость подхода к решению проблемы обеспечения приватности по остаточному принципу. Чтобы представить, к каким последствиям для человека это может привести, достаточно посмотреть фильмы «Сеть», «Хакеры», «Враг государства».

Кодекс справедливого использования информации

Несмотря на то, что некоторые специальные технологии могут быть использованы для защиты персональной информации, подавляющее большинство достижений в области современных информационных технологий работают на противоположную цель.

Впервые на эту опасность обратили внимание в ФРГ ещё в конце 60-х годов XX века, когда и была сформулирована новая социальная проблема защиты персональных данных. В США Э. Ричардсон создал в 1972 году комиссию по изучению влияния компьютерных технологий на приватность. После нескольких лет слушаний в конгрессе США комиссия пришла к выводу, что повод для тревоги имеется. В результате отчета Ричардсона, был разработан билль о правах в компьютерную эпоху, получивший название «Кодекс справедливого использования информации». Этот кодекс остается одним из самых значимых трудов в области обеспечения приватности при использовании компьютеров на сегодняшний день.

Кодекс справедливого использования информации базируется на пяти принципах:

1. Не должно существовать систем, накапливающих персональную информацию, сам факт существования которых является секретом.

2. Каждый человек должен иметь возможность контролировать, какая информация о нем хранится в системе и каким образом она используется.

3. Каждый человек должен иметь возможность не допустить использования собранной о нем информации для одной конкретной цели, с другой неоговоренной целью.

4. Каждый человек должен иметь возможность корректировать информацию о себе.

5. Каждая организация, занимающаяся созданием, сопровождением, использованием или распространением массивов информации, содержащих персональные данные, должна обеспечить использование этих данных только в тех целях, для которых они собраны, и принять меры против их использования не по назначению.

Наибольшее значение указанный отчет имел не для Соединенных Штатов, а для Европы. В течение нескольких лет после публикации отчета практически все страны Европы приняли соответствующие законы, базирующиеся на изложенных выше принципах. Во многих странах для приведения в действие новых законов были созданы специальные комиссии по защите данных и другие учреждения со специальными полномочиями. Существует мнение, что повышенное внимание к электронному

аспекту приватности в Европе обусловлено горьким опытом нацистской Германии в 40-е годы XX века: гитлеровская тайная полиция использовала информацию правительств и частных организаций в оккупированных странах для выявления людей, представлявших угрозу для оккупантов. Послевоенная Европа осознала всю потенциальную опасность накопления персональной информации даже самыми демократическими правительствами, прислушивающимися к общественному мнению. В настоящее время уже более двадцати стран мира приняли законы по защите персональных данных и имеют соответствующие механизмы для контроля за их соблюдением.

4.2. Влияние средств массовой информации на человека

Методы влияния СМИ на человеческое сознание.
Влияние телевидения на детей. Влияние просмотра сцен насилия по телевидению на поведение человека.

Основные термины и понятия:
Внушение
Дезинформация
Информационный (общественный) резонанс
Массовая информация
Общественное мнение
Средство массовой информации
Стереотип

Деятельность средств массовой информации имеет определяющее значение в формировании общественного мнения.

Массовая информация – *предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы.*

Средство массовой информации – *периодическое печатное издание, радио-, теле-, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации.*

Как правило, средства массовой информации (СМИ) разделяют на два типа: печатные и электронные (или телерадиовещательные).

К электронным относятся СМИ, использующие электронные каналы передачи – радио и телевидение. Электронные СМИ более оперативны, в них существует явление «прямого эфира» – моментальной передачи информации о событиях. Недостаток электронных СМИ – привязанность теле- и радиопередач ко времени эфира. Из-за ограниченного количества каналов радио и телевидение обычно более строго регулируются государством, чем печатные СМИ. Хотя телевизионные сети, как частные, так и государственные, как правило, вещают на определенную страну, их влияние часто распространяется далеко за ее пределами.

Иногда к электронным СМИ относят также интернет-газеты, ленты новостей. Однако интернет-СМИ хоть и передаются с помощью «электронного» сигнала, но по способу подачи информации, и особенно по способу её восприятия, ближе всё-таки к печатным СМИ: они передают текст и иллюстрации. Разумнее всего отнести интернет-СМИ в отдельную группу СМИ.

К печатным относят те СМИ, которые производят при помощи печатного станка – газеты, журналы. У печатных СМИ свои преимущества: к газетной или журнальной статье можно вернуться спустя день или столетие. В отличие от электронных СМИ, печатные требуют грамотности от тех, кому они адресованы, но текст дает больший простор для воображения, нежели визуальный ряд или звук.

Методы влияния СМИ на человеческое сознание

СМИ через воздействие на общество в целом воздействуют на каждого человека в отдельности, формируя определенные одинаковые эмоции и действия. Таким образом, благодаря СМИ формируется общественное мнение.

Общественное мнение – *состояние массового сознания, заключающее в себе скрытое или явное отношение различных социальных общностей к проблемам, событиям действительности.*

В практике СМИ сегодня широко используются методы подсознательного воздействия, когда отношение общества к тем или иным явлениям окружающего мира формируется с помощью **стереотипных** представлений, которые внедряются в поток новостей, автоматически вызывая в массовом сознании либо отрицательную, либо положительную реакцию на конкретное событие.

Стереотип – *принятый в исторической общности образец восприятия, фильтрации, интерпретации информации при распознавании и узнавании окружающего мира, основанный на предшествующем социальном опыте.*

Много психологических исследований посвящено формированию у людей стереотипов. Стереотипы эффективно управляют всем процессом восприятия информации. Процесс восприятия – это всего-навсего механическая подгонка еще неизвестного явления под устойчивую общую формулу (стереотип). Поэтому пресса стандартизирует сообщение, т.е. особым образом «подводит» информацию под стереотип, всеобщее мнение. Человек должен воспринимать сообщение без усилий и безоговорочно, без внутренней борьбы и критического анализа.

Стереотипы формируются под воздействием двух факторов: бессознательной коллективной переработки и индивидуальной социокультурной среды, а также, безусловно, при целенаправленном идеологическом воздействии с помощью СМИ. С помощью стереотипов легко манипулировать сознанием человека, поскольку стереотип тесно связан с жизнедеятельностью общества в целом и конкретных групп людей в частности, например, в сознании жителей нашей страны сохранилась как стереотип «философия надежды», ориентация на идеальные образцы. У американцев существуют свои стереотипы. Люди в США воспитываются так, что не верят в безысходность ситуации: они считают, что при соответствующем умении любая задача может быть решена. У них присутствует «оптимизм до последнего».

Большинство исследователей указывают на связь стереотипов с гигантским влиянием СМИ, формирующих отношение к миру, на поведение, воспроизводящее поступки «героев»,

созданных прессой, радио или телевидением. Так, например, в настоящее время неким стереотипом становится человек, ориентированный на достижение, целеустремленный, рассчитывающий на свои собственные силы.

СМИ приучают человека мыслить стереотипами и снижают интеллектуальный уровень сообщений так, что превратились в инструмент оглупления. Этому послужил главный метод закрепления нужных стереотипов в сознании – **повторение**.

Задача прессы в процессе убеждения – создать прочное, устойчивое отношение к данному явлению. Благодаря своей биологической природе, человек подвержен **внушению,** подражательности и заразительности.

Внушение – *это воздействие на личность, приводящее к появлению у человека помимо его воли и сознания определенных чувств и/или побуждающее человека к совершению определенных действий.*

Находясь под внушением, человек не контролирует направленное на него воздействие. Проще всего внушить человеку то, к чему он предрасположен в силу своих потребностей и интересов. Однако внушить что-то можно и вопреки его воле, вызывая определенные чувства и состояния, толкающие к совершению поступка, возможно, совершенно не следующего из принимаемых им норм и принципов поведения. Сама по себе деятельность СМИ, ставящая задачей внушить что-либо обществу, является негуманной, поскольку люди не могут контролировать направленное на них воздействие и, соответственно, оказываются бессильными перед подобными внушениями.

Один из приемов внушения, который используется в современной журналисткой практике – создание **информационного резонанса**. Когда информационное сообщение вызывает большой информационный (общественный) резонанс, это означает, что последовала масса разносторонних комментариев, опубликованных в различных СМИ и содержащих разные, в том числе, и противоположные, оценки. Информационная тема, вызвавшая резонанс, не просто привлекла внимание СМИ и их аудитории, она превратилась в доминирующую тему.

Информационный (общественный) резонанс (фр. *resonanse*, от лат. *resono* – откликаюсь) – *одновременное повышенное искусственное привлечение средствами массовой информации общественного внимания к тому или иному социальному или политическому событию, сопряжённое с замалчиванием других событий, имеющих равную информативную значимость.*

Информационный резонанс применяется как инструмент для эффективной манипуляции общественным мнением. Будучи искусственно созданным, информационный резонанс выдаётся за проявление коллективной воли общества и используется заинтересованными лицами для формирования «нужного» общественного мнения, внедрения в общественное сознание под видом объективной информации желательного для указанных лиц содержания. Информационный резонанс может использоваться теми или иными группами для давления на судебные органы, исполнительную и законодательную власть, правительство, общественные организации и политические партии. При создании нужного общественного мнения, средства массовой информации апеллируют к человеческим эмоциям, замалчивают «неудобные» детали того или иного события, подчёркивают нужные им обстоятельства, преувеличивая реальные масштабы того или иного происшествия.

В феврале 2008 года граждане России начали стремительно раскупать соль, словно хотели запастись ею на всю жизнь. Паника началась в Туле, где за выходные 11 и 12 февраля цена пачки соли повысилась с 6 до 60 рублей – на 1000%. Соль стала вдвое дороже сахара, чего не зафиксировано с отчетного для статистики 1913 года. За три дня в Тамбовской области были скуплены трехмесячные запасы соли. В течение декады паника перекинулось на другие города. В Санкт-Петербурге и в Москве за неделю жители раскупили этот продукт в объёме, равном полуторамесячной реализации. Наибольшей панике поддалось население небольших городов.

Признаками информационного резонанса являются:

– появление большого количества разнородных комментариев, то есть комментариев, опубликованных в разных СМИ и содержащих различные, в том числе, и противоположные оценки, выводы и прогнозы;

– публикация относительно большого числа статей, связанных с резонирующим информационным сообщением, и соответствующих сюжетов в выпусках теленовостей и аналитических телепрограммах;

– увеличение объема статей, связанных с резонирующим сообщением, и хронометража соответствующих сюжетов в выпусках теленовостей;

– публикация такого рода статей на первых полосах газет, а соответствующих сюжетов – в начале выпусков теленовостей и аналитических телепрограмм;

– объявление соответствующих тем «темами дня (недели, месяца)»;

– публикация в газетах и журналах, а равно на сайтах в сети Интернет, заочных «круглых столов» и иных форм дискуссий по темам, связанным с резонирующим информационным сообщением;

– объявление тем, связанных с резонирующим информационным сообщением, темами телевизионных ток-шоу;

– проведение по темам и вопросам, связанным с резонирующим информационным сообщением, интерактивных опросов в ходе телевизионных программ, а также голосований на сайтах в сети Интернет;

– проведение по темам и вопросам, связанным с резонирующим информационным сообщением, социологических и рейтинговых исследований или опросов, имитирующих социологические и рейтинговые исследования, и публикация их результатов;

– публикация статей и телевизионных сюжетов, рассказывающих об истории тем и вопросов, связанных с резонирующим информационным сообщением, а равно статей и сюжетов, проводящих аналогию (осуществляющих противопоставление) с зарубежными странами;

– повышение статуса комментаторов, готовых публично высказываться на темы, связанные с резонирующим сообщением.

СМИ манипулирует националистическими стереотипами и негативными установками для провоцирования определенных действий. Так, например, в настоящее время для россиян очень болезненным является национальный вопрос, который практически ежедневно поднимают СМИ. Сформирован даже некий стереотип «лиц кавказской национальности», к которым большинство граждан нашей страны относятся с подозрением. Сообщения в СМИ подаются в эмоциональной и драматизированной форме. Экономические и социальные трудности объясняются присутствием «инородцев», мешающих налаживанию нормальных жизненных условий. Пресса иногда поддерживает экстремистские лозунги решительного изгнания людей другой национальности. Национальные вопросы нередко связываются с религиозными.

Механизм создания «**образа врага**» нередко используется для создания негативной общественной реакции, в основе механизма заложена идея дегуманизации – враг представляется непохожим на вас: он другой национальности, вида, умственных способностей, кроме того, он агрессивен и ничего хорошего от него ждать нельзя. Рисуются только отрицательные черты, сведения о положительном утаиваются. Например, английская газета «John Bull», издававшаяся в годы первой мировой войны, нередко пользовалась этим механизмом для создания антифашистских настроений.

Немало внушающих элементов содержат радио- и телепередачи. Например, религиозная буддистская организация «Аум сенрике» в течение длительного времени использовала популярный радиоканал «Маяк» для своих проповедей. За это время она приобрела такое количество приверженцев вероучения, которое в несколько тысяч раз превышало число последователей на родине основателя учения, который был привлечен к уголовной ответственности за причастность к убийству людей.

Таким образом, элементы внушения можно «подать» в любое время в «упаковке» с новостями, передачами, фильмами; можно манипулировать человеческим сознанием с помощью радио и даже путем подачи информации в определенном виде в печатной продукции. Попадая в подсознание человека, они заставляют его действовать определенным образом, а поскольку взаимодействие человека со СМИ происходит ежедневно, то и

влияние на общество и на каждого человека в отдельности можно назвать очень существенным. Многие методы хорошо изучены и давно стали «классикой» манипулирования. Эти методы уже настолько «срослись» с деятельностью СМИ, что стали как бы составным компонентом деятельности.

Задача журналиста может заключаться в большей степени в достижении собственных целей и целей организации, которую он представляет. Для направленного воздействия на общественное мнение ему необходимо держать под контролем поток информации и манипулировать им. Пропаганда за многие годы отработала большое количество приемов для манипулирования общественным сознанием, которые действительно эффективны и позволяют влиять на массу определенным образом. Для воздействия на аудиторию журналист использует определенные методы, так, например, можно выделить **метод дезинформации**.

Дезинформация – *распространение искаженных или заведомо ложных сведений для достижения определенных целей.*

Так как телекомпании выражают (в той или иной степени) интересы своих владельцев, телеэфир не может быть той ареной, где из столкновений разных мнений рождается истина, а телезритель, соответственно, лишается возможности рассмотреть явление с разных точек зрения и сделать осознанный выбор.

Так, программы теленовостей могут лишь с одной стороны отражать действительную картину мира. На изложение фактов в телевизионных новостях влияют не только ограничения, касающиеся важности и значимости событий, но и политические пристрастия журналистов. Репортеров и редакторов в первую очередь интересует информация, которая:

– имеет отношение к конфликту или скандалу;

– касается странных и необычных случаев или известных людей;

– пригодна для превращения в драматичную и лично затрагивающую зрителей;

– проста для изложения за короткий отрезок времени;

– содержит визуальные элементы;

– соответствует теме, которая в настоящее время привлекает особое внимание общества.

У отдающих предпочтение фильмам и развлекательным программам подростков формируется картина мира, не соответствующая действительности:

– ТВ-полицейские раскрывают почти все преступления, что создает иллюзию полной победы над преступностью;

– в конце фильма невинный человек оправдывается и не оказывается в тюрьме;

– фигура 90-60-90 самая красивая;

– мужчины предстают более властными, доминантными, агрессивными, твердыми, настойчивыми, рациональными и умными, чем женщины, а женщины – более привлекательными, альтруистическими, общительными, моложавыми.

Частые показы насилия по телевидению «культивируют» устойчивое впечатление о мире как ненадежном, злом и опасном. Пожилые люди редко становятся героями фильмов и передач. Подобная недооценка пожилых людей формирует представление о них как о незначительной части общества. Пожилые люди изображаются во второстепенных ролях.

Дезинформация подается, как правило, из разных источников и фиксируется в подсознании человека. Далее дезинформация используется в момент принятия какого-либо важного решения, и когда будет известна правда – цель дезинформации уже будет достигнута. Таким образом, этот метод довольно эффективен. Но метод дезинформации является откровенно «грубым» и нечасто используется в современных СМИ. Можно сказать, что наиболее устойчивой является информация, рационально осмысленная и эмоционально усвоенная человеком.

Метод семантического манипулирования предполагает тщательный отбор и специальную компоновку понятий, вызывающих либо позитивные, либо негативные ассоциации, что позволяет влиять на восприятие информации (мы – борцы за независимость, процветание России, они – оккупанты, поработители народа; за нами все прогрессивное человечество, простой народ, за ними – олигархи, бандиты, чиновники). Поскольку метод основан на определенных ассоциациях, он позволяет легко повлиять на человека в силу его привычек и убеждений.

Когда утаить информацию невозможно, часто используется **метод отвлечения**. Общество не терпит информационного вакуума, поэтому чтобы отвлечь аудиторию от одной информации, необходимо переключить ее внимание на другую, поданную в максимально сенсационном виде. Цель новой информации – создать отвлекающую альтернативу и снизить актуальность предыдущей информации.

Способ подачи информации позволяет отправителю контролировать уровень ее восприятия аудиторией. По способу подачи материала Г. Шиллер выделяет два метода манипулирования: метод дробления и метод немедленной подачи информации. Сущность **метода дробления (фрагментации)** заключается в том, что по мере усложнения телевизионных программ длительность каждого их элемента сокращается во времени, что создает противоречие между действительным содержанием какого-либо события и временем, отведенным для его демонстрации, т.е. информация, поданная мелкими порциями, не позволяет ею эффективно воспользоваться. **Немедленность подачи информации**, по мнению Г. Шиллера, не только тесно связана с методом фрагментации, но и является обязательным элементом его осуществления. Однако такое ложное чувство срочности создает ощущение чрезвычайной важности передаваемой информации, хотя может таковой вовсе не являться, наоборот, отвлекая внимание человека от действительно значимой информации. Быстро чередующиеся сообщения об авиационных катастрофах, военных действиях, предвыборных поездках политических лидеров мешают составлению верных оценок и суждений, т.к. большинство важных событий обретают смысл лишь по истечении определенного времени.

Еще одним методом СМИ является **мифотворчество** (от греч. *mythos* – предание, сказание) – в технике внушения поддержание мифов играет огромную роль. Мифы внедряются в сознание, влияют на чувства и поведение людей. Мифы очень жизнеспособны, и их жизненность объясняется тем, что, опираясь на реальные факты и события, они воспринимаются как истина, догмат. Истинные же факты зачастую воспринимаются людьми как небылицы. Именно так воспринимались рассказы афганцев о том, что они участвовали в настоящей войне,

поскольку пропагандой в массовом сознании был «закреплен» миф об ограниченном введении советских войск в Афганистан.

Наверное, было бы гуманнее отказаться от мифотворчества, поскольку человек испытывает большую психологическую драму именно тогда, когда рушатся его иллюзии, а не когда он испытывает реальные трудности. В основе механизма мифологизации лежат подтасовка, сокрытие фактов, событий, документов. Но мифы всегда имеют под собой реальную основу, некое реально произошедшее событие, определенный свершившийся факт. Быстрому их распространению часто способствует низкая информационная культура, склонность к некритическому восприятию действительности. Большое количество мифов порождается условиями монополизации информации. Неосведомленность граждан позволяет властным структурам оказывать через СМИ скрытое воздействие на общественное мнение.

Еще один метод, позволяющий влиять на общественное мнение – это **имидж**. Функции имиджа и стереотипа различны. Стереотип обозначает образ, отражающий свойства и характеристики, по крайней мере отчасти присущие объекту, имидж – это искусственно сфабрикованный образ. Имидж создается путем навязывания определенных ассоциаций, он всегда связан с воображением. Имидж создает реальную социально-психологическую установку, определяющую поведение человека по отношению к объекту. И, поскольку воздействует на психику человека, следовательно, легко воспринимается, запоминается и потому часто используется в рекламе, имидж можно эффективно использовать как средство пропаганды, как инструмент управления сознанием.

Создатели рекламы утверждают, что «люди курят не сигареты, а их образ», «женщины покупают не косметику, а желание быть красивой» и т.д. Так, например, хорошо знаком образ мужественного ковбоя, предпочитающего сигареты «Marlboro».

СМИ формирует огромное разнообразие имиджей политиков, актеров, музыкантов, режиссеров. В немалой степени этому способствует телевидение, которое является основой создания сценического имиджа (Мэрилин Монро). Формируя имидж, СМИ формируют и представление о человеке, привлекает к нему внимание населения. Особенно запоминающимися выглядят первое время эпатажные, яркие, оригинальные образы.

И, чтобы образ не стал «затертым», СМИ часто представляют его в несколько ином «свете», что часто вновь привлекает аудиторию.

Сложно определить наиболее эффективный метод, поскольку каждый из них оказывает определенное целенаправленное влияние. Все эти средства внушения оказывают огромнейшее влияние на человеческое сознание, заставляя самого человека действовать и думать определенным образом.

Влияние телевидения на детей

Телевидению как средству массовой коммуникации отводится ряд функций: образовательная, развлекательная, воспитательная, организующая и т.п. Телевидение призвано удовлетворять информационные потребности общества и предоставлять объективную информацию о состоянии и развитии окружающего мира. В настоящий момент телевизоры имеют свыше 98% россиян, а для жителей сельской местности телевидение до сих пор остается единственным повседневно доступным средством массовой информации.

В течение жизни количество времени, проводимое человеком перед телеэкраном, меняется. Оно резко возрастает между 2-м и 4-м годами жизни – от 15 минут до 2,5 часов в день. Примерно до 8-летнего возраста оно остается неизменным, возрастая затем к 12 годам до максимума, составляющего около 4 часов в день. В одиннадцать-четырнадцать лет телевидение является самым влиятельным фактором на социализацию личности, ему принадлежит 68% влияния. Немаловажная роль отводится телевидению и среди факторов сопротивления воспитанию – 30,8%.

В ранние годы взрослой жизни, когда люди посвящают много времени общению, учебе и воспитанию детей, воздействие телевидения начинает уменьшаться. Однако в более поздний период взрослой жизни, когда дети уже подросли, наблюдается новый подъем. Фактически наиболее активными телезрителями являются пожилые люди. Другие группы населения, проводящие много времени у телеэкрана – это женщины и малообеспеченные люди. Интересно, что многие из групп, посвящающих большое количество времени просмотру телепередач, – это те, кто менее всего представлен в телепрограммах, персонажами которых являются преимущественно

представители среднего класса, мужчины, высококвалифицированные специалисты и богатые люди.

Говоря о **физическом воздействии**, ученые выявляют несколько факторов, негативно влияющих на формирование детского организма. Во-первых, перед экраном ребёнок долгое время сидит неподвижно, что нарушает его естественную двигательную активность, которая в этом возрасте необходима для нормального гармоничного развития. Психологи называют такое лишение физической активности депривацией, которую в детском возрасте можно характеризовать как насилие. Дело в том, что в своем развитии ребёнок проходит несколько стадий. Первая стадия развития мозга завершается в 3-летнем возрасте. На данном отрезке жизни ребенку жизненно важно активно познавать мир, и если в этот период малыш недополучит впечатлений, знаний, опыта, то многие нейрональные связи у него не образуются, а объем мозга будет на 25–30% меньше, чем должен быть. Упущенное в эти годы наверстать невозможно, поэтому специалисты призывают ограничивать просмотр телевизора для детей старшего возраста 1,5 часами в день. Малышам до 2 лет Американская академия педиатров вообще не рекомендует смотреть телевизор.

Во-вторых, в первые 4 года у человека развивается острота зрения, а в первые десять лет – тонкая моторика, управляющая глазной мускулатурой. Когда ребёнок смотрит телевизор, он длительное время находится на одном расстоянии от объекта, и ограничивает поле зрения крошечным участком (даже при чтении книги глаз получает в пять раз большее поле зрения). В итоге мышцы глаз не тренируются, их активность снижается примерно на 90% (!), и у ребёнка появляется так называемый «оцепеневший» взгляд. Впрочем, «застывший» взгляд появляется не только из-за фиксации глаз на одной точке, но, прежде всего, из-за того, что во время просмотра телевизора у человека происходит изменение активности токов головного мозга и наступает так называемое «альфа-состояние» – состояние близкое к трансу.

В-третьих, дети, которые проводят много времени перед телевизором, заболевают ожирением. Ученые Колумбийского университета исследовали 2800 детей с лишним весом в возрасте до 5 лет разного пола, этнической принадлежности и социального уровня жизни. Сначала измерялся основной обмен веществ,

то есть количество энергии, которая необходима организму для поддержания нормальных физиологических функций. После этого ученые измеряли изменение энергии в ходе 25-минутного телепросмотра. И в том, и другом случае дети спокойно лежали на диване и ничего не делали. Результаты были поразительными. Оказалось, что пока телевизор не работал, расход энергии был одним, но как только ребёнок начинал просмотр, расход энергии резко падал. Получается, что, просто *бездельничая, человек сжигает больше калорий, чем, проведя это же время у телевизора*. Таким образом, выяснилось, что телеэкран воздействует на весь организм в целом, и даже на обмен веществ.

Психическое влияние проявляется в негативном воздействии телевидения на интеллект, способности к игре, школьной успеваемости, чтении и развитии речи. В своих работах Дороти и Джером Сингер писали: «наши исследования четко показали, что дети, часто смотрящие телевизор, хуже умеют читать, хуже отличают реальное от вымысла; у них хуже развито воображение; они с большим страхом воспринимают мир; им свойственна повышенная тревожность сознания в сочетании с большей агрессивностью. Все это приводит к тому, что, когда ребёнок идет в школу, он меньше приспособлен к жизни». Об этом же не так давно во всеуслышание объявил американский специалист в области физиологии головного мозга Хорст Прен, отметивший, что «такие дети страдают полной потерей способности к воображению». Почему у ребёнка плохо развивается фантазия, если он смотрит красочные, яркие мультфильмы и фильмы со спецэффектами? Телепросмотр не побуждает ребёнка к самостоятельному творению образов в отличие, например, от чтения.

Многие психологи и педагоги (не только в Америке или Европе, но и в России) говорят о том, что у многих детей наблюдается отставание в развитие речи. Число учеников в школах для детей с отставаниями в развитии речи в Германии выросло на 58%. Английское Общество помощи детям с дефектами речи в 1996 г. сообщило, что уже каждый третий ребёнок в Англии «заметно отстает в речевом развитии». Здесь властям даже пришлось вводить специальные аварийные программы для первоклассников – 7-летних детей обучают тому, как здороваться или спрашивать дорогу. Специалисты считают, что всё это – результат дефицита личного общения. Родители приходят

вечером домой, усаживаются перед телевизором и разговаривают с детьми только скупыми односложными предложениями. А то и вовсе хранят гробовое молчание, ограничиваясь междометиями. Многие родители возражают на это, что телевизор будет развивать речь ребёнка, тем более, что сейчас достаточно детских образовательных программ. Однако оказывается, когда человек произносит слова, в речевой процесс включается все его тело, совершая определенные микродвижения. Но что удивительнее, тело слушателя во время беседы совершает точно такие же движения с небольшим запаздыванием в 40–50 миллисекунд. Это происходит неосознанно, и движения не видны глазу. То есть, для того, чтобы произнести одно слово, мы задействуем все тело. Это относится исключительно к звукам речи, причем, не важно на каком языке.

Ученый Уильям Кондон выяснил, что двухдневный младенец реагирует и на китайскую речь, и на английскую точно теми же микродвижениями, какие производит говорящий. Вовлекаясь всем существом (в прямом и переносном смысле) в общение, ребёнок учится говорить и на уровне сознания, издавая различные подражательные звуки: агуканье, бульканье, кряхтение. Прежде чем произнести свое первое слово, малыш целый год тренирует мышцы тела и лица, учится координировать более сотни мускулов, задействованных в артикуляции, ориентируясь на взрослых. А когда ребёнок слышит речь из динамиков телевизора или радиоприемника, его тело никак не реагирует на звуки.

В 1996 году английский логопед Салли Уорд опубликовала результаты своих десятилетних исследований. Она установила, что 20% обследованных детей в возрасте девяти месяцев отстают в развитии, если их родители используют телевизор как няньку. Если дети продолжают смотреть телевизор, к 3-летнему возрасту задержка составляет уже целый год.

Многие ученые говорят о гипнотическом воздействии телевизора на мозг. Телевизионные приемы – склейки кадров, различные ракурсы съемки, резкие, громкие звуки – активируют ориентировочный рефлекс у человека, удерживая его внимание

на экране. Если внимательно посмотреть рекламные ролики, то можно заметить, что кадры сменяются примерно через каждые три-четыре секунды. Это необходимо для того, чтобы удержать внимание зрителя. А поскольку дети начинают реагировать на телевизор уже с 6–8 недели, именно поэтому их так завораживает реклама. Кстати, дети лет до семи-восьми воспринимают рекламу буквально. Если говорится, что «йогурт «….» – самый лучший», малыш будет в этом убежден настолько, что никакие разумные доводы мамы и папы его не переубедят.

Оказывающей негативное воздействие на физическое, умственное или нравственное развитие несовершеннолетних, может считаться информация:

1) связанная с изображением физического или психического насилия: детальной демонстрации убийства, мучения людей, животных, причинения им увечий, а также вандализма, положительно оцениваемого насилия, смакования насилия и жестокости;

2) демонстрирующая тело умершего или тяжело раненого человека, исключая случаи, когда это необходимо для установления его личности;

3) эротического характера: возбуждающая половое желание, демонстрирующая половой акт, его имитацию или другое сексуальное удовлетворение, половые органы, приспособления сексуального характера;

4) вызывающая страх или ужас;

5) положительно оценивающая зависимость от наркотиков, психотропных веществ, табака или алкоголя, побуждающая к их употреблению, изготовлению, распространению или приобретению;

6) поощряющая членовредительство или самоубийство;

7) положительно оценивающая уголовную деятельность или идеализирующая преступников;

8) связанная с имитацией преступной деятельности;

9) подстрекающая к дискриминации по признаку национальной, расовой, половой, религиозной принадлежности, происхождению, сексуальной ориентации и др.;

10) использующая непристойные фразы, слова и жесты.

Влияние просмотра сцен насилия по телевидению на поведение человека

Статистика свидетельствует, что если ребёнок по 3–4 часа в день смотрит взрослые телепередачи, то еще до окончания начальной школы он увидит около 8 тысяч убийств. А ведь дети не способны критически воспринимать получаемую информацию и дистанцироваться от нее. Поэтому, когда ребёнок видит сцены насилия в кино или телепередаче, это вызывает у него сильнейшие агрессивные импульсы. Учёные считают, что СМИ должны думать о психологическом ущербе, который может нанести населению «слишком грубо поданная информация». Вот почему после событий 11 сентября 2001 года в США были предприняты значительные ограничения на подачу связанной с Нью-Йоркской трагедией информации о человеческих жертвах. С. Кара-Мурза считает, что тема разрушения и гибели стала главной на телевидении, которое вводит зрелище смерти в дом каждой семьи вне всяких норм, в огромных количествах и в самом неприглядном виде. Нормальный человек погружён в состояние непрерывного шока. По его мнению, на частом показе смерти настаивают рекламодатели. Специалисты по рекламе, придерживаясь принципов фрейдизма, считают, что зрелище смерти сильнее всего возбуждает внимание и интерес телезрителей, т.к. удовлетворяет подсознательный комплекс Танатоса (инстинкт смерти). Сенсационность и срочность – это технологии, обеспечивающие формирование необходимого уровня нервозности и предрасположенности к панике, которые разрушают психическую защиту личности и способствуют возникновению психических расстройств.

Многочисленные эксперименты доказывают, что просмотр фильмов со сценами агрессии приводит к большей агрессивности, чем просмотр нейтральных фильмов. Насилие влияет и на представление детей об окружающих их людях. Главные герои телевизионных фильмов чаще добиваются успеха, когда нападают на кого-то, чем когда не нападают. В этом случае насилие становится приемлемым средством достижения желанных целей. Подростки, в больших количествах наблюдающие боевые действия и приключения (также со сценами насилия), приходят к мысли, что мир намного более опасен, чем думают их сверстники,

которые нечасто смотрят телевизор. Постоянные телезрители сильнее верят в то, что сами могут стать жертвами насилия.

Частые просмотры телепрограмм со сценами насилия могут способствовать развитию преступных наклонностей, а также предрасположенности к насилию. Мальчики восьми лет, обнаружившие самые сильные пристрастия к кинофильмам с кровавыми драками и убийствами, с большой вероятностью окажутся среди совершивших тяжкие преступления по достижении ими 30-летнего возраста.

Пропорции сочетания «негативного» и «позитивного» официально считаются неизученными. Представим правила освещения негативных событий (Авт. семинар Г. С. Чеурина – «Экологическое выживание» (Серт. 271 от 02.07.2002 г.)). Согласно этим правилам, основная часть любой транслируемой информации (текста, видеосюжета, фильма) должна нести **позитивный** настрой. В любой катастрофе всегда есть место для проявления светлых человеческих качеств, человеколюбия, например, оказание помощи и поддержки, проявление заботы и внимания к нуждающимся, самоотверженность и отвага спасателей. Если без негативной информации не обойтись, то допускается её транслировать при следующих условиях: негативная информация размещается в начале текста (видеосюжета) в объеме не более 25% от общего объема информации. Оставшиеся 75% общего объема информации (в завершении) – только позитивная информация. Освещение события в таком соотношении будет **увеличивать устойчивость** социальных систем.

Специалисты считают, что факт влияния просмотра теленасилия на агрессивность уже может считаться доказанным и это влияние осуществляется, по крайней мере, пятью путями:

1) с помощью имитирующего научения (при наблюдении). Дети склонны имитировать поведение своих родителей, других детей, героев фильмов и передач, в особенности, когда их действия имеют положительное подкрепление. В этом случае ребёнок принимает данную модель и идентифицирует себя с ней;

2) теленасилие делает детей нечувствительными к насилию. Чем больше ребёнок смотрит теленасилия, тем более положительную установку на агрессивное поведение он принимает. Более того, дети, которые увлечены теленасилием, склонны подозревать других в использовании агрессивных действий, что

является эмоциональным искажением, также увеличивающим вероятность использования ими агрессивного поведения;

3) оправдание насилия является еще одним из факторов влияния теленасилия, стимулирующих агрессивное поведение. Ребёнок с высоким уровнем агрессивности прибегает к теленасилию для того, чтобы избавиться от чувства вины и получить оправдание своей собственной агрессивности. Таким образом, впоследствии он становится ещё более склонным к применению агрессивного поведения для разрешения возникающих социальных проблем;

4) теленасилие содержит в себе ключевые стимулы, пробуждающие агрессивные мысли, фантазии, чувства и действия. Это объясняет известный эффект, обнаруженный в ходе психологических экспериментов: когда дети наблюдали один вид агрессивного поведения, а затем демонстрировали агрессивные действия другого рода. Даже совершенно посторонние объекты, связываемые ребенком с агрессией, могут впоследствии служить стимулом для запуска насильственного поведения;

5) дети, увлеченные теленасилием, обнаруживали более низкий уровень физиологического возбуждения в ответ на показ сцен насилия, чем контрольная группа детей. В связи с этим они стремятся к постоянному поддержанию этого уровня, вновь обращаясь к теленасилию.

На замечание о том, что насилие представлено в СМИ в его положительных, узаконенных формах и, следовательно, не оставляет негативного отпечатка на нравственной сфере зрителей, можно возразить, что, напротив, дети склонны имитировать поведение именно агрессивных персонажей, действия которых представляются в фильме или передаче как социально приемлемые. Следует учитывать и тот факт, что дети младше 11 лет не способны к проведению четкого разделения между фантазией и реальностью.

Среди просмотра телепередач отдельно следует выделить просмотр мультфильмов, который также не может не оказывать определенного воздействия на ребёнка. Критически оценив и сравнив мультфильмы отечественного производства (включая, в основном, мультфильмы советского периода) и западного, можно сделать ряд выводов о том, что:

– многократное повторение сцен садизма в западных мультфильмах, когда герой мультфильма причиняет кому-то боль, вызывает у детей у детей фиксацию на агрессии и способствует выработке соответствующих моделей поведения;

– агрессия в мультфильмах сопровождается красивыми, яркими картинками. Герои красиво одеты, или находятся в красивом помещении или просто рисуется красивая сцена, которая сопровождается убийством, дракой, и другими агрессивными моделями поведения;

– часто персонажи западных мультфильмов уродливы и внешне отвратительны. Ребёнок идентифицирует себя не только с поведением персонажа. Механизмы имитации у детей рефлекторные и такие тонкие, что позволяют улавливать малейшие эмоциональные изменения, мельчайшие мимические гримасы. Если чудища злобные, тупые, безумные, то идентифицируя себя с таким персонажами, дети соотносят свои ощущения с выражением их лиц. Это впоследствии отражается на поведении детей: невозможно перенять злобную мимику и оставаться в душе добрым.

В нашей стране воздействие экранного насилия на поведение практически не изучается. Визуальная информация, которая уже больше десятилетия на Западе фильтруется специально созданными для этого комитетами, у нас не подвергается практически никакой критике со стороны. Подобное явление, с нашей точки зрения, не может пройти бесследно, но любые законодательные решения должны предваряться серьезными отечественными исследованиями этой важной проблемы.

4.3. Влияние рекламы на человека

Понятие рекламы. Влияние рекламы на детей. Особенности рекламы для детей в различных странах. Приемы рекламного воздействия. Реклама нездорового образа жизни.

Основные термины и понятия:
Реклама

Понятие рекламы

Современный мир насыщен рекламой, рекламные средства многочисленны, разнообразны и многолики, однако реклама не

является порождением нашего времени. Корни рекламы уходят в глубокое прошлое. Первой рекламой в письменном виде считают египетский папирус, хранящийся в Лондоне, в котором сообщалось о продаже раба. В Китае в X веке существовала печатная реклама. К рекламе также относятся и эмблемы торговцев Месопотамии. Раньше рекламные объявления рисовали на скалах вдоль торговых путей, на камнях, меди и кости. Поворотным моментом в истории рекламы явился 1450 год – изобретение Иоганном Гутенбергом печатного станка. Во второй половине XVIII века появились первые германские периодические издания, где стали публиковаться и рекламные объявления, а в 1812 году в Англии появляется первое рекламное агентство.

Развитие рекламы в России прошло те же основные этапы, что и в странах Европы и Северной Америки: от зазывал и коробейников до рекламных материалов в 1703г. в первой русской газете «Ведомости». Особое значение для развития рекламы в тот период имели ежегодные ярмарки, сопровождавшиеся изданием большого количества рекламных афиш, плакатов и коммерческих справочных листовок. К началу 20 века появились специальные рекламные издания.

Существует много определений рекламы. Слово реклама произошло от французского Reclame (от лат. *reclamare* – выкрикивать, откликаться, возражать, выражать неудовольствие). Реклама (от англ. *advertising*) также означает уведомление и истолковывается как привлечение внимания потребителя к продукту (товару, услуге) и распространение советов, призывов, предложений, рекомендаций приобрести данный товар или услугу.

Реклама – *информация о товарах, различных видах услуг и т.п. с целью оповещения потребителей и создания спроса на эти товары, услуги и т.п.*

В некоторых определениях рекламы отсутствует информационный аспект и она понимается только как воздействие на психику человека. Например, «**реклама** – *вид деятельности либо произведенная в ее результате продукция, целью которой является реализация сбытовых и других задач промышленных, сервисных предприятий и общественных организаций путем распространения оплаченной ими информации, сформированной*

таким образом, чтобы оказывать усиленное воздействие на массовое или индивидуальное сознание, вызывая заданную реакция выбранной потребительской аудитории», а также «*сущность рекламы в широком смысле этого слова, заключается в планомерном воздействии на психику человека с целью вызвать у него непреодолимое желание приобрести или сохранить известные блага*».

В настоящее время реклама преследует несколько задач.

Первая – это оповещение о существовании определенного товара или услуги, информирование населения о чем-то новом.

Вторая – актуализация до сих пор скрытой потребности человека в чём-либо. Например, человек ощущает легкую жажду, с которой нетрудно справиться. Но при виде красиво оформленного холодного напитка с ярким слоганом, человек начинает чувствовать её гораздо сильнее и понимает: в нём его спасение. Подобное послание достаточно откровенно использует наглядные образы, знаки с устойчивым, открытым для всех смыслом. Оно также смещает внимание в область скрытых потребностей, пробуждает и усиливает то, на чём можно было бы и не акцентировать внимания.

Третья – формирование новых потребностей. Например, малыш не знал о существовании видеоигр, ограничиваясь настольными. Но, увидев соответствующий ролик, начинает выпрашивать у родителей нечто новое.

Четвертая – формирование рекламой отношения к окружающему миру. Её создатели вкладывают немало усилий, чтобы их творение максимально обращалось к чувствам человека и находило отклик. Реклама навязчиво предлагает следовать её эстетическим и даже моральным эталонам, она не просто информирует о продукте или услуге, а еще и формирует выгодное ей самоопределение личности. Наряду с товаром пропагандируются образ жизни, отношение к близким, поведение в определенных ситуациях и т.д.

Таким образом, реклама является средством манипулирования личностью, призванным скорректировать её потребности и вкусы в соответствии с нуждами рекламодателя (а не потребителя), и тем самым задать нужную траекторию движения денежных средств.

Влияние рекламы на детей

Возраст, на который рассчитана реклама, постоянно снижается, поэтому среди детей растут потребительские настроения. Сейчас двухлетний ребёнок является полноправным объектом воздействия телевизионной и других видов рекламы. Ребёнок интересен рынку и производителям рекламы из трех соображений:

1) ребёнок имеет свои собственные деньги и тратит их, часто повинуясь рекламе;

2) ребёнок влияет на решение родителей о том, что покупать;

3) к тому времени, когда ребёнок вырастает, его потребительские запросы и привычки уже оказываются сформированными благодаря рекламе, которую он видел в далеком детстве.

Согласно исследованиям, ребёнок в возрасте до 8 лет не способен критически воспринимать рекламу и склонен относиться к ней с полным доверием. Дети не способны отличить, где заканчивается передача и начинается реклама. Если учесть, что в числе наиболее рекламируемых продуктов – конфеты, сахарсодержащие хлопья, сладкие напитки и всякого рода закуски, таким образом, реклама формирует неверное представление о здоровом сбалансированном питании.

Последствия влияния рекламы на детей следующие:

1. Удар по кошельку родителей. Каждый родитель знает, что стоит ему зайти в магазин с ребенком, ему придется там что-то купить: шоколадку, жевательную резинку, игрушку и т.п., потому что ребёнок не успокоится до тех пор, пока его желание не будет удовлетворено.

2. Формирование стереотипов поведения и личностных ценностей. По телевидению показывают, как люди становятся миллионерами за полчаса, а звезды эстрады рождаются за четыре недели, пища готовится моментально, а новорожденные кричат всего пять секунд. У детей создается установка, что любую проблему можно решить только при помощи покупки товара, лишая их самостоятельности выбора и применения собственных сил. К тому же, формирование потребительских привычек толкает детей на постоянные траты, не объясняя, где брать деньги на эти покупки.

3. Реклама вредит здоровью подрастающего поколения, особенно реклама вредных продуктов типа чипсов, фаст-фуда и

сладкой газированной воды, которые приводит к нарушению обмена веществ и ожирению.

4. Реклама приводит к различного вида зависимостям, особенно если речь идет о рекламе коротких SMS-сервисов, где подросток спокойно может поиграть в рулетку, и как отмечают психологи, после двух-трех сеансов может начать развиваться игровая зависимость, с которой потом очень трудно бороться.

5. Реклама ведет к ранней сексуальности. Полуобнаженные модели, на которых старается равняться молодое поколение и поведение которых принимает за эталон, присутствуют во многих рекламных роликах даже самых безобидных товаров.

Особенности рекламы для детей в различных странах

Европейский Союз. Большинство европейских общественных объединений потребителей призывают к жесткому ограничению коммерческой активности, адресованной детям. Только 4 государства Европейского Союза (Франция, Ирландия, Нидерланды и Великобритания) не считают вредной рекламу, адресованную детям. Испания считает запрет рекламы антидемократическим. Существующие в настоящее время предложения по гармонизации законодательства в этой области в рамках Европейского союза вызывают ряд вопросов относительно того, насколько далеко может зайти законодательное регулирование.

Единого общеевропейского мнения относительно этических требований к рекламе, предназначенной для детей, не существует. Телевизионная реклама, ориентированная на детей младше 12 лет, запрещена в Норвегии и Швеции, в Греции запрещен показ рекламы игрушек для детей между 7 часами утра и 10 часами вечера. Треть стран Европейского Союза приняла законы, ограничивающие рекламу, направленную на детей. Шведское законодательство относительно детской рекламы – самое жесткое. В 1991 году в Швеции была запрещена любая реклама в детский прайм-тайм – время, когда у телевизоров собирается максимальная детская аудитория. В Греции действует запрет на рекламу игрушек с 7:00 до 22:00, кроме того, полностью запрещена реклама военных игрушек. В некоторых странах Европы запрещено спонсорство детских передач, распространение рекламы, предназначенной для детей до 12 лет, и

размещение рекламы за 5 минут до и после трансляции детских передач.

В Великобритании ограничения затрагивают рекламу, которая может оказывать вредное воздействие на физическое, психическое здоровье и нравственность детей или которая использует свойственную детям доверчивость. Реклама не должна призывать детей приобретать рекламируемый продукт. Также в стране действует Кодекс стандартов телевизионной рекламы, в котором есть глава, касающаяся требований к рекламе в детских передачах. Она гласит, что реклама в детских передачах или предназначенная для детей не может содержать информацию о товарах и услугах, не предназначенных ее целевой аудитории (например, лекарств, препаратов для похудения, низкокалорийных продуктов). В разрывах детских передач нельзя размещать анонсы передач, не предназначенных для детей, а также рекламу товаров и услуг, заказываемых по почте, электронной почте, телефону или посредством иных современных средств передачи информации. Соблюдение законодательства о рекламе контролирует британская Служба по стандартам рекламы (Advertising Standards Authority – ASA), которая может осуществлять мониторинг рекламы и обязана реагировать на жалобы граждан, касающиеся соблюдения законодательства о рекламе.

США. Федеральная комиссия по торговле США устанавливает основные правила распространения рекламы. Ею, например, запрещена реклама для детей до 12 лет на товары и услуги, заказываемые по телефону. Контроль над рекламой в США осуществляет Федеральная комиссия по торговле (Federal Trade Commission). Кроме того, в США действует специальный орган по контролю над детской рекламой (Children's Advertising Review Unit – (CARU)), который является подразделением созданного общественными объединениями в области рекламы Национального совета по контролю над рекламой (National Advertising Review Council). CARU осуществляет контроль за предназначенной для детей рекламой, в том числе размещенной в сети Интернет, и с этой целью проводит мониторинг более десяти тысяч телевизионных рекламных сообщений, просматривает печатную рекламу и рекламу в сети Интернет, а также прослушивает радиорекламу.

Австралия. В Австралии действуют Детские телевизионные стандарты, первый вариант которых вступил в силу в январе 1990 года. И хотя впоследствии в эти стандарты был внесен ряд изменений, политика в этой области в основном оставалась прежней. Целью Детских телевизионных стандартов является обеспечение для детей доступа к множеству высококачественных программ, сделанных специально для них. Реклама, предназначенная для детей, должна отвечать всем требованиям, установленным Детскими телевизионными стандартами. Они применяются к рекламе, специально предназначенной для детей, в программах возрастных категорий C, G и PG.

Детские телевизионные стандарты запрещают размещать рекламу в передачах для дошкольников и устанавливают ограничения на рекламу в программах категории C. Допускается 5 минут рекламы в каждых 30 минутах материала категории C.

Детские телевизионные стандарты содержат требования к представлению рекламы и других материалов для детей, таких как указание цен, конкуренция; запрет на передачи по продаже товаров, на рекламу алкогольных напитков, на ограничение времени рекламы в передачах категории C, запрет вводящей в заблуждение рекламы и обязательность четкого и основанного на фактах представления материала.

Главной задачей этих ограничений является обеспечение того, чтобы рекламный материал был ясным и понятным для детей. Детский телевизионный стандарт устанавливает, что реклама не должна вводить в заблуждение или обманывать детей, никакие другие стандарты не могут отменить этого требования. Программы и коммерческая реклама не должны унижать отдельных лиц или группы граждан по признаку расы, национальности, этнической принадлежности, пола, сексуальных предпочтений, религии или духовной или физической немощи; представлять образы или события таким образом, чтобы чрезмерно испугать детей или внушить им беспокойство; пропагандировать небезопасное использование продуктов или опасные для жизни и здоровья ситуации, которые могут спровоцировать детей на потенциально опасные действия; рекламировать продукты, официально объявленные небезопасными службой здравоохранения или иным уполномоченным органом.

Особенности российского рынка рекламы. Первоначально при разработке и принятии ФЗ «О рекламе» от 18 июля 1995 года № 108-ФЗ законодатели придерживались точки зрения, что размещение рекламы в детских программах оказывает вредное воздействие на детей, поэтому такая реклама не допускалась. Однако под давлением руководства телерадиокомпаний и производителей детских передач, утверждавших, что без рекламы невозможно обеспечить финансирование вещания для детей, в новый закон от 13 марта 2006 года № 38-ФЗ была введена статья 6 «Защита несовершеннолетних в рекламе». Согласно этой статье «в целях защиты несовершеннолетних от злоупотреблений их доверием и недостатком опыта в рекламе не допускаются:

– дискредитация родителей и воспитателей, подрыв доверия к ним у несовершеннолетних;

– побуждение несовершеннолетних к тому, чтобы они убедили родителей или других лиц приобрести рекламируемый товар;

– создание у несовершеннолетних искаженного представления о доступности товара для семьи с любым уровнем достатка;

– создание у несовершеннолетних впечатления о том, что обладание рекламируемым товаром ставит их в предпочтительное положение перед их сверстниками;

– формирование комплекса неполноценности у несовершеннолетних, не обладающих рекламируемым товаром;

– показ несовершеннолетних в опасных ситуациях;

– преуменьшение уровня необходимых для использования рекламируемого товара навыков у несовершеннолетних той возрастной группы, для которой этот товар предназначен;

– формирование у несовершеннолетних комплекса неполноценности, связанного с их внешней непривлекательностью».

Кроме того, в соответствии с частью 4 статьи 5 «Общие требования к рекламе» реклама не должна:

– побуждать к совершению противоправных действий;

– призывать к насилию и жестокости.

В части 6 этой статьи указано, что «в рекламе не допускается использование бранных слов, непристойных и оскорбительных образов, сравнений и выражений».

Законом установлены ограничения на длительность и периодичность размещения рекламы в детских теле- и радиопередачах.

К положительным достижениям этого закона можно отнести запрет в радио- и телепрограммах рекламы алкоголя, табака и ограничение на рекламу пива.

С учетом зарубежного опыта, следует признать, что установленные указанным законом ограничения недостаточны. В первую очередь необходимо запретить размещение в передачах для детей рекламы продукции и услуг, не предназначенных для детей, например лекарственных и гигиенических средств. Следует ограничить рекламу, использующую эротические образы, например рекламу жевательной резинки, сопровождающуюся эротическим поцелуем.

Возможно, нужно задуматься о том, чтобы с учетом европейского и американского опыта внести ограничения на рекламирование сладостей и не требующих приготовления продуктов питания, способствующих развитию ожирения у детей. Необходимо обратить внимание на анонсы телепрограмм, хотя они и не считаются рекламой. Вставленные в детскую передачу или демонстрируемые непосредственно до или после детского фильма или программы анонсы, содержащие подборку наиболее «эффектных» кадров с насилием и эротикой, могут оказывать даже более вредное воздействие на психическое здоровье и нравственное развитие детей, чем сам рекламируемый фильм или передача.

Приемы рекламного воздействия

Основной стратегической задачей рекламы является увеличение продаж продукции той или иной компании. Также нет сомнений в том, что потребитель знает как об этой задаче, так и о различных методах рекламы.

Метод **утвердительных высказываний** состоит в использовании утверждений, которые представляются в качестве факта, при этом подразумевается, что эти заявления самоочевидны и не требуют доказательств. Практически вся реклама построена на использовании этого метода. Более того, нередко эти высказывания с рациональной точки рения и в отрыве от рекламы выглядят некоторым преувеличением. Например, такие слоганы как: «Не зря все дети любят Huggies» (реклама памперсов «Huggies») или «Новый год вдвойне вкусней, если с вами MilkyWay» (реклама шоколада «MilkyWay»).

Сущность метода **выборочного подбора информации** состоит в специальном подборе и использовании только тех фактов, которые являются выгодными для информационно-психологического воздействия рекламы. С практикой использования этого метода мы встречаемся в политической борьбе, управлением социально-политическими процессами, избирательных кампаниях. Однако в случае рекламы в большинстве случаев потребитель не имеет сомнений об использовании как метода «выборочный подбор информации», так и метода «утвердительных высказываний». В результате этого, изолированное использование этих методов в рекламе без реализации других не приводит к значительному воздействию на потребителя, однако их отсутствие может привести к уменьшению воздействия рекламы.

Одним из широко используемых методов в рекламе является использование разнообразных **лозунгов, девизов и слоганов**. Это позволяет «сконцентрировать» основные особенности, название и/или образ рекламируемого товара в одну фразу, которая и внедряется в сознание потребителя. Другой особенностью метода является то, что при использовании слогана запоминается не только и не столько особенности конкретного продукта, сколько его идеализированный и положительный образ. Например, вместо торговой марки «Аквафреш» используется слоган «Тройная защита для всей семьи».

При «использовании слоганов» особенно важным является создание четкой ассоциации торговой маркой с самим слоганом, для чего в его состав нередко включают название торговой марки или компании: «Blend-a-med – пусть улыбка сияет здоровьем», «Весело и вкусно – McDonalds». Для улучшения восприятия и запоминаемости слоганов реклама использует яркие и короткие фразы, рифму. Например: «Чистота – чисто Тайд», «Мезим – для желудка не заменим», «Разыгрался аппетит – не тормози – сникерсни!», «Миф-автомат – чисто идеально и цена реальна» и др.

Использование слоганов не является исключительной особенностью коммерческой рекламы, аналогичный метод используется и в политической рекламе. Например, на выборах в Государственную Думу РФ использовались такие лозунги как: «Демократическое единство – во имя жизни, свободы и достоинства»

(Федеральная партия «Демократическая Россия»), «Никто, кроме нас с Вами!» (Конгресс русских общин) и др.

Обычно у рекламы отсутствует возможность воздействовать на потребителя более или менее долгое время. Это связано как с особенностями размещения рекламы, большой стоимостью рекламного времени и/или площади, так и с особенностями восприятия рекламы потребителем, которые, как правило, стараются избегать воздействия рекламы. В связи с этим у рекламодателей возникает острая необходимость повысить воздействие рекламы в условиях недостатка времени, площади, короткого времени восприятия рекламы потребителем и т.д. Для этого реклама в рамках одного сообщения и объявления **концентрируется лишь на некоторых чертах (особенностях) имиджа и/или качеств** товара. В качестве таких особенностей и черт могут выступать: образ товара создающего хорошее настроение, увеличивающий привлекательность, способствующий улучшению здоровья, являющийся признаком высокого социального статуса, связанный с заботой о семье, имеющего высокие потребительские качества, меньшую цену, по сравнению с аналогичными товарами, высокую скорость работы, больший срок действия или надежность и т.д. Этот метод нередко использует сразу несколько рекламных роликов/сообщений, раскрывающих туили иную черту одного и того же товара, использующих ту или иную стилистику в зависимости от аудитории.

Наблюдается определенная аналогия с методом **упрощения проблемы**, который нередко используется в политической борьбе, когда информация о конкретной проблеме упрощается и сводится к нескольким, выигрышным для того или иного политика, чертам.

Метод **дополнительного свидетельства** основан на том предположении, что если совместно с тем или иным утверждением приводится также дополнительное свидетельство о его подтверждении, то потребитель психологически склонен больше доверять этому утверждению. Такого рода дополнительное подтверждение или свидетельство может быть как обезличенным, так и принадлежать организации или группе, которая обладает определенным авторитетом и/или возможностью судить о содержании утверждения. В первом случае это могут быть «клиническая практика» («клиническая практика доказала…» –

рекламный ролик жевательной резинки Dirol), «известная компания» («… разработанная известной фармацевтической компанией» – реклама зубной пасты «Аквафреш»), «проведенные испытания» и «стоматологи» («испытания показали, что … именно поэтому стоматологи рекомендуют …» – реклама жевательной резинки Orbit), «компьютерная система» («…система компьютерного контроля гарантирует результат…» – рекламный ролик программы по обучению английскому языку Bridge to Bridge), «наши знания и опыт» («наши знания и опыт гарантируют …» – реклама кофе «Tchibo») и др. Во втором случае используются несколько более конкретизируемые ссылки: «специалисты Mobil» («специалисты Mobil знают …» – реклама автомобильного масла Mobil), «лаборатория Garnier» («гарантия лаборатории Garnier-Париж» – реклама шампуня «Fructis») и др. Однако, в целом ряде случаев для повышения доверия используется точное указание фамилии, имени и работы высказывающее то или иное суждение по поводу рекламируемого товара. В этом случае, потребитель психологически склонен доверять этому суждению в большей мере. Например, в рекламе Head & Shoulders выступает некий Игорь Енушков – стилист, в рекламе Pantene Pro-V – журналистка Кэтлин Баэрд. Необходимо отметить, что используемые в рекламе люди совсем не обязательно имеют реальных прототипов.

Реклама нездорового образа жизни

Средства массовой информации пестрят материалами о курении и спиртных напитках. Дети видят, как курят их любимые киногерои. Сигареты и алкогольные напитки являются неотъемлемой частью посещений концертов и спортивных мероприятий. Реклама и кино показывают любимчиков публики с сигаретой в зубах, потягивающими виски, утверждая, что «все так делают». Реклама склоняет подростков к курению и употреблению спиртных напитков. Подростки, просматривающие множество рекламы пива, вин, ликеров и сигарет, соглашаются с тем, что она побуждает у них желание подражать увиденному. Не случайно три наиболее широко рекламируемых марки сигарет являются наиболее популярными среди подростков.

Разработчики рекламы сигарет и алкогольных напитков умышленно упускают негативную информацию о своей продукции.

В результате молодые люди не подозревают о том, какому риску они подвергаются, используя их. Иногда также поступают телевидение и печатные издания. Например, журнал печатает материалы о причинах возникновения онкологических заболеваний, но не указывает одну из основных причин – курение. Почему так происходит? Владельцы журнала получают деньги за размещение рекламы сигарет в своем журнале или даже владеют другой компанией, занимающейся производством сигарет.

Средства массовой информации широко рекламируют нездоровое питание, одновременно призывая людей терять лишний вес и поддерживать стройную фигуру. С другой стороны, повальное увлечение телевидением отвлекает людей от занятий физическими упражнениями.

Исследования показали, что девочек всех возрастов волнует проблема собственного веса. Многие из них садятся на диеты в достаточно раннем возрасте. Средства массовой информации подчас пропагандируют нереальный внешний вид идеального человека. Часто хорошо сложенный человек, изображения которого демонстрируется на экране или в печатных изданиях, является образом, сложенным из частей разных людей. Этот монтаж создается с использованием дублеров, аэрографов и компьютерной графики.

4.4. Интернет и безопасность детей

Опасности сети Интернет. Интернет-зависимость в подростковой среде.

Основные термины и понятия:
Интернет-зависимость

Опасности сети Интернет

Объем ресурсов Интернета растет в геометрической прогрессии и, наряду с полезной и необходимой информацией, пользователи сталкиваются с ресурсами неэтичного и агрессивного характера (порнография, терроризм, наркотики, националистический экстремизм, секты, неэтичная реклама и многое другое). Согласно различным исследованиям:

– только в возрасте между 8 и 13 годами дети составляют половину общего числа пользователей Интернет;

– уже в 2001 году 25% пятилетних детей в США пользовались Интернетом. Эта цифра достигает 75% среди детей возраста 15-17 лет;

– 44% детей, регулярно использующих Интернет, один раз подвергались сексуальным домогательствам при виртуальном общении, 11% подверглись этому несколько раз;

– 14,5% детей, принявших участие в опросе, назначали встречи с незнакомцами через Интернет, 10% из них ходили на встречи в одиночку, а 7% никому не сообщили, что с кем-то встречаются;

– 19% детей иногда посещают порносайты, еще 9% делают это регулярно;

– 38% детей, просматривают страницы о насилии;

– 16% детей, просматривают страницы с расистским содержимым;

– 26% детей, участвуют в чатах о сексе;

– 50% детей выходят в Интернет одни.

Риск получения ребенком доступа к неподходящей информации в Интернете включает в себя:

– сайты, посвященные продаже контрабандных товаров или другой незаконной деятельности;

– сайты, подвергающие риску конфиденциальность посетителей;

– сайты, размещающие изображения порнографического или иного неприемлемого сексуального содержания;

– сайты с рекламой табака и алкоголя;

– сайты, посвященные изготовлению взрывчатых веществ;

– сайты, пропагандирующие насилие, и нетерпимость, суицидальное поведение, наркотики;

– сайты различных сект, террористических организаций;

– сайты, где продают оружие, наркотики, отравляющие вещества, алкоголь;

– сайты, позволяющие детям принимать участие в азартных играх в режиме реального времени (on-line);

– сайты, на которых могут собирать и продавать частную информацию о детях и семье.

Кроме того, дети могут выдать информацию о кредитной карте родителей или ее пароль (а также любые другие пароли),

выдать личную информацию о семье, купить вещи без ведома родителей, нарушить авторские права, совершить компьютерные преступления, а также получить доступ, передать, или стереть нужные файлы. В некоторых случаях, они, возможно, даже не знают, что совершают это. Наконец, существует риск атаки на компьютер вирусами или хакерами. Бесконтрольный доступ детей к Интернету может привести к:

– киберзависимости,

– нарушению нормального развития ребёнка,

– неправильному формированию нравственных ценностей,

– знакомству с человеком с недобрыми намерениями,

– заражению компьютера вредоносными программами при скачивании файлов.

Интернет-зависимость в подростковой среде

Размещённые в Интернете гигантские объёмы информации могут признаваться как ценнейшим хранилищем накопленных человечеством каталогизированных знаний, так и «мусорной корзиной» малоценных и никем не систематизированных сведений. С другой стороны, Интернет является своеобразной средой функционирования подростка, обладающей своими законами формирования внутренних отношений и собственным, уникальным набором факторов, воздействующих на личность.

Блуждание по Интернету нередко затягивает, причем независимо от исходных предубеждений. Подобное затягивание в познавательные, развлекательные или коммуникативные сферы применения Интернета иной раз проходит, как считают специалисты, по модели наркотической зависимости. При рассмотрении феномена зависимости от Интернета как психического заболевания встают вопросы диагностирования симптомов, характеризующих данное заболевание. К феномену зависимости от Интернета относятся следующие поведенческие характеристики:

– неспособность и нежелание отвлечься даже на короткое время от работы в Интернете, а уж тем более прекратить такую работу;

– досада и раздражение, возникающие при вынужденных отвлечениях;

– навязчивые размышления об Интернете в периоды отвлечения;

– стремление проводить за работой в Интернете всё увеличивающиеся отрезки времени;

– готовность тратить на обеспечение собственной работы в Интернете всё больше денег;

– неспособность спланировать время окончания конкретного сеанса работы в Интернете;

– готовность лгать друзьям и членам семьи, преуменьшая длительность и частоту работы в Интернете;

– способность и склонность забывать при работе в Интернете о служебных обязанностях и важных встречах, пренебрегая при этом служебной карьерой;

– стремление и способность освободиться на время работы в Интернете от ранее возникнувшего чувства вины или беспомощности, от состояний тревоги или депрессии;

– нежелание воспринимать и принимать критику подобного образа жизни со стороны близких и начальства;

– готовность мириться с потерей друзей и разрушением семьи из-за поглощенности работой в Интернете;

– пренебрежение собственным здоровьем и, в частности, резкое сокращение длительности сна, готовность систематически работать в Интернете в ночное время;

– избегание физической активности или стремление сократить её, оправдываемое необходимостью выполнения срочной работы, связанной с Интернетом.

Интернет объединяет большие группы подростков, формирует круг интересов и общения, стимулирует развитие межличностных отношений и имеет свои положительные и отрицательные факторы влияния на индивидуальную сферу психической деятельности своих членов.

Интернет-субкультура обладает практически полным набором необходимых признаков:

– собственным сленгом;

– внутренней иерархией;

– набором устоявшихся идей, составляющих мировоззренческую позицию членов субкультуры;

– определенными этическими нормами;

– достаточным количеством формальных и неформальных лидеров, формирующих вокруг себя устойчивые сообщества пользователей, осуществляющих идейное предводительство.

Среди отрицательных факторов влияния Интернет-культуры на личность необходимо назвать в первую очередь её деперсонифицирующее воздействие, перенос коммуникативной активности из реальных условий социума в сеть, аутизацию.

Интернет являет собой изобилие компьютерных игр, находящихся в свободном доступе пользователя. Кроме версий, реализуемых в автономном режиме, имеется большое количество сетевых игр – от шахмат и карточных игр, реализованных в online-режиме, до специфических, исключительно компьютерных игр – стратегий, квестов, и т.д.

Геймерство – самая распространенная среди подростков форма Интернет-зависимости. Преобладание этой формы обусловлено отсутствием необходимости в каких-либо навыках работы с персональным компьютером, увлекательностью многих игр и предоставляемой играми возможностью аутоидентификации с самыми различными героями. Такие игры значительно популярнее приключенческой и фантастической литературы, что связано с динамичностью их и, главное, сложным, меняющимся по ходу действия сюжетным алгоритмом, интерактивностью сюжета. Многие игры сочетают в своём сюжете несколько линий, позволяющих проявить как созидательные и поисковые, так и деструктивные качества пользователя.

4.5. Жестокие компьютерные игры

Опасность жестоких компьютерных игр.
Влияние жестоких компьютерных игр на поведение человека.

Опасность жестоких компьютерных игр

Во время Второй мировой войны вдруг обнаружилось, что большинство американских солдат неспособно убивать противника. Неспособно из-за изъянов военной подготовки – солдат учили стрелять по нарисованным мишеням. Очень часто многие солдаты под влиянием страха, стресса и прочих обстоятельств просто не могли применить оружие. Стало ясно, что солдатам необходимо прививать соответствующие навыки. Возникла потребность в создании тренажеров, на которых солдаты учились бы убивать. Вместо традиционных мишеней нужно было ис-

пользовать силуэты человеческих фигур. Применение симуляторов решало этот вопрос. Морская пехота США получила лицензию на право использовать в качестве тактического тренажера игру «DOOM». В сухопутных войсках взяли на вооружение «Супер-Нинтендо». В классической игре «утиная охота» заменили пластмассовый пистолет пластмассовой штурмовой винтовкой М-16, а вместо уток на экране появляются фигурки людей.

В ряде компьютерных игр присутствует антиобщественная тематика, и, к сожалению, именно такие игры особенно популярны среди детей и подростков 8–15 лет. По данным одного проведённого в США исследования, почти 80% видеоигр, наиболее любимых молодёжью, отличаются жестокостью. В играх «Вина» «action» на насилие уходит 91% в 91% времени, причем в 27% игр насилие приводит к смерти. Райер, президент компании «Virtual Image Production», говорит, что «игры перестали быть просто играми. Они превратились в средство обучения. И мы учим детей получать радость, нажимая на курок. Однако мы не обуждаем их задуматься, к каким последствиям это приводит в реальной жизни».

Еще в 1976 году общественный протест против агрессивных игр вызвала приставочная игра «Смертельная гонка» («Death Race»). Она сводилась к тому, чтобы автомобилем сбивать пешеходов, пересекающих экран в различных направлениях. Побеждал тот, кто задавит больше всего людей. Современные, более хитроумные игры отличаются лучшей графикой и создают у игрока иллюзию того, что он на самом деле совершает самые кровавые зверства. К тому времени, когда игрок проходит все уровни современной игры подобного содержания, он успевает догнать и убить до 33000 человек. Существуют игры и с таким сценарием, где бейсбольной битой надо ударить по голове ни в чем неповинного человека, чтобы забрать у него автомобиль.

Среди игр на быстроту реакции есть так называемые «стрелялки от первого лица», которые часто подвергаются критике за содержащуюся в них жестокость. В целом, когда в СМИ говорят об опасности компьютерных игр, обычно имеют в виду именно «стрелялки». Игра, как правило, сводится к тому, чтобы, выбрав оружие, убивать врагов, будь то люди или кто-то еще.

Например, игра, может начинаться очень «по-домашнему»: человек пошёл за молоком, а потом «достаёшь пистолет и начинаешь стрелять в прохожих». В России такие игры продаются без ограничений, хотя во многих странах подобные компьютерные развлечения строго варьируются по возрастным категориям, например «от 18 лет», а в некоторых странах подобные игры вообще запрещены.

Влияние жестоких компьютерных игр на поведение человека

Военный психолог Д. Гроссман в своей книге «Об убийстве» пишет, что механизм воздействия электронных игр схож с боевой подготовкой, во время которой солдаты учатся преодолевать врожденный барьер перед совершением убийства («On Killing»). К примеру, было обнаружено, что у многих пехотинцев отвращение к убийству исчезает, когда во время учений они стреляют не по обычным мишеням, а по мишеням в виде человеческих фигур. Такой же эффект, по мнению Гроссмана, оказывают и пропитанные насилием игры: они прививают детям «вкус и навык к убийству».

С тех пор, как существуют компьютерные игры, содержащие элементы насилия, агрессии и т.п., в СМИ периодически появляются сообщения о трагедиях, разыгравшихся на почве фанатичного увлечения виртуальными играми. Более того, с определённой периодичностью власти различных стран предпринимают ограничительные меры, касающиеся продажи, выпуска и распространения агрессивных электронных игр.

В США уровень тяжких преступлений в середине 2000-х возрос по сравнению с серединой 50-х в 7 раз. В Канаде, по сравнению с 1964 годом, число попыток убийства возросло в 5 раз. В Индии за 15 лет количество убийств на душу населения удвоилось, в Норвегии и Греции увеличилось почти в 5 раз, в Австралии и Новой Зеландии – почти в 4. В Швеции по той же категории преступлений рост трехкратный, а в семи других европейских странах – двукратный. Причем в таких странах, как Норвегия, Швеция и Дания, уровень тяжких преступлений сохранялся неизменным почти тысячу лет!

Популярные видеоигры категории Е (по классификации видеоигр в США), рекомендованные для детей старше шести лет, воспитывают склонность к насилию и жестокости. Здесь нужно бить, стрелять и убивать, и за это полагается вознаграждение. Пусть убийство и вознаграждение за него виртуальные – в сознании компьютерного поколения виртуальная реальность не отличается от настоящей жизни. Если учесть, что около 70% американских детей проводят время у компьютеров или электронных игровых приставок к телевизорам, стоит ли удивляться тому, что в США (и других странах тоже) повсеместно школьники открывают огонь из пистолетов и ружей в школах, смешивая игру с действительностью?

Весной 1999 года Президент США Билл Клинтон в своем телевизионном обращении к американскому народу заявил: «мы должны думать дважды, когда речь идет о "стрелялках от первого лица"». Поводом к его выступлению стала перестрелка в школе. Два подростка убили одиннадцать одноклассников. Один из стрелявших был не только игроком в DOOM, но и разработчиком (на любительском уровне) новых «уровней» этой игры.

В 2004 году в Великобритании 14-летний подросток Стефан Пакира был жестоко убит своим приятелем, 17-летним Уорреном Лебланом. Леблан заманил Пакира в местный парк, где зверски избил и зарезал. На суде обвиняемый заявил, что был «одурманен» игрой Manhunt. И хотя суд города Лестер посчитал, что Леблан совершил убийство с целью ограбления, мать убитого подростка, Г. Пакира, полагает, что подросток просто имитировал игру, в которой присуждаются очки за жестокие убийства. Показательно, что объёмы продаж компьютерной игры Manhunt («Облава») значительно выросли после этого судебного процесса, широко освещавшегося в СМИ. Игра была «сметена» с полок магазинов в Манчестере, Эдинбурге, Бирмингеме, Ливерпуле, Белфасте и Глазго. Многие люди, не знавшие раньше о существовании «Manhunt», теперь желали ее приобрести. Многими крупными торговыми сетями игра была изъята из продажи.

Четыре национальных организации здравоохранения США, среди которых American Medical Association, выпустили документ, в котором утверждают, что виртуальное насилие напрямую связано с реальным. По мнению ученых, чья работа продолжалось около 9 месяцев и содержит в себе около 1000 отчетов, исследований и т.д., «виртуальное насилие может вызвать у человека агрессивное отношение, поведение, а также просто увеличить агрессивность». Игры делают насилие «привлекательной и обыденной» вещью.

Проведенные эксперименты показывают, что

– наиболее агрессивные люди постоянно играют в компьютерные игры с элементами насилия,

– любой человек сможет на время увеличить уровень своей агрессии, даже недолго поиграв в подобные игры.

Главной опасностью «жестоких» игр психологи считают то, что они порождают стопроцентно агрессивную реакцию на практически любую конфликтную ситуацию. Формируется подсознательный условный рефлекс, подсказывающий, как вести себя в случае возникновения той или иной проблемы. Причем чем больше времени человек проводит за компьютером (играя в «жестокие» игры), тем выше вероятность того, что любая, даже просто неоднозначная ситуация, требующая анализа и размышлений, будет воспринята им как конфликтная, которую он будет решать единственным доступным ему способом, а именно – силой.

Случай в Падуке (США). Четырнадцатилетний подросток украл у соседа пистолет 22-го калибра. До этого он никогда не занимался стрельбой. Потом он принес оружие в школу, сделал восемь выстрелов и ни разу не промахнулся! Восемь пуль – восемь жертв. Из них пять попаданий в голову, остальные – в верхнюю часть туловища. Как отмечают все свидетели трагедии, он стоял, как вкопанный, паля прямо перед собой, не уклоняясь ни вправо, ни влево. Такое впечатление, что он методично, одну за другой, поражал цели, появлявшиеся перед ним на экране. Как бы играл в свою компьютерную игру!

К сведению, для среднестатистического офицера полиции нормальным считается, когда из пяти пуль в цель попадает одна.

В плане воздействия на мозг человека «жестокие» компьютерные игры намного опаснее фильмов (или книг) с аналогичным содержанием. Играя на компьютере, человек сам принимает решения (идентифицируя себя с персонажем игры), тогда как при просмотре видеоряда он лишь пассивный наблюдатель. К тому же фильм длится пару часов, а за одной видеоигрой ребёнок в среднем может провести до 100 часов. В фильмах, как показали исследования, людей привлекает не количество жертв на экране, а общий динамизм и высокая скорость развития сюжета.

Ученые университета Тохоку в Японии обнаружили, что компьютерные игры стимулируют лишь те участки головного мозга, которые отвечают за зрение и движение, но не способствуют развитию других важных его участков. Игры останавливают развитие лобных долей мозга, которые отвечают за поведение человека, тренировку памяти, эмоции и обучение. Таким образом, параллельно с формированием жестокости у современного поколения подростков происходит падение умственных способностей.

Вопросы для самоконтроля

1. Почему защита информации о частной жизни граждан стала проблемой в наше время?
2. Какие существуют механизмы защиты информации о частной жизни граждан?
3. В чём особенность влияния СМИ на детей?
4. Какая информация оказывает негативное воздействие на развитие несовершеннолетних?
5. Какими путями просмотр телепередач со сценами насилия повышает агрессивность детей?
6. Перечислите способы защиты человека от негативного влияния информации.
7. Назовите последствия влияния рекламы на детей.
8. Какие существуют особенности рекламы для детей в различных странах?
9. Каким образом следование рекламным призывам может привести к ухудшению здоровья человека?
10. Каковы возможные опасности для ребёнка в сети Интернет?
11. По каким поведенческим характеристикам можно судить о формировании у человека зависимости от Интернета?

ГЛАВА 5. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЧЕЛОВЕКА В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

5.1. Слухи как неформальный обмен информацией

Слухи как социально-психологический феномен. Определение слуха. Классификация слухов. Причины возникновения и механизмы распространения слухов. Управление слухами. Особенности распространения слухов в чрезвычайных ситуациях. Распространение слухов через Интернет на примере теракта в США 11 сентября 2001 года.

Основные термины и понятия:
Дезавуирование
Слух
Сплетня

Слухи как социально-психологический феномен

Феномен слухов не только известен с древних времен, но и издавна использовался в самых разных целях. Обмен специфическими сигналами о вероятной опасности, о чем-то полезном и жизненно важном появился у наших предков намного раньше, чем первые признаки речи. Возможность передачи значимой информации от одного индивида к другому обеспечивала выживание племени. Много веков слухи, устные сообщения с негарантированной достоверностью, распространяющиеся в конкретной группе людей, были единственным «средством массовой информации».

Располагая доступной информацией, человек ищет объяснение окружающим явлениям, складывается его субъективное видение действительности. Если сведений не хватает, то, избегая неопределенности, вызывающей ощущения дискомфорта, он стремится к восполнению пробелов. Наиболее естественный и легкий выход – обратиться к «собратьям», переживающим ту же ситуацию. В это время любую новую информацию по теме он мгновенно встраивает в свою картину мира и передает её вместе с собственными интерпретациями далее другим участникам.

Систематическое изучение феномена слухов началось только после Первой мировой войны в США и в Германии. В Америке скоро появились коммерческие фирмы, специализировавшиеся

на распространении слухов, где можно было заказать нужный сюжет в нужной аудитории, оплатив «услугу» по прейскуранту. Это делалось, например, в целях рекламы товара, или подавления конкурента, или борьбы с профсоюзом. Так, среди рабочих конкурирующего предприятия распространялся такой слух, который мог спровоцировать их на забастовку. Или, наоборот, хозяин, узнав о готовящейся забастовке на его собственном предприятии, заказывал распространение среди жён рабочих слуха такого содержания, которое подрывало доверие к профсоюзным лидерам и т.д.

Более 70% россиян отмечают, что сталкиваются со слухами, из них около 45% чаще чем 1–2 раза в неделю. Слухи рассматриваются сегодня не только как стихийное коммуникативное явление, но и как технология влияния на общественное сознание, эффективное средство информационно-психологического противодействия.

Определение слуха

Существует множество определений слуха. В словаре В. И. Даля **слух** понимается как «*молва, вести, наслух, говор в народе, слава, огласка*». В словаре В. В. Бурцевой **слух** рассматривается как «*весть, известие о ком-л., чём-л.*».

Кроме приведенных выше, существуют и другие, более содержательные определения:

1) **слух** – *специфический вид межличностной коммуникации, в процессе которой сюжет, до известной степени отражающий некоторые реальные или вымышленные события, становится достоянием обширной аудитории.*

2) **слух** – *циркулирующая форма коммуникации, с помощью которой люди, находясь в неопределенной ситуации, объединяются, создавая разумную ее интерпретацию, сообща используя при этом свои интеллектуальные возможности*.

Множество определений подчеркивают лишь некоторые аспекты и характеристики слухов, т.к. непросто однозначно охарактеризовать такое сложное явление. Б. В. Дубин, А. В. Толстых полагают, что слух – своего рода «черный рынок» информации: ценность слуха в том, что он утаен, неофициален, передается «своим», а значит – о «чужих». Иначе говоря, это вести обо всем интересном чужом (или как бы чужом) для своих.

Тем самым слухи выполняют своеобразную роль в «стратификации» общества недифференцированным и неспециализированным сознанием: мир привычно и устойчиво делится на «своих» и «чужих».

> **Слух** – *информация, которая распространяется без предоставления общепринятых свидетельств достоверности.*

Можно отграничить слух от ряда других информационно-психологических явлений. Так, высокая степень обобщенности отличает слух от сплетни, доноса, дезинформации; привязка ко времени и среде своего возникновения – от байки, поверья; наличие свежей новости – от легенды, анекдота, неофициальность – от официальной информации. Существует родственное понятие «сплетня», которую от слуха отличает тот факт, что сплетня – это сознательное и злостное придумывание и перевирание фактов.

Таким образом, слухи, во-первых – это известие, новость, сообщение, информация. Во-вторых, сообщение, недостаточно отражающее реальное положение дел или их искажающее. В-третьих, с помощью слухов создается и передается общественное мнение, настроение, социальные стереотипы и установки аудитории, информационная ситуация в регионе. В-четвертых, они являются средством психологического воздействия: изменения мнений, отношений, настроений, поведения, удовлетворения потребностей людей и социальных групп.

Классификация слухов

В социальной психологии выработан подход к классификации слухов. В качестве оснований для такой классификации выделяют информационную, экспрессивную и результативную характеристики слухов.

По **информационному** основанию – это слухи достоверные и недостоверные, стихийные и фабрикуемые, а по **экспрессивному** – слухи-желания, слухи-пугала и агрессивные слухи. Слух-желание отражает и удовлетворяет надежды, стремления людей, разочарование по поводу несбывшегося желания и деморализует их. Слух-пугало приводит к тревоге, неуверенности и

страху среди членов определенной социальной группы. Агрессивный слух вызывает неприязнь, ненависть к конкретным лицам или социальным группам, вносит разлад, подозрительность, взаимное недоверие во взаимоотношения людей.

По **результатам** влияния на сознание и поведение людей выделяют слухи:

1) будоражащие общественное мнение, но не выходящие за рамки явно выраженного асоциального поведения;

2) вызывающие антиобщественное поведение известной части населения;

3) разрушающие социальные связи между людьми и выливающиеся в массовые беспорядки.

По **происхождению** слухи могут быть спонтанно и стихийно возникающими либо умышленно фабрикуемыми, целенаправленно распространяемыми. Возможны и промежуточные разновидности. Иногда слух зарождается стихийно, но, попав на определенную почву, находит заинтересованных ревностных распространителей, готовых приукрасить информацию в соответствии со своими интересами. Бывает и наоборот, когда первоначально слух запущен умышленно, но впоследствии, попадая в стихийно действующие социально-психологические механизмы, многократно ими усиливается.

По **степени достоверности** слухи бывают абсолютно недостоверные, недостоверные с элементами правдоподобия, правдоподобные, достоверные с элементами неправдоподобия. Специалисты отмечают, что эффект от использования ложной информации носит кратковременный характер и, как правило, ограничивается временем осуществления пропагандистских акций в условиях дефицита информации.

Причины возникновения и механизмы распространения слухов

Механизмы порождения и распространения слухов рассматриваются в современной науке как правило с двух точек зрения: социологической и психологической. Социологи обращают особое внимание на роль слухов в жизни больших и малых социальных групп, психологи – на то, какое место занимают слухи в процессе удовлетворения индивидуальных человеческих потребностей. Эти подходы являются скорее дополняющими,

нежели исключающими друг друга, поскольку рассматривают механизмы порождения слухов на различных уровнях социальной организации: групповом и индивидуальном.

На общесоциальном уровне слухи служат различным целям. Они применяются в качестве «пробного шара»: запуская соответствующий слух, выясняется, кто и как будет реагировать на его содержание. Зная, какую реакцию оно вызывает, можно соответствующим образом спланировать будущие действия. Однако слухи могут оказывать серьезное (чаще всего − негативное) влияние на поведение людей. По данным Национальной Консультативной Комиссии по гражданским беспорядкам США, слухи значимо усиливали напряженность и массовые волнения в американском обществе в конце 60-х гг. прошлого века.

Воздействие слухов на групповом уровне проявляется в виде поддержания групповых или классовых границ: члены определенной социальной группы при помощи слухов подчеркивают различия между собой и «чужими», что способствует формированию групповой идентичности. «Присоединение» к слуху со стороны конкретного человека означает его интегрированность в коллектив. Разделяя информацию, которая содержится в слухе, циркулирующем в его группе, человек консолидируется с этой группой, у него возникает и усиливается «Мы-чувство». Слухи выполняют функцию «социального барометра», выступая индикатором социального климата группы. Они как бы выражают мнение группы по определенному вопросу, напоминая членам группы, какую позицию им следует занимать по данному вопросу.

Среди **причин возникновения** и живучести слухов наиболее значимыми являются: возможность удовлетворения с помощью слухов актуальных потребностей людей; недостаток информации, необходимой для организации деятельности по удовлетворению актуальной потребности; многомерность, субъективная неоднозначность событий.

Слухи стихийно возникают или целенаправленно фабрикуются и распространяются для удовлетворения конкретных потребностей людей. В перечень основных потребностей, удовлетворяемых посредством слухов, включают:

– утилитарные потребности;

– потребности в престиже;

– потребности в познании;

– эмотивные потребности.

Утилитарные потребности связаны с достижением людьми (социальными группами) определенных целей: овладение объектом информации, укрепление позиций в группе, ослабление или вывод из борьбы конкурента, формирование у людей определенных мнений, настроений, побуждение их к конкретному выбору, поведению и т.д. Механизмом реализации данной потребности может выступать агрессия: человек сознательно распространяет слухи, чтобы причинить боль другому, говорит неправду и сплетничает, делая из кого-либо «козла отпущения».

Другой целью распространения может быть желание помочь другим людям (родным, близким, знакомым, случайно оказавшимся рядом), предупредить их о надвигающихся опасностях и неприятностях, дать возможность самим или совместно подготовиться к неблагоприятным событиям.

Потребность в престиже удовлетворяется в том случае, когда владение информацией (раньше других либо информацией эксклюзивного характера) повышает престиж человека. В основе стремления к престижу лежит потребность обратить на себя внимание. Другими словами, сплетником движет обычное желание выделиться, похвастаться.

Сообщая другому сведения, составляющие содержание слуха, человек поднимает себя в своих глазах («никто не знает, а я знаю!»). У окружающих создается впечатление о некой «принятости», «вхожести» носителя эксклюзивной информации в референтные группы, формируется мнение о нем как о человеке осведомленном. В данном случае слух рассматривается в качестве товара.

Не случайно, пересказав даже самую нелепую «байку» от своего имени, человек, чтобы оставаться последовательным, начинает изобретать аргументы в ее пользу, клянется в ее правдивости, вступает в спор с окружающими, всеми силами стремится убедить их в достоверности слуха. Это происходит потому, что распространитель информации связывает доверие к сообщению с доверием к себе самому. В случае если ему не верят, он испытывает дискомфорт.

В процессе групповой дискуссии может возникать своеобразное соперничество, провоцирующее стремление каждого участника к достижению первенства в скорости, подробности, красочности изложения содержания слуха.

Эмотивные потребности удовлетворяются за счет того, что слухи, как правило, порождают сильные эмоции позитивной или негативной модальности. Человек, распространяющий слухи, может испытывать наслаждение, удовольствие от их содержания, от реакций на них людей. Причиной их распространения может быть личное озлобление, ненависть по отношению к конкретным людям (социальным группам).

Благодаря слухам могут разряжаться сильные негативные переживания людей (стремление «выплеснуться», «хоть немного облегчить душу»). В данном случае действует механизм проекции. Распространяя слухи, человек неосознанно выражает свои страхи, желания и враждебные чувства и надеется, что сомнения и беспокойства будут развеяны окружающими. Здесь важную роль играет стремление к получению эмоциональной поддержки. Распространяя тревожные слухи, он надеется на их опровержение другими, что, в свою очередь, помогает снизить его собственную тревогу. Человек получает подсознательное облегчение от того, как адресат реагирует на сообщение – удивлением, испугом, восхищением, благодарностью; для усиления впечатления информация нередко «творчески» обогащается неприятными подробностями. Такой механизм особенно силен у людей, неудовлетворенных своим социально-психологическим статусом и не нашедших достойного места в жизни.

В контексте реализации данной потребности срабатывает механизм оказания услуги. Распространяя слухи, человек может стремиться сделать приятное другому, выдавая желаемое за действительное. Поэтому слухи повторяются и теми, кто в них не верит, но благодаря им выражает свои чувства или отношение к кому-либо или чему-либо.

Слухи нередко помогают людям сохранить последовательность, стабильность своих представлений о мире: в них часто содержится информация позволяющая разделить мир на «своих» и «чужих». При таком разделении мира появляется возможность для коррекции своей самооценки с помощью процедур «низвержения» и «вознесения».

Познавательные потребности и интересы удовлетворяются слухами тогда, когда информация об интересующих человека событиях отсутствует или некачественна. Ряд авторов указывает на то, что важной причиной для возникновения слухов является искажение информации при устной ее передаче «из уст в уста». Чем длиннее цепочка, чем большее количество людей участвует в коммуникативном процессе, тем значительнее искажаются сведения.

Слух, если и не удовлетворяет полностью любопытство человека, его интерес к конкретному предмету, событию, то в значительной мере приглушает его.

Взаимосвязь между потребностями человека, владением необходимой информацией и переживаемыми эмоциями изучается современными учеными (П. В. Симонов), которые доказывают, что для удовлетворения актуальной в каждый момент времени потребности человек должен совершать вполне определенные действия, поэтому ему важна информация о предметах и условиях, удовлетворяющих эту потребность. Чем острее проявляется потребность, тем больше нуждается человек в соответствующей информации.

В зависимости от наличия и качества информации, необходимой для организации действия по удовлетворению потребности, у человека возникают те или иные эмоции.

Для отражения характера этой зависимости предлагается своеобразная формула:

Э = П(Н-С),

где Э – эмоции, П – потребности, Н – необходимая для деятельности информация, С – сообщенная (полученная) информация.

Данную формулу можно проиллюстрировать на следующем примере: группе специалистов предстоит действовать на зараженной местности. Если группа сформирована из опытных работников, неоднократно выполнявших подобные задачи, то потребность в информации о характере и способах действий у них может оказаться минимальной, а эмоции по данному поводу будут незначительными. Эмоции также слабо выражены, если информация, необходимая для организации действий по удовлетворению потребности, равна той, которая имеется в распоряжении специалистов. В этих случаях нет места и для циркуляции

слухов. Информационное пространство группы заполнено, и, если в него проникают слухи, они быстро «гасятся».

Когда же информация, прогностически необходимая для осуществления деятельности и удовлетворения потребности, отсутствует (равна 0), отрицательные эмоции проявляются максимально. Эта ситуация особенно благоприятна для возникновения и распространения слухов. Острая необходимость действовать для удовлетворения потребности, с одной стороны, и отсутствие информации – с другой, делают человека неразборчивым в оценке ее источников. Чем менее информированы люди по привлекшему их внимание событию, тем более они возбуждены эмоционально и тем менее рационально их поведение. Длительный дефицит информации вызывает информационный голод, при котором люди, образно говоря, заглатывают чудовищные небылицы.

Именно в связи с этим процесс распространения слухов катализируется цензурой. Строгая цензура особенно в военное время способствует распространению деморализующих слухов.

Сила воздействия слухов в значительной мере зависит от их **источника**. Часто информация подобного рода исходит от человека, относящегося к одной из следующих категорий:

– близкие люди: родственники, приятели, соседи, сослуживцы и т.п. Доверие к ним объясняется просто: «свой не обманет»;

– случайные встречные, не замеченные ни в чем плохом просто в силу малой известности: попутчики в транспорте, стоящие рядом в очереди, собутыльники... Все эти люди имеют в глазах слушателя одно достоинство: «А какой смысл им меня обманывать? Мы ведь никогда больше не увидимся!»;

– так называемые личные авторитеты: для больного – это врач, оказавший ему помощь, для призывника из деревни – видавший виды офицер, для спортсмена – тренер, для мелкого воришки – «пахан» с большим тюремным стажем. В роли такого «авторитета» может выступить приехавший в захолустье житель столицы с атрибутами «крутого».

В большинстве указанных случаев важно, чтобы:

а) между источником информации и её потребителем существовала авторитетная дистанция (возрастная, материальная, иерархическая и т.п.);

б) присутствовал элемент восхищения собеседником хотя бы по какому-то одному параметру, совершенно необязательно относящемуся к существу слуха (самый сильный, самый богатый, самый красивый...);

в) источник принадлежал к кругам, которые недоступны слушателю («Знакомая тетка работает в Белом доме...» или: «Вчера на свадьбе у брата сидел рядом с одним полковником...»).

Г. Олпорт и Л. Постман предупреждают, что нельзя рассматривать слух как линейно детерминированное явление. По их мнению, слух – это «непростой механизм», который служит сложной цели. Например, агрессивный слух позволяет нанести удар ненавистному противнику и тем самым высвобождает первичное эмоциональное побуждение. В то же время он оправдывает чувства, которые человек испытывает к ситуации, объясняет, почему эти чувства возникают. То есть он рационализирует неоднозначную ситуацию.

Исследователи слухов указывают на то обстоятельство, что их появление становится возможным благодаря многомерности, многоплановости событий, неравенству реальности самой себе, наличию у нее как бы второго дна, когда она делится на близкую и далекую, видимую и подлинную.

Как считает американский специалист по вопросам коммуникации в условиях кризиса Уолтер Джон, чаще всего распространению слухов способствуют следующие **обстоятельства**:

– недостаток официальной информации и сообщения их первоисточников;

– сообщения из первоисточников не полные;

– положение характеризуется повышенным уровнем тревоги и опасений;

– ошибочная информация порождает сомнения;

– отсутствие внимания к требованиям личности;

– затягивание принятия решений по серьезным вопросам;

– ощущение невозможности повлиять на свою судьбу;

– наличие общих организационных проблем;

– конфликты организаций и отдельных личностей.

В литературе выделяются социально-психологические условия, побуждающие людей **воспринимать** слухи.

К таким обстоятельствам прежде всего относятся:

1. Тревожная, напряженная, трудная обстановка, содержащая проблемы, угрозы, опасности, в которой люди ищут пути обезопасить себя и своих близких.

2. Стремление предупредить наступление неприятных событий, заблаговременно к ним подготовиться и уменьшить возможный урон, если избежать его невозможно.

3. Наличие психологического заражения, подражания, группового давления, стремления обезопасить себя вместе со всеми.

4. Уверенность в достоверности сообщения. Не зная откуда исходит слух, люди склонны предполагать, что информация представлена из надежных источников. Это создает иллюзию достоверности сообщения и формирует эффект ложного консенсуса, т.е. уверенности в том, что слух разделяют большинство людей.

5. Психологические особенности людей, предрасполагающие к восприятию слухов. Здесь, во-первых, следует выделить высокую внушаемость части людей, их неспособность самостоятельно и критически оценить правдоподобность и обоснованность слуха. Во-вторых, особой подверженностью слухам отличаются люди чрезмерно любопытные, вечно «принюхивающиеся», прислушивающиеся к любому разговору, каким бы далеким он от них ни был. Наконец, в большей степени восприимчивыми к слухам оказываются люди, испытывающие недовольство, фрустрацию, усталость, не занятые какой-либо деятельностью, находящиеся в состоянии длительного ожидания.

6. Социально-психологические особенности групп и совместной деятельности. Отмечается, что слухи активнее распространяются в группах, в которых царят бездеятельность, однообразие, скука.

При большом спектре причин распространения и принятия слухов главным является **информационный вакуум** в значимой для людей сфере, который заполняется стихийно или целенаправленной вражеской пропагандой.

Важным для понимания законов распространения слухов является вопрос о **каналах их передачи**. Более 58% опрошенных россиян указывают, что основным каналом распространения слухов являются средства массовой информации и коммуникации. Около 68% респондентов сталкиваются со слухами

при общении с сослуживцами, приятелями, соседями, 20% «подпитываются» ими в транспорте, на улице и в очередях, 10% – в семье.

В ходе информационно-психологического противодействия в условиях военных действий для распространения слухов активно используются листовки, радио, средства звуковещания, вхождение в сети боевого управления противника и др.

Г. Олпорт и Л. Постман в 1947 году сформулировали «базовый закон слухов», отражающий зависимость интенсивности (количества) слухов от важности событий (вопросов) и неоднозначности сведений о них. Формула, отражающая этот закон, имеет следующий вид:

$R = i * a,$

где R – это область распространения слуха, интенсивность его распространения, длительность существования и степень доверия слуху;

i – это степень значимости слуха для слушателя или читателя, если он окажется правдивым;

a – это степень неопределенности или сомнительности слуха.

Таким образом, область распространения слуха, интенсивность его распространения, длительность существования и степень доверия ему приблизительно равны значимости слуха для слушателя, если он окажется правдивым, умноженной на неопределенность слуха, особенно неопределенность его опровержения. Однако обычное опровержение слуха не устраняет его неопределенность, а порой даже увеличивает. Для устранения неопределенности необходимо привести объективные причины, доказывающие, почему слуху не стоит верить.

Когда и значимость, и неопределенность достигают высшей точки, то область распространения слуха также находится на самом высоком уровне. Но если хотя бы один из этих факторов немного уменьшается, то область распространения слуха сокращается довольно значительно. Самый интересный аспект этой математической зависимости наблюдается в том случае, когда неопределенность или значимость снижается до нуля. Так как всё, что умножается на нуль, равняется нулю, слух исчезает.

Согласно указанной выше формуле, слухи распространяются тогда, когда отражаемые в них события важны для аудитории,

а полученные относительно них известия либо недостаточны, либо субъективно двусмысленны. Двусмысленность возрастает, если известия сообщены неясно, противоречиво либо если человек не в состоянии понять полученное им сообщение. По мнению авторов, важность и двусмысленность не складываются, а перемножаются – если либо важность, либо двусмысленность равна нулю, слух не возникают.

С учетом наиболее важных детерминант и переменных, связанных с распространением слухов, психологи разработали своеобразную формулу для вычисления (прогнозирования, оценки) интенсивности их распространения. Она имеет следующий вид:

С = И /(КС(В)*ДИ)

где С – интенсивность циркуляции слухов, И – интерес аудитории к теме, КС – количество официальных сообщений по теме на данный момент времени (В), ДИ – степень доверия к источнику официальных сообщений.

Из формулы видно, что быстрота распространения слухов прямо пропорциональна интересу аудитории к теме и обратно пропорциональна количеству официальных сообщений по данной теме и степени авторитетности источников официальной информации.

Слухи быстрее распространяются в социально однородной среде, где проявляются общие интенсивные переживания многих людей, имеющих одинаковое отношение к событиям, объектам. Поэтому специалисты по информационно-психологическим акциям, как правило, делят аудиторию на гомогенные по потребностям целевые группы. Для каждой из таких групп фабрикуется «свой» слух. На уровне группы происходит повышение гомогенности мнений: внутригрупповое обсуждение слухов способствует кристаллизации общей точки зрения и снижению межиндивидуальной вариативности мнений, что, в конечном счете, повышает гомогенность группы.

В распространении слухов половая принадлежность не имеет особого значения. Мужчины в равной степени «сплетничают», различается лишь тематика сплетен. Они концентрируют свое внимание на равенстве («его повысили раньше, чем меня, но я же делал не меньше?»), безопасности и контроле над ресурсами, тогда как женщины обмениваются ценными сведениями о

членах семьи сотрудников, личной жизни «других» и т.д. А. В. Дмитриев отмечает, что «мужчины больше, чем женщины, склонны производить, распространять и принимать такой вид слухов, как политические новости (официальные и неофициальные), женщины – новости, связанные с ростом цен, семейной жизнью».

При анализе множества фактов распространения слухов выяснилось, что слух пользуется большим успехом, если несет дискомфортную информацию, т.е. такую, которая вызывает страх, тревогу, возмущение, прерывает обычный ход событий. Существует своего рода приоритет негативных слухов перед позитивными. Объяснить это довольно сложно, но практика подтверждает значительно более сильное влияние негативных слухов по сравнению с позитивными. Возможно, это следствие вполне оправданного нашей историей хронического недоверия властям. Негативный слух живуч еще и потому, что его порой невозможно опровергнуть, ибо приходится решать задачу доказательства, что «ты не верблюд». Невозможно, строго говоря, доказать что г-н Иванов И. И. вообще не берет взяток. Можно доказать, что он не взял в конкретной ситуации от конкретного лица и даже вообще никогда не был замечен в лихоимстве. Но невозможно со 100%-й уверенностью утверждать, что Иванов И. И. не брал в других обстоятельствах или не возьмет в будущем.

Управление слухами

Рассматривая общий механизм управления слухами, в первую очередь отметим невозможность силового контроля над ними. В разных странах периодически предпринимались попытки введения негативных санкций за распространение слухов. Однако нет никаких данных, подтверждающих эффективность силовых методов борьбы со слухами. В России, как известно, слухи активно распространялись даже в период широкомасштабных репрессий. Введение цензуры только способствует распространению слухов.

Трудности в решении проблемы слухов силовыми методами заставили обратить серьезное внимание на их профилактику, уничтожение «питательной среды», в которой они возникают. В большинстве случаев со слухами начинают бороться лишь после того, как они широко распространились, тогда как самый

эффективный путь борьбы со слухами – это предупреждение ситуации, их порождающих. Главное заключается в том, чтобы быстро и точно оповещать людей и придерживаться принципа постоянной двусторонней коммуникации.

Для **профилактики** слухов следует реализовать комплекс мер направленный на:

– предвидение и противостояние чувствам тревоги и неопределенности;

– поддержание информационной открытости и правдивости;

– запрет на искажение фактов;

– предоставление населению требуемого объема фактической информации;

– снятие ограничений на каналы передачи информации;

– формирование у людей убежденности в деструктивной природе слухов.

Практические задачи сводятся к созданию слухоустойчивой среды в рамках отдельных, относительно замкнутых групп (воинское подразделение, экспедиция, политическая партия, предприятие, фирма и т.д.), при проведении избирательных и прочих кампаний, а также противодействием конкретному циркулирующему слуху.

Б. В. Дубин и А. В. Толстых упоминают следующие мероприятия профилактического и контрдейственного характера:

1. Прогнозирование потенциальных и изучение процессуальных и эмоциональных составляющих распространения слухов. Следует изучить ситуацию и получить ответы на вопросы:

1) среди каких социальных групп распространяются слухи?

2) каковы виды и содержание слухов?

3) какие чувства отражают слухи?

2. Индоктринация («прививка от слухов») наиболее вероятных объектов-мишеней воздействия предполагает первоначальное представление аудитории малой порции информации о событии, «переваривание» ее людьми, выработку ими определенной позиции принятия или непринятия с последующим предъявлением основного массива информации. Важное профилактическое значение имеет оперативное информирование «группы риска» по темам возможной дезинформации, т.е. превентивные опровергающие действия.

3. Завоевание доверия аудитории официальными источниками информации за счет использования психологических механизмов: «первичность сообщения», «авторитетный коммуникатор», «голос пророка» и др.

4. Обеспечение доступности информации. В некоторых учреждениях организуются специальные «линии слухов» – внутренние телефонные номера, по которым сотрудники могут позвонить и получить ответ по интересующей теме.

5. Поддержание эффективного руководства на всех уровнях, повышение авторитета руководителей и доверия к ним.

Если слух все-таки начали распространять, нужно противодействовать им немедленно с тем, чтобы контролировать их. Уолтер Джон предлагает следующую стратегию, к которой можно прибегнуть в **борьбе** со слухами:

1) приступить к планированию и какому-либо корректирующему действию;

2) проанализировать масштабы распространения, серьезность причин и влияние слухов;

3) проанализировать конкретные причины, мотивы и источники распространения слухов;

4) поговорить с людьми, на которых подействовали слухи или которые понесли убытки вследствие их распространения, добиться взаимопонимания с ними, высказать свою обеспокоенность по поводу распространения слухов и готовность активно бороться с ними.

5) без промедления предоставить полную информацию по поводу конкретного дела;

6) пресечь ложные слухи с помощью контрслухов, поручив это надежным коллегам или доверенным лицам;

7) собрать вместе официальных лиц и неформальных лидеров, тех, кто формирует общественное мнение, и других влиятельных людей, чтобы обсудить и прояснить ситуацию, заручиться их поддержкой.

Пресечение слухов предполагает осуществление разноплановых мероприятий, направленных на снижение заразительности, распространяемости и живучести. Прежде всего, это:

1. **Игнорирование неправдоподобных слухов** (технология «Бойкот») с одновременной демонстрацией опровергающих фактов. Однако игнорирование слуха может привести к тому,

что он, продолжая жить по своим законам, нанесет чувствительный ущерб. Неэффективными оказываются и беспредметные риторические опровержения типа: «Не верьте враждебным слухам!».

2. **Контрслух** («фланговая» атака) – слух противоположного содержания. Суть «фланговой» атаки состоит в следующем. Никоим образом не упоминая о слухе или его сюжете, под различными предлогами настойчиво передается значимая информация противоположного содержания. Но это очень тонкая задача, требующая предельного внимания к мелочам. Высока вероятность того, что такие меры усугубят обстановку. При малейшей оплошности скажется эффект психической инерции (или апперцепции), т.е. сложившейся установки на восприятие новой информации: последующие сведения преломляются через призму предыдущих.

3. **Контраргументация**. Распространяя правду, нужно избегать ссылок на слухи. Нет необходимости самому повторять слухи до тех пор, пока они не приобрели огромных масштабов. Если же это произошло, нужно идти к людям и публично изобличать тех, кто распространяет слухи.

4. **Дезавуирование** слухов. Активное разоблачение слухов возможно с использованием технологий «Таблица слухов», «Клиника слухов».

Дезавуирование – *(от франц. desavouer – отказываться, выражать неодобрение), в международном праве опровержение главой государства или правительства действий или заявлений дипломатического или иного официального представителя, превысившего свои полномочия.*

«Таблица слухов» оформляется таким образом, чтобы в ней в одной колонке были перечислены «бродившие» некоторое время слухи, а в другой – реально наступившие события. Такая таблица может публиковаться в СМИ и отражаться в настенной информации.

Прием «Клиника слухов» – это сбор будоражащих общественное мнение слухов, их групповое обсуждение и осмеяние. Сюжеты слухов могут проигрываться «в лицах» с элементами психодрамы.

Но предпринимаемые усилия по дезавуированию слухов могут способствовать их распространению. Ведь опровержение любой информации неизбежно включает две части: 1) доведение до аудитории опровергаемого сообщения и 2) его разоблачение. При этом нежелательная информация доходит и до тех, кто ранее с ней знаком не был. В этом случае возможны два исхода: а) опровержение признается истинным, а слух – ложным, б) слух рассматривается как достоверный, а опровержение – как стремление скрыть истину. Поэтому перед началом кампании по развенчанию слуха следует тщательно просчитать, какое количество людей уже знает о нем, и решить, чего больше – пользы или вреда от его публичного опровержения.

5. **Развенчание источников** (распространителей) враждебных слухов. В некоторых ситуациях (война, социальные конфликты, чрезвычайное положение, трагические последствия) виновники распространения слухов (особенно агрессивных и разобщающих) должны нести суровое наказание.

6. **«Лобовая» атака**. Для принятия эффективных мер надо адекватно оценить информационную обстановку, и прежде всего такой её параметр, как доверие к источнику. Если есть уверенность в том, что данный источник информации (политический, административный, профсоюзный лидер, журналист, газета, радио – или телеканал и т.д.) в данной аудитории пользуется высоким доверием, целесообразна «лобовая» атака. При этом пересказывается сюжет слуха, самокритично объясняются его причина и повод и излагается альтернативная или более приемлемая версия. Если прямая форма изложения не приемлема, используется другая, более мягкая. Однако лобовая атака на слух контрпродуктивна, если нет уверенности в том, что наш источник в данной аудитории обладает непререкаемым авторитетом. Тогда уже нужно прибегать к более тонким приемам «фланговой» атаки.

7. **Юмор.** Весёлая своевременная шутка для слуха подчас целесообразнее, чем целая серия мероприятий.

8. **Подтверждение** слуха. Бывают ситуации, когда лучший способ уничтожить слух – подтвердить его, тем самым отсечь от сюжета неизбежные наслоения (в силу тенденций, о которых ранее говорилось) и взять ситуацию под контроль. В противном

случае, упрямо стремясь опровергнуть слух, мы рискуем нанести обществу ещё больший ущерб.

9. **Доведение до абсурда.** Прием «доведение до абсурда» подразумевает распространение информации, не противоположной содержанию, а наоборот, усиливающей тенденцию, лежащую в основе первоначального слуха. Счастливые перспективы или драматизм ситуации доводятся до таких масштабов, что воспринимается как нереальные.

Учитывая негативную роль слухов в организации, можно сформулировать следующие **принципы профилактики** слухов:

1. Оперативное реагирование в виде предоставления достоверной информации со стороны официальных источников.

2. Исчерпывающее информирование, предполагающее систематическое предоставление информации по интересующему персонал вопросу.

3. Обратная связь. Отслеживание мнения сотрудников по поводу планируемых, происходящих или происшедших изменений позволяет организации корректировать свою политику.

4. Однозначная трактовка информации, выражаемая в понятном языке, его простоте и однозначности.

Особенности распространения слухов в чрезвычайных ситуациях

Современный мир со своими опасными технологиями, как и экстремальные ситуации, вовлекая в себя различные по масштабу группы людей (вплоть до всего общества), содержат многочисленные поводы для возникновения слухов: «на Новомосковском химзаводе (г. Тула) произошла утечка фенола…»; «в Подмосковье из-за отключения электроэнергии произошли выбросы радиоактивных веществ…»; фекальный выброс добрался по Москве-реке до Воскресенска и Коломны…». В последние годы имеют широкое распространение так называемые «слухи об отравлениях». В них сообщается о вредных последствиях употребления разного рода продуктов питания. Некоторые авторы считают, что источником веры в такого рода слухи является латентная тревожность, стимулируемая непрерывным проникновением новых технологий во все области жизни.

Среди социально-психологических обстоятельств, побуждающих людей **распространять** слух в чрезвычайных ситуациях, следует особо выделить два:

1) чувство солидарности – стремление помочь другим людям (близким, друзьям, соседям), предупредить их и дать возможность самим или совместно подготовиться к встрече с неприятным событием;

2) компенсация неудовлетворенности от единоличного обладания тревожной информацией – человек получает подсознательное облегчение от того, что другой, получивший от него информацию, реагирует удивлением, испугом, восхищением, благодарностью за сообщение.

Политической и экономической нестабильности, кризисам, банкротствам, катастрофам, стихийным бедствиям, чрезвычайным обстоятельствам, эпидемиям, международной напряженности, угрозе начала войны, неблагоприятному ее ходу и т.п. всегда сопутствуют слухи. По большей части это слухи тревожные, нежели радующие и успокаивающие. В боевой обстановке они способны вызывать панику. Еще Чингисхан прибегал к подобному методу, распространяя слухи об огромных размерах своей армии, что снижало боевой дух врагов. Введение в заблуждение может осуществляться и в направлении преуменьшения собственной силы и возможностей. Фашистская Германия, например, посредством слухов старалась убедить жителей Великобритании в слабости и неспособности Германии к активной борьбе. Назывались даже конкретные даты поражения Германии. Когда же указанная дата наступала, Германия все еще продолжала активно сражаться, что приводило англичан в уныние и вызывало недовольство правительством.

Характерен пример из истории Второй мировой войны. Утром 7 декабря 1941 года Япония без объявления войны нанесла мощный авиационный удар по главной базе Тихоокеанского флота США Перл-Харбор на острове Оаху, принадлежащем к группе Гавайских островов. Он застал находившийся там флот врасплох. После удара японские самолеты возвратились на свои авианосцы, которые взяли курс назад в Японию. В разрушенной базе никто не знал, куда делся враг. В ней царила паника, и ходили невероятные слухи, которые увеличивали хаос, растерянность и потери: японцы высадили десант на востоке ост-

рова Оаху, захватили населенный пункт на западе острова, вся северная часть острова была уже в руках врага. В разные концы отправлялись отряды для их уничтожения, но парашютистов не обнаруживали. Говорили, что живущая на острове японская диаспора вот-вот начнет восстание, что японские агенты отравили уже ряд источников воды. Услышав это, люди, пившие воду, почувствовали себя плохо и были доставлены в госпитали. Жители Оаху, японцы по происхождению, принимались за переодетых вражеских солдат, задерживались и доставлялись в комендатуру и полицию. Когда спустилась ночь и было введено полное затемнение, обстановка усложнилась. Без конца поступали сведения об обнаруженных группах врага. То там, то здесь вспыхивала стрельба: стреляли часовые, которым что-то померещилось в темноте, целые подразделения вели огонь друг подругу. Группа американских самолетов после разведки в море возвращалась на свой аэродром с зажженными бортовыми огнями. Всем кораблям и зенитным батареям строжайшим образом было приказано не открывать огня – самолеты свои. Но стоило им появиться у Перл-Харбора, как линкор «Пенсильвания», подав пример «бдительности», ощетинился огнем. В одно мгновение застреляло все, что могло стрелять. Пять своих самолетов были тотчас сбиты, но боевой дух на кораблях поднялся: наконец «японцев проучили».

Главное, что тревожит людей и способствует возникновению и хождению слухов в чрезвычайных ситуациях:

– неясность обстановки, непредсказуемость ее развития;

– отсутствие ощущения себя в безопасности, когда человек испытывает тревогу, страх;

– плохая (скудная, нерегулярная, запаздывающая, неполная, неубедительная, неправдивая) информация о ситуации;

– неуверенное руководство (отсутствие его решительности, твердости, оперативности, несвоевременность и неполнота принимаемых мер, недостатки обеспечения, помощи людям и их защиты, недоверие людей к руководству).

Податливость людей слухам в экстремальных ситуациях возрастает из-за общей неразберихи, неустроенности, усталости, часто – изнуренности, повышенной тревожности, присутствием среди них потерпевших, больных, раненых, чувствующих себя беззащитными. Слухи, возникая в экстремальных ситуациях, оказывают преимущественно отрицательное влияние на людей,

повышая психологическую напряженность, тревожность, неуверенность, нездоровые настроения, растерянность, страхи, отчаяние. Они подталкивают людей к неоправданным действиям. Большинство слухов малодостоверно, содержит в себе больше неправды, чем правды; поступая в соответствии с такими слухами, люди совершают ошибки, промахи, порой очень тяжелые.

Вера в истинность слуха также способствует его распространению. Человек, передавший слух, который оказался недостоверным, может навлечь на себя упреки лиц, поверивших этому слуху. Поэтому люди склонны воздерживаться от трансляции чрезмерно недостоверных слухов. На передачу слуха влияет и оценка его содержания с точки зрения возможных последствий описываемого события. Слух, воспринимаемый как не имеющий последствий, распространяется менее активно, чем слух, который, по мнению собеседников, имеет последствия.

Слухи и разного рода домыслы возникают в основном тогда, когда не хватает фактов. Поскольку слухи вызываются обеспокоенностью, их самыми распространенными темами становится возбуждающие эмоции проблемы, связанные с опасностью для жизни или угрозой благосостоянию людей. Слухи могут доводить их до крайности, порождать групповые нарушения общественного порядка. Слухи о полном исчезновении продуктов, распространяемые оппозицией, приводят к тому, что люди действительно скупают все товары, вызывая рост цен и дефицит. Вину же за сложившуюся ситуацию жители возлагают на правительство, стоящее у власти.

Распространение слухов через Интернет на примере теракта в США 11 сентября 2001 года

Новая технология сменила систему монолога СМИ на диалог Интернета, сняв большое число ограничений (хотя и не все) с права порождения своего мнения. Интернет на сегодня является наименее контролируемой информационной областью, что облегчает размещение там нужной информации. Он постепенно становится одним из привычных каналов коммуникации для конкретных типов аудитории. Оказалось, что Интернет как менее контролируемое информационное пространство оказывается выгодной площадкой для запуска нужной информации в нужное время.

Интернет является идеальным способом распространения слухов, в том числе и тех, которые могли оказаться полезными для террористов, например, для провоцирования паники и отвлечения внимания спецслужб. После террористических атак 11 сентября 2001 года в англоязычный Интернет периодически вбрасывалась весьма странная информация, на которую реагировали даже солидные средства массовой информации.

Уже 16 сентября, через пять дней после атак на Нью-Йорк и Вашингтон, возможностями Интернета воспользовались откровенные мошенники. В Сети появилось письмо, получателям которого предлагалось пожертвовать определенную сумму денег группе хакеров, которые обещали определить местоположение Усамы Бен Ладена.

На следующий день появилось сообщение, согласно которому очередная крупная атака террористов состоится 22 сентября. Автор письма утверждала, что своими ушами слышала, как несколько подвыпивших людей, похожих на арабов, на английском языке обсуждали планы страшной атаки с помощью грузовиков со взрывчаткой, которые будут взорваны в Бостоне. Впоследствии подобные слухи появлялись примерно раз в 1,5–2 месяца. Каждый раз в них называлась новая дата и новые цели, однако к середине 2003 года подметные письма такого рода стали редкостью. Однако некоторые из них стали широко известны, в том числе и благодаря солидным изданиям. Газета Asia Times в 2002 году опубликовала статью, что «Аль Каида» заблаговременно спрятала несколько атомных бомб в семи крупных городах США и готова взорвать их. Источником информации было интервью с одним из помощников Бен Ладена, распространенное по электронной почте.

Показательна история, которая стала очень популярной в средствах массовой информации арабского мира. Ливанская телекомпания «Аль Манар» и иорданская газета «Аль Ватан» первыми сообщили, что 4 тыс. евреев, работавших в зданиях Всемирного Торгового Центра, заблаговременно получили предупреждение от израильской разведки и 11 сентября 2001 года не вышли на работу. Источником информации было анонимное письмо, полученное по электронной почте. Аналогичная фальшивка появилась чуть позже – на сей раз в письме сообщалось, что группа американских евреев бурно выражала свою радость

при виде рушащихся небоскребов. Далее в Сети начало циркулировать сообщение, что погибший лидер террористов – египтянин Мухаммед Атта – за месяц до случившегося был по неизвестным причинам (но с понятной целью) освобожден из израильской тюрьмы. Также циркулировали электронные послания с описаниями загадочных историй: якобы американская полиция арестовывала подозрительных личностей с оружием, картами секретных объектов, атомных электростанций и пр., но освобождала их, потому что у задержанных были израильские дипломатические паспорта (другие версии – после звонка из израильского посольства, после появления израильского посла, после команды из Белого Дома и пр.).

Появились и иные – арабские и мусульманские – версии: например было сообщение о том, что еще 10 сентября нью-йоркские таксисты-мусульмане отказывались выполнять рейсы в центр Нью-Йорка.

Неизвестные авторы фальшивок пытались играть на человеческих глупостях. К примеру, затаившихся в США членов «спящих ячеек» террористических структур предлагалось выявить всем миром, используя весьма оригинальную тактику. Письмо призывало: «Разденься и испугай террористов!». Добропорядочным патриотичным американкам предлагалось в 7 часов вечера одновременно выйти на улицы в полностью обнаженном виде. «Как известно, – утверждал автор письма – мусульманам запрещено смотреть на обнаженных женщин, за исключением их собственных жен. Исламские террористы будут вынуждены закрыть глаза – тут их и схватят». В письме также утверждалось, что идея организации столь массового стриптиза исходит от американских спецслужб.

Бен Ладен на длительное время стал, вероятно, самой популярной персоной Интернета. Американские пользователи Всемирной Сети, например, узнали, что именно Бен Ладен владеет несколькими известными компаниями США (в их числе назывался и один из крупнейших банков мира – Citibank). Эти «новости» охотно публиковали редакторы многочисленных сайтов. Подразумевалось, что американцы не будут покупать товары и услуги у этих фирм, дабы финансово не поддерживать «террориста номер один».

Про Бен Ладена также сообщалось, что он умер от почечной недостаточности (в апреле 2005 года в Сеть был запущен слух о смерти Бен Ладена), что его видели в Детройте (Бостоне, Атланте и пр.), что американские войска взяли его в плен в Афганистане и «придерживают» объявление о поимке ко дню президентских выборов (слух появился в октябре 2004 года) и т.д. Появились и «личные письма» Бен Ладена, отправленные соратникам откуда-то из афганских пещер, в которых Бен Ладен призывал крепить конспирацию и духом окрепнуть в борьбе.

5.2. Принятие решений в чрезвычайных ситуациях

Принятие решения. Виды решений. Этапы принятия решения. Особенности индивидуального и группового принятия решений.

Основные термины и понятия:
Групповое мышление
Принятие решения

Ежедневно человек принимает множество разнообразных решений. В одних случаях принятие решения (ПР) не оказывает существенного влияния на жизнь и дальнейшую судьбу человека, а в других – наоборот. Грамотные действия, основанные на адекватной оценке ЧС и прогнозе ее возможного развития и последствий, могут значительно повысить шансы человека на выживание.

Понятие «принятие решения» можно трактовать в узком и широком смысле. **В узком смысле принятие решения** — *это заключительный акт деятельности по выявлению, анализу различных вариантов решения, направленный на выбор и утверждение лучшего варианта решения.* В данном случае решение рассматривается как акт выбора, осуществляемый индивидуальным или групповым лицом, принимающим решение (ЛПР) с помощью определенных правил. В этой связи, например, говорят: «Руководитель принял решение». В узком плане решение можно также трактовать как результат выбора, тогда оно представляет собой предписание к действию (план работы, вариант проекта и т.п.).

В широком смысле принятие решения – *это процесс, протекающий во времени, осуществляемый в несколько этапов.* Другими словами, это совокупность всех этапов и стадий по подготовке (выработке) решения, включая заключительный этап непосредственного принятия решения. Именно в таком широком смысле этот термин будет использоваться в данной книге. После принятия решения осуществляется деятельность по реализации принятого решения. Иногда этот этап также включается в понятие «принятие решения».

Вопросами подготовки и принятия решений занимаются многие науки. Представители каждого научного направления, исходя из специфики рассматриваемых задачи и используемых методов, дают различные определения понятию «принятие решения». Математики рассматривают принятие решения с позиций рекомендуемых ими методов и алгоритмов; социологи — с точки зрения процессов, протекающих в обществе; психологи пытаются «заглянуть в душу человека», определяя мотивы принятия того или иного решения. Экономическая составляющая присутствует практически в любом комплексном решении и касается вопросов рационального распределения и использования ресурсов, определения рациональных объемов производства, повышения экономической эффективности отдельных направлений производственно-хозяйственной деятельности и др. Юристы рассматривают принятие решения с точки зрения права.

Принятие решения – *процесс выбора варианта действий в имеющейся ситуации из многих возможных.*

Другими словами, принятие решения – это всегда выбор одной альтернативы из ряда имеющихся. Если нет альтернатив, то нет выбора и, следовательно, нет и решения. Таким образом, характерной особенностью любой ситуации, связанной с принятием решения, является наличие нескольких альтернативных (взаимоисключающих) вариантов действий, из которых надо выбрать наилучший. Выбор одного из вариантов действий и представляет собой решение ЛПР. Причем варианты действий направлены как на проведение определенных изменений, так и на сохранение (поддержание) существующего положения, например высокой рыночной доли, производительности труда.

Наиболее сложные решения связаны с проведением различных изменений, прежде всего стратегического характера.

Наилучший вариант действий принято называть *оптимальным*. Решение называется оптимальным, если оно обеспечивает экстремум (максимум или минимум) критерия выбора при индивидуальном ЛПР или удовлетворяет принципу согласования суждений при групповом ЛПР. В условиях неопределенности не всегда возможно нахождение оптимального решения в строго формальном виде. Во многих случаях ЛПР осуществляет оптимизацию в неявном виде, опираясь на некоторые общие принципы и свои предпочтения. В этом плане понятие оптимальности будет трактоваться не так строго, как принято в математике.

Решение называется *допустимым* (рациональным), если оно удовлетворяет определенным ограничениям: ресурсным, правовым, морально-этическим. Это варианты действий, эффективность которых может удовлетворить ЛПР, которое всегда стремится найти оптимальный или хотя бы рациональный вариант.

Обобщенной характеристикой решения является его *эффективность*. Эта характеристика включает эффект решения, определяющий степень достижения целей, отнесенный к затратам на их достижение. Решение тем эффективнее, чем больше степень достижения целей и меньше затраты на их реализацию.

Важной особенностью решения является *целенаправленность* и *сознательность* выбора. Бесцельный выбор, импульсивное действие не рассматривается как решение.

Можно говорить, что при принятии решения используется три элемента человеческой психики: ум, чувство и воля. Ум предполагает использование знаний, логического мышления, научных методов при принятии решений (рациональный подход). На основе этого осуществляется генерация и анализ вариантов решений. Такое решение может быть получено как в результате осознанного поиска с расчетами и экспериментами, так и в результате подсознательного процесса мышления — интуиции. Характерной особенностью интуиции является скрытность логического вывода. Человек не может объяснить, как на основе интуиции логически получено решение.

Чувство характеризует субъективный характер принятия решения, то, что оно преломляется через призму характера и

интересов ЛПР. Это находит свое отражение в предпочтениях ЛПР. Предпочтения ЛПР – это синтетическое сочетание рациональности вариантов решений и мотивов поведения ЛПР, его интересов. Предпочтение ЛПР отражает не только объективную рациональную характеристику решения, но и психологию мышления ЛПР, его понимание полезности решений.

ЛПР также должно использовать свою волю как при выборе решения, так и при его реализации. Необходимость волевого акта ЛПР при выборе решения определяется тем, что ЛПР формирует решение через борьбу интересов и мнений. Очевидно, что чтобы принятое решение было реализовано, ЛПР должно приложить много энергии, преодолеть сопротивление отдельных лиц и организаций, найти союзников.

Любая ЧС всегда ярко эмоционально окрашена, поэтому в ней часто бывает трудно проследить причинно-следственные связи, очертить четко проблему, определить пути ее решения. Инструкции и руководства, однозначно указывающие порядок действий в ЧС, не могут учесть всех особенностей сложившейся ситуации. В таких условиях, когда известное и очевидное, на первый взгляд, решение может быть не всегда оптимальным, умение принимать решение становится особо значимым.

Виды решений

Организационные решения. Подобного рода решения принимаются должностными лицами для того, чтобы выполнить свои функциональные обязанности. Цель организационного решения состоит в том, чтобы обеспечить выполнение задач, стоящих перед организацией.

Организационные решения подразделяются на: *запрограммированные,* когда должностное лицо (руководитель) в сложившейся обстановке располагает ограниченным числом альтернатив и последовательность его действий достаточно ясна, поскольку должна соответствовать заранее определенному алгоритму, тем или иным предписаниям закона; и *незапрограммированные* решения, которые принимаются в нестандартных, неопределенных ситуациях, допускающих большое разнообразие выбора действий (альтернатив). Считается, что чаще всего ситуации складываются таким образом, что принимаемые решения находятся между указанными выше крайними вариантами,

т.е. носят смешанный характер. В зависимости от того, что побуждает должностное лицо (руководителя) отдать предпочтение тому или иному решению, они делятся на следующие виды.

Интуитивные решения принимаются на основе ощущения, интуиции, что они правильны. Принятию подобного рода решений способствует своеобразное озарение, или инсайт (от англ. *insight* – постижение, озарение) – «внезапное, невыводимое из прошлого опыта понимание существенных отношений и структуры ситуации в целом, посредством которого достигается осмысленное решение проблемы».

Решения, основанные на суждениях. В отличие от интуитивных, решения, основанные на суждениях, принимаются на основе знаний, приобретенного жизненного и профессионального опыта человека. Недостаток подобного рода решений состоит в том, что из-за чрезмерной ориентации лица, принимающего решение, на свои знания, прежний опыт, из-за воздействия на его сознание смысловой установки, он может не учесть новые, вновь возникшие обстоятельства и вследствие этого упустить связанные с ними новые альтернативы.

Рациональные решения принимаются на основе объективного анализа имеющейся информации. Принятие подобного рода решений проходит несколько этапов.

Этапы принятия решения

К решению предъявляются ряд общих требований:

– обоснованность, т.е. ПР на базе верной и полной информации;

– своевременность, т.е. учет того, что преждевременные или запоздалые решения могут быть не эффективны, либо привести к развитию негативных тенденций (подача звуковых сигналов бедствия человеком, находящимся под обломками после землетрясения, наиболее целесообразны в «час тишины»);

– необходимая полнота содержания, охватывающая цель, сроки, пути и способы ее достижения, средства, ресурсы, а также порядок взаимодействия между исполнителями;

– согласованность (преемственность) с принятыми ранее решениями.

Не смотря на то, что ПР в ЧС осложняется ограниченностью времени на его разработку, оно включает в себя следующие последовательные этапы:

1) предварительная формулировка проблемы, цели и задач;
2) сбор и анализ информации;
3) уточнение цели и задач;
4) выбор критериев оценки эффективности решения;
5) поиск возможных альтернативных вариантов решений;
6) обработка вариантов решений (анализ, сравнение, обоснование);
7) оценка последствий и возможностей решений;
8) принятие решения.

Далее следует детализация решения до конкретных исполнителей, если работа выполняется группой людей, и реализация принятого решения в определенные сроки с привлечением необходимых (имеющихся) ресурсов.

Рассмотрим подробнее некоторые ключевые моменты процесса ПР.

Цель – представляемый результат деятельности человека или группы людей. Любая ЧС представляет собой комплекс проблем, для решения которого допускается разбить большую цель на более мелкие, соблюдая их иерархичность, т.е. цели нижнего уровня (более близкие, тактические, конкретные) подчиняются целям более высокого уровня (дальние, стратегические, более абстрактные). Правильно поставленная цель содержит в себе сроки ее выполнения, используемые ресурсы и критерии достижения цели. Начало может иметь следующий вид: «мы будем считать, что цель достигнута, если…». Формулировка цели должна быть конкретной, без условностей, позитивной и настраивающей на конструктивные действия.

Одним из факторов, определяющих качество и эффективность ПР является объем и ценность (полезность) информации, причем главной характеристикой информации следует считать ее ценность. Очень часто огромные массивы информации избыточны и не несут никакой пользы для процесса ПР. Увеличение объема информации может лишь усилить убежденность человека в своей правоте, никак не влияя на правильность решения. Окружающая среда, как источник информации, воздействует на

все органы чувств человека и всегда содержит больше информации, чем мы способны сознательно зарегистрировать и понять. С учетом вышесказанного, в условиях с высоким уровнем неопределенности, а именно в ЧС, имеет смысл обращать внимание не только на собственные слух, зрение, осязание, обоняние, вкус, но также и на показания «внутреннего компаса» и интуицию. Неоднократные опыты показывают, что человек способен воспринимать действие магнитного поля Земли. Интуиция включает в себя не только чувства человека по отношению к принятому решению, но и чувства по поводу того, как человек пришел к этому решению. Ощущения часто предопределяют последствия решения, поэтому, принимая решение, следует четко зафиксировать свое состояние вопросом «что я чувствую?».

Информация, используемая для ПР, требует предварительной подготовки: необходимо устранить ту информацию, которая не имеет прямого отношения к проблеме и ПР. Неправильная обработка и интерпретация информации искажает ее точность и достоверность. Учитывая возможные изменения обстановки и недостаточную оснащенность населения современными, в том числе автономными, средствами связи, рассуждения о своевременности получения информации в ЧС не имеет смысла.

Критерии оценки эффективности решения следует разбить на первостепенные (ключевые) и второстепенные. Критерии соотносят достаточный уровень эффективности с целесообразной тратой сил, времени и средств. Заметим, что формулировка «максимум эффективности при минимуме затрат» внутренне противоречива, т.к. минимум затрат равен 0, тогда и эффективность тоже будет равна 0. Тщательно продуманное решение может оказаться неэффективным, если оно не может предвосхитить возможного изменения ситуации. Недооценка будущего, игнорирование событий, имеющих низкий уровень вероятности возникновения, безусловно, упрощают ПР, но повышают степень риска. Для повышения устойчивости принятого решения в изменяющихся условиях необходимо рассматривать проблему в целом, используя системный подход, а не «выдергивать» какую-либо ее черту.

Понять особенности ситуации помогает формулирование альтернативных решений, которые есть всегда. Альтернативные

варианты действий помогают преодолеть явление группового мышления и негативные тенденции ПР, рассмотренные выше. При обработке вариантов решений и оценке их последствий и возможностей следует обратить внимание на внимательное рассмотрение всех спорных вопросов. В любой ситуации, даже самой экстремальной, следует помнить, что исправление плохих последствий займет гораздо больше времени, чем некоторое раздумье перед принятием решения.

Особенности индивидуального и группового принятия решений

В возникающих чрезвычайных ситуациях человек редко оказывается в одиночестве. Люди стремятся объединиться в группы, т.к. при этом осознанно или подсознательно они чувствуют себя в большей безопасности. Из-за высокой психологической напряженности в указанной ситуации человек порой не способен контролировать свои поступки. Еще труднее – управлять поведением другого человека, коллектива, слабо организованной группы. «Братья по несчастью» так или иначе, будут влиять на поведение друг друга. Незнание особенностей мышления и поведения группы людей в чрезвычайных ситуациях может привести к ослаблению противодействия внешним угрозам и снижению ее потенциала выживаемости.

Принятие решения – одновременно умственный, эмоциональный и волевой акт. На оценку и ПР оказывают влияние множество условий: эрудированность, темперамент, характер человека, его готовность к действиям в сложившейся ситуации, мотивация достижения цели, а также человеческие эмоции, ощущения, воображение, представление, способность к абстрактному мышлению и др. Указанные факторы могут не только способствовать, но и мешать объективности ПР. Исследования в области обработки информации и ПР человеком позволили выявить ряд тенденций мышления, оказывающих значительное влияние на ПР (см. таблицу).

В случае угрозы для жизни и здоровья группы людей, в условиях ограниченного времени для принятия решения возникает явление **группового мышления**.

Таблица

Тенденции мышления, оказывающие влияние на принятие решения

ТИП ТЕНДЕНЦИИ	**ОПИСАНИЕ ТЕНДЕНЦИИ**
Поиск подтверждающих данных	Готовность собирать факты в пользу определенных умозаключений и пренебрежение данными, противоречащими им
Непоследовательность	Неспособность применять одни и те же критерии в сходных ситуациях
Консерватизм	Неспособность изменить (или постепенно менять) собственное мнение при появлении новой (-ых) информации/фактов
Новизна	Произошедшие в последний момент события доминируют над более давними
Доступность	Склонность полагаться на отдельные, легко восстанавливаемые в памяти события в ущерб другой относящейся к делу информации
Привязка	Прогнозы подвержены чрезмерному влиянию первоначальной информации, которая оценивается как наиболее весомая
Обманчивые взаимосвязи	Убежденность в очевидности неких схем и/или причинной связи двух переменных, в действительности не связанных между собой
Избирательное восприятие	Склонность воспринимать проблему сквозь призму собственной позиции или опыта
Объяснение успеха и неудач	Успех приписывается умению, а неудача объясняется невезением или чьей-то (не своей) ошибкой, что не позволяет человеку извлекать уроки и осознавать собственные ошибки
Оптимизм, принятие желаемого за действительное	Желательный для человека исход влияет на его прогноз развития событий
Недооценка неизвестности	Излишний оптимизм, потребность снизить беспокойство приводят к недооценке будущей неизвестности

Специалисты, изучающие данное явление, выделяют пять условий, которые способствуют групповому мышлению:

1) привлекательность членства в данной группе.

2) наличие властного, авторитарного лидера, навязывающего свою точку зрения всей группе.

3) закрытость группы, ее самоизоляция.

4) решения группы не подвергаются внешней экспертизе.

5) сильное групповое давление, обусловленное взаимовлиянием членов группы друг на друга.

Групповое мышление характеризуется комплексом признаков, способных в чрезвычайной ситуации развить негативные тенденции и уменьшить эффективность действий группы:

– Упрощение ситуации, презрение к рациональным высказываниям.

– Возникновение иллюзии неуязвимости, которая приводит к чрезмерному оптимизму. Группы склонны к принятию более рискованных решений, нежели индивидуумы.

– Поляризация мнений членов группы. Разнородные взгляды приобретают однозначность. Победившая точка зрения после обсуждения становится более жесткой и однозначной, чем до обсуждения.

– Иллюзия единодушия. Если человек держит при себе свои опасения и сомнения и так поступает большинство членов группы, то создается уверенность, что все придерживаются озвученного ранее мнения и согласны с ним.

– Игнорирование одной информации и стимулирование другой. Больше приводится доводов в пользу совместно принятых решений.

– Возникновение «защитников умов», ограждающих группу от информации, которая не соответствует принятому стереотипу. Они подавляют признаки разногласий (в том числе скрытых) среди членов группы.

– Давление (прямое и косвенное) на членов группы, не подчиняющихся большинству.

Следует отметить, что под влиянием стресса группа становится более конформистской, чем обычно и соглашается на различные предложения лидера, не подвергая их необходимому анализу. Желая достичь согласия внутри группы, стать ее членом,

отдельные личности присоединяются к мнению большинства вопреки собственному мнению.

Кроме указанных свойств, есть еще и другие, возникновение которых зависит от специфики сложившейся ситуации, например, вера в свою моральную непогрешимость и стереотипы в отношении «чужих».

Если для прояснения ситуации у группы есть потребность в информации, но отсутствует возможность ее получения, возникают слухи. Легкая внушаемость некоторых людей, некритичное отношение к поступающей информации, неспособность самостоятельно и трезво оценить правдоподобность и обоснованность слуха превращает людей в неконтролируемую толпу и способствует появлению паники.

Вопросы для самоконтроля

1. Каковы условия для возникновения и распространения слухов?
2. В чём суть «базового закона слухов»?
3. Какие меры следует предпринять для профилактики слухов?
4. Каковы особенности распространения слухов в чрезвычайных ситуациях?
5. На примере покажите процесс принятия решения.
6. В чем отличие индивидуального принятия решений от группового?
7. В чём опасность группового мышления?

ГЛАВА 6. ИНФОРМАЦИОННАЯ ПРЕСТУПНОСТЬ

Стремительное развитие процесса информатизации общества и его распространение практически на все сферы жизни и деятельности людей создает объективные условия для появления нового вида правонарушений – информационной преступности. Информационная преступность имеет те же корни, что и преступность в целом, но обладает рядом особенностей, которые позволяют отнести её проявления к особому типу «преступлений высоких технологий». Большая часть преступлений данного разряда формально может оцениваться как мошенничество, незаконные финансовые операции, обман потребителя и т.д.

Основные **виды** информационных преступлений:

– информационные преступления в интеллектуальной сфере;

– информационные преступления против личности;

– компьютерные преступления.

Перечисленные виды преступлений не исчерпывают всех видов возможных правонарушений в информационной сфере, но позволяют получить общие представления о проблеме информационной преступности и методах борьбы ней.

6.1. Информационные преступления в интеллектуальной сфере

Наиболее распространенными преступлениями данного вида являются нарушения прав граждан или организаций на интеллектуальную собственность. Наглядным примером здесь является распространение на информационном рынке так называемой «пиратской» информационной продукции – компьютерных программ, баз данных, аудио- и видеоклипов популярных композиторов, исполнителей и музыкальных ансамблей и т.п.

Рынки «пиратской» информационной продукции существуют сегодня практически во всех странах. Особенно сильно они развиты там, где процесс информатизации общества ещё находится в начальной стадии и информационное законодательство практически отсутствует.

В последние годы в развитых странах стали приниматься законы, которые квалифицируют распространение «пиратской» продукции как информационное преступление и предусматривают

за совершение таких преступлений не только крупные штрафные санкции, но и тюремное заключение. В России проблема борьбы с такого вида преступлениями ещё находится в самой начальной стадии, хотя ряд законов, охраняющих право интеллектуальной собственности, в нашей стране уже приняты и вступили в силу.

Некоторые специалисты считают, что проблемы защиты от копирования и пиратства на самом деле не существует. Не столь важно защитить от копирования коммерческий продукт. В условиях конкуренции ключевым моментом является распространение продукта на рынке. Многие компании руководствуются принципом: «пираты не причинят нам ущерба, если наша продукция не пользуется спросом. Почти все те, кто крадет наши программы, не в состоянии заплатить за них. Однако когда эти пираты окажутся перед выбором, они будут покупать нашу продукцию, а не продукцию конкурентов». Пиратство оказывается неожиданным средством рекламы. Компания Microsoft имела в виду именно это, когда переводила свои программы на китайский язык и распространяла их в этой стране. Было очевидно, что программы будут взламываться, но потери будут составлять меньше одной десятой со всех продаж. Часто цитировали слова одного из сотрудников Microsoft, Стивена Бальмера: «готовность к тому, что ваши программы будут взламывать, означает, что вы понимаете – это будут ваши программы, а не конкурентов. Важно, чтобы в развивающихся странах на рынке были широко распространены краденые программы». Когда Китай войдет в число свободных стран, он будет ориентироваться на продукцию Microsoft.

6.2. Информационные преступления против личности

Одной из сравнительно новых проблем обеспечения информационной безопасности является проблема защиты информационных прав личности. Такие права охраняются законодательством ряда стран, в том числе и России. В Конституции РФ содержатся следующие положения, гарантирующие право на информацию всех граждан России:

– «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» (ст. 29, п. 4);

– «Гарантируется свобода массовой информации. Цензура запрещается» (ст. 29, п. 5);

– «Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, если иное не предусмотрено законом» (ст. 24, п. 2);

– «Сокрытие должностными лицами фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, влечет за собой ответственность в соответствии с федеральным законом» (ст. 41, п. 3).

Ещё один вид информационных преступлений связан с нарушением прав личности на информационную безопасность. Такие права также закреплены в Конституции Российской Федерации, которая определяет их следующим образом:

– «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени» (ст. 23, п. 1);

– «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» (ст. 23, п. 2);

– «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается» (ст. 24, п. 1).

Приведенные выше конституционные положения направлены на защиту персональной информации о гражданах страны, сбор и незаконное распространение которой может служить основой для вымогательства, шантажа, слежки за их частной жизнью, психологического давления и т.п.

6.3. Компьютерные преступления

Особенности компьютерных преступлений. Уголовно-правовая характеристика компьютерных преступлений.
Криминалистическая характеристика компьютерных преступлений.
Предотвращение и раскрытие компьютерных преступлений.

Основные термины и понятия:
Компьютерное преступление

С развитием компьютерных технологий всё больше компаний переходят на автоматизированные системы учёта. В результате увеличиваются как объём информации, хранящейся на различных электронных носителях, так и её ценность (которая, в первую очередь, определяется суммой возможных убытков при потере данных или их попадании к конкуренту). Однако, электронные средства хранения более уязвимы, чем бумажные: размещаемые на них данные можно и уничтожить, скопировать, незаметно видоизменить. Последнее представляет наибольшую опасность для компаний. По данным Миннесотского университета, 93% компаний, лишившихся доступа к своим данным на срок более 10 дней, покинули бизнес, причем половина из них заявила о своей несостоятельности немедленно.

Компьютерное преступление – *преступление, совершенное с помощью вычислительной техники и вычислительных сетей, направленное на незаконное похищение информации или приводящее к её модификации либо разрушению.*

К числу наиболее уязвимых объектов с точки зрения компьютерных преступлений относятся:

– автоматизированные информационные системы органов государственной власти различного уровня;

– системы управления объектами жизнеобеспечения и критическими технологиями;

– системы управления войсками, вооружениями и военной техникой;

– учетные автоматизированные системы правоохранительных органов;

– кредитно-финансовая система – банки, особенно коммерческие;

– государственные и муниципальные регистрационные системы;

– биржи (суммы сделок, закупочные и предельные цены и т.д.);

– информационные системы подразделений таможни;

– учетные автоматизированные системы налоговых служб.

Особенности компьютерных преступлений

Правонарушения в киберпространстве включают в себя всё, что происходит в физическом мире: воровство, рэкет, вандализм, страсть к подглядыванию и подслушиванию, вымогательство, мошенничество и обман. Хотя нападения в цифровом мире могут иметь те же цели и использовать многие из тех методов, что и нападения в физическом мире, всё же они будут существенно различаться. Они будут проще, шире распространены и более разрушительны. У Интернета есть три новых свойства, которые помогают осуществить преступную атаку.

1) **автоматизация**. Компьютеры имеют неоспоримое преимущество при решении повторяющихся задач. Быстрая автоматика совершает атаки, даже если возможное число успешных попыток мизерно. Атаки, которые были слишком несущественны, чтобы обращать на них внимание в физическом мире, могут быстро стать основной угрозой в цифровом.

2) **действие на расстоянии**. Нападающим в Интернете не нужно находиться где-то рядом местом атаки. Нападающий может сидеть за компьютером в Санкт-Петербурге и атаковать компьютер Ситибанка в Нью-Йорке. Раньше, если человек строил товарный склад в Томске, ему приходилось беспокоиться только о преступниках, которые могли бы приехать в Томск и взломать этот склад. Теперь, благодаря Интернету, все компьютеры стали равноудалены от любого другого компьютера, и человеку надлежит принимать во внимание преступность всего мира. Кроме этого, Интернет затрудняет поиск преступников и их обвинение.

3) **легкость передачи опыта удачных атак по Интернету**. Только первому нападающему приходится быть изобретательным, все остальные могут просто использовать его программы. Однажды выпущенные в свет, они уже не поддаются контролю.

Отличием преступлений в обычном физическом мире от преступлений с помощью компьютерных технологий является масштабность. Интенсивное развитие трубопроводной, транспортной, энергетической и телекоммуникационной сетей Нью-Йорка за последние 20 лет привело к образованию так называемых критических узлов городской инфраструктуры, один из

которых – комплекс зданий Международного торгового центра – стал объектом террористических актов 11 сентября 2001 г.

Обрушение комплекса зданий в результате двух воздушных ударов помимо невосполнимой утраты тысяч человеческих жизней уже в первые часы катастрофы повлекло за собой вывод из строя нескольких подземных станций метро, разрушение путепроводов, отключение энергетической системы, уничтожение информации в компьютерах сотен фирм и офисов, потерю десятка тысяч волоконно-оптических каналов передачи данных, перегрузку трафика Интернета, падение курса акций и закрытие биржи на несколько дней.

Согласно оценкам независимой исследовательской корпорации Computer Economics, сумма ущерба, нанесенного информационной инфраструктуре США в результате террористических актов в Нью-Йорке и Вашингтоне с учетом финансовых потерь и затрат на восстановление, составила величину порядка $15,8 млрд., при этом свыше 25000 специалистов из телекоммуникационных компаний всего мира в течение нескольких недель были заняты восстановлением утраченных и перераспределением сохранившихся информационных и телекоммуникационных ресурсов, и порядка 100000 человек, занятых в сфере банковских и финансовых операций в режиме реального времени, были вынуждены сменить место работы по техническим причинам.

Опасность сложившейся ситуации заключается в том, что многие системы (трубопроводная, транспортная, телекоммуникационная) связаны с энергетической системой, и сбой в ней может привести к авариям и катастрофам в других системах. Такую взаимозависимость можно было наблюдать в Москве при масштабном отключении летом 2005 года электричества из-за аварии. Масштаб последствий громаден и включает в себя социальные, транспортные, медицинские, экологические, экономические последствия.

В приведённом ниже примере авария стала результатом стечения обстоятельств, однако никто не может гарантировать защиту критической инфраструктуры современного города от тщательно спланированных диверсионных (террористических) действий группы лиц, как это было представлено в фильме «Крепкий орешек – 4».

Отключение электричества 25 мая 2005 года парализовало жизнь Москвы и затронула также Московскую, Калужскую, Тульскую и Рязанскую области – в общей сложности 24 города. В Москве одновременно перестают работать несколько веток метрополитена: Калужско-Рижская, Каховская, Замоскворецкая, Серпуховская, Таганско-Краснопресненская, Люблинская. Всего в подземной ловушке оказалось 43 метросостава, в которых находились около 20 тыс. человек. Останавливаются также пригородные электропоезда нескольких направлений. На наземных автомагистралях отключаются светофоры, перестают ходить троллейбусы и трамваи. Оказавшись отключенными от сети, прекращают работу ТЭЦ, водонапорные и газораспределительные станции. Закрываются заводы, офисы, магазины и предприятия общепита. Сети мобильной связи в срочном порядке переходят на резервные источники энергии. У сотовых операторов начинаются перебои – оборудование едва справляется с перегрузкой из-за огромного количества звонков (по последним оценкам, их было втрое больше, чем в новогоднюю ночь). Оказывается обесточенной телефонная станция ММТС № 9, через которую проходит большая часть интернет-трафика − московского, российского и зарубежного. Провайдеры один за другим прекращают работу, и в течение часа Интернет практически перестает функционировать: не отвечают на запросы даже Yandex, Rambler и серверы информагентств. Из-за перебоев с электричеством лишены возможности работать финансовые учреждения: ММВБ временно закрывает торги в 12:30, РТС – семь минут спустя. Сбербанк выпускает предупреждение о том, что операции могут происходить с задержкой. Из-за энергосбоя остановился Московский нефтеперерабатывающий завод. В Москву-реку были сброшены 10 тыс. куб. м сточных вод Курьяновской станции аэрации. После этого экологи строго запретили купаться во всех водоемах столицы.

Уголовно-правовая характеристика компьютерных преступлений

В качестве орудия совершения преступления может выступать машинная информация, компьютер, компьютерная система или компьютерная сеть.

В главе 28 Уголовного кодекса РФ определяются общественно опасные деяния, совершаемые с использованием средств компьютерной техники. К ним относятся следующие статьи:

1. Ст. 272. Неправомерный доступ к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

2. Ст. 273. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами.

3. Ст. 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ.

УК РФ содержит понятие «компьютерная информация», под которой понимается информация на машинном носителе, в ЭВМ, системе ЭВМ или их сети.

Преступления, имеющие своим предметом только лишь аппаратно-технические средства вычислительных машин (хищение, уничтожение), подпадают под другой тип уголовных правонарушений, закрепленных в главе 21 «Преступления против собственности».

Глава 28 УК РФ имеет своей целью охрану именно информационной безопасности и только в силу этого защиту и аппаратно-технических средств, которые являются материальными носителями информационных ресурсов. Последствия неправомерного использования информации могут быть самыми разнообразными: нарушение неприкосновенности интеллектуальной

собственности, разглашение сведений о частной жизни граждан, имущественный ущерб в виде прямых убытков и неполученных доходов, потеря репутации фирмы, различные виды нарушений нормальной деятельности предприятия, отрасли и т.д. Поэтому преступления данного вида помещены в раздел «Преступления против общественной безопасности и общественного порядка».

Криминалистическая характеристика компьютерных преступлений

При ограблении банка потери в среднем составляют около 20 тысяч долларов, а при компьютерном преступлении более полумиллиона долларов. Число компьютерных преступлений растет. По оценке специалистов США, ущерб от компьютерных преступлений увеличивается на 35% в год и составляет около 3,5 миллиардов долларов.

Наиболее типичными целями компьютерных преступлений являются:

– хищение средств из автоматизированных денежных фондов путем подделки счетов и платежных ведомостей, совершения покупок с их фиктивной оплатой, перечисления денег на фиктивные счета и т.п.;

– кража информации из баз данных и компьютерных программ;

– преднамеренное искажение хранящейся в системе или же передаваемой ею информации;

– нарушение нормального функционирования информационно-телекоммуникационных систем, включая их физическое повреждение или уничтожение.

Для подавляющего большинства компьютерных преступлений характерны корыстные мотивы – 52% всех компьютерных преступлений; с разрушением и уничтожением средств компьютерной техники сопряжено 16% преступлений, с подменой исходных данных – 12%, с хищением данных и программ – 10%, с хищением услуг – 10%.

Основная часть угроз исходит от персонала компаний. Опасность от внешних злоумышленников не так велика, как это представляется средствами массовой информации. Неавторизованные пользователи проникали в корпоративные сети только в 24% случаев. Поставщики и покупатели являлись источниками атак лишь в 12% случаев.

В этой связи особый интерес приобретает характеристика личности преступника. С криминалистической точки зрения можно выделить несколько самостоятельных обособленных групп компьютерных преступников.

К первой группе можно отнести лиц, сочетающих определенные черты профессионализма с элементами изобретательности и развлечения. Такие люди, работающие с компьютерной техникой, весьма любознательны, обладают острым умом, а также склонностью к озорству. Они воспринимают меры по обеспечению безопасности компьютерных систем как вызов своему профессионализму и стараются найти технические пути, которые доказали бы их собственное превосходство. При этом они не прочь поднять свой престиж, похвастaвшись перед коллегами умением найти слабости в компьютерной системе защиты, а иногда и продемонстрировать, как эти слабости можно использовать. Постепенно они набирают опыт, приобретают вкус к такого рода деятельности и пытаются совмещать свои занятия с получением некоторой материальной выгоды. Такой путь проходит большинство хакеров.

Вторую группу составляют лица, страдающие особого рода информационными болезнями, развившимися на почве взаимодействия со средствами компьютерной техники. Некоторые люди попадают в такие ситуации, когда не могут адаптироваться к требованиям современной компьютерной технологии. У них развивается болезненная реакция, приводящая к неадекватному поведению. Чаще всего она трансформируется в особый вид компьютерного преступления – компьютерный вандализм. Обычно он принимает форму физического разрушения компьютерных систем, их компонентов или программного обеспечения. Часто этим занимаются из чувства мести уволенные сотрудники, а также люди, страдающие компьютерными неврозами.

К третьей группе, представляющей наибольший интерес, относятся специалисты или профессиональные компьютерные преступники. Эти лица обладают устойчивыми навыками, действуют расчётливо, маскируют свои действия, всячески стараются не оставлять следов. Цели их преимущественно корыстные. Особенно опасно, если лица такой направленности оказываются среди сотрудников организации или среди авторизованных пользователей информационной системы.

Существенную роль в структуре криминалистической характеристики компьютерных преступлений играют также сведения о потерпевшей стороне. Изучение жертв компьютерных преступлений часто дает больше информации для решения вопросов компьютерной безопасности, чем изучение лиц, совершающих компьютерные преступления. По опубликованным данным, относящимся к группе развитых стран, среди жертв собственники системы составляли 79%; клиенты – 13%; третьи лица – 8%.

Как вид компьютерных преступлений можно выделить Интернет-преступления. К ним относятся распространение через сеть Интернет порнографии, реклама запрещённых услуг (например, проституции), распространение сведений об изготовлении наркотиков, оружия и т.д. В данном случае Интернет проявляет свою роль более в качестве универсального средства коммуникации, нежели арены и инструмента собственно противоправной деятельности. Расследование Интернет-преступлений крайне затруднено, часто они остаются нераскрытыми. Однако преступнику бывает весьма нелегко воспользоваться результатами своей деятельности.

Предотвращение и раскрытие компьютерных преступлений

Действия компьютерных преступников, как правило, тщательно готовятся, маскируются и обнаруживаются лишь спустя некоторое достаточно продолжительное время. Шансов быть пойманным у компьютерного преступника гораздо меньше, чем у грабителя банка, и даже при поимке у него меньше шансов попасть в тюрьму. Обнаруживается в среднем 1% компьютерных преступлений.

Существует много косвенных признаков того, что в организации, учреждении готовится или осуществляется компьютерное преступление. Выявление этих признаков не требует специальных знаний и, учитывая это обстоятельство, можно предусмотреть дополнительные меры по совершенствованию компьютерной безопасности и предотвращению преступлений.

Наиболее общие признаки таковы:

– сотрудники дают подозрительные объяснения по поводу распределения денежных и материальных средств;

– производится перезапись данных без серьезных на то причин;

– данные заменяются, изменяются или стираются;

– данные не обновляются;

– на ключевых документах появляются подделанные подписи;

– появляются фальшивые записи;

– персонал системы без видимых на то оснований начинает работать сверхурочно;

– персонал возражает против осуществления контроля за записью данных;

– у сотрудников, непосредственно работающих с компьютерами, появляется ненормальная реакция на рутинные вопросы;

– некоторые сотрудники отказываются уходить в отпуск;

– отдельные работники начинают слоняться без дела в других подразделениях;

– жалобы клиентов становятся хроническими.

Организации-жертвы компьютерных преступлений с неохотой сообщают об этом в правоохранительные органы. Латентность компьютерных преступлений чрезвычайно высока. Часто виновные лица просто увольняются или переводятся в другие структурные подразделения. Иногда с виновного взыскивается ущерб в гражданском порядке.

Борьбой с преступлениями в сфере высоких технологий занимаются сотрудники специального подразделения. Основной задачей такого подразделения является выявление, пресечение и раскрытие преступлений, совершенных с использованием телекоммуникационных, сетевых и компьютерных технологий, противодействие различного рода незаконным действиям с банковскими расчётными картами, борьба с распространением в Интернет порнографии и т.д. Сотрудники подразделения используют в своей деятельности современное программное обеспечение и технику. Значительное место в работе подразделения занимает квалифицированная помощь другим подразделениям и службам милиции в раскрытии высокотехнологичных преступлений.

Вопросы для самоконтроля

1. Приведите примеры преступлений в сфере информационных технологий.

2. Перечислите основные виды информационных преступлений.

3. Какие существуют информационные права у личности?

4. Что называют «компьютерным преступлением»?

5. Перечислите наиболее уязвимые объекты с точки зрения компьютерных преступлений.

6. В чём заключаются отличия компьютерных преступлений от преступлений, совершаемых в физическом мире?

7. Каковы цели компьютерных преступлений?

8. Каковы признаки того, что в организации, учреждении готовится или осуществляется компьютерное преступление?

ГЛАВА 7. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Для защиты информации при помощи устройств применяются три основных класса контроля доступа. К ним относятся:

1) контроль, основанный на обладании (ключи);

2) контроль, основанный на личных характеристиках (биометрические приборы);

3) контроль, основанный на знании (пароли).

В случае контроля, основанного на обладании, речь идет о предметах, принадлежащих пользователю, – физическом ключе, магнитной карте и т.д.

Биометрические приборы анализируют специфические физические особенности пользователя (подпись, отпечатки пальцев или рисунок линий на ладони) и сравнивают их с теми, что наличествуют у них в памяти.

Последний вид контроля над доступом, наиболее распространенный, основан на обладании специфической информацией. Это означает, что правом доступа обладают лишь те лица, которые способны продемонстрировать свое знание определенного секрета, обычно пароля.

Меры контроля доступа должны обеспечить две вещи. Во-первых, человек должен попасть в систему, а во-вторых, система должна оставить других снаружи. Независимо от того, какая система защиты используется, чаще всего первым шагом работы является идентификация и аутентификация пользователя: кто вы такой и можете ли доказать, что вы это вы?

Идентификация – *отождествление, установление соответствия одной сущности другой.*

Аутентификация – *совокупность процедур, цель которых – доказательство того, что идентифицированная сущность является именно той, за которую она себя выдает.*

Пользователь идентифицируется именем (идентификатором), а потом аутентифицируется паролем (или другим признаком

аутентификации). Как только информационная система (компьютер) узнает вас, он сможет выяснить, что вам разрешено и чего не позволено делать.

7.1. Технологии идентификации человека

Технологии идентификации человека в истории. Идентификация по фотографии. Идентификация по отпечаткам пальцев. Идентификация по ДНК. Компьютерная биометрия. Уязвимость биометрических систем.

Технологии идентификации человека в истории

В 1563 году книге «Сочинения об Азии» исследователь Хоайо де Баррос описывал как китайские торговцы «паспортизировали» детей, делая отпечатки их ладоней и ступней при помощи бумаги и чернил. При раскопках в Израиле археологи обнаружили наборы глиняной посуды, на каждом предмете отчетливо видны отпечатки больших пальцев, которые гончар использовал как персональное клеймо.

В литературе можно найти много примеров ошибочной идентификации: «Принц и нищий» Марка Твена, пьесы Шекспира. Эти истории дошли до наших дней, потому что такого рода ошибки были редкостью. В Европе фамилии не использовались вплоть до Средневековья и вплоть до промышленной революции в мире не было нужды в системе точной идентификации.

Развитие крупных городов и наплыв иммигрантов во второй половине XIX века для правительств многих стран превратилось в серьезную проблему. В Европе и США принимались жесткие иммиграционные законы, призванные сократить приток иностранцев, что потребовало создания системы точной идентификации, которая позволяла бы властям отличать граждан от неграждан. Система идентификации нужна была и для отделения рецидивистов от совершивших преступление впервые. Кроме этого, требовалась новая концепция реабилитации преступников, предоставлявшая возможность людям, совершившим ранее преступления, реабилитироваться и встать на путь исправления.

Проблема идентификации осужденных привлекла внимание парижского антрополога А. Бертильона (1853–1914 гг.). Он заметил, что, даже если человек назовется другим именем, сменит прическу, наберет вес, некоторые части его тела останутся

неизменными. Он создал систему антропологического опознавания, базирующуюся на этих неизменных признаках. Производились точные измерения головы, рук, ступней и ушей подозреваемого, фиксировалось наличие шрамов, родимых пятен, другие отличительные телесные признаки. Эта информация вместе с именем подозреваемого заносилась в специальные карты, которые затем хранились в центральном полицейском участке.

Система Бертильона стала вехой в развитии криминалистики. Человек мог быть арестован и описан в 1881 году одним полицейским и опознан три года спустя другим полицейским в результате обнаружения совпадения признаков после просмотра картотеки. Бертильон создал систему, позволяющую идентифицировать человека по записям, в то время как ранее это мог сделать только человек с хорошей зрительной памятью.

В течение десяти лет после официального принятия указанной системы в декабре 1882 года парижская полиция выявила 4564 человека, назвавших полиции вымышленное имя. Система Бертильона дала возможность французским судьям выносить более жесткие приговоры рецидивистам. Буквально через несколько лет уровень преступности в Париже снизился. Бертильон объяснял это тем, что карманники сочли за лучшее мигрировать в места, где шанс их идентификации был ниже.

Идентификация по фотографии

Сегодня наиболее распространенной формой идентификации является помещение фотографии на официальный документ. Повсюду в мире универсальным способом идентификации личности является паспорт. Во многих европейских странах паспорт дополняется идентификационной карточкой.

Надёжность идентификационных удостоверений (например, водительских) зависит от двух факторов. Во-первых, нужно быть уверенным, что удостоверение выдано соответствующему лицу. Во-вторых, само по себе удостоверение должно быть хорошо защищено от подделки. Удостоверения, которые легко подделать, провоцируют преступления, т.к. удостоверение может быть украдено, изменено и затем использовано в преступных целях. В настоящее время при изготовлении удостоверений используются специальные материалы и технологии, что затрудняет их подделку.

Идентификация по отпечаткам пальцев

Определяемые комбинацией генов и случайными процессами во время развития плода, отпечатки пальцев на протяжении всей жизни остаются такими же, как при рождении. Отпечатки пальцев неуничтожимы. Причина их стойкости кроется в том, что рисунок линий формируется глубинными слоями эпидермиса, и единственный способ изменить чьи-либо отпечатки заключается в полном удалении кожи с подушечек и заменой её кожей с других участков тела.

Но важность отпечатков пальцев для раскрытия преступлений не только в том, что они уникальны, но и в том, что они остаются на месте преступления. В отличие от системы Бертильона, нет необходимости фиксировать отпечатки пальцев всего населения, достаточно лишь сравнить обнаруженные отпечатки с отпечатками подозреваемого.

Правоохранительные органы настаивают на создании реестра отпечатков пальцев, но они постоянно сталкиваются с неприятием этой идеи обществом по целому ряду причин:

– чьи-либо отпечатки пальцев могут оказаться на месте преступления по вполне законной причине. Присутствие идентифицируемых отпечатков создает презумпцию виновности;

– отпечатки могут быть случайно или преднамеренно перепутаны в лаборатории;

– хранимые файлы с отпечатками могут быть преднамеренно изменены с целью обвинения невиновного;

– экспертные заключения по анализу отпечатков могут быть перепутаны или специально изменены.

Дактилоскопирование не может гарантировать идентификацию, оно лишь обеспечивает связь конкретного пальца с записью в файле. Изменив файл, изменится идентификация.

Дактилоскопия как средство строгой идентификации может быть использована репрессивными и тоталитарными режимами. Пропускная система во времена апартеида в Южной Африке и идентификационные карточки, выдаваемые палестинцам на оккупированных Израилем территориях, являются примерами таких систем идентификации.

Идентификация по ДНК

Идентификация по дезоксирибонуклеиновой кислоте (ДНК) основана на анализе цепочек генов и является почти безупречной. Сегодня у неё три основных применения:

– установление отцовства;

– определение принадлежности крови и семенной жидкости, оставленных на месте преступления;

– идентификация человеческих останков.

Всё чаще анализ ДНК применяется для идентификации человеческих останков. Поскольку молекула ДНК чрезвычайно стабильна, необходимый для анализа материал может быть получен из останков через годы или даже через тысячи лет после смерти человека.

Несмотря на всю мощь технологий идентификации ДНК, им присущи некоторые фундаментальные проблемы:

1) ДНК не во всех случаях является уникальной: однояйцовые близнецы по определению имеют один и тот же набор хромосом. Приблизительно 0,338% населения являются однояйцовыми близнецами, т.е. три человека из тысячи.

2) При экспертизе анализируются только «мусорные участки» ДНК (ДНК двух отдельно взятых людей совпадают почти на 99%). Поскольку эти фрагменты генома не участвуют в жизнеобеспечении клеток или организма в целом, из поколения в поколение происходят их случайные изменения, или мутации. Специалисты не могут полностью исключить возможность случайного совпадения и неверной идентификации.

3) Для проведения теста требуется лабораторное оборудование и квалифицированные специалисты.

Так же не следует исключать возможность того, что образцы крови или семенной жидкости с места преступления могут быть подменены при транспортировке, как случайно, так и умышленно.

Компьютерная биометрия

Все современные системы биометрической идентификации состоят из двух частей. Первая – это устройство, которое производит измерение какого-либо параметра человеческого тела и преобразует его в цифровую форму. Вторая – большая база данных, хранящая результаты биометрических измерений

сотен, тысяч или даже миллионов людей. За последние годы было разработано множество систем биометрической идентификации.

Рисунок сетчатки глаза. Сетчатка похожа по своей индивидуальности на отпечатки пальцев. В этом случае анализируется уникальный рисунок внутри глаза человека. В 1980-е годы были популярны системы, анализирующие картину, образуемую венами и артериями глаза. Однако, в отличие от отпечатков пальцев, рисунок сетчатки подвержен изменениям: у женщин во время беременности под воздействием гормонов плода в глазу могут образовываться новые сосуды, меняющие рисунок. Эта система дискриминирует женщин, которым приходится объясняться при каждом несовпадении изображений сетчатки.

Сканирование радужной оболочки. Сканирование радужной оболочки является наиболее точным и стабильным. Узор на радужке формируется до рождения и остается неизменным на протяжении всей жизни (кроме случаев травм и хирургического вмешательства). Даже однояйцовые близнецы имеют различающиеся радужные оболочки. Вероятность совпадения биометрических показателей радужки двух людей составляет один шанс из 10^{78}.

> *В настоящее время разработаны высокоскоростные сканеры радужной оболочки, которые могут получать изображение радужки человека, сидящего в машине, движущейся со скоростью 90 км/час.*

Однако сканирование радужки идентифицирует не человека, а лишь его радужную оболочку. Узнать по результатам сканирования имя человека можно только после поиска в компьютерной базе данных. Если база данных была взломана и модифицирована, сканирование радужной оболочки не даст правильной идентификации.

Анализ почерка. Анализ почерка и собственноручной подписи является одной из первых биометрических систем в мире. Сегодня изображение подписи может быть оцифровано и сравнено с имеющимися образцами. Если подпись ставится на специальном электронном планшете, компьютер может также

анализировать скорость перемещения пера и силу нажатия. Комбинируя эти три параметра (траекторию, скорость и силу нажатия) можно построить биометрическую модель, которую очень сложно подделать.

Отпечатки ладоней и их геометрия. При идентификации по отпечатку ладони и её геометрии анализируется рисунок складок и относительная длина пальцев. Данный способ страдает нестабильностью по сравнению с анализом отпечатков пальцев, т.к. измеряемые параметры меняются со временем.

Характеристики голоса. Системы голосового анализа пытаются идентифицировать говорящего путем сравнения произносимых им фраз с заранее записанными.

Распознавание лица. Системы распознавания лица идентифицируют человека на основе визуального сходства. В отличие от других систем биометрической идентификации, распознавание лица носит пассивный характер: оно может осуществляться без ведома человека, позволяя производить идентификацию в лифте или при проходе через дверь.

Термограмма лица. Идентификация по термограмме лица использует особенности расположения проходящих непосредственно под кожей кровеносных сосудов. Считается, что термограмма лица более надёжный способ идентификации, чем простое визуальное распознавание.

Несмотря на имеющиеся достижения в использовании компьютерной биометрии, ни одна из описанных выше систем идентификации не прошла какого-либо научного обследования, как это было с идентификацией по ДНК в конце 1980-х – начале 1990-х годов.

Уязвимость биометрических систем

Отпечатки пальцев, сканирование радужной оболочки глаза и анализ генных последовательностей часто рассматриваются как абсолютно безупречные способы идентификации человека. Считается, что они настолько хороши, что в ближайшей перспективе можно вполне отказаться от разного рода идентификационных карточек и паспортов. Вместо этого будет существовать единая база данных, с помощью которой гражданин может быть идентифицирован на основе уникальных признаков

его собственного тела. Но остаются невыясненными ряд важных вопросов:

– Кто будет контролировать доступ к банку данных?
– Кто будет иметь право вносить в него изменения?
– Что делать, если вдруг компьютерная система даст сбой?

7.2. Применение паролей в механизме аутентификации человека

Классификация паролей. Правила создания паролей.

Пароли, как правило, рассматриваются в качестве ключей для входа в систему, но они используются во всех тех случаях, когда требуется твердая уверенность в том, что соответствующие действия будут производиться только законными владельцами или пользователями программного обеспечения.

Классификация паролей

Пароли подразделяются на несколько основных групп:
– пароли, генерируемые системой;
– полуслова;
– ключевые фразы;
– интерактивные последовательности типа «вопрос – ответ»;
– пароли, устанавливаемые пользователем.

Случайные пароли и коды, **устанавливаемые системой**, могут быть нескольких разновидностей. Системное программное обеспечение может применить полностью случайную последовательность символов – случайную вплоть до регистров, цифр, пунктуации, длины.

Полуслова частично создаются пользователем, а частично – каким-либо случайным процессом. Это значит, что если даже пользователь придумает легко угадываемый пароль, например, «секрет», компьютер дополнит его, образовав более сложный пароль типа «секрет,2rs87».

Ключевые фразы трудно угадать и легко запомнить. Фразы могут быть осмысленными или не иметь смысла. В программировании постепенно намечается тенденция к переходу на более широкое применение ключевых фраз.

Интерактивные последовательности **«вопрос – ответ»**, предлагают пользователю ответить на несколько вопросов, как правило, личного плана. В компьютере хранятся ответы на множество таких вопросов. При входе пользователя в систему компьютер сравнивает полученные ответы с «правильными».

Пароли, устанавливаемые **пользователем**. Большинство паролей относятся к типу «выбери сам». Обычно пароль содержит не менее четырех-пяти букв. Существуют также и другие меры, призванные не позволить пользователю создать неудачный пароль. Например, система может настаивать на том, чтобы пароль включал в себя строчные и заглавные буквы вперемешку с цифрами; заведомо очевидные пароли, например, «компьютер», ею отвергаются.

Правила создания паролей

При установке пароля существует ряд правил, которых следует придерживаться.

Пароли **не должны** состоять из:

– только цифр или одинаковых букв;

– Вашего имени, отчества или фамилии ни в каком виде (т.е. написаны в строчном, в прописном, в смешанном виде, задом наперед, два раза и т.д.);

– имен Вашей (его) супруги (а) или детей;

– личной информации. Сюда входят: номера телефонов, номера в пропусках и других документах, номер или марка вашего автомобиля, Ваш почтовый адрес и т.д. и т.п.;

– слов, которые можно найти в словаре (любом, включая иностранные) или в каком-либо списке слов.

Запрещается использовать в качестве пароля название учётной записи (идентификатора входа (*login*)) ни в каком виде, а так же легко угадываемые сочетания символов.

Для проверки сложности паролей используют специальные контроллеры паролей. Контроллеры осуществляют попытки взлома пароля по разным методикам, например:

1. Проверка использования в качестве пароля входного имени пользователя, его инициалов и их комбинаций.

2. Проверка использования в качестве пароля слов из различных словарей:

– мужские и женские имена;

– названия стран и городов;

– имена персонажей мультфильмов, кинофильмов, научно-фантастических произведений и т.п.;

– спортивные термины (названия спортивных команд, имена спортсменов, спортивный жаргон и т.п.);

– числа (цифрами и прописью);

– строки букв и цифр (например, AA, AAA, AAAA и т.д.);

– библейские имена и названия;

– биологические термины;

– жаргонные слова и ругательства;

– последовательности символов в порядке их расположения на клавиатуре (например, QWERTY, ASDF, ZXCVBN и т.д.);

– часто употребляемые иностранные слова.

3. Проверка различных перестановок слов из п.2, включая:

– замену первой буквы на прописную;

– замену всех букв на прописные;

– замена одной строчной буквы на прописную;

– замена двух строчных букв на прописные (около 1500000 слов);

– замена трех строчных букв на прописные и т.д.;

– замену буквы O на цифру 0 и наоборот (цифру 1 на букву I и т.д.);

– превращение слов во множественное число.

Приведенные выше примеры позволяют сформулировать ряд способов снижения уязвимости паролей. Пароль **должен** отвечать следующим требованиям:

а) быть определенной длины;

б) включать в себя как прописные, так и строчные буквы;

в) включать в себя одну и более цифр;

г) включать в себя, как минимум, один нецифровой и неалфавитный символ.

В частности пароли **должны**:

– быть составлены так, чтобы Вы могли быстро набрать их на клавиатуре. Это осложнит возможность подглядеть пароль;

– быть легко запоминаемы, чтобы не было необходимости записывать их;

– длина пароля, должна составлять не менее 8 символов;

– содержать небуквенные символы (т.е. цифры, знаки пунктуации, специальные символы);

– при выборе пароля, рекомендуется использовать комбинацию из строчных и прописных букв, цифр, знаков препинания и специальных символов;

– каждый пароль должен содержать как минимум две буквы (большие или малые) и хотя бы одну цифру или знак;

– новый пароль должен отличаться от старого хотя бы тремя символами. При сравнении не делается различий между большими и малыми буквами;

– каждый пароль должен отличаться от входного имени, прочитанного слева направо или задом наперед, и от его циклических сдвигов. При сравнении не делается различий между большими и малыми буквами;

– пользователь обязан не реже одного раза в месяц производить смену основного пароля.

Важнейшими характеристиками пароля являются его длина и период смены (или период жизни). Чем больше длина пароля, тем больше усилий придется приложить нарушителю для его определения. Чем больше период жизни пароля, тем более вероятно его раскрытие.

7.3. Информационная безопасность компании

Человеческий фактор в обеспечении информационной безопасности компании. Система информационной безопасности компании. Безопасное использование Интернет-ресурсов в компании.

Количество компьютерных преступлений в России ежегодно растет. Это связано с повышением ценности конфиденциальной информации: она приобрела реальную стоимость, которая определяется величиной прибыли от ее использования или размером вероятного ущерба владельцу. В результате мотивы к совершению преступлений в сфере высоких технологий множатся. Как и возможности: корпоративные компьютерные сети расширяются, конфигурация их меняется, объектов вторжений в информационные системы становится все больше, а инструмен-

ты атак постоянно обновляются. Это лишь краткий список причин, вызывающих рост информационной преступности.

Человеческий фактор в обеспечении информационной безопасности компании

Недооценивая важность защиты информации, компании делают основной упор на физическую безопасность (пропускной режим, охрану, систему видеонаблюдения и так далее). Но если десять лет назад это было оправдано, то сейчас ситуация существенно изменилась. Сейчас самая конфиденциальная информация лежит не в сейфе у директора, а на жестком диске компьютера. Чтобы заполучить необходимую информацию и нанести компании финансовый ущерб, достаточно проникнуть в ее информационную систему или вывести из строя какой-либо узел корпоративной сети. Подобные вторжения вызывают как прямой ущерб (зачастую измеряемый шести-семизначными суммами), так и косвенный: неисправность узла приводит к затратам на его восстановление (обновление или замену программного обеспечения, зарплату обслуживающего персонала). Атака на web-сервер компании и замена его содержимого на любое другое может привести к снижению доверия к фирме и, как следствие, потере части клиентуры и доходов.

В зависимости от вида деятельности и целей компании можно выделить наиболее важные направления обеспечения информационной безопасности. Для одних приоритетом является предотвращение утечки информации (маркетинговых планов, перспективных разработок и так далее). Другие могут пренебречь конфиденциальностью внутренней информации и сосредоточить внимание на ее целостности. Например, для банка важно в первую очередь обеспечить подлинность обрабатываемых платежных поручений. Для интернет-провайдера, компании, обладающей web-сервером, или оператора связи на первое место выходит задача обеспечения доступности и безотказной работы всех (или наиболее важных) информационных систем.

Наиболее распространенный миф из области защиты информации, бытующий в бизнес-среде: основная опасность исходит от внешних злоумышленников, проникающих в компьютерные системы. Бесспорно, ее нельзя недооценивать, но она слишком преувеличена. Обратимся к статистике. До 80% всех ком-

пьютерных преступлений связано с вольными или невольными внутренними нарушениями со стороны работающих или уволенных сотрудников. Почему они совершают преступления против собственной компании? Причин множество. Самая распространенная – неудовлетворенность статусом или зарплатой. Другой нередкий случай: сотрудник при увольнении затаил обиду и хочет отомстить компании, ее руководству. Больших бед можно ждать, если злоумышленник облечен внушительными полномочиями и имеет доступ к широкому спектру информации. Громадный ущерб, например, способен нанести сотрудник отдела автоматизации, информатизации и телекоммуникаций, обладающий достаточными квалификацией и опытом: ему могут быть известны пароли ко всем используемым системам. Таких «лазутчиков» трудно обнаружить: они способны обходить защитные механизмы.

Исходя из вышесказанного, прежде всего, следует убедиться в лояльности персонала компании.

Принимая сотрудника на работу, необходимо всеми доступными средствами навести о нем справки. Рекомендуется:

– применять специальные психологические тесты, которые помогут оценить его лояльность и психологические качества;

– продумать систему материального и морального поощрения за сохранение лояльности;

– оговорить в контракте с сотрудником условия сохранения конфиденциальности не только на период совместной работы, но и на определенный срок после завершения ваших взаимоотношений. Только в этом случае можно предъявлять какие-либо претензии.

Однако больше всего убытков компании причиняет неграмотность и халатность персонала:

В своё время неграмотное использование электронной почты привело к распространению по всему миру таких компьютерных вирусов, как Love San и I love you, убытки от которых составляют десятки, а то и сотни миллионов долларов. Половина паролей, придуманных рядовыми сотрудниками, состоят из цифр дат рождения и имени дочери или сына. Такие пароли легко вскрыть. Но даже если системный администратор назначает пароль из трудно запоминаемой комбинации букв и цифр, работники, не долго думая, на виду у всех приклеивают его на мо-

нитор или ставят галочку «запомнить пароль», чтобы не набирать каждый раз заново. В результате доступ к компьютеру и корпоративной сети открыт любому желающему.

Большинство специалистов связывают беспечность менеджмента и персонала, во-первых, с небольшим числом получивших огласку хищений информации «в особо крупных размерах»; во-вторых, с низким уровнем внутрикорпоративной дисциплины и обучения персонала правилам информационной безопасности. Между тем ряд отечественных компаний, например крупные холдинги, накопили большой опыт создания систем информационной безопасности.

Система информационной безопасности компании

Следует придерживаться комплексного подхода к решению проблемы защиты информации. Для того чтобы риск коммерческой деятельности был минимальным, надо оценить всевозможные угрозы безопасности информации с учетом двух факторов: предполагаемой вероятности возникновения угрозы и возможного ущерба от ее осуществления.

На первом этапе проводится информационное обследование. Определяется, от чего в первую очередь необходимо защищаться компании. Объективность оценки угроз достигается детальным анализом функционирования компании и привлечением независимых экспертов. Строится «модель нарушителя», которая описывает его квалификацию, средства для реализации атак, обычное время их проведения и прочее. В результате вырабатываются рекомендации для устранения выявленных угроз, правильного выбора и применения средств защиты.

Второй этап – приобретение, установка и настройка рекомендованных средств и механизмов, в совокупности обеспечивающих защиту системы обработки данных от посторонних лиц, системы обработки данных от пользователей, пользователей друг от друга, каждого пользователя от себя самого, системы обработки от самой себя.

Что нужно делать для того, чтобы защитить информационную корпоративную сеть?

– Убедиться в том, что ни один человек не имеет доступа сразу ко всем функциям системы сверху донизу.

– Потребовать от каждого пользователя ввода пароля при вхождении в систему.

– Предоставлять права суперпользователя как можно меньшему числу людей.

– Резервную копию наиболее важных компонентов системы необходимо делать ежедневно.

– Раз в неделю делать резервную копию всей системы.

– Установить строгий контроль за доступом к лентам с резервными копиями.

– Текущую резервную копию хранить отдельно, в надежном удаленном месте.

– Регулярно копировать информацию, хранящуюся на настольных и портативных компьютерах, а также на серверах.

– Менять пароли, по крайней мере, каждые три месяца.

– Разместить серверы в безопасном, недоступном для посторонних месте.

– Человек, обеспечивающий текущее функционирование системы, не должен отвечать за создание резервных копий.

– Регулярно обновлять программное обеспечение.

– Установить программное обеспечение, позволяющее обнаружить попытку несанкционированного доступа и своевременно получить соответствующее предупреждение.

– Выделять на нужды безопасности не менее 3–5% бюджета информационной службы.

– Персонал группы информационной безопасности должен выявлять случаи проявления сотрудниками неуверенности или недовольства (особенно это касается тех служащих, которые имеют доступ к важным сведениям).

– Уделять повышенное внимание вопросам безопасности в периоды массовых увольнений или слияния с другими фирмами. Сотрудники, раздраженные таким поворотом событий, могут предпринять действия, которые негативным образом отразятся на работе компании.

– Наладить мониторинг сети. Специальные программные средства выдадут предупреждение в том случае, если пользователь проник в запрещенную для него область сети или работает в неположенное время.

– Установить контроль за электронной перепиской с целью выявления подозрительных внешних контактов.

– Проверять правильность и надежность создаваемых резервных копий. Возложите задачу резервного копирования еще на кого-нибудь, если сотрудник, постоянно занимающийся этими вопросами, попал под подозрение.

– При подписании контракта с сотрудником оговорить все условия работы и меры наказания, принимаемые в случае различных нарушений и невыполнения предъявляемых требований.

– Люди, занимающие ключевые посты в информационной службе, должны быть заинтересованы в укреплении позиций компании.

С течением времени средства защиты устаревают, выходят новые версии систем обеспечения информационной безопасности, постоянно расширяется список обнаруженных атак и «брешей», меняются технология обработки информации, программные и аппаратные средства, персонал компании. Создание системы информационной безопасности – бесконечный эволюционный процесс, требующий немалых затрат.

Важнейший элемент системы – корпоративная **политика информационной безопасности**. Основные принципы политики безопасности таковы:

– никто не имеет права подходить к компьютеру сотрудника кроме самого сотрудника и системного администратора;

– компьютер никогда не остается без присмотра включенным;

– никто не может увидеть ни одного файла с компьютера сотрудника по сети;

– применяются только те службы и протоколы, которые необходимы в данный момент.

По мнению специалистов, даже выполнение элементарных требований безопасности (четкое разграничение прав доступа пользователей к системе, соблюдение правил «интернет-гигиены», использование лицензионного программного обеспечения и услуг квалифицированного системного администратора) позволяет компании вдвое снизить риск компьютерного преступления.

Абсолютно безопасный компьютер – это компьютер выключенный. Поэтому идеально безопасной системы не существует. Как только в ней появляется хоть один человек, она не-

безопасна. Люди были и есть самое слабое звено информационной безопасности. Когда речь идет об информационной безопасности, важно понимать: суть проблемы не в аудите, не в программах и даже не в конкретных людях, а в эффективно работающих процедурах, направленных на предотвращение несанкционированного доступа, поддержание системы в закрытом состоянии, в механизмах быстрого реагирования в случае нарушения целостности данных. Риск, порождаемый человеческим фактором, можно значительно снизить политикой, инструкциями, положениями и регламентами, а также с помощью средств пропускного режима, техническими средствами.

Безопасное использование Интернет-ресурсов в компании

Интернет стал рабочим инструментом, без которого уже невозможно представить себе повседневную деятельность множества людей. Это и глобальная справочно-информационная система, и способ доступа к технологиям, и транспорт для передачи данных, и, наконец, оперативное и доступное средство коммуникации.

Одной из особенностей Интернета является то, что на определенном этапе он развивался стихийно. Это, с одной стороны, обеспечило массовый характер его использования, а с другой – породило ряд проблем с серьезными последствиями:

– поскольку Интернет является каналом во внешний мир, он стал основным источником распространения вредоносного мобильного кода (вирусов, червей, троянских программ);

– глобальная сеть стала использоваться в качестве канала, через который осуществляются атаки на локальные вычислительные сети организаций, отдельные серверы и компьютеры;

– Интернет стал активно применяться в качестве средства скрытого проникновения в корпоративные локальные вычислительные сети;

– в настоящее время Интернет может рассматриваться как один из основных каналов утечки конфиденциальной информации. Имея доступ к Интернету со своего рабочего места и зная, что канал не контролируется, любой пользователь может беспрепятственно отправить за пределы организации любую конфиденциальную информацию;

– бесконтрольный доступ к Интернету значительно снижает производительность труда в коллективе. Простота освоения, легкость поиска необходимой информации и другие полезные качества Интернета – вот причины того, что данный сервис широко применяется, в том числе и для личных целей. По данным компании IDC, около трети своего рабочего времени сотрудники различных организаций и компаний проводят в Интернете в целях, не имеющих прямого отношения к их работе;

– снижение пропускной способности сети. Согласно статистике, 44% сотрудников организаций используют корпоративные ресурсы для просмотра видео, прослушивания аудиозаписей (через потоковые аудио- и видеоканалы), играют в сетевые игры, загружают файлы большого объема (например, файлы мультимедиа: графические, музыкальные файлы, фильмы и т.п.), что создает значительную нагрузку на локальные вычислительные сети.

Проблему безопасного и продуктивного использования Интернет-ресурсов можно решить двумя способами. Первый – радикальное запрещение использования Интернета без необходимости. Если принят принцип «запрещено все, что явно не разрешено», пользователям разрешается доступ только к строго определенным сайтам. Второй способ – более гибкий, он позволяет пользователям действовать по принципу «разрешено все, что не запрещено». В этом случае сотрудник может свободно пользоваться ресурсами Интернета, однако его действия находятся под контролем. Это значит, что если пользователь выполнит действия, противоречащие политике безопасности, это будет обнаружено и пресечено.

В настоящее время «радикальный» способ по-прежнему находит применение. Он используется, в первую очередь, организациями, в которых циркулирует информация с грифом «секретно». К таким организациям относятся различные научно-исследовательские институты, военные организации, государственные органы и специальные службы. В таких «секретных» организациях существуют инструкции и документы, которые строго регламентируют поведение пользователей, связанное с получением информации и её передачей за пределы организации. А это значительно облегчает деятельность контролирующих служб по обеспечению должного уровня защиты.

Другой пример «радикального» способа – применение в компаниях так называемых Интернет-киосков, когда пользователям предоставляется доступ к Интернет-ресурсам через выделенные терминалы. Как правило, в этом случае действия пользователей строго регламентируются, а трафик, проходящий через данный терминал, контролируется специальными средствами.

Большинство же коммерческих организаций и компаний предпочитают более гибкий способ регламентации общения с внешним миром. Чтобы обеспечить гибкий контроль использования Интернет-ресурсов, необходимо ввести в компании соответствующую политику использования ресурсов. Эта политика может реализовываться как «вручную», так и автоматически (при помощи специальных программ). «Ручная» реализация означает, что в организации имеется специальный штат сотрудников, которые ведут мониторинг активности пользователей.

Вопросы для самоконтроля

1. Перечислите основные классы контроля доступа.
2. Перечислите методы биометрической идентификации человека.
3. Насколько методы биометрической идентификации человека могут быть точны?
4. В чём уязвимость биометрической идентификации человека?
5. Перечислите правила создания паролей.
6. Почему в обеспечении защиты информации человек является «самым слабым звеном»?
7. Что представляет собой политика информационной безопасности организации?
8. Каковы способы безопасного использования Интернет-ресурсов?

ГЛАВА 8. ИНФОРМАЦИОННЫЕ И ПСИХОЛОГИЧЕСКИЕ ВОЙНЫ

Информационное пространство с конца XX века фактически стало театром военных действий, где каждая противоборствующая сторона стремится получить преимущество, а в случае необходимости разгромить противника. Общедоступность и высокая оперативность обновления информации о боевой обстановке, в сочетании с её наглядностью и высокой достоверностью «единой цифровой картины поля боя», превращают информацию не только в мощное оружие, но и уязвимую цель для противника. Размах противоборства в информационной сфере достиг таких масштабов, что потребовалось создание специальной концепции получившей название «информационной войны» или «информационного противоборства».

8.1. Информационная война

Понятие информационной войны. Информационное оружие. Информационная атака. Стратегическое информационное противоборство.

Основные термины и понятия:
Информационная война
Информационное оружие
Стратегическое информационное противоборство
Холодная война

Понятие информационной войны

Первоначально некто Томас Рона использовал термин «информационная война» в отчете, подготовленным им в 1976 году для компании Boeing, и названный «Системы оружия и информационная война». Т. Рона указал, что информационная инфраструктура становится ключевым компонентом американской экономики. В то же самое время, она становится и уязвимой целью как в военное, так и в мирное время. Этот отчет и можно считать первым упоминанием термина «информационная война».

Публикация отчета Т. Рона послужила началом активной кампании в средствах массовой информации. Сама постановка проблемы весьма заинтересовала американских военных, которым свойственно заниматься «секретными материалами». Военно-воздушные силы США начали активно обсуждать этот предмет уже с 1980 года. К тому времени было достигнуто единое понимание того, что информация может быть как целью, так и оружием.

В связи с появлением новых задач после окончания «холодной войны» термин «информационная война» был введен в документы Министерства обороны США. Он стало активно упоминаться в прессе после проведения операции «Буря в пустыне» в 1991 году, где новые информационные технологии впервые были использованы как средство ведения боевых действий. Официально же этот термин впервые введен в директиве министра обороны США DODD 3600 от 21 декабря 1992 года.

Спустя несколько лет, в феврале 1996 года, Министерство обороны США ввело в действие «Доктрину борьбы с системами контроля и управления». Эта публикация излагала принципы борьбы с системами контроля и управления как применение информационной войны в военных действиях. Публикация определяет борьбу с системами контроля и управления как «объединенное использование приемов и методов безопасности, военного обмана, психологических операций, радиоэлектронной борьбы и физического разрушения объектов системы управления, поддержанных разведкой, для недопущения сбора информации, оказания влияния или уничтожения способностей противника по контролю и управлению над полем боя, при одновременной защите своих сил и сил союзников, а также препятствование противнику делать тоже самое». В этом документе была определена организационная структура, порядок планирования, обучения и управления ходом операции. Наиболее важным является то, что эта публикация определила понятие и доктрину войны с системами контроля и управления. Это было впервые, когда Министерство обороны США, определил возможности и доктрину информационной войны.

В конце 1996 г. Роберт Банкер, эксперт Пентагона, на одном из симпозиумов представил доклад, посвященный новой военной доктрине вооруженных сил США XXI столетия

(концепции «Force XXI»). В ее основу было положено разделение всего театра военных действий на две составляющих: традиционное пространство и киберпространство, причем последнее имеет даже более важное значение. Р. Банкер предложил доктрину «киберманевра», которая должна явиться естественным дополнением традиционных военных концепций, преследующих цель нейтрализации или подавления вооруженных сил противника.

Таким образом, в число сфер ведения боевых действий, помимо земли, моря, воздуха и космоса теперь включается и инфосфера. Как подчеркивают военные эксперты, основными объектами поражения в новых войнах будут информационная инфраструктура и психика противника (появился даже термин «*human network*»).

В настоящее время существует несколько вариантов трактовок термина «информационная война». Однако наиболее полным можно считать вариант термина, представленный в Уставе Сухопутных войск США FM 100-6 «Информационные операции» (август, 1996 г.). Согласно этому документу,

> **Информационная война** – *это комплекс мероприятий по достижению информационного превосходства путем воздействия на информацию, информационные процессы, информационные системы и компьютерные сети противника при одновременной защите своей информации, информационных процессов, информационных систем и компьютерных сетей.*

Военные определяют три **цели** информационной войны:

– контроль информационного пространства, чтобы мы могли использовать его, защищая при этом наши военные информационные функции от вражеских действий (контринформация);

– использование контроля за информацией для ведения информационных атак на врага;

– повышение общей эффективности вооруженных сил с помощью повсеместного использования военных информационных функций.

Ключевая цель информационной войны – достижение информационного доминирования. Информационное доминирование имеет своей задачей не дать противоположной стороне воспользоваться информационным пространством в полной мере.

Наиболее известным примером информационной войны считается холодная война 1946–1991 годов (точнее, её идеологический аспект). Часть исследователей считает, что распад СССР был обусловлен применением информационных методов. В приведенном примере, **информационная война** – *комплекс мероприятий по информационному воздействию на массовое сознание для изменения поведения людей и навязывания им целей, которые не входят в число их интересов, а также защита от подобных воздействий.*

Холодная война – *глобальная геополитическая, экономическая и идеологическая конфронтация между СССР и его союзниками, с одной стороны, и США и их союзниками – с другой.*

Чтобы понять различия в способах достижения цели в классической и информационной войнах, рассмотрим ситуацию, когда необходимо ограничить стратегические возможности противника по переброске войск путем уменьшения запасов топлива.

В традиционной войне сначала выявляются нефтеперегонные заводы, которые будут наиболее подходящими целями при атаке. Устанавливается, какие заводы производят больше всего топлива. Для каждого завода выявляется местоположение перегонных емкостей. Организуется атака, при которой взрываются только перегонные емкости, всё остальное оборудование остается нетронутым (для экономии средств).

В информационной войне потенциальной целью становится автоматизированная система управления нефтеперегонного завода. На начальной стадии операции выполняется проникновение в систему управления данного завода и её анализ. Обнаруживается несколько уязвимых информационных зависимостей, дающих средства воздействия на работу нефтеперегонного завода в нужное время. Позднее, в нужное время, работа завода принудительно останавливается.

Информационные войны могут вестись:

– между государствами;

– между финансово-промышленными группами;

– между властью и финансово-промышленными группами, – между властью и оппозицией, которую в свою очередь поддерживают определенные финансово-промышленные группы (иностранные государства);

– между разными сегментами власти, поддерживающие различные финансово-промышленные группы (иностранные государства).

Информационное оружие

Стратегия применения информационного оружия носит исключительно **наступательный характер**, который во многом определяет лицо информационной войны и позволяет априори определить потенциального информационного агрессора.

Информационное оружие – *это комплекс специализированных методов и средств, предназначенных для контроля информационных ресурсов объекта воздействия и временного или безвозвратного вывода из строя функций или служб информационной инфраструктуры в целом или отдельных её элементов.*

Основными способами и методами применения информационного оружия могут быть:

– нанесение ущерба отдельным физическим элементам информационной инфраструктуры (разрушение сетей электропитания, создание помех, использование специальных программ, стимулирующих вывод из строя аппаратных средств, а также биологических и химических средств разрушения элементарной базы);

– уничтожение или повреждение информационных, программных и технических ресурсов противника, преодоление систем защиты, внедрение вирусов, программных закладок и логических бомб;

– воздействие на программное обеспечение и базы данных информационных систем и систем управления с целью их искажения или модификации;

– угроза или проведение террористических актов в информационном пространстве (раскрытие и угроза обнародования или обнародование конфиденциальной информации об элементах национальной информационной инфраструктуры, общественно значимых и военных кодов шифрования, принципов работы систем шифрования, успешного опыта ведения информационного терроризма и др.);

– захват каналов СМИ с целью распространения дезинформации, слухов, демонстрации силы и доведения своих требований;

– уничтожение и подавление линий связи, искусственная перегрузка узлов коммутации;

– воздействие на операторов информационных и телекоммуникационных систем с использованием мультимедийных и программных средств для ввода информации в подсознание или ухудшения здоровья человека;

– воздействие на компьютерное оборудование боевой техники и вооружений с целью вывода их из строя.

Информационное оружие можно классифицировать по методам воздействия на информацию, информационные процессы и информационные системы противника. Это воздействие может быть ***физическим, информационным, программно-техническим или радиоэлектронным.***

Физическое воздействие оказывается на элементы информационной системы. Для физического влияния применяются следующие средства:

– противорадиолокационные ракеты;

– специализированные аккумуляторные батареи генерации импульса высокого напряжения или электромагнитного импульса;

– графитовые бомбы;

– биологические и химические средства.

> *С помощью противорадиолокационных ракет в первые дни воздушной операции коалиционных миротворческих сил в зоне Персидского залива (1991 г.) было выведено из строя 80% наземных РЛС Ирака.*

Простейшие малогабаритные генераторы электромагнитного излучения на расстоянии до 500 м могут внести опасные

искажения в работу приборов самолета, совершающего взлет или посадку, а также заглушать двигатели современных автомобилей, оснащенных микропроцессорной техникой.

Графитовые бомбы применялись американскими вооруженными силами в ходе войны в Персидском заливе и в Косово. Их поражающий эффект достигается путем создания над объектом облака площадью до 200 м^2 из произведенных на основе углерода и обладающих сверхпроводимостью тонких волокон. При соприкосновении волокон с токонесущими элементами (изоляторы, провода и т.д.) происходило короткое замыкание и вывод из строя электроцепей.

Биологические средства представляют собой особые виды микробов, способные уничтожать электронные схемы и изолирующие материалы, используемые в радиоэлектронной технике.

Информационные методы воздействия реализуются посредством всей совокупности средств массовой информации и глобальных информационных сетей типа Интернет.

Так как основным элементом информационной инфраструктуры являются **люди**, мотивация деятельности которых базируется на их физиологических, социальных и информационных потребностях, то правильно рассчитанное применение так называемых информационно-психологических методов воздействия оказывает прямое влияние на уровень безопасности государства. Проходя через сознание каждого члена общества, длительное массированное информационно-психологическое воздействие разрушающего характера создает реальную угрозу существованию нации в результате трансформации её исторически сложившейся культуры, основных мировоззренческих и идеологических установок.

Станции голосовой дезинформации, разрабатываемые в настоящее время в США, позволят входить в радиосети объекта воздействия и смоделированным компьютерными средствами голосом командира подразделения (части) противника отдавать приказы и распоряжения подчиненным им войскам, тем самым, нарушая управление войсками.

Средствами реализации **программно-технических методов** являются компьютерные вирусы, логические бомбы и аппаратные закладки, а также специальные средства проникновения в информационные сети. Данные средства используются для

сбора, изменения и разрушения информации, хранящейся в базах данных, а также для нарушения или замедления выполнения различных функций информационно-вычислительных систем.

Программно-технические средства можно классифицировать согласно выполняемым с их помощью задачам на средства:

– сбора информации,

– искажения и уничтожения информации,

– воздействия на функционирование информационных систем.

Средства сбора информации позволяют производить несанкционированный доступ к компьютерным системам, определять коды доступа, ключи к шифрам или другую информацию о зашифрованных данных и по каналам обмена передавать полученные сведения заинтересованным организациям.

Задачи сбора информации решаются и с помощью специально разработанных программных продуктов. Программа записывает все команды, вводимые в нее, и в определенное время передает информацию об этих командах. При этом система и элементы защиты его не распознают.

Созданы и постоянно модернизируются специальные технические устройства, позволяющие считывать информацию с мониторов компьютеров. Перспективным является создание миниатюрных специализированных комплексов сбора, обработки и передачи информации, которые могут внедряться под видом обычных микросхем в состав самых различных радиоэлектронных устройств.

Средства искажения и уничтожения информации включают программные продукты, относящиеся к компьютерным вирусам.

Компьютерный вирус – программа, которая характеризуется следующими свойствами:

– возможностью самопроизвольного копирования себя в другие файлы, на гибкие и жесткие накопители информации и распространения по сетям ЭВМ;

– возможностью самовоспроизведения;

– возможностью выполнения без явного вызова;

– возможностью изменения штатных режимов функционирования технических средств и (или) разрушения информации, хранящейся на гибких и жестких магнитных носителях;

– возможностью маскировки от средств обнаружения.

К средствам воздействия на функционирование информационных систем относятся «логические бомбы», «бомбы электронной почты» и т.д.

Логическая бомба представляет собой инструкцию, находящуюся в неактивном состоянии до получения команды на выполнение определенных действий для изменения или разрушения данных, а также нарушения работоспособности информационно-вычислительных систем.

В ходе войны в Персидском заливе Ирак не смог применить закупленные во Франции системы ПВО, т.к. их программное обеспечение содержало логические бомбы, активизированные с началом боевых действий.

Бомбы электронной почты – это большой объём несанкционированных сообщений с целью увеличения нагрузки на сервер таким образом, чтобы он стал недоступен или его ресурсы стали недостаточными для нормальной работы.

В марте 1999 г. на трое суток был заблокирован сервер НАТО. Неизвестный адресат регулярно присылал на адрес Североатлантического блока около 2000 телеграмм в день, которые переполнили электронный «почтовый ящик».

Радиоэлектронные методы воздействия предполагают использование как в мирное, так и в военное время средств радиоэлектронного подавления и радиоэлектронной разведки. Основным предназначением такого оружия является:

– контроль информационных ресурсов потенциального противника;

– скрытое или явное вмешательство в работу его систем управления и связи в целях дезорганизации, нарушения нормального функционирования или вывода их из строя.

Радиоэлектронные методы воздействия применяются самостоятельно либо в сочетании с другими средствами воздействия на противника.

Информационная атака

Информационная атака является составным элементом информационной войны и характеризуется искажением информации без видимого изменения сущности, в которой она находится. Различают два вида информационных атак: прямую и косвенную. Проиллюстрируем разницу между ними на следующем примере: необходимо заставить противника считать, что авиаполк находится в таком месте, где в реальности его нет.

Косвенная информационная атака: используя инженерные средства, строятся макеты самолетов и ложные аэродромные сооружения, имитируется деятельность по работе с ними. Противник будет наблюдать ложный аэродром, и считать его настоящим.

Прямая информационная атака: информация о ложном авиаполке помещается в хранилище информации у противника. Результат будет точно такой же, но средства, задействованные для получения этого результата, будут сильно отличаться.

Другим примером прямой информационной атаки может быть изменение информации в базе данных противника об имеющихся коммуникациях в ходе боевых действий (внесение ложной информации о том, что мосты разрушены) для изоляции отдельных частей противника. Аналитики противника на основе имеющейся у них информации примут решение производить переброску войск через другие коммуникации.

Стратегическое информационное противоборство

Стратегическое информационное противоборство (ИП) первого поколения рассматривается наряду с традиционными средствами противоборства (ядерными, химическими, биологическими и др.). ИП больше ориентировано на дезорганизацию деятельности систем управления и проводится скорее как обеспечение действий традиционных сил и средств.

Стратегическое ИП первого поколения – *один из нескольких компонентов будущего стратегического противоборства, применяемый совместно с другими инструментами достижения цели.*

Понятие «стратегическое информационное противоборство первого поколения» фактически вобрало в себя основные методы информационной войны, которые США реализуют в настоящее время на государственном и военном уровнях и от которых не намерены отказываться в обозримом будущем. Дальнейшая разработка проблемы привела к введению понятия «стратегического информационного противоборства второго поколения».

Стратегическое ИП второго поколения – *принципиально новый тип стратегического противоборства, вызванный к жизни информационной революцией, вводящий в круг возможных сфер противоборства информационное пространство и ряд других областей (прежде всего экономику) и продолжающийся долгое время: недели, месяцы и годы.*

Развитие и совершенствование подходов к ведению стратегического ИП второго поколения в перспективе может привести к полному отказу от использования военной силы, поскольку скоординированные информационные акции могут позволить обойтись без этой крайней меры. Если последствия стратегического ИП первого поколения еще могут быть прогнозируемы с использованием существующих методик, то второе поколение противоборства на текущий момент весьма трудно формализуемо, и существующие методики прогноза могут быть применены к анализу последствий весьма условно.

В условиях определенной трансформации взглядов на проблему ведения ИП, изменяются и задачи, которые нужно решать для достижения поставленной цели. Так, для информационного противоборства первого поколения это:

– огневое подавление (в военное время) элементов инфраструктуры государственного и военного управления;

– ведение радиоэлектронной борьбы;

– получение разведывательной информации путем перехвата и расшифровки информационных потоков, передаваемых по каналам связи, а также по побочным излучениям;

– осуществление несанкционированного доступа к информационным ресурсам с последующим их искажением или хищением;

– формирование и массовое распространение по информационным каналам противника или глобальным сетям дезинформации для воздействия на оценки, намерения лиц, принимающих решения;

– получение интересующей информации путем перехвата открытых источников информации.

Информационное противоборство второго поколения предусматривает несколько другой подход:

– создание атмосферы бездуховности и безнравственности, негативного отношения к культурному наследию противника;

– манипулирование общественным сознанием и политической ориентацией социальных групп населения страны с целью создания политической напряженности и хаоса;

– дестабилизация политических отношений между партиями, объединениями и движениями с целью провокации конфликтов, разжигания недоверия, подозрительности, обострения политической борьбы, провоцирование репрессий против оппозиции и даже гражданской войны;

– снижение уровня информационного обеспечения органов власти и управления, инспирация ошибочных управленческих решений;

– дезинформация населения о работе государственных органов, подрыв их авторитета, дискредитация органов управления;

– провоцирование социальных, политических, национальных и религиозных столкновений;

– инициирование забастовок, массовых беспорядков и других акций экономического протеста;

– затруднение принятия органами управления важных решений;

– подрыв международного авторитета государства, его сотрудничества с другими странами;

– нанесение ущерба жизненно важным интересам государства в политической, экономической, оборонной и других сферах.

В целом следует отметить, что с конца 90-х годов основной тенденцией в развитии понимания роли и места информационного противоборства является осознание факта, что стратегическое ИП является самостоятельным принципиально новым видом стратегического противоборства, способным разрешать конфликты без применения вооруженной силы.

8.2. Психологическая война

Понятие психологической войны. Цели психологической войны. Психологическая война в истории человечества. Использование пропаганды во второй мировой войне. Психологическая операция. Виды психологического воздействия. Средства психологического воздействия. Инструментарий психологических операций.

Основные термины и понятия:
Информационно-психологическая война
Психологическая война
Психологическая операция

Понятие психологической войны

Хотя методы психологического воздействия в военных целях известны с древних времен, психологическая война в ее современном понимании возникла и сформировалась только в XX веке. Этому послужило несколько причин.

Во-первых, уже после первой мировой войны стало понятно, что физические формы воздействия на противника чрезвычайно затратны. Военная победа, полученная таким способом, зачастую не окупает потерь в живой силе и технике. Научно-технический прогресс и изобретение средств массового уничтожения вообще поставили под сомнение целесообразность полномасштабных физических войн, т.к. уничтожаются территории, ресурсы, потенциальные рабы и агрессор сам может пострадать в результате применения такого оружия.

Во-вторых, возможность вести широкомасштабную психологическую войну прямо зависит от уровня развития информационно-пропагандистской машины. Только к началу XX века средства массовой информации превратились в неотъемлемый, широко распространенный и очень важный элемент повседневной жизни всех экономически развитых стран мира. Торговля, политика, культура, общественная жизнь уже не могли нормально функционировать без газет, журналов, брошюр, плакатов, устной, наглядной и печатной рекламы. Поэтому использование их в военных целях оказалось неизбежным.

В-третьих, современный мир стал другим. Значительно возрос образовательный и культурный уровень, изменилась психология широких масс. Власть имущие уже не могут, как в

древности, просто сказать народам, что война ведется ради получения добычи и рабов. Сегодня политики и стоящие за ними финансовые круги не могут прямо заявить, что война ведется ради захвата источников сырья и рынков сбыта, ради уничтожения своих экономических конкурентов, ради подавления освободительных движений в колониальных и полуколониальных странах, ради сохранения власти транснациональных корпораций в странах «третьего мира», а отнюдь не ради обороны или защиты свободы и демократии. Поскольку власть имущие никогда не могут сказать народам правду об истинных целях войны, они прибегают к психологическому насилию, лжи, пропагандистской травле тех, кто не согласен стать пушечным мясом. Прибегнуть к психологической войне заставило то, что современные войны, которые ведут правящие круги, противоречат интересам народов.

В настоящее время практически все вооруженные силы развитых государств имеют в своём составе структуры, отвечающие за оказание информационно-психологическое воздействие на военнослужащих и население противника. В армии ФРГ – это органы оперативной информации, Великобритании и Республике Корея – психологических операций, в Китае – пропаганды среди войск и населения противника, в Швеции – психологической обороны. Наиболее мощным аппаратом психологических операций обладают США. Участие контингентов ВС США в военных конфликтах и миротворческих операциях в обязательном порядке сопровождается информационно-психологическим воздействием на противника, осуществляемое оперативными структурами психологических операций.

Рассматривая вопросы информационно-психологического воздействия, обычно пользуются термином психологическая война.

Психологическая война – *совокупность различных форм, методов и средств воздействия на людей с целью изменения в желаемом направлении их психологических характеристик (взглядов, мнений, ценностных ориентаций, настроений, мотивов, установок, стереотипов поведения), а также групповых норм, массовых настроений и общественного сознания в целом.*

Психологическая война может проходить в любое (как в военное, так и в мирное) время и в любом месте, например на линии фронта и в тылу у противника.

В каком отношении друг к другу находятся информационные и психологические войны? Информационные и психологические войны тесно связаны с понятием информационного пространства. Психологическая война использует сегмент информационного пространства для оказания информационно-психологического воздействия на определенную аудиторию, а информационные войны направлены на контроль информационного пространства в целом.

Информационно-психологическая война – *открытые и скрытые целенаправленные информационные воздействия социальных, политических, этнических и иных систем друг на друга с целью получения определенного выигрыша в материальной сфере, направленные на обеспечение информационного превосходства над противником и нанесения ему материального, идеологического или иного ущерба.*

Цели психологической войны

Цели психологической войны можно классифицировать по нескольким различным основаниям.

По *условиям* различают психологическую войну, осуществляемую в мирное, военное и послевоенное время, а также в ходе миротворческих операций.

По *объектам* воздействия психологическую войну ведут против военнослужащих, гражданского населения, высшего военно-политического руководства противника и его союзников. Кроме того, предпринимаются специальные мероприятия, направленные на формирование нужного отношения к возможной войне (агрессии) со стороны мирового общественного мнения и стран-союзников.

По *времени* осуществления цели и задачи психологической войны подразделяют на долгосрочные (стратегические), среднесрочные (оперативные) и краткосрочные (тактические).

Основными целями психологической войны могут являться:

а) предотвращение возможного военного конфликта;

б) ослабление морального духа личного состава вооруженных сил и гражданского населения противника;

в) склонение их к отказу от участия в боевых действиях;

г) создание предпосылок для достижения намеченных военно-политических целей с минимальными людскими потерями и материальными затратами.

Рассмотрим основные цели психологической войны в мирное, военное и послевоенное время.

Основная цель психологической войны в мирное время заключается в том, чтобы путем воздействия на морально-политическое и психологическое состояние населения и вооруженных сил противника предотвратить военный конфликт (либо подготовить его) невоенными средствами.

В военное время цели психологической войны сводятся к тому, чтобы подорвать моральный и боевой дух населения и личного состава вооруженных сил противника, снизить его боеспособность, подавить волю к сопротивлению, побудить к уклонению от участия в боевых действиях, дезертирству, неповиновению командирам, сдаче в плен.

В послевоенное время мероприятия психологической войны осуществляют в основном с целью закрепления результатов своей победы над противником, либо для нейтрализации результатов его победы.

Психологическую войну против гражданского населения ведут с целью внедрения в его сознание идей, взглядов и представлений, снижающих готовность людей активно участвовать в войне, расшатывающих их морально-политическое единство, заставляющих выступать против войны.

Основная цель психологического воздействия на военнослужащих противника заключается в подрыве их боевого духа, в склонении к прекращению сопротивления, к сдаче в плен или уклонению от боевых действий.

Психологическая война в истории человечества

Уже в древности полководцы знали о зависимости военных побед или поражений от психологического состояния войск. Они отмечали, что важна не только нравственная сила своей армии, но и необходимость ослабления морально-психологического потенциала противника. Первая попытка

обобщить основные направления деятельности по ослаблению морально-психологического потенциала войск и населения противника была предпринята в Китае полководцем Сунь-Цзы (V век до н.э.) в трактате «Искусство войны».

Самым древним способом подрыва морального состояния противника является **устрашение** его своей (иногда мнимой) боевой мощью.

Монгольский предводитель Чингиз-хан и полководцы древнего Рима ещё до начала сражения преднамеренно распускали слухи о превосходстве своих войск, их невиданной храбрости и неодолимой решимости добыть победу.

Перед походом в Грецию в 480 г. до н.э. персидский военачальник Ксеркс в целях максимального эмоционального воздействия на противника распространял слухи о многочисленности своего войска. Он утверждал, что «если все персидские войны выстрелят из луков, то стрелы затмят солнце». Кроме того, осознавая недостаточность доведения информации устрашающего характера по каналу «из уст в уста», Ксеркс осуществил обратный отпуск греческого лазутчика, предварительно продемонстрировав ему многочисленность персидского войска.

В эпоху феодализма психологическое влияние на противника имело преимущественно религиозные формы. Воздействие на вооруженные силы обеих сторон велось распространением письменных и устных сообщений с перечислением всех возможных небесных и земных кар, которые могут пасть на голову тех, кто «выступает против истинной веры». Наряду со стратегической линией церковной пропаганды, изображавшей агрессивные войны как войны священные, в ходе крестовых походов отрабатывались приемы, которые впоследствии стали типичными для психологической войны. К ним можно отнести дискредитацию противника путем распространения версии об их зверствах, разжигание разногласий между государствами Востока и т.д.

Не менее активно использовали каноны религии и мусульманские завоеватели, державшие своих подданных в состоянии перманентной «священной войны» (джихад, газават), в ходе которой догмы непримиримости к иноверию уживались с тактическими хитростями. Тем, кого стремились обратить в мусульманство, сулили различные привилегии, включая освобождение от налогов или рабства.

Один из первых примеров применения **дезинформации** в военных целях относится к XIII веку.

> *Вторгшиеся в Венгрию в 1241 году монголы среди захваченных трофеев нашли королевскую печать. По приказу Батыя грамотные пленные от имени короля Белы написали на венгерском языке указ о прекращении сопротивления, копии которого, скрепленные королевской печатью, были разосланы в разные концы ещё не завоеванной страны.*

Бурное развитие средств печати в XIX создало широкие возможности целенаправленного воздействия на миллионы людей. Общественное мнение, эффект гласности, возможность манипулировать сознанием приобрели такую силу, с которой не могли уже не считаться ни монархи, ни полководцы. Наполеон издавал свои газеты на оккупированных немецких территориях. Как писали современники, он не только указывал о чем писать в газетах, но и о том, о чем молчать. Известно его суждение о роли газет: «четыре газеты смогут причинять врагу больше зла, чем стотысячная армия».

Успешную **пропаганду** на войска и население противника вели русские полководцы. А.В. Суворов в 1799 г. в ходе итальянского похода русской армии впервые осуществил психологическую операцию как составную часть единого плана боевых действий. Приемлемая для объекта воздействия оценка обстановки, убедительная аргументация и образный язык сделали обращение Суворова к солдатам пьемонтской армии весьма действенным: на сторону русско-австрийских войск пьемонтцы переходили не только поодиночке, но даже целыми частями.

Письменное обращение к народу Польши М. И. Кутузова, датированное 27 декабря 1812 г., впервые использовалось как охранная грамота (листовка-пропуск в плен).

Командование российской армии использовало обратный отпуск военнопленных в целях **пропаганды плена**.

В начале 1813 года французское командование, обеспокоенное участившимися случаями сдачи в плен, объявило по армии, что все солдаты по возвращении из плена будут продолжать свою службу ещё в течение 25 лет, а те, кто закончит кампанию в рядах армии, навсегда будут освобождены от дальнейших призывов. Во французских войсках объявили также, что русские вообще в плен не берут, а если некоторым оставляют жизнь, то только для того, чтобы мучить в лагерях. Флигель-адъютант князь В. С. Трубецкой, ознакомившись с этими документами, написал Аракчееву: «не думаете ли вы, ваше сиятельство, что полезно было бы нынешних пленных освободить и отправить их с тем, чтобы они рассказали товарищам своим, как у нас с ними обходятся». Это и было сделано в течение 1813–1814 гг. Вернувшиеся из плена опровергли тезисы наполеоновской пропаганды. Всего, по данным штаба Кутузова, из 640 тыс. французов, перешедших российскую границу в течение 1812 г., 160 тыс. сдались в плен.

В период англо-бурской войны (1899–1902 гг.) был реализован не только первый опыт освещения военных действий, но и опыт дезинформации общественного мнения с помощью киноновостей. Британские зрители увидели обстрел команды британского Красного креста, которая пыталась спасти раненых. Однако в реальности всё было сделано платными актерами с подачи правительства с целью получения общественной поддержки.

В Первой мировой войне впервые были широко использованы печатные средства воздействия на противника. При штабах воюющих армий создавались соответствующие отделы и подразделения, призванные организовать «войну слов» – агитацию противника.

Английское правительство создало специальные органы, снабжавшие печатные издания других стран британскими версиями о ходе войны. Было налажено издание журнала «Война в иллюстрациях», информационных бюллетеней, выпускались военные фильмы о положении на фронтах. Англичане вели секретную работу, направленную на США, чтобы заставить их вступить в войну. Активно использовался контроль над телеграфным кабелем, который соединял Северную Америку и Европу. В этом случае можно было не проверять деятельность журналистов на фронтах, поскольку все передаваемые сообщения контролировались.
В 1918 г. каждую неделю запускалось более 2000 шаров, которые несли по 1000 листовок. Всего с мая по октябрь 1918 г. в Австро-Венгрии были распространены союзниками 60 миллионов штук 643 видов разных листовок на 8 языках, а также 10 миллионов штук 112 разных газет на четырех языках.

В конце войны Антанта сделала первые шаги по координации своих пропагандистских усилий: возник специальный штаб по разложению вражеских войск. Россия в этой пропагандистской войне участвовала с меньшим размахом, т.к. была слабо технически подготовлена.

В Германии до августа 1918 года было запрещено заниматься изданием и распространением листовок, поскольку это, по мнению руководства страны, противоречило правилам ведения войны. Когда же запрет был снят и Германия приступила к массовому изданию листовок, время было упущено и добиться сколько-нибудь ощутимых результатов до конца войны ей не удалось. Гитлер считал, что первая мировая война вообще была проиграна Германией из-за проигрыша войны в области пропаганды.

История войн наглядно продемонстрировала необходимость проведения и эффективность умело организованной работы по воздействию на морально-психологический потенциал противника. Начав формироваться в качестве средства устрашения, теория информационно-психологического воздействия в XX веке стала неотъемлемой частью военного искусства.

Использование пропаганды во Второй мировой войне

Сразу после окончания Первой мировой войны в западных странах было проведено множество исследований в области военной пропаганды, объединенные в 1921 г. в единую теорию психологической войны немецким ученым Фуллером.

Сделав соответствующие выводы из опыта первой мировой войны, руководители фашистской Германии с большим вниманием отнеслись к проблемам ведения военной пропаганды. Зал съезда национал-социалистов в Нюрнберге в 1936 году украшал лозунг: «Пропаганда помогла нам прийти к власти. Пропаганда поможет нам удержать власть. Пропаганда поможет нам завоевать весь мир».

Своего самого крупного успеха немецкая пропаганда добилась в 1940 году в период оккупации Франции. За несколько месяцев до вторжения во Францию немцы стали активно использовать так называемые «черные» передатчики, которые выдавали себя за французские радиостанции. Через них распространялись всевозможные слухи, подвергалось критике французское правительство, сеялись неуверенность и панические настроения среди населения и военнослужащих. В результате к моменту решительного наступления немецких войск морально-боевой дух французской армии был настолько подорван, что она была не в состоянии оказать серьезное сопротивление.

Министерство пропаганды Германии отпечатало к 22 июня 1941 г. свыше 30 млн. листовок, красочных пропагандистских брошюр карманного формата на 30 языках народов СССР и подготовило несколько радиопередач. На Восточном фронте было сосредоточено 17 рот пропаганды. В течение первых двух месяцев войны ими было распространено около 200 млн. листовок. В 1943 году пропагандистские войска становятся самостоятельным родом войск, их численность достигает 15 тысяч человек.

Органы пропаганды стран антигитлеровской коалиции в своей деятельности делали основной упор на следующие виды пропаганды в зависимости от ожидаемого эффекта: конверсионную, разделительную, деморализующую и пропаганду плена.

Военная пропаганда – это использование информационных каналов в интересах политической поддержки ведущихся военных действий и общих целей, поставленных перед собою воюющими сторонами.

Конверсионная пропаганда – это массированное пропагандистское воздействие на ценностные ориентации человека или групп людей с целью изменения его (их) установок, отношений, суждений и взглядов на политику, проводимую высшим военно-политическим руководством страны.

Разделительная пропаганда – это пропагандистское воздействие, направленное на разжигание межгрупповых противоречий на основе различий религиозного, национального, социального, профессионального и др. характера с целью ослабления единства в рядах противника вплоть до его раскола.

> *К концу Второй мировой войны западные союзники разбрасывали над Германией фальшивые почтовые марки рейха с портретом Гиммлера в расчёте на то, что циркуляция таких марок сможет вызвать подозрения у Гитлера и тем самым спровоцировать распри среди нацистского руководства.*

Деморализующая пропаганда – это пропагандистское воздействие, направленное на ослабление психики человека, обострения его чувства самосохранения с целью снижения морально-боевых качеств вплоть до отказа от участия в боевых действиях.

Среди мотивов, использовавшихся для дестабилизирующего воздействия на психику населения и военнослужащих противника, можно выделить следующие:

– «голод» – эксплуатация продовольственных затруднений противника (на позиции сбрасывались красочные открытки, изображающие различные кушанья и деликатесы);

– «траур» – напоминание о смерти;

– «проигранное дело» – внушение противнику, что его положение безысходно;

– «семейные мотивы» – использование темы «детей, ждущих возвращения отца», спекуляции по поводу жен, изменяющих фронтовикам с «тыловыми крысами»;

– «превосходство в силе» – показ неспособности противника противостоять силе союзников.

Пропаганда плена – это пропагандистское воздействие на человека или группы людей, направленное на формирование положительных установок по отношению к сдаче в плен как единственно разумному и безопасному выходу из сложившейся обстановки.

Генерал-лейтенант В. Мюллер, исполнявший обязанности командующего 12-м армейским корпусом, 8 июля 1944 года сдался в плен, а затем отдал приказ о капитуляции личному составу объединения. В листовке под названием «Генерал Мюллер поступил разумно» был помещён его портрет, а также фотокопия приказа с факсимиле. Уже 9 июля 2 тыс. человек сдались в плен, а в целом приказу генерала из 33 тыс. окруженных последовало 15 тыс. военнослужащих.

Из Корсунь-шевченковского котла вышли 55 тыс. солдат и офицеров с листовками, призывавшими к сдаче в плен, написанными генералами Зейдлицом и Корфесом.

Пропаганда носила многоканальный характер, включающий и кино. Например, для Голливуда были определены пять тем, обладающих наибольшей приоритетностью:

- объяснять, почему американцы сражаются;
- изображать Объединенные Нации и их народы;
- воодушевлять работу и производство;
- поднимать дух на домашнем фронте;
- поднимать героизм вооруженных сил.

Советская кинохроника заработала спустя две недели после начала нападения немецких войск. Ежегодно производилось 20 художественных фильмов.

Психологическая операция

Содержание психологического воздействия реализуется путем проведения психологических операций. Психологическая операция – главный элемент содержания психологической войны. Её проведение предполагает использование на практике в условиях вооруженной борьбы сложной совокупности согласованных

по целям, задачам, месту, времени и объектам видов, форм, способов и приемов информационно-психологического воздействия.

Психологические операции проводятся с тех времен, когда люди начали общаться друг с другом. В самом раннем периоде они представляли собой непосредственное общение, в ходе которого человек оказывал влияние на другого человека или группу людей посредством жестов, слов, действий или комбинацией этих приемов убеждения. Сегодня способы воздействия на поведение стали более разнообразными, но цель психологических операций остается неизменной. Они призваны способствовать достижению целей военных операций своих вооруженных сил как в мирное, так и в военное время посредством разнообразных способов изменения мнений, чувств и отношений, а в конечном итоге поведения групп людей, являющихся объектами психологических операций.

Психологическая операция – *это проводимая в мирное или военное время плановая пропагандистская и психологическая деятельность, рассчитанная на иностранные враждебные, дружественные иди нейтральные аудитории с тем, чтобы влиять на их отношение и поведение в благоприятном направлении для достижения как политических, так и военных национальных целей.*

Психологические операции подразделяются на следующие уровни: стратегические, оперативные и тактические.

Стратегические психологические операции осуществляются в интересах достижения долгосрочных целей, призванных создать благоприятную психологическую обстановку для ведения военных действий. Такие операции обычно носят глобальный характер.

Оперативные психологические операции осуществляются в интересах достижения среднесрочных целей, в поддержку военных кампаний иди крупных операций. Объектом таких операций обычно является население определенного региона.

Тактические психологические операции осуществляются в интересах достижения краткосрочных целей, в поддержку командиров тактического звена. Объектом таких операций обычно является противостоящая группировка войск противника.

Психологические операции состоят из **политических, военных, экономических, дипломатических** и собственно **информационно-психологических мероприятий**, направленных на конкретные группы населения и военнослужащих противника с целью внедрения в их сознание необходимых идеологических и социальных установок, формирования ложных стереотипов поведения, трансформации в нужном направлении их настроений, чувств, воли, склонению их к отказу от боевых действий, предательству, сдаче в плен или дезертирству.

При правильном планировании психологические операции **предшествуют** применению военной силы, а затем **сопровождают** либо **дополняют** её использование. Они осуществляются в рамках государственной политики, а их военная и прикладная стороны согласовываются и координируются с деятельностью соответствующих правительственных учреждений.

В качестве схемы психологической операции против гражданского населения, рассмотрим этапы подготовки общественного мнения к войне в регионе Z. Пропагандисты должны убедить общество, что военные действия неизбежны и отвечают интересам нации, правовым нормам и принципам гуманизма.

Этап 1. Обществу внушают: в регионе Z сложилась аномальная ситуация.

Шаг 1. Создается виртуальный образ. В СМИ появляются репортажи-инсценировки, сделанные якобы в регионе Z. Иллюзия достоверности достигается рядом специальных трюков (дрожащая телекамера). *Репортер «под свист пуль» рассказывает, что в регионе Z неспокойно, потому что тут диктатура/безвластие.*

Шаг 2. Свидетельства «очевидцев». Специально подготовленные свидетели и пострадавшие разоблачают дикие порядки, царящие в регионе Z. *«Чудом выжившая» девочка рассказывает, как расстреляли её отца и брата. «Такое у нас происходит каждый день», – будничным тоном говорит она.*

Шаг 3. Наклеивание ярлыков. Путем настойчивого использования определенных метафор в общественное сознание внедряются стойкие негативные ассоциации и ярлыки. *«Политический режим в регионе Z – фашистский», «Власти региона Z – бандиты и террористы».*

Этап 2. Пропаганда навязывает обществу определенную программу действий.

Шаг 1. Ложная аналогия. Психологическая ловушка, основанная на тяге людей к типологизации событий. *«Когда-то в Косове (в Чечне, в Афганистане и т.д.) было так же, как сейчас в регионе Z. Поэтому мы знаем, что случится, если сейчас не принять меры».*

Шаг 2. Исключение альтернатив. Спорное решение выдается за единственно возможное, альтернативные предложения замалчиваются. Общество настойчиво убеждают: иного не дано. *«В регион Z нужно ввести войска». «…Нужно ввести войска». «…Ввести войска».*

Шаг 3. Историческая подтасовка. Намеренная подгонка исторических фактов под заданную версию текущих событий. *«Регион Z всегда был взрывоопасным. Только нам удавалось поддерживать там гражданский мир и обеспечивать благополучие граждан».*

Этап 3. В регионе Z начинаются военные действия, приводящие к гибели людей и серьезным разрушениям.

Шаг 1. «Забалтывание» темы. Сообщения из района боевых действий оттесняются на второй план, «забиваются» массой ярких «легких» новостей. *«Сенсация! В зоопарке города N родился первый в мире фиолетовый крокодил… Певец М. покалечил тёщу… Сегодня в регионе Z был сбит наш вертолёт… В Эфиопии засуха… В Риме выставка…».*

Шаг 2. Понижение эмоциональной оценки. Информация о жертвах и разрушениях сообщается нейтральным, бесстрастным тоном, чтобы общество начало относиться к войне как к рутине. *«Сегодня подорвался на мине БТР третьего полка. Погибли 12 человек. Напомним, что это уже третий инцидент с начала недели: во вторник в перестрелке пострадали двое рядовых, а в среду смертельное ранение получил один военнослужащий».*

Шаг 3. Фальшивая социология. Подтасовка замеров общественного мнения для оправдания неудачной военной операции. *«Вопреки досужим домыслам о непопулярности операции в регионе Z 76% наших граждан – за продолжение боевых действий».*

Отдельные шаги приведенной выше схемы в реальности выглядели следующим образом.

Подготовка к военной операции в зоне Персидского залива шла под лозунгами восстановления утраченной независимости Кувейта, защиты Саудовской Аравии, ОАЭ, Катара и Омана от агрессивных намерений С. Хусейна, защиты свободы мирового судоходства в Персидском заливе, защиты нарушаемых прав курдов и шиитов Ирака и необходимостью установления демократического режима правления в этой стране. Сообщалось о наличии у Ирака огромных запасов химического оружия и планах его возможного применения, об активных работах по созданию ядерного боеприпаса, о поддержке С. Хусейном ряда террористических организаций и т.д. Ярким эпизодом пропагандистской кампании явились свидетельские показания кувейтской девочки о зверствах со стороны иракских солдат на территории Кувейта. Якобы они вынесли из родильного отделения пятнадцать новорожденных и положили их умирать на бетонный пол. В течение сорока дней после данных свидетельств Президент США Дж. Буш десять раз обращался к этой теме в своих выступлениях. Впоследствии оказалось, что девочка была дочерью посла Кувейта в США и её история не более чем вымысел.

Массированной дезинформации подверглось мировое сообщество относительно так называемой «гуманитарной катастрофы» в Косово. После ввода на территорию Косова миротворческих сил представители гуманитарных организаций завезли 40 тысяч пластиковых пакетов для перезахоронения жертв так называемого «холокоста косовских албанцев». Однако было обнаружено не более 2 тысяч трупов. Впоследствии премьер-министр Великобритании Тони Блэр подвергся резкой критике со стороны оппозиции и СМИ за обман английского народа.

Психологические операции по осуществлению **культурной экспансии и диверсий** проводятся с целью распространения своих культурных идеалов и принципов среди населения других стран, что, с одной стороны, приводит к установлению

моральной и нравственной зависимости вторых от первых, а с другой – способствует нарушению устоявшихся культурно-этических представлений в обществе, приводит к деградации национальной сознания.

Особый эффект дает разжигание национально-культурных противоречий. Этнические, религиозные и другие меньшинства представляют собой первоочередной объект воздействия.

Национально-религиозные противоречия послужили основой для затяжного конфликта в Югославии, на территории Северного Кавказа и в Закавказье.

> *Накануне войны в Персидском заливе проводилась целенаправленная американская пропаганда на курдов. США удалось спровоцировать антиправительственные выступления в Иракском Курдистане, что вынудило Багдад направить туда дополнительные войска.*

Консолидирующие психологические операции проводятся в интересах воздействия на население нейтральных и дружественных стран, а также на население своего государства. Они преследуют цель формирования лояльного отношения, а на своё население и население дружественных государств с целью активной поддержки политики, проводимой субъектом воздействия.

Главными целями психологических операций при осуществлении миротворческой деятельности являются предотвращение или прекращение вооруженного конфликта.

Виды психологического воздействия

По мнению отечественных и зарубежных специалистов психологическое воздействие подразделяется на следующие виды:

– информационно-психологическое;
– психогенное;
– психотронное;
– психоаналитическое;
– нейролингвистическое;
– психотропное.

Информационно-психологическое воздействие – это воздействие словом, информацией. Психологическое воздействие

такого вида ставит своей основной целью формирование определенных идеологических (социальных) идей, взглядов, представлений, убеждений, одновременно оно вызывает у людей положительные или отрицательные эмоции, чувства и даже массовые реакции, например, панику.

Психогенное воздействие осуществляется в результате физического воздействия на мозг человека в результате травмы головы или воздействия физических факторов (звука, освещения, температуры и т.д.), а также шокового воздействия окружающих условий или каких-то событий (например, картин массовых разрушений, многочисленных жертв и т.д.). В результате психогенного воздействия человек не в состоянии рационально действовать, теряет ориентацию в пространстве, испытывает аффект или депрессию, впадает в панику, в состояние ступора и т.д. В связи с этим появилось такое понятие как психогенные потери личного состава.

В ходе арабо-израильской войны (1973 г.) египтяне применили против Израиля реактивные системы залпового огня. Из 1500 израильских военнослужащих поступивших после огневого налета в госпиталь 800 не имели никаких физических повреждений.

Психотронное (парапсихологическое, экстрасенсорное) воздействие – это воздействие на людей, осуществляемое путем передачи информации через внечувственное (неосознаваемое) восприятие.

Массовая «телевизионная эпидемия» вспыхнула в Японии 1 декабря 1997 года после демонстрации очередной серии мультфильма «Покемон». Более 700 детей были доставлены в больницу с симптомами эпилепсии. По мнению психиатров, массовый недуг вызвали эпизоды, сопровождавшиеся многочисленными ослепительными разноцветными вспышками. Медики доказали, что мерцание красного цвета с частотой от 10 до 3030 вспышек в секунду вызвало сначала раздражение глазных нервов и частичный спазм сосудов головного мозга, а затем потерю сознания, судороги и даже спазматическое прекращение дыхания (удушье).

Наиболее известным здесь является «феномен 25 кадра», хотя его эффективность до конца не изучена. Кроме того, известны факты проведения работ по созданию генераторов высокочастотной и низкочастотной кодировки мозга.

Психоаналитическое воздействие – воздействие на подсознание человека терапевтическими средствами, особенно в состоянии гипноза или глубокого сна. Словесные внушения (команды) в закодированной форме выводятся на любой носитель звуковой информации (аудиокассеты, радио или телепередачи, шумовые эффекты). Человек слушает музыку или шум прибоя в комнате отдыха, следит за диалогами персонажей фильма, и не подозревает, что в них содержатся невоспринимаемые сознанием, но всегда фиксируемые подсознанием команды, заставляющие его впоследствии делать то, что предписано.

Нейролингвистическое воздействие – вид психологического воздействия, изменяющий мотивацию людей путем введения в их сознание специальных лингвистических программ. Главным средством воздействия выступают специально подобранные вербальные (словесные) и невербальные лингвистические программы, усвоение содержания которых позволяет изменить в заданном направлении убеждения, взгляды и представления человека (как отдельного индивида, так и целых групп людей). Однако необходимость непосредственного контакта с объектом ограничивает сферу использования этого вида психологического воздействия.

Психотропное воздействие – воздействие на психику человека с помощью медицинских препаратов, химических или биологических веществ.

Не все указанные виды психологического воздействия используются в равной степени. В основном в ходе ведения психологической войны применяются информационно-психологическое и психогенное воздействие.

Психологическое воздействие в условиях вооруженной борьбы зависит от тех целей и задач, ради решения которых оно предпринимается, а также от возможностей (сил и средств), требующихся для этого.

Средства психологического воздействия

В ходе ведения психологической войны на людей оказывается психологическое воздействие, которое может осуществляться различными средствами.

Во-первых, **информационными средствами**. Например, в предвоенный период правительство любой страны через средства массовой информации стремится сформировать у своего населения патриотические взгляды и убеждения, обеспечить в массовом сознании приоритет целей государственной политики. В то же время вероятный противник старается внедрить в сознание населения и военнослужащих этого государства выгодные только ему, противоположные по направленности идеи и настроения. Например, разжигает националистические предрассудки, недовольство политическими или экономическими мероприятиями правительства, что нередко ведет к снижению уровня морально-психологического состояния населения и личного состава вооруженных сил.

Во-вторых, психологическое воздействие может осуществляться **военными средствами**. Например, СССР размещал с целью психологического давления свои войска и ракеты возле границы с Китаем, во Вьетнаме, на территории Кубы. США неоднократно стремились достичь своих политических целей с помощью демонстрации военной силы, направляя военно-морскую группировку в кризисные районы мира.

В-третьих, для психологического воздействия может использоваться **система торговых и финансовых санкций**, направленных на подрыв экономики потенциального противника. Так, экономические санкции (в том числе и от имени ООН) вводились против Ирака, Югославии, Кубы, Ливии, Судана и ряда других стран. Эти действия влекут за собой значительное снижение уровня жизни большинства населения, многочисленные бытовые трудности, рост заболеваемости, нехватку продовольствия и, как следствие, массовое недовольство граждан существующим положением.

В-четвертых, психологическое давление может осуществляться **политическими средствами**. Сюда можно отнести создание или поддержку существующих оппозиционных партий, движений с целью оказания политического давления на руководство страны.

Инструментарий психологических операций

Все средства воздействия обладают разными характеристиками, поэтому реальным их использованием становится многоканальное воздействие, когда каждое из средств выполняет свою функцию. Так, информация по радио, в отличие от листовки, может легче пересекать границы и воздействовать на гражданское население. В то же время листовка обладает определенным преимуществом, стимулирующим сдачу в плен, например, когда она подается как пропуск через линию фронта. Слухи и общение лицом к лицу эксплуатируют особенности устного общения, они также могут распространяться вне особых материальных преград, тогда как радио, к примеру, требует наличия радиоприемника у аудитории для того, чтобы коммуникативная цепочка могла замкнуться.

Листовки. Экстремальные условия нахождения на линии фронта каждый раз вызывают к жизни самые простые источники передачи информации, например, листовки. Другой причиной обращения именно к данному средству может служить необходимость выхода на конкретную аудиторию с учетом имеющихся на тот период в обществе информационных потоков.

> *В Боснии НАТО вело информационные программы против антинатовских сербских программ, включая телевизионное вещание. Когда обнаружилось, что восточная Босния лежит вне действия этих станций, были применены листовки. В них подчеркивались такие темы, как роль официальных лиц в демократических обществах, роль полиции в поддержании порядка и т.д.*

В период войны в Персидском заливе применение листовок привело к следующим результатам: 98% военнопленных видели листовки, 80% – поверили их сообщениям, 70% – сказали, что на них повлияли листовки в их желании сдаться. Всего было сброшено 29 миллионов копий 38 различных видов листовок, приблизительный суммарный вес которых составил 29 тонн. Листовки могут сбрасываться с помощью соответствующей бомбы, доставляющей до 60 тысяч экземпляров. Могут использоваться вертолеты. Листовки могут просто раздаваться солдатами. Но они в любом случае должны доходить до населения.

Например, после землетрясения в Армении отмечалось, что все напечатанные объявления скапливались в органах власти и население не знало самой простой информации.

Листовки должны создаваться с учетом требований аудитории. Стиль листовок должен стремиться к разговорным вариантам как понятным большому числу аудитории.

В целом, по представлениям американских аналитиков, листовки обладают следующим набором преимуществ:

– печатное слово более авторитетно и престижно;

– печатное слово передается от одного лица к другому без изменений;

– печатное слово может быть усилено рисунками и фотографиями, которые понятны даже неграмотным;

– печатное слово можно распространить на большую аудиторию;

– печатное слово может перечитываться для усиления воздействия;

– сложные материалы могут быть объяснены в деталях;

– листовки можно спрятать и прочесть в одиночестве;

– сообщения можно печатать на любых поверхностях.

Громкоговорители. Листовки может читать только грамотное население. Их приготовление и распространение требует определенного времени. Эти два фактора не столь важны при вещании на противника с помощью громкоговорителей, установленных на машинах. В этом случае поступление информации становится динамичным, снимается проблема книжного стиля, поскольку может идти просто прямой разговор с противником.

Высадка на Панаму в 1983 г. обеспечивалась командами с громкоговорителями, которые позволяли уменьшать сопротивление и контролировать местное население. Уроки, вынесенные американскими военными из этого применения, заключались в следующем:

− удостовериться, что вещание в принципе слышно для противника;

− использовать заранее напечатанные листовки для поддержки вещания;

− учитывать аспекты местной культуры.

В период войны в Персидском заливе применение громкоговорителей привело к следующим результатам: 34% военнопленных

слышали их, 18% – поверили их сообщениям, 16% – сказали, что на их желание сдаться повлияли сообщения, переданные по громкоговорителям.

В принципе это достаточно динамичный метод воздействия, несущий в себе всю силу устного слова, по этой причине эффективность его достаточно высока.

Радиовещание. Радиоинформация может без затруднений пересекать любые границы, именно поэтому радиовещание было основным средством воздействия в период «холодной войны». Пропагандисты часто сбрасывают радиоприемники в район расположения противника, чтобы облегчить функционирование данного канала коммуникации. Это сделала Германия по отношению к Австрии, эта же схема повторилась в войне в Персидском заливе. В данном случае это было особенно важно, поскольку ЦРУ задействовало несколько радиостанций, ведущих вещание в схеме «черной пропаганды», которые создавали ощущение существования заговоров против Саддама внутри Ирака.

В ситуации в Боснии использовались самолеты EC-DOE, позволяющие вещать во всех диапазонах, а также вести телевизионные передачи. Эти самолеты также позволяли глушить теле- и радиопередачи сербов.

В период войны в Персидском заливе применение радиовещания привело к следующим результатам: 58% военнопленных слышали программы, 46% – поверили тому, что услышали, 34% – сказали, что на их желание сдаться повлияли радиопередачи.

Радио может действовать на любом расстоянии, конкурируя с местными средствами коммуникации, отстаивая иную точку зрения. Перед высадкой на Гаити свергнутый президент Аристид обращался к населению с помощью радио. Поскольку тысячи гаитянцев пытались переправиться на лодках в сторону США, радиовещание позволило обратиться к ним, чтобы сказать о запрете въезда в США. Радио передавало новости, местную музыку, дискуссии, все на креольском языке, на котором говорит большинство населения. Именно радио в совокупности с психологическими операциями признается американскими военными главным фактором восстановления гражданского правительства на острове и уменьшения жертв среди населения.

В случае вьетнамской войны радио стало основным средством проведения психологических операций. При этом США использовали радиостанции, которые работали в режиме «черной пропаганды», например, «Радио Ханой», которое вещало с самолета, летавшего вдоль берегов Вьетнама, что не только не позволяло обнаруживать его местонахождение, но и делало его сигналы столь же сильными, как и у местных станций. В 1967 г. с воздуха были сброшены радиоприемники для населения, чтобы облегчить получение радиоинформации.

Слухи. Слухи адекватны своей информационной среде, идеально ей соответствуя. Только этим можно объяснить процесс их распространения, который дополнительно никем не поддерживается, в отличие от любых СМИ. В обычном тексте завышена роль коммуникатора, тогда как слухи завышают роль слушающего, что в принципе характерно для явлений массовой культуры.

Слух достаточно часто является результатом давления официальной информационной сферы. В неофициальную сферу может уходить как информация, нежелательная для официальной сферы, так и информация, сознательно запускаемая в устной форме. Например, японцы считают, что реклама лекарств и врачей эффективнее в устной среде, чем на глянцевой обложке. Они предложили следующее название для этой передачи: «разговоры у колодца». Вспомним также достаточно частый вопрос перед выборами «за кого вы будете голосовать?». Человеку не хватает официальной информации, которая, казалось бы, существует в избытке, он хочет получить неофициальное подтверждение своей окончательно не сформировавшейся точке зрения.

Слух является стимуляцией обсуждения определенной проблемы. А из социальной психологии известно, что в результате группового обсуждения мнение группы усиливается. Рассказ о будущем землетрясении или конце света в ближайшую пятницу может быть настолько интенсивным действием, что он не нуждается в прикреплении к личности.

Слухи о зверствах противника, которые активно порождаются во время войны, выполняют у солдат роль компенсации в их тяжелой для психики деятельности. Враг в слухе предстает как самый ужасный, поэтому его существование разрешает солдату то, что в мирной жизни казалось бы ему невозможным.

Отдельной проблемой является определение удачных мест для распространения слухов и формы их «запуска в народ». В первую мировую войну американские пропагандисты смогли при отсутствии сети современных СМИ закрыть все свое население с помощью так называемых «четырехминутников». Для них готовились сообщения с фронтов, которые рассылались телеграфом по всей стране. Длина такого текста не должна была превышать четырех минут для пересказа, отсюда это название. «Четырехминутники» выходили в церковь, госпиталь, школу и зачитывали эту телеграмму. В результате без всякого телевидения страна получала ту информацию, которая требовалась на тот момент.

Интернет. Возникновение нового канала коммуникации естественно включает его в арсенал возможного использования в рамках психологических операций. Интернет на сегодня является наименее контролируемой информационной областью, что облегчает размещение там нужной информации. Таким образом, Интернет используется в двух вариантах:

- как вариант облегченного перехода в СМИ;
- как вариант воздействия на лидеров мнения (лиц принимающих решения).

Не менее значимой является роль Интернета при решении военных задач. Например, в случае высадки на Гренаду с одним из двадцати типов целевой аудитории, выделенных в рамках кампании обеспечения, общение велось исключительно по Интернету. Известно, что каждый тип целевой аудитории должен получать не только созданные для себя сообщения, но и передаваться они должны по привычному для данной аудитории каналу коммуникации. Интернет постепенно становится одним из таких привычных каналов коммуникации для конкретных типов аудитории.

Американские аналитики также отмечают другие варианты интереса к Интернету с точки зрения военного ведомства: «Интернет может быть добавлен к репертуару инструментария психологических операций, а также помощи в достижении нестандартных военных целей». Отмечается, что мониторинг Интернета может дать возможность создания системы раннего оповещения о конфликтах. Комментарии, размещенные в Интернете, позволяют анализировать конфликты малой интенсивности.

В случае конфликтов сильной интенсивности Интернет может оказаться вообще единственным средством связи. В целом Интернет вносит следующие изменения в варианты решения тех или иных задач:

– Интернет разрушает монополию масс-медиа, в результате чего СМИ лишаются возможности определения, что именно должно представлять интерес для массовой аудитории.

– Видео- и аудиосообщения по Интернету станут играть новую роль: политические группы будут распространять по Интернету видеоклипы в поддержку своих взглядов.

– Интернет будет использоваться правительствами: правительства Перу и Эквадора уже вели пропагандистскую войну с помощью Интернета.

– Интернет будет играть все возрастающую роль в международных конфликтах, поскольку позволяет влиять на политические и журналистские элиты мира.

Интернет как менее контролируемое информационное пространство каждый раз оказывается выгодной площадкой для запуска нужной информации в нужном месте и в нужное время.

Общение лицом к лицу. В период войны в Боснии велась работа в системе лицом к лицу, для чего были созданы тактические команды по психологическим операциям, которые могли беседовать с местным населением в кафе, ресторане, частных домах. Они были направлены на разъяснение миссии НАТО в Боснии. Это важный аспект выдачи информации именно в устном режиме, который в принципе является для любого человека основным.

П. Лазарсфельд выделяет пять причин, делающих непосредственное общение эффективнее массовых коммуникаций:

– личных контактов труднее избежать;

– контакты лицом к лицу носят достаточно гибкий характер, позволяющий менять содержание в соответствии с сопротивлением аудитории;

– личные отношения, стоящие позади общения лицом к лицу, позитивно поддерживают принятие сообщения и наказывают за отторжение его;

– люди больше верят тому, кого знают, чем безличностным массовым коммуникациям;

– личные контакты позволяют достичь цели даже без

реального убеждения человека принять чужую точку зрения, например, друг может проголосовать, как его просят, даже не меняя своих позиций.

В случае партизанской войны ЦРУ, например, уделяет особое внимание общению с населением, поскольку партизанская война превращает психологические операции в решающий фактор. Требуется, чтобы каждый партизан мог во время личностного контакта привести крестьянину 5–10 логических причин, почему ему должны дать кров и пищу. 200–300 агитаторов должны уметь собирать митинг из 10–20 тысяч участников. Контроль такого митинга включает скрытых командиров, охранников, шокирующих сил, являющихся инициаторами инцидентов, выкрикивающих слоганы, носящих плакаты и др.

Самой простой вид общения – лицом к лицу – является и наиболее эффективным, позволяющим производить психологические операции в привычном для аудитории коммуникативном режиме, в котором оказывается задействованным меньшее число защитных факторов.

Вопросы для самоконтроля

1. Покажите на примерах значение информации в условиях войны.
2. Каковы особенности информационной войны?
3. Каковы цели информационной войны?
4. Перечислите основные способы и методы применения информационного оружия.
5. Перечислите методы и средства воздействия на гражданское население в ходе современной информационной войны.
6. Что такое «психологическая война»?
7. Каковы цели психологической войны?
8. Приведите примеры психологической войны в истории человечества.
9. Перечислите виды психологического воздействия, которые используются в психологических войнах.
10. Перечислите средства психологического воздействия, которые используются в психологических войнах.
11. Каков инструментарий психологических операций?

СПИСОК ЛИТЕРАТУРЫ

1. *Айков, Д.* Компьютерные преступления / Д. Айков, К. Сейгер, У. Фонсторх. – М. : Мир, 1999. – 351 с.

2. *Аронсон, Э.* Эпоха пропаганды : Механизмы убеждения повседневное использование и злоупотребление / Э. Аронсон, Э. Р. Пратканис. – СПб. : Прайм-ЕВРОЗНАК, 2003. – 384 с.

3. Безопасность дома, портал безопасности корпорации Microsoft [Электронный ресурс]. – Электрон. текстовые дан. – Режим доступа: http://www.microsoft.com/rus/protect/default.mspx, свободный. – Загл. с экрана.

4. Безопасность. Образование. Человек. Информационный портал ОБЖ и БЖД: Всё о Безопасности Жизнедеятельности [Электронный ресурс]. – Электрон. текстовые дан. – Режим доступа: http://www.bezopasnost.edu66.ru, свободный. – Загл. с экрана.

5. *Бетелин, В*. Информационная безопасность в России: опыт составления карты / В. Бетелин, В. Галатенко // Jet Info № 1. – 1998. – С. 5.

6. Библиотека «ПСИ-ФАКТОРА» [Электронный ресурс]. – Электрон. текстовые дан. – Режим доступа: http://psyfactor.org/lybr.htm, свободный. – Загл. с экрана.

7. Богданов, Е. Н. Психологические основы «Паблик рилейшнз» : учеб. пособие для студентов вузов / Е. Н. Богданов, В. Г. Зазыкин. – 2-е изд. – СПб. : Питер, 2004. – 204 с.

8. *Бодров, В. А*. Информационный стресс : учеб. пособие для студентов вузов / В. А. Бодров. – М. : ПЕР СЭ, 2000. – 352 с.

9. *Бурлаков, И. В*. Homo Gamer : Психология компьютерных игр / И. В. Бурлаков. – М. : Независимая фирма «Класс», 2000. – 141 с. – (Библиотека психологии и психотерапии, вып. 86).

10. *Гарфинкель, С*. Всё под контролем : Кто и как следит за тобой / С. Гарфинкель ; пер. с англ. В. Масянкина. – Екатеринбург : У-Фактория, 2004. – 432 с.

11. *Гафнер, В. В*. Информационная пассивность педагога / В. В. Гафнер // Народное образование. – 2005. – № 2. – С. 235–239.

12. *Гафнер, В. В*. О профессиональной компетентности учителя ОБЖ / В. В. Гафнер // ОБЖ. Основы безопасности жизни. – 2005. – № 11. – С. 31-34.

13. *Гафнер, В. В*. О профессиональной компетентности учителя ОБЖ / В. В. Гафнер // ОБЖ. Основы безопасности жизни. – 2005. – № 12. – С. 40-44.

14. *Гафнер, В. В*. Предвидеть и предупреждать. Профессиональная компетентность учителя ОБЖ как психолого-педагогическая проблема / В. В. Гафнер // ОБЖ. Основы безопасности жизни. – 2004. – № 9. – С. 15–17.

15. *Гафнер, В. В*. Профессиональная деформация и компетентность педагога / В. В. Гафнер // ОБЖ. Основы безопасности жизни. – 2004. – № 10. – С. 22–24.

16. *Гафнер, В. В*. Профессиональная переориентация бывших военнослужащих и проблема становления профессиональной компетентности учителя ОБЖ / В. В. Гафнер // ОБЖ. Основы безопасности жизни. – 2004. – № 11. – С. 47–49.

17. *Гафнер, В. В*. Совмещение преподавания: «за» и «против». Совмещение преподавания нескольких учебных предметов как препятствие становления профессиональной компетентности педагога / В. В. Гафнер // ОБЖ. Основы безопасности жизни. – 2004. – № 12. – С. 53–55.

18. *Грачев Г. В*. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты / Г. В. Грачев. – М.: Изд-во РАГС, 1998. – 125 с.

19. *Грачев, Г. В*. Личность и общество: информационно-психологическая безопасность и психологическая защита / Г. В. Грачев. – М.: ПЕР СЭ, 2003. – 304 с.

20. *Грачев Г. В*. Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия / Г. В. Грачев, И. К. Мельник. – М.: Алгоритм, 2002. – 288 с.

21. *Гриняев, С. Н*. Поле битвы – киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны / С. Н. Гриняев. – Мн.: Харвест, 2004. – 448 с.

22. *Дмитриев, А. В*. Слухи как объект социологического исследования / А. В. Дмитриев // Социс. – 1995. – № 1. – С. 5– 11.

23. *Днепров, А. Г*. Защита детей от компьютерных опасностей (+ CD) / А. Г.Днепров. – СПб.: Питер, 2008. – 192 с.

24. Доктрина информационной безопасности Российской Федерации // Указ Президента РФ № Пр-1895 от 9.09.2000.

25. *Доценко, Е. Л.* Психология манипуляции: феномены, механизмы, защита / Е. Л. Доценко. – М.: Речь, 2004. – 304 с.

26. *Дубин, Б. В.* Слухи как социально-психологический феномен / Б. В. Дубин, А. В. Толстых // Вопросы психологии. – 1993. – № 3. – С. 15-31

27. *Загородников, С. Н.* Основы информационного права : учеб. пособие для студентов вузов / С. Н. Загородников, А. А. Шмелев. – М.: Акад. Проект : Парадигма, 2005. – 192 с.

28. Информационная безопасность России / Ю. С. Уфимцев, Е. А. Ерофеев и др. – М.: Экзамен, 2003. – 560 с.

29. Информационное оружие, как средство ведения информационного противоборства [Электронный ресурс]. – Электрон. текстовые дан. – Режим доступа: http://www.vrazvedka.ru/main/analytical/lekt-03.shtml, свободный. – Загл. с экрана.

30. Информационно-психологическая и психотронная война : хрестоматия. – Мн.: Харвест, 2003. – 432 с.

31. *Кара-Мурза, С.* Манипуляция сознанием / С. Кара-Мурза. – М.: Эксмо, 2005. – 832 с.

32. *Караяни, А. И.* Слухи как средство информационно-психологического противодействия / А. И. Караяни // Психологический журнал. – 2003. – № 6. – Том 24.

33. *Карпов, А. В.* Психология групповых решений / А. В. Карпов. – М.: Ярославль, 2000. – 532 с.

34. *Карчевский, Н. В.* Компьютерные преступления: определение, объект и предмет [Электронный ресурс] / Н. В. Карчевский. – Электрон. текст. дан. – Режим доступа: http://www.ifap.ru/pi/05/karchev.htm, свободный. – Загл. с экрана.

35. *Козлов, В. Е.* Теория и практика борьбы с компьютерной преступностью / В. Е. Козлов. – М.: Горячая линия-Телеком, 2002. – 336 с.

36. *Колесникова, Т. И.* Психологический мир личности и его безопасность / Т. И. Колесникова. – М.: ВЛАДОС-ПРЕСС, 2001. – 176 с.

37. *Колин, К. К.* Социальная информатика : учеб. пособие для студентов вузов / К. К. Колин. – М.: Акад. Проект : Фонд «Мир», 2003. – 432 с.

38. *Корделлан, К.* Дети процессора: Как Интернет и видеоигры формируют завтрашних взрослых / К. Корделлан, Г. Грезийон ;

пер. с фр. А. Лущанова. – Екатеринбург: У-Фактория, 2006. – 272 с.

39. *Корнилова, Т. В*. Психология риска и принятия решений / Т. В. Корнилова. – М.: Аспект Пресс, 2003. – 286 с.

40. *Кравченко, А. В*. Интернет и компьютерный терроризм [Электронный ресурс] / А. В. Кравченко. – Электрон. текст. дан. – Режим доступа: http://www.crime-research.ru/library/kravch.htm, свободный. – Загл. с экрана.

41. *Крысько, В. Г*. Секреты психологической войны (цели, задачи, методы, формы, опыт) / В. Г. Крысько. – Мн.: Харвест, 1999. – 448 с.

42. *Куприянов, А. И*. Основы защиты информации : учеб. пособие для студ. высш. учеб. заведений / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. – М.: Издательский центр «Академия», 2006. – 256 с.

43. *Лисичкин, В. А*. Третья мировая (информационно-психологическая) война / В. А. Лисичкин, Л. А. Шелепин. – М.: Институт социально-политических исследований АСН, 2000. – 304 с.

44. *Макаренкова, В*. Видеоигры в информационной и психологической борьбе / В. Макаренкова // «Зарубежное военное обозрение». – 2005. – № 2.

45. *Мельников, В. П*. Информационная безопасность : учеб. пособие для студентов сред. проф. образования / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – М.: Академия, 2005. – 336 с.

46. *Мельникова, А. А*. Язык и национальный характер. Взаимосвязь структуры языка и ментальности / А. А. Мельникова. – СПб.: Речь, 2003. – 320 с.

47. Методика информационной безопасности / Ю. С. Уфимцев, В. П. Буянов и др. – М.: Экзамен, 2004. – 544 с.

48. *Миронова, Т. Л*. Русский язык и национальная безопасность [Электронный ресурс] / Т. Л. Миронова. – Электрон. текстовые дан. – Режим доступа: http://www.lindex.lenin.ru/Lindex4/Text/8770.htm, свободный. – Загл. с экрана.

49. *Моляков, А*. Особенности проявления паники в условиях экологического бедствия / А. Моляков // Психологический журнал. – 1992. – № 2. – Том 13.

50. *Назаретян, А. П*. Агрессивная толпа, массовая паника, слухи / А. П. Назаретян. – СПб.: Питер, 2004. – 192 с.

51. *Нарицын, Н. Н.* Азбука психологической безопасности / Н. Н. Нарицын. – М.: Русский журнал, 2000. – 224 с.

52. *Нечаев В. В.* Человек и информационная цивилизация – ритмо-информациологический подход / В. В. Нечаев, А. В. Дарьин // Проблемы информатизации: теоретич. и науч.-практич. журнал / РАН; Мин-во науки и технологий РФ. – 1999. – Вып. 1.

53. *Номоконов, В. А.* Глобализация информационных процессов и преступность [Электронный ресурс] / В. А. Номоконов. – Электрон. текст. дан. – Режим доступа: http://www.crimeresearch.ru/library/nomokon.htm, свободный. – Загл. с экрана.

54. Гражданский кодекс Российской Федерации № 230-ФЗ от 18.12.2006.

55. Об информации, информационных технологиях и о защите информации // Закон Российской Федерации № 149-ФЗ от 27.07.2006.

56. О государственной тайне // Закон Российской Федерации № 5485-1 от 21.07.1993.

57. *Одинцов, А. А.* Экономическая и информационная безопасность : справ. : учеб. пособие для студентов вузов / А. А. Одинцов. – М.: Экзамен, 2005. – 576 с.

58. *Одинцов, А. А.* Экономическая и информационная безопасность предпринимательства : учеб. пособие для студентов вузов / А. А. Одинцов. – М.: Академия, 2006. – 336 с.

59. *Оганджанян, Ш.* Чем промывают мозги / Ш. Оганджанян // Всё ясно. – 2006. – № 4 (62). – С. 39-41.

60. Основы информационной культуры : учеб.-метод. пособие / авт.-сост. В. И. Золотарева [и др.]. – М.: МИФИ, 2005. – 128 с.

61. *Олпорт, Г.* Становление личности: избранные труды / Г. Олпорт. – М.: Смысл, 2002.

62. *Петров В. П.* Информационная безопасность человека и общества: учебное пособие / В. П. Петров, С. В. Петров. – М.: Изд-во НЦ ЭНАС, 2007. – 336 с.

63. *Плаус, С.* Психология оценки и принятия решений / С. Плаус. – М.: Филинъ, 1998. – 368 с.

64. *Пономарев, Д. А.* Информационные технологии как криминогенный фактор организованной преступности в условиях глобализации [Электронный ресурс] / Д. А. Пономарев. –

Электрон. текст. дан. – Режим доступа: http://www.ifap.ru/pi/06/r16.htm, свободный. – Загл. с экрана.

65. *Почепцов, Г. Г.* Информационные войны / Г. Г. Почепцов. – М.: Рефл-бук ; К.: Ваклер, 2001. – 576 с.

66. *Почепцов, Г. Г.* Психологические войны / Г. Г. Почепцов. – М.: Рефл-бук ; К.: Ваклер, 2001. – 528 с.

67. Правовое обеспечение информационной безопасности : учеб. пособие для студентов вузов / С. Я. Казанцев, О. Э. Згадзай, Р. М. Оболенский и др.; под ред. С. Я. Казанцева. – М.: Академия, 2005. – 240 с.

68. Психология экстремальных ситуаций / сост. А. Е. Тарас, К. В. Сельченок. – М.: АСТ, Мн.: Харвест, 2001. – 480 с.

69. *Райнер, П.* Застывший взгляд / П. Райнер. – М.: Evidentis, 2003. – 224 с.

70. Растим здоровых, умных, добрых: воспитание младшего школьника : пособ. для средн. и высш. педагогич. учебн. заведений / сост. Л. В. Ковинько. – М.: Академия, 1996. – 288 с.

71. Реклама: внушение и манипуляция: учеб. пособие / сост. Д. Я. Райгородский. – Самара: БАРАХ-М, 2001. –752 с.

72. *Розен, Э.* Анатомия слухов: маркетинговые приемы / Э. Розен. – СПб.: Питер, 2006. – 240 с.

73. *Рубанов В. А.* Информационная безопасность России в условиях глобализации [Электронный ресурс]. – Электрон. текстовые дан. – Режим доступа: http://www.oxpaha.ru/analytics, свободный. – Загл. с экрана.

74. *Садердинов, А. А.* Информационная безопасность предприятия : учеб. пособие / А. А. Садердинов, В. А. Трайнев, А. А. Федулов. – 2-е изд. – М.: Дашков и К, 2005. – 336 с.

75. *Светлакова, Н. Б.* Реклама, которая вас убивает / Н. Б. Светлакова. – М.: Вече, 2007. – 176 с.

76. *Синельников, В. В.* Таинственная сила слова. Формула любви. Как слова воздействуют на нашу жизнь / В. В. Синельников. – М.: Центрполиграф, 2006. – 255 с.

77. *Спенсер, Д.* «Да» или «Нет» / Д. Спенсер. – СПб.: Питер Пресс, 1996. – 128 с.

78. *Столяренко А. М.* Экстремальная психопедагогика / А. М. Столяренко. – М.: ЮНИТИ-ДАНА, 2002. – 608 с.

79. *Тоффлер Э.* Третья волна. – М.: АСТ, 2004. – 783с.

80. *Тоффлер, Э.* Шок будущего. – М.: АСТ, 2004. – 557 с.

81. Филин В. А. Видеоэкология. Что для глаза хорошо, а что – плохо / В. Филин. – М.: Видеоэкология, 2006. – 512 с.

82. *Харрис, Р.* Психология массовых коммуникаций / Р. Харрис. – СПб.: Прайм-ЕВРОЗНАК, 2002. – 448 с.

83. *Черноушек, М.* Психология жизненной среды / М. Черноушек ; пер. с пол. И. И. Попа. – М.: Мысль, 1989. – 176 с.

84. *Шелли, Л.* Организованная преступность, терроризм и киберпреступность [Электронный ресурс] / Л. Шелли ; пер. с англ. Т. Л. Тропиной. – Электрон. текст. дан. – Режим доступа: http://crime.vl.ru/docs/stats/stat_123.htm, свободный. – Загл. с экрана.

85. *Шнайер, Б.* Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер. – СПб.: Питер, 2003. – 368 с.

86. *Щербаков, А. Ю.* Введение в теорию и практику информационной безопасности / А. Ю. Щербаков. – М.: Издатель Молгачева С. В., 2001. – 352 с.

87. *Эмото, М.* Послания воды: Тайные коды кристаллов льда / М. Эмото; пер. с англ. О. Горбунова. – М.: ООО Изд-во «София», 2006. – 96 с.

88. *Эриксен, Т. Х.* Тирания момента. Время в эпоху информации / Т. Х. Эриксен; пер. с норв. – М.: Весь Мир, 2003. – 208 с.

89. *Ярочкин, В. И.* Система безопасности фирмы / В. И. Ярочкин. – М.: Ось-89, 2003. – 352 с.

90. *Ярочкин, В. И.* Информационная безопасность : учеб. для студентов вузов / В. И. Ярочкин. – М.: Акад. Проект, 2008. – 544 с.

91. Язык наш поводырь наш в рай или ад : сб. статей / под ред. Г. Емельяненко. – СПб.: Изд-во Л.С. Яковлевой, 2001. – 336 с.

92. Jet Info, информационный бюллетень [Электронный ресурс]. – Электрон. текстовые дан. – Режим доступа: http://www.jetinfo.ru, свободный. – Загл. с экрана.

ПРИЛОЖЕНИЯ

Приложение 1

Видеоэкология

Проблемы видеоэкологии наиболее характерны для больших городов, где окружающая визуальная среда не соответствует физиологическим нормам зрения. Применение новых конструкционных материалов в городском строительстве обусловило изменение вида современного города. Здесь преобладает темно-серый цвет зданий, прямые линии и углы городских строений, статичность построек и обилие больших плоскостей. Все это изолировало человека от естественной визуальной среды и обусловило на территориях современных городов наличие «неблагоприятных» для зрения человека полей. В видеоэкологии такие поля называют гомогенными и агрессивными.

В гомогенной визуальной среде из-за дефицита зрительных элементов мозг получает недостаточно информации от органа зрения. В городах гомогенная среда может быть образована торцами зданий, большими стеклянными поверхностями, асфальтовым покрытием, цветовой скудостью окраски зданий, пустырями и неблагоустроенными участками.

Агрессивное поле содержит слишком много одинаковых зрительных элементов. Агрессивные поля бывают трех видов: одинаковые вертикальные линии, большое количество маленьких, равномерно рассредоточенных по поверхности элементов, от которых рябит в глазах, и концентрические кольца. Примерами в городе могут служить большое количество одинаковых окон на стене многоэтажного здания, стены, выложенные кафельной плиткой, решетки правильных геометрических форм и др.

Исследованиями установлено, что если в поле зрения попадает одновременно более 10–13 одинаковых элементов, то человек уже готов к раздражению. Так уж устроен наш глаз, что каждую секунду готов за что-то «зацепиться», зафиксировать четко выделяющуюся и различимую деталь. Этой деталью может быть и лепная фигура на фронтоне здания, башенка, арка и даже труба на крыше здания.

Агрессивные поля провоцируют синдром «неосознанной агрессии» – хулиганство, пьянство, сквернословие. Чем хуже визуальная среда, тем больше антиобщественных поступков, тем выше раздражительность. У жителей, проживающих в микрорайонах, где господствуют голые стены, асфальт, железобетон, прямые тротуары, одинаковые бордюры, выстроенные в ряд гаражи-«ракушки», радость зрительного общения с окружающим миром постепенно уступает место раздражению. Возникает некий подсознательный, зачастую неконтролируемый, протест, желание сменить обстановку. И как следствие – пренебрежительное отношение к своему дому, жилищу, к лужайке во дворе. А отсюда – вытоптанные газоны, испорченные лифты и телефоны-автоматы, грязные подъезды.

Неблагоприятная визуальная среда приводит к расстройству зрения, влияет на состояние центральной нервной системы. Обнаружено, что у городских школьников близорукость встречается в 1,5–2 раза чаще, чем у сельских, что обусловлено урбанизированной визуальной средой. У людей с больной нервной системой в агрессивной визуальной среде может появиться головокружение, тошнота, у эпилептиков – очередной припадок, а у здоровых людей могут обнаружиться отклонения в психике. По данным Всемирной организации здравоохранения (ВОЗ), процессы урбанизации ведут к неуклонному росту психических заболеваний. За последнее десятилетие число психически больных людей в Москве возросло на порядок. Врачи-психиатры считают, что 80% их пациентов в крупных городах имеют «синдром большого города», основные признаки которого – подавленное состояние, психическая неуравновешенность, агрессивность.

Агрессивность зрительной среды резко возрастает при дополнительном шумовом воздействии. Установлено, что ритмизация сигналов, которые поступают на входы двух основных сенсорных систем человека (зрения и слуха), ведет к росту агрессивности. По мнению В. А. Филина, при этом на зрительный вход поступают сигналы от «агрессивных полей», состоящих из одинаковых элементов, а также от равномерно перемещающихся механизмов (эскалаторы, лифты, колеса, конвейеры), а на слуховой вход – от ритмической музыки. Ритмические сенсорные сигналы могут провоцировать эпилептические припадки.

В первую очередь это касается дискотек, где ритмизация слуховых и световых сигналов достигает предельных величин.

Агрессивно и многолюдье в городах. Толчея на улицах, в метро воспринимается как среда из большого числа одинаковых видимых объектов. Так, спускаясь в час пик по эскалатору, человек видит большое число головных уборов, но из-за высокой плотности толпы он не может разглядеть всего человека. Многолюдье становится активным стрессором.

Телевизор – та же самая неблагополучная визуальная среда. Глаз не любит того, что так часто допускает телеэкран – наложение одного изображения на другое. Зрению комфортно, если вторая картинка начинается после того, как оборвалась первая. Когда на экране сразу два кадра, механизмы глаза приходят в замешательство. Для аппарата аккомодации большая нагрузка – чередование крупного и мелкого планов, как это часто делается в видеоклипах.

Приложение 2

Улучшение визуальной среды обитания

Неблагополучная визуальная среда квартир преследует нас буквально повсюду: одноцветный, без рисунка кафель, унылые жалюзи, подвесные потолки, обои в клеточку, мебель в полосочку. Однотонные симметричные «стенки» с повторяющимся ритмом полок с точки зрения видеоэкологии считаются неправильными. Нет необходимости срочно браться за дорогостоящий ремонт и замену мебели. Иногда бывает достаточно добавить в интерьер несколько ярких живых деталей: зелень, цветы, шторы с замысловатым рисунком, картины, эстампы, календари, яркая безделушка.

Стены – самые что ни на есть гомогенные плоскости, которые обязательно нужно чем-нибудь разнообразить. Ниши и арки зрительно разбивают пространство на более мелкие части. Для тех же целей подойдут картины (натюрморт или пейзаж), фотографии. Обои для стен лучше выбрать с растительным рисунком. Другое средство борьбы с агрессивными голыми стенами – полки и стеллажи. Хорошо, если расположение полочек, уставленных мелкими статуэтками и сувенирами, будет противоречить всяким законам геометрии. Грамотно расположенные в интерьере жилища цветы прекрасно украсят стену. Хорошо, если они стоят на разноуровневых подставках.

Линолеум под ногами в клеточку или ламинат в полосочку можно застелить паласами с ненавязчивыми неконтрастными рисунками. От агрессии прямых линий потолка поможет лепнина. В старинных зданиях гипсовые цветочки скругляли углы комнаты, а в современных условиях помогут жидкие обои.

Ярко-полосатую обивку мебели можно накрыть тканью с асимметричным рисунком или художественной вышивкой. Следует отказаться от постельного белья и ночной рубашки в горошек, в полосочку или другого агрессивного рисунка.

Приложение 3

Правила пользования Интернетом (рекомендации для родителей)

1. Установите четкие правила пользования Интернетом для ребёнка, чтобы контролировать расписание, время подключения и способ использования им Интернета. Убедитесь, что установленные правила выполняются. Особенно важно контролировать выход ребёнка в Интернет в ночное время.

2. Ребёнок должен понять, что его виртуальный собеседник может выдавать себя за другого. Отсутствием возможности видеть и слышать других пользователей легко воспользоваться. «10-летний Интернет-друг» ребёнка по чату в реальности может оказаться злоумышленником, поэтому запретите ребенку назначать встречи с виртуальными знакомыми.

3. Не разрешайте ребенку предоставлять личную информацию через Интернет. Ребенку нужно знать, что нельзя через Интернет давать сведения о своем имени, возрасте, номере телефона, номере школы или домашнем адресе, и т.д. Убедитесь, что у него нет доступа к номеру кредитной карты или банковским данным. Научите ребёнка использовать прозвища (nik) при общении через Интернет: анонимность – отличный способ защиты. Не выкладывайте фотографии ребёнка на веб-страницах или публичных форумах.

4. Оградите ребёнка от ненадлежащего веб-содержимого. Научите его, как следует поступать при столкновении с подозрительным материалом, расскажите, что не нужно нажимать на ссылки в электронных сообщениях от неизвестных источников, открывать различные вложения. Такие ссылки могут вести на нежелательные сайты, или содержать вирусы, которые заразят компьютер. Удаляйте со своего компьютера следы информации, которую нежелательно обнаружить ребенку (журнал событий браузера, электронные сообщения, документы и т.д.).

5. Установите на компьютер антивирусную программу.

Приложение 4

Снижение телеагрессии у детей

Согласно имеющимся исследованиям, наблюдаемое насилие скорее всего увеличит вероятность агрессивного поведения представителей аудитории при следующих условиях:

1) если они не видят, что агрессор наказан или пострадал каким-либо иным образом;

2) если они не считают агрессию неприемлемой или неоправданной;

3) если они идентифицируют себя с агрессорами, представляя себя на их месте;

4) если они фокусируют внимание на агрессии, а не на других аспектах происходящих событий;

5) если они психологически не дистанцируются от увиденного или услышанного, например, не говорят себе, что всё происходящее на экране – неправда.

Роль семьи в снижении негативного влияния телевидения на ребёнка переоценить невозможно. Для родителей можно рекомендовать следующие правила поведения, снижающие телеагрессию:

1. Ограничивайте время просмотра телепередач.

2. Выбирайте программу по возрасту ребёнка и не позволяйте ему смотреть особенно агрессивные сцены.

3. Анализируйте вместе с ребенком и комментируйте ему по ходу то, что видите. Подчеркивайте страдание жертв агрессии.

4. Критикуйте. Скажите ребенку, что Вы думаете о жестокости, укажите другие способы разрешения конфликта, приводите примеры из других программ и из Вашей жизни.

5. При просмотре даже самых жестоких сцен огромное значение имеет то, с чем столкнулся ребёнок перед этим и что происходит во время просмотра. Если ребёнок сидит у на коленях у родителей, то он по-другому переживает фильм, чем тогда, когда смотрит сам, а перед этим был наказан. Не оставляйте ребёнка одного перед телевизором и дайте ему понять, что он смотрит.

6. Не злоупотребляйте телевизором сами. Пойдите с ребенком в лес, парк, почитайте книгу, сходите на выставку, поговорите с ним о Ваших и его проблемах.

Приложение 5

Гигиенические требования к просмотру телепередач

Существует ряд требований к гигиене просмотра телепередач: достаточное расстояние от экрана до телезрителя (не ближе 2 м, если размер экрана по диагонали 35–47 см, и на расстоянии 3–5 м, если размер экрана 50–61 см по диагонали), дополнительная подсветка вечером и частичное затемнение днем, уровень громкости, не превышающий естественную потребность. Для дошкольника оно не должно превышать 1,5 часа в неделю, для младшего школьника – 3 часа, включая просмотры и в выходные дни, для подростка – не более 5 часов. Ставить телевизор надо над полом на высоте 80–90 см.

Часто разлагающая работа средств массовой информации не видна сразу. Дети могут не проявлять навязанных им убеждений, например, до подросткового возраста. В чрезмерном увлечении детей телевидением виноваты, в первую очередь, взрослые, неправильно понимающие роль телевидения в воспитании. Направлять и корректировать отношение детей к телевидению можно только до тех пор, пока у них не сформировалась привычка проводить время перед телевизором. Единственно надёжный путь – своевременно заинтересовать детей другими источниками информации, которые способны сделать жизнь человека интересной и эмоционально богатой.

Приложение 6

Основы грамотного восприятия средств массовой информации ребёнком

Родителям следует внимательно относиться к тому, какие телевизионные программы смотрят их дети, в какие компьютерные игры играют, какие журналы читают. Однако, учитывая тот факт, что средства массовой информации окружают нас повсюду и не могут поддаваться жесткому контролю со стороны родителей, одним из методов фильтрации поступающей информации является развитие у детей способностей правильно ее анализировать и оценивать. Другими словами, дети должны обладать грамотностью общения с СМИ.

Так же как дети учатся относиться критически к доступной им печатной информации, так же они должны поступать с тем, что видят и слышат. Можно научить ребёнка видеть явные и скрытые стороны информации, поступающей из СМИ.

Основы грамотного общения со СМИ, которые должен знать ребёнок, следующие:

1) всё, что мы видим на экранах наших телевизоров, читаем на страницах прессы, слушаем по радио и т.д., создано руками обычных людей. Над созданием любого сообщения трудится определенная группа людей, которые решают, каким ему быть, что пускать в эфир, а что можно «вырезать». Любое сообщение преследует конкретную цель.

2) любой вид средств массовой информации пользуется определенными правилами или говорит на конкретном языке. Например, для привлечения внимания читателей газеты, некоторые заголовки печатаются более крупным шрифтом, звуковые СМИ используют музыку для стимулирования определенных человеческих эмоций. Когда дети будут знать об этих нюансах, они начнут понимать, с какой целью делается то или иное сообщение, и не будут безропотно попадать под влияние.

3) одно и то же сообщение будет восприниматься поразному разными людьми. То, как человек воспринимает получаемую информацию, зависит от его личного жизненного опыта, возраста, моральных ценностей, воспоминаний и образования.

4) каждое сообщение средств массовой информации несет свои ценности и точку зрения. Дети должны уметь сравнивать свои ценности с предлагаемыми. Важно, чтобы ребёнок знал, что у него есть выбор, принимать или не принимать их.

Помимо ответов на вопрос «как и почему создаются сообщения СМИ?», родители или другие взрослые могут помочь детям в разном возрасте развивать навыки грамотности восприятия поступающих сообщений. Следующие упражнения заставят задуматься детей над тем, кто работает над созданием таких сообщений и почему.

1. Пусть ребёнок выберет какое-нибудь сообщение и ответит на приведенные ниже вопросы. Наиболее удобны в этом случае телевизионные рекламные выпуски, т.к. они обычно представлены в краткой форме и содержат убедительные слова и выражения, образы и музыкальное оформление. Также можно поработать над видеоиграми или музыкальными программами.

Вопросы:

а. Опишите людей, которые заняты в создании этого сообщения. Это могут быть писатели, фотографы, дизайнеры, профессионалы спецэффектов или каскадеры.

б. В зависимости от того, какого рода сообщение вы выбрали, поговорите о выборе используемых визуальных эффектов (освещение, угол съемки, создание образов с помощью компьютерной графики и т.д.). Можно поговорить о звуковом оформлении (какие слова произносятся, кто их произносит, музыкальное сопровождение, спецэффекты и др.). И, наконец, задайте вопросы: Для чего были выбраны все эти эффекты для данного сообщения? Усиливают ли они значение и восприятие предлагаемой информации?

в. Какие цели преследуют создатели сообщения: подача информации, побуждение вас к определенным действиям (например, покупка конкретного продукта), просто развлечение и создание хорошего настроения? Часто настоящее значение сообщения спрятано как бы между строк.

г. Что думает ваш ребёнок об услышанном или увиденном? Согласен он или нет с предлагаемым сообщением и почему? Причины, по которым сообщение может быть принято или отвергнуто, – его достоверность и совпадение с личными моральными ценностями.

По мере того, как ребёнок научится отвечать на подобные вопросы, он получит возможность видеть настоящий смысл предлагаемых сообщений.

2. Игра «Определите спонсоров». Помогите детям научиться различать обычные программы и рекламную информацию их спонсоров. Это может быть не так уж просто во время просмотра детских передач, т.к. многие рекламные ролики представляют героев любимых телевизионных передач.

Проведите «тест вкуса» для сравнения широко рекламируемых марок с общепринятыми или не рекламируемыми. Проведите эксперимент, например, с сухими завтраками или безалкогольными напитками. Посмотрите, могут ли ваш ребёнок и его друзья определить разницу и какова степень влияния рекламы на их оценки.

Просмотрите газетные заголовки, фотографии и расположение статей на странице в газете или журнале. Как они влияют на выбор предмета чтения ребёнка? Прочтите несколько статей и проанализируйте, насколько их содержание соответствует заголовкам и фотографиям.

При совместном просмотре кинофильмов, видеокассет и видеоигр, поговорите с ребенком о том, что происходит на экране и насколько происходящее соответствует реальной жизни. Например, сможет ли человек вести автомобиль на бешеной скорости по узкой улице и не разбить автомобиль?

При покупке продуктов сравнивайте продукты с рекламными «завлекалочками», знакомыми ребенку. Обращайте внимание на ингредиенты, наклейки и упаковку. Говорится ли что-нибудь об этом в рекламе? Дает ли реклама конкретную информацию о продукте? Насколько реальный продукт соответствует рекламной информации или изображению на упаковке?

Сколько марок пива, сигарет или других подобных продуктов может назвать ребёнок? Если он назовет хотя бы один, это может стать первым шагом для начала разговора о влиянии рекламы. Обсудите с ним степень риска для здоровья употребление этих продуктов и, что говориться об этом в рекламной информации.

Смотрите с детьми музыкальные видеоклипы. О чем они? Соответствует ли видео-история словам песен? Какие чувства вызывает у вашего ребёнка просмотр видео? Замечает ли ребёнок

какие-нибудь стереотипные образы, насилие или эротику? Показаны ли факты табакокурения, употребления алкогольных напитков или наркотиков? Попробуйте посмотреть видеоклипы с выключенным звуком и посмотрите, насколько отличается их восприятие.

Кроме указанных упражнений, для формирования грамотного восприятия средств массовой информации у детей родителям рекомендуется придерживаться следующих рекомендаций:

1. Составьте план. Заранее спланируйте время, объем и вид получаемой информации от СМИ так же, как вы планируете любую другую деятельность.

2. Ограничьте время. Ограничьте время просмотра телевизора, видеомагнитофона, DVD, игры на компьютере и сеанса в сети Интернет. Американская академия педиатрии не рекомендует выделять более 1–2 часов в день на просмотр телевидения для старших детей, а детям до 2 лет смотреть телевизор вообще не стоит.

3. Выделите основные направления получаемой информации. Помогите детям и подросткам выбрать видеофильмы, программы для просмотра или видеоигры, которые соответствуют их возрасту и интересам. Заведите привычку составлять своеобразный рейтинг передач для просмотра вашими детьми и давать родительские наставления, касающиеся информации, поступающей из СМИ. Используйте этот рейтинг в принятии решений, какие сообщения СМИ следует узнать вашим детям.

4. Будьте настойчивы и доступны при постановке правил получения информации вашими детьми. Если вы не одобряете их выбор, объясните, почему и помогите им выбрать что-то более подходящее по вашему мнению.

5. Не ставьте телевизоры, видеомагнитофоны, видео- и DVD приставки или компьютеры в детской спальне. Поставьте их там, где вы сможете контролировать их использование. Если же все-таки эта техника находится в спальне, вы должны быть в курсе их вкусов. Если у них есть доступ в Интернет, контролируйте их, когда они находятся в сети.

6. Сделайте просмотр телепередач и фильмов совместным семейным занятием. Используете малейшую возможность для совместного просмотра, прослушивания или прочтения информации, интересующей детей, и дальнейшего ее обсуждения.

Научите детей во время непосредственного получения информации оспаривать ее или ставить под вопрос. Особенно это касается актов насилия, сомнительных фактов, обманчивых соображений или рекламных акций продукции, вредной для здоровья.

7. Задавайте вопросы детям, вызывайте их на дискуссию, старайтесь сформировать жизненную позицию ребёнка – быть критичным к увиденному или услышанному из СМИ. Сравните, насколько совпадают жизненные ценности, которые вы стараетесь привить детям и те, которые преподносятся с экранов телевизоров или страниц прессы.

8. Будьте внимательны к побочным эффектам средств массовой информации. Часто родители смотрят сквозь пальцы на получение их детьми информации, если только она не содержит явных признаков насилия или сексуальной окраски.

Приложение 7

Основы критического восприятия рекламы ребёнком

Родители должны общаться с детьми и обсуждать рекламу понятным для них языком, используя образные сравнения, выражения и понятия. Например, подростку можно сказать, что реклама превращает товар в «поп-звезду». Она наряжает его, делает макияж, освещает яркими прожекторами, в общем, сильно приукрашивает. Таким образом, рекламодатель как бы выделяет свой товар «из толпы», надеется вызвать в нас интерес и желание купить именно его «звезду». Для наглядности сходите с ребенком в магазин и спросите у него, какие из представленных на полках продуктов больше всего обращают на себя внимание – яркой упаковкой или необычным дизайном. А потом объясните, что упаковка также служит рекламным целям и ничего не говорит о содержании, то есть не факт, что продукт будет отвечать требованиям ребёнка (вкусом или качеством). Подростку необходимо объяснить, что реклама – это не действительность, а всего лишь броская мишура, не позволяющая товару остаться незамеченным.

Детям помладше полезно сначала рассказать, что такое реклама и для чего она нужна. В качестве примера родители могут использовать рекламные объявления из журналов или газет. Например, психологами применяется процедура, когда ребенку показывают образец рекламы и задают следующие вопросы:

– Что ты видишь, глядя на этот рекламный плакат?

– Что тебе в нем нравится или не нравится?

– Какой товар он рекламирует?

– Что ты теперь думаешь об этом товаре?

– Какие вопросы тебе следует задать, прежде чем купить этот товар?

При этом ребёнка поощряют искать дополнительную информацию к той, что дает рекламное объявление. Как пользоваться этим товаром? Хорошо ли он работает? Действительно ли покупателю нужно именно это? Какие существуют аналоги, и по какой цене?

Подобные вопросы часто вызывают оживленную дискуссию между детьми и родителями. Более того, они станут первыми

шагами ребёнка на пути к разумному потреблению товаров и услуг. Дети должны знать, что целью рекламы является не развлечь читателя или зрителя, а заставить его купить, раскошелиться. От печатных объявлений можно переходить к телерекламе и поговорить о том, что помогает товару выглядеть таким привлекательным. Полезно вместе с ребенком составить список положений из рекламного ролика, а затем разбить их на две группы: факты и мнения. А потом попросить его подумать, какие из положений могут быть верны, а какие бездоказательны.

Что касается малышей лет до четырех-пяти, то их лучше вообще не знакомить с телевидением (есть видеодиски, где фильмы и мультики без рекламы) или, по крайней мере, выключать на время рекламы звук. Не спешите приохотить детей к телевизору – в наш компьютеризованный век они еще успеют пообщаться с говорящим экраном. В первые годы жизни ребёнка лучше приучать к чтению и живому, естественному, традиционному общению – сделать так, чтобы телевизор впоследствии не стал конкурентом родителям.

Когда дети смотрят телевизор, присутствующим рядом взрослым следует убедиться, что малыши знают, где реклама начинается, а где заканчивается, а то они могут принять ее за часть передачи. Это можно сделать, сказав в самом начале ролика: «о, это реклама. После нее будет продолжение программы». Ребёнка несложно научить узнавать начало рекламного блока по непродолжительному затемнению экрана или фразам типа: «... оставайтесь с нами, мы продолжим после рекламной паузы...». Просматривая рекламный ролик, необходимо разговаривать с ребенком о том, какие его элементы могут ввести в заблуждение – это способствует формированию ответственности, навыка самостоятельного анализа увиденного, что, в свою очередь, приводит к росту чувства компетентности и уверенности в принятии решений.

Приложение 8

Свод правил по защите персональной информации

Канадская ассоциация стандартов приняла в сентябре 1995 года стандарт приватности под названием *«Свод правил по защите персональной информации»*. Свод правил обеспечения приватности стал для организаций пошаговой инструкцией по защите приватности личности. Эти шаги включают, в первую очередь, определение целей сбора информации, получение разрешения от людей, ограничение сбора, обеспечение точности и принятие адекватных мер против случайного разглашения.

«Свод правил по защите персональной информации» базируется на десяти независимых принципах:

1. Подотчетность. Организация несет ответственность за находящуюся в её ведении персональную информацию и должна назначить одного или нескольких сотрудников, отвечающих за выполнение организацией настоящих принципов,

2. Определение целей. Цели, с которыми осуществляется сбор персональной информации, должны быть определены до начала сбора информации.

3. Разрешение. Информирование человека и получение разрешения от него являются обязательными для сбора, использования или раскрытия персональной информации, за исключением случаев, когда это невозможно.

4. Ограничение сбора. Сбор персональной информации должен быть ограничен в соответствии с целями сбора, определенными организацией. Информация должна собираться честными и законными методами.

5. Ограничения на использование, раскрытие и хранение. Персональная информация не должна использоваться или раскрываться в целях, отличных от тех, для которых она собрана, кроме как по разрешению человека или в связи с требованиями закона. Персональная информация не должна храниться дольше, чем это необходимо для достижения заявленных целей.

6. Точность. Персональная информация должна быть настолько точной, полной и актуальной, насколько это необходимо для целей её использования.

7. Меры безопасности. Персональная информация должна быть защищена при помощи мер безопасности, уровень которых соответствует уровню её конфиденциальности.

8. Открытость. Организация должна предоставлять людям свободный доступ к информации о принятой в ней политике и методиках использования персональной информации.

9. Обеспечение доступа. По запросу, каждый человек должен быть проинформирован о существовании, использовании и раскрытии своей персональной информации, и ему должен быть предоставлен доступ к ней. Он должен иметь возможность оспорить точность и полноту информации, а также внести соответствующие поправки.

10. Обработка жалоб. Каждый человек должен иметь возможность направить ответственному сотруднику (или сотрудникам) организации жалобу по факту невыполнения изложенных принципов.

В нашей стране нормативно-правовая база по защите персональных данных граждан существует, был принят ФЗ «О персональных данных». Но с другой стороны, торговля государственными и коммерческими базами данных в России широко ведется с начала 90-х годов прошлого века.

Приложение 9

Видеоигры как средство информационно-психологической войны

Видеоигры являются широко используемой формой воздействия на людей с целью трансформации в нужном направлении их настроений, чувств, воли, внедрения в сознание необходимых идеологических и социальных установок, формирования определённых стереотипов мышления и поведения.

В видеоиграх всё рассчитано на сильное эмоциональное воздействие, а эмоции как раз и являются обходным путем к человеческому сознанию. Известно, что 80% всего запечатленного в памяти человека материала эмоционально окрашено, 16% – безразлично, 4% – носит неопределенный характер. Именно в воздействии на эмоционально-чувственную психологическую сферу человека путем эмоционального заражения заключается сущность психологической войны.

Огромный потенциал видеоигр как формы внушения определил их место в психологической и информационной войне. Сегодня компьютерные игры стали одним из самых действенных инструментов распространения государственной идеологии, формирования национального самосознания граждан, создания благоприятного образа страны и ее вооружённых сил в мире и т.д.

Индустрия развлечений превратилась в крупнейший производитель и распространитель американских идеологических концепций. После терактов 11 сентября 2001 года в Нью-Йорке и Вашингтоне США предложили миру концепцию борьбы с международным терроризмом. Новая идеология стала идейным оправданием и обеспечением долговременных геостратегических планов Белого дома по установлению нового мирового порядка при доминирующей роли Соединенных Штатов. Стремясь внедрить в сознание населения планеты идею борьбы с международным терроризмом, США, занимающие ведущее место в мировой игровой индустрии, создают и распространяют компьютерные игры, сюжет которых строится на антитеррористической тематике.

Главная идея большинства видеоигр, разработанных в этой стране – спасение мира американским суперсолдатом от угрозы международного терроризма. С помощью подобного рода видеоигр формируется образ современного военнослужащего армии США. Именно его роль чаще всего предлагают принять игроку в американских видеоиграх. Современный герой – бесстрашный, сильный, умный воин, способный противостоять значительно превосходящему по численности противнику, рискующий жизнью ради национальных интересов страны и блага всего мирового сообщества.

Поскольку международный терроризм объявлен основной угрозой миру, в борьбе с ним, по утверждению американских стратегов, допустимы все средства, в том числе силовые. Эта же идея заложена в современных видеоиграх. Они внедряют в сознание мировой общественности право сильного, формируют терпимое отношение к жестокости, насилию, вырабатывают стереотип решения конфликтных ситуаций с помощью оружия. Особенно это касается видеоигр из жанра «стрелялок». При этом происходит символизация американской армии как обладающей самым технологичным вооружением. Пропаганда превосходства в военной силе имеет своей целью убедить личный состав своей армии в грядущей победе, а население и военнослужащих противника в бесперспективности вооруженного сопротивления. Видеоигры, которые создаются по заказу Пентагона и используются как форма психологической борьбы, обычно распространяются бесплатно. По этому поводу древняя восточная мудрость гласит: «если хочешь легко забрать у человека что-то большое, дай ему какую-нибудь мелочь...».

Внедряя и закрепляя в сознании игроков образ врага, видеоигры не только склоняют общественное мнение к поддержке нынешних военных операций, но и подготавливают почву для будущих войн. В «войне XXI века» противником объявлены террористы и «государства-изгои». Поскольку понятие «международный терроризм» очень неопределенно, оно позволяет отнести к разряду противников любые неугодные США государство, нацию, группировку и т.д. Видеоигры конкретизируют образ потенциального врага. В распространяемых на Западе играх чаще всего в этом качестве представлены люди с восточным типом лица, что вписывается в объявленный Вашингтоном после

терактов 11 сентября 2001 года антитеррористический крестовый поход. По мере появления новых видеоигр список стран, на территории которых выполняют «миссию спасения мира» американские военнослужащие, стремительно увеличивается.

Наиболее велика роль видеоигр в психологической работе как традиционно важного компонента морально-психологической подготовки военнослужащих. Ее цель – обеспечить эмоционально-волевую устойчивость личного состава к внешним раздражителям в условиях реальной боевой обстановки. Основное преимущество видеоигр заключается в том, что при отсутствии реальной угрозы для жизни и здоровья обучающихся психологические условия виртуальной реальности приближены к боевым, то есть достигается эффект, психологически сравнимый с условиями реального боя. Видеоигры дают возможность приобрести опыт ведения военных операций заблаговременно, без существенных затрат и риска для жизни людей.

Огромное влияние, которое видеоигры оказывают на психику и подсознание пользователей, уже вызвало беспокойство политического руководства некоторых стран. Продолжительное наблюдение жестоких сцен и виртуальное участие в них ведут к снижению порога эмоциональной чувствительности к жестокости вообще, уменьшается вероятность того, что будет оказана помощь и пострадавшим в реальных ситуациях, насилие в играх усиливает восприятие мира как места, где царит зло и жестокость. Усиливается страх стать жертвой насилия, и в результате утверждается психология самозащиты и недоверия к окружающим. По мнению психологов чем чаще геймеры сталкиваются с жестокостью в играх, тем больше вероятность того, что они будут рассматривать насилие как наиболее эффективный способ решения конфликтов в реальной жизни.

Приложение 10

Кино как средство информационно-психологической войны

Кино как вид пропаганды способно оказывать чрезвычайно высокое эмоциональное воздействие. Оно активно генерирует в воображении зрителя иллюзорную картину мира в очень идеализированном виде. В соответствии с авторским замыслом кино может произвольно создавать у зрителя ощущение «справедливости» и моральной правоты того или иного персонажа, независимо от его действительной роли в истории. При этом пропагандистское влияние на человека происходит скрыто, на эмоциональном уровне, вне его сознательного контроля. Никакие рациональные контраргументы в этом случае не срабатывают.

> *На рациональном уровне мы все хорошо осознаем, кем был Адольф Гитлер. Однако используя игру талантливых актеров и специальные драматические приемы, кинорежиссер вполне может представить все так, что симпатии зрителей однозначно окажутся на стороне фюрера. Его преступления покажутся вовсе не преступлениями, а благородным делом – ведь сами жертвы будут выглядеть злодеями, заслуживающими быть убитыми. И сидящие в кинозале люди будут искренне рыдать, наблюдая как честный и благородный фюрер пускает себе пулю в висок в апреле 1945-го...*

Манипулирование ощущением «справедливости» того или иного персонажа активно использует Голливуд. Зная, что Америка, проиграв войну во Вьетнаме, тем не менее с успехом выиграла её на киноэкранах, создав известные американские боевики серии «Рэмбо». «Плохие парни» в американских боевиках всегда четко соответствуют текущему внешнеполитическому курсу Соединенных Штатов. Если в прошлые десятилетия киносупермены типа Рэмбо или Джеймса Бонда мужественно сражались преимущественно с коварными советскими шпионами и полковниками из КГБ, то по сюжету фильма, вышедшего в 2002 году, Агент 007 попадает в плен уже к северокорейцам (современным представителям «мировой оси зла») и подвергается там зверским пыткам.

Трудно переоценить то значение, которое экспансия западной масс-культуры вообще, и западного кинематографа в частности, сыграли в развале советской системы. Целенаправленно в общество были внедрены западная картина мира и западные стандарты жизни. Одной из причин поражения Советского Союза в холодной войне стал проигрыш именно на уровне масс-культуры. Советская пропагандистская машина не смогла создать привлекательный виртуальный мир, который был бы зрелищным, захватывающим, интересным для массовой аудитории и одновременно «правильно» интерпретировал мировую историю, пропагандировал советские ценности и образ жизни.

Еще одной популярной темой сегодня является переписывание истории второй мировой войны. Посмотрев американские блокбастеры, зрителю дают понять, что хребет нацизму был сломан не в Сталинграде и под Курском, а во время спасения из плена американского рядового Райана.

Успехи западной кинопропаганды на этом поприще столь значительны, что давно должны обеспокоить общественность в государствах с «незападным» типом культуры. Так, на вопросы, кто впервые создал атомную электростанцию, атомный ледокол, искусственный спутник Земли, самую мощную ракету-носитель, корабли на подводных крыльях и воздушной подушке, вывел человека в космос, одержал решающую победу во второй мировой войне, значительная часть российской (!) молодежи сегодня называет... Соединенные Штаты.

СЛОВАРЬ ОСНОВНЫХ ТЕРМИНОВ

Аутентификация – совокупность процедур, цель которых – доказательство того, что идентифицированная сущность является именно той, за которую она себя выдает.

База данных – объективная форма представления и организации совокупности данных (статей, расчетов и так далее), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ).

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.

Данные – фиксируемые в виде определенных сигналов воспринимаемые факты окружающего мира.

Дезинформация – распространение искаженных или заведомо ложных сведений для достижения определенных целей.

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Допуск к государственной тайне – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций на проведение работ с использованием таких сведений.

Доступ к сведениям, составляющим государственную тайну – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

Защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и

непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

Защита сведений, составляющих государственную тайну, и их носителей – деятельность органов защиты этой тайны, направленная на обеспечение безопасности информации, отнесенной к государственной тайне, предотвращение её утечки и её максимально эффективное использование.

Знание – форма существования и систематизации результатов познавательной деятельности человека.

Идентификация – отождествление, установление соответствия одной сущности другой.

Интеллектуальной собственность – совокупность исключительных прав на результаты интеллектуальной деятельности, а также на некоторые иные приравненные к ним объекты, такие как средства индивидуализации участников гражданского оборота и производимой ими продукции (работ, услуг).

Информатизация – организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.

Информационная безопасность – это защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры.

Информационная безопасность РФ – состояние защищённости её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Информационная война – комплекс мероприятий по достижению информационного превосходства путем воздействия на информацию, информационные процессы, информационные системы и компьютерные сети противника при одновременной защите своей информации, информационных процессов, информационных систем и компьютерных сетей.

Информационная картина мира – информационное поле, позволяющее адекватно воспринимать окружающий мир и взаимодействовать с ним, способствовать его и собственному развитию, осуществлять информационный обмен.

Информационная революция – преобразование общественных отношений из-за кардинальных изменений в сфере обработки информации.

Информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Информационная сфера (среда) – сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационное общество – концепция постиндустриального общества; ступень развития цивилизации, в которой главными продуктами производства являются информация и знания.

Информационное оружие – комплекс специализированных методов и средств, предназначенных для контроля информационных ресурсов объекта воздействия и временного или безвозвратного вывода из строя функций или служб информационной инфраструктуры в целом или отдельных ее элементов.

Информационный (общественный) резонанс – одновременное повышенное искусственное привлечение средствами массовой информации общественного внимания к тому или иному социальному или политическому событию, сопряжённое с замалчиванием других событий, имеющих равную информативную значимость.

Информационно-психологическая война – открытые и скрытые целенаправленные информационные воздействия социальных, политических, этнических и иных систем друг на друга с целью получения определенного выигрыша в материальной сфере, направленные на обеспечение информационного

превосходства над противником и нанесения ему материального, идеологического или иного ущерба.

Информационные продукты (продукция) – документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей.

Информационные процессы – процессы создания, сбора, обработки, накопления, хранения, поиска, распространения и потребления информации.

Информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других видах информационных систем).

Информационные услуги – действия субъектов (собственников и владельцев) по обеспечению пользователей информационными продуктами.

Информация – сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии, которые воспринимают информационные системы (живые организмы, управляющие машины и др.) в процессе жизнедеятельности и работы.

Коммерческая (служебная) тайна негосударственной организации – сведения, не являющиеся государственными секретами, которые связаны с производственной, управленческой, финансовой или иной деятельностью организации и распространение которых может нанести ущерб её интересам.

Компьютерное преступление – преступление, совершенное с помощью вычислительной техники и вычислительных сетей, направленное на незаконное похищение информации или приводящее к ее модификации либо разрушению.

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия её обладателя.

Массовая информация – предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы.

Международный информационный обмен – передача и получение информационных продуктов, а также оказание информационных услуг через Государственную границу Российской Федерации.

Общественное мнение – состояние массового сознания, заключающее в себе скрытое или явное отношение различных социальных общностей к проблемам, событиям действительности.

Общественное сознание – совокупность идей, взглядов, представлений, существующих в обществе в данный период, в которых отражается социальная действительность.

Пароль – секретная строка символов (букв, цифр, специальных символов), предъявляемая пользователем компьютерной системе для получения доступа к данным и программам. Пароль является средством защиты данных от несанкционированного доступа.

Персональные данные (информация о гражданах) – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

Принятие решения – процесс выбора варианта действий в имеющейся ситуации из многих возможных.

Пропаганда – воздействие на сознание (подсознание), политические и ценностные ориентации объектов (групп объектов) посредством распространения воззрений, идей, учений с целью формирования мировоззрения, соответствующих интересам воздействующей стороны.

Профессиональная тайна – информация, защита которой от несанкционированного распространения является обязанностью субъекта в силу выполняемых им профессиональных функций.

Психологическая война – совокупность различных форм, методов и средств воздействия на людей с целью изменения в желаемом направлении их психологических характеристик (взглядов, мнений, ценностных ориентаций, настроений, мотивов, установок, стереотипов поведения), а также групповых норм, массовых настроений и общественного сознания в целом.

Психологическая операция – проводимая в мирное или военное время плановая пропагандистская и психологическая деятельность, рассчитанная на иностранные враждебные, дружественные иди нейтральные аудитории с тем, чтобы влиять на их отношение и поведение в благоприятном направлении для достижения как политических, так и военных национальных целей.

Реклама – информация о товарах, различных видах услуги т.п. с целью оповещения потребителей и создания спроса на эти товары, услуги и т.п.

Сервер – аппаратно-программный комплекс, исполняющий функции хранения и обработки запросов пользователей и не предназначенный для локального доступа пользователей (выделенный сервер, маршрутизатор и другие специализированные устройства) ввиду высоких требований по обеспечению надежности, степени готовности и мер безопасности информационной системы предприятия.

Система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.

Слух – информация, которая распространяется без предоставления общепринятых свидетельств достоверности.

Средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Средство массовой информации – периодическое печатное издание, радио-, теле-, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации.

Учетная запись – информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (адрес электронной почты, телефон и т.п.).

Учебное издание

Гафнер Василий Викторович

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Ответственный редактор *А.М. Спивак*
Корректор *Л.М. Акентьева*
Обложка *М.Л. Сафиуллина*

Подписано в печать 16.06.10 г.
Формат $60 \times 90^1/_{16}$. Гарнитура Таймс.
Усл. печ. л. 15,1. Тираж 2500.
Заказ №

ООО «ФЕНИКС»
344082, г. Ростов-на-Дону, пер. Халтуринский, 80

ЧЕЛОВЕК ЕСТЬ МЕРА БЕЗОПАСНОСТИ САМОГО СЕБЯ И ОКРУЖАЮЩЕГО МИРА

Информационный портал

"БЕЗОПАСНОСТЬ. ОБРАЗОВАНИЕ. ЧЕЛОВЕК."

посвящен обеспечению
личной, национальной и глобальной безопасности

http://www.bezopasnost.edu66.ru

На сайте существуют следующие разделы:

НОРМАТИВНЫЕ ДОКУМЕНТЫ

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ БЖ

МЕТОДИКА ОБУЧЕНИЯ БЖ

КУЛЬТУРА БЕЗОПАСНОСТИ

ПСИХОЛОГИЯ БЕЗОПАСНОСТИ

КОМПЕТЕНТНОСТЬ УЧИТЕЛЯ ОБЖ

НАУКА И БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

ССЫЛКИ НА ПОЛЕЗНЫЕ РЕСУРСЫ ИНТЕРНЕТА

На сайте полезную информацию найдут учителя ОБЖ,
преподаватели БЖД, специалисты по безопасности,
учащиеся и студенты, родители.

edu66@list.ru

Издательство Феникс

РЕГИОНАЛЬНЫЕ ПРЕДСТАВИТЕЛЬСТВА:

Заместитель директора
по развитию сети представительств
СЁМКИН Сергей Владимирович
Тел.: 8-918-570-00-01
e-mail: semkin1975@gmail.com

• •

г. МОСКВА
Москва, 17-й Проезд Марьиной рощи, д. 1
(метро «Тимирязевская»)
Тел.: (495) 618-03-34; **e-mail**: fenix-m@yandex.ru
Директор: МОИСЕЕНКО Сергей Николаевич

• •

Москва, шоссе Фрезер, 17,
район метро «Авиамоторная»
Тел.: (495)517-32-95; **тел/факс**: (495) 789-83-17
e-mail: mosfen@pochta.ru, mosfen@bk.ru
Директор: МЯЧИН Виталий Васильевич

• •

Торговый Дом «КноРус»
Москва, ул. Б. Переяславская, 46
Тел.: (495)680-02-07, 680-72-54,
680-91-06, 680-92-13;
e-mail: phoenix@knorus.ru
ТАРАСОВА Стелла Борисовна

• •

г. САНКТ-ПЕТЕРБУРГ
Тел.: 8-911-101-74-44; **e-mail**: fenix.szfo@gmail.ru
Директор: БОБРОВСКАЯ Лариса Михайловна

Издательство Феникс

РЕГИОНАЛЬНЫЕ ПРЕДСТАВИТЕЛЬСТВА:

г. ЕКАТЕРИНБУРГ
620085, г. Екатеринбург, ул. Сухоложская, д. 8
Тел.: (343) 297-25-75; **e-mail**: fenixkniga@mail.ru
Директор: КУТЯНИНА Олеся Сергеевна

• •

г. ЧЕЛЯБИНСК
ООО «Интер-сервис ЛТД»,
454007, г. Челябинск, ул. Артиллерийская, д. 124
Тел.: (351) 247-74-13; **e-mail**: zakup@intser.ru
Менеджер: ШАРМАНОВА Любовь

• •

г. НОВОСИБИРСК — ООО «ТОП-Книга»
г. Новосибирск, ул. Арбузова, 1/1
Тел.: (3832) 36-10-28, доб. 1438;
e-mail: phoenix@top-kniga.ru
Менеджер: МИХАЙЛОВА Наталья Валерьевна

• •

УКРАИНА — ООО ИКЦ «Кредо»
г. Донецк, ул. Куйбышева, 131
Тел.: +38 (8062) 345-63-08, 348-37-91,
348-37-92, 345-36-52, 339-60-85, 348-37-86;
e-mail: moiseenko@skif.net
МОИСЕЕНКО Владимир Вячеславович

• •

г. САМАРА (Нижнее Поволжье)
Самара, ул. Товарная 7Е (территория базы «Учебник»)
Тел.: (846)-951-24-76;
e-mail: fenixma@mail.ru
Директор: МИТРОХИН Андрей Михайлович

Издательство Феникс

Отдел оптовых продаж:
344082, г. Ростов-на-Дону, пер. Халтуринский, 80
Контактные телефоны: (863) 261-89-53, 261-89-54, 261-89-55, 261-89-56, 261-89-57, **факс:** 261-89-58

Начальник отдела
РОДИОНОВА Татьяна Александровна
e-mail: torg152@aaanet.ru

Менеджер по развитию
НЕВЕНЧЕНКО
Олеся Николаевна
e-mail: nevenchenkool@mail.ru

Менеджер по продажам на территории Москвы, Центра европейской части России и Республики Казахстан
ЧЕРМАНТЕЕВА
Татьяна Степановна
e-mail: torg155@aaanet.ru

Менеджер по продажам
АНИКИНА
Елена Николаевна
e-mail: torg153@aaanet.ru

Менеджер по продажам
ФРАНК
Татьяна Викторовна
e-mail: sibir@aaanet.ru

Менеджер по продажам на территории ближнего и дальнего зарубежья
ВЕРЕЩАГА Марина Николаевна
e-mail: torg103@aaanet.ru

Менеджер по продажам
ФЕДОТОВА Ирина Петровна
e-mail: torg@aaanet.ru

Менеджер по продажам
БИБИК Николай Викторович
e-mail: pr2@aaanet.ru

Менеджер по продажам
БЕСКРОВНЫЙ
Виктор Александрович
e-mail: ural@aaanet.ru

Менеджер по продажам
ВОРОНИН
Алексей Александрович
e-mail: torg180@aaanet.ru

Вы можете получить книги издательства «Феникс» по почте, сделав заказ:
344082, г. Ростов-на-Дону, пер. Халтуринский, 80
ООО «Феникс», «Книга — почтой», **Лоза Игорю Викторовичу**
Тел.: 8-909-440-64-21, **e-mail:** tvoyakniga@mail.ru; www.shop50.ru

Издательство Феникс

Приглашает к сотрудничеству
АВТОРОВ для издания:

- ☑ учебников для ПТУ, ссузов и вузов;
- ☑ научной и научно-популярной литературы по МЕДИЦИНЕ и ВЕТЕРИНАРИИ, ЮРИСПРУДЕНЦИИ и ЭКОНОМИКЕ, СОЦИАЛЬНЫМ и ЕСТЕСТВЕННЫМ НАУКАМ;
- ☑ литературы по ПРОГРАММИРОВАНИЮ и ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ;
- ☑ ПРИКЛАДНОЙ и ТЕХНИЧЕСКОЙ литературы;
- ☑ литературы ПО СПОРТУ и БОЕВЫМ ИСКУССТВАМ;
- ☑ ДЕТСКОЙ и ПЕДАГОГИЧЕСКОЙ литературы;
- ☑ литературы по КУЛИНАРИИ и РУКОДЕЛИЮ.

. . . . . .

ВЫСОКИЕ ГОНОРАРЫ!!!
ВСЕ финансовые ЗАТРАТЫ БЕРЕМ НА СЕБЯ!!!
При принятии рукописи в производство
ВЫПЛАЧИВАЕМ гонорар на 10% ВЫШЕ
ЛЮБОГО РОССИЙСКОГО ИЗДАТЕЛЬСТВА!!!
Рукописи не рецензируются
и не возвращаются!

. . . . . .

Руководитель редакционно-издательского отдела:
Спивак Александр Михайлович
Тел.: 8 (863) 261-89-77
e–mail: spivak@aaanet.ru
САЙТ http://www.phoenixrostov.ru