Министерство образования и науки Российской Федерации
Федеральное агентство по образованию
Государственное образовательное учреждение
высшего профессионального образования
«Уральский государственный педагогический университет»

В. В. Гафнер

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие

Часть 2

Екатеринбург 2009

УДК 347-049.5(075.8)
ББК Ц9я7
Г 24

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.

Г 24 Информационная безопасность: учебное пособие в 2 ч. / В. В. Гафнер ; ГОУ ВПО «Урал. гос. пед. ун-т». – Екатеринбург, 2009. – Ч.2. – 196 с.

ISBN 978-5-7186-0414-6

Учебное пособие «Информационная безопасность» предназначено для студентов педагогических ВУЗов, обучающихся по специальности 050104 – 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.

Пособие может быть полезно специалистам в области безопасности жизнедеятельности, учителям ОБЖ, учащимся, родителям.

УДК 347-049.5(075.8)
ББК Ц9я7

ISBN 978-5-7186-0414-6

СОДЕРЖАНИЕ

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 – «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 первой части пособия рассматривается значение информации в современном мире и образовании, основы правового обеспечения информационной безопасности, а также меры по обеспечению информационной безопасности РФ.

Во второй части пособия рассмотрены вопросы обеспечения информационной безопасность человека в повседневной жизни и в чрезвычайных ситуациях, представлены 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. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЧЕЛОВЕКА

1.1. 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.

1.2. 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 «Mallboro».

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 *безделничая, 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.

1.3. 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 18 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 услуги 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 (the Children's Advertising Review Unit – (CARU), который является подразделением созданного общественными объединениями в области рекламы Национального совета по контролю над рекламой (the 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 используется сразу несколько рекламных роликов/сообщений, раскрывающих ту или 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 кампания» («… разработанная известной фармацевтической кампанией» – 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.

1.4. 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 ведения

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.

1.5. 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 использовать 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 процентов видеоигр, наиболее любимых молодёжью, отличаются жестокостью. В играх типа «action» на насилие уходит 91% времени, причем в 27% игр насилие приводит к смерти. Рик Дайер, президент компании «Virtual Image Productions», говорит, что «игры перестали быть просто играми. Они превратились в средство обучения. И мы учим детей получать радость, нажимая на курок. Однако мы не побуждаем 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 E (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 человеческое сознание?
4. В чём особенность влияния телевидения на детей?
5. Какую информацию следует считать оказывающей негативное воздействие на физическое, умственное или нравственное развитие несовершеннолетних?
6. Какими путями просмотр телепередач со сценами насилия повышает агрессивность детей?
7. Перечислите способы защиты человека от негативного влияния информации.
8. Назовите последствия влияния рекламы на детей.
9. Какие существуют особенности рекламы для детей в различных странах?

10. Каким образом следование рекламным призывам может привести к ухудшению здоровья человека?

11. Перечислите возможные опасности для ребёнка в сети Интернет.

12. По каким поведенческим характеристикам можно судить о формировании у человека зависимости от Интернета?

ГЛАВА 2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЧЕЛОВЕКА В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

2.1. 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 ее 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 убийственнее, 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 (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 г. 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 острова 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.

2.2. 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 3. 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.

3.1. 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.

3.2. 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.

3.3. 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, похвастав 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 4. 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.

4.1. 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?

4.2. 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.

4.3. 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 инструменты 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 компьютерных 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 монитор 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 небезопасна. 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 ее 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 5. 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».

5.1. 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 «кибераневра», 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.

5.2. 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 кинохроник. 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 содержании 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.

Позитивные результаты общения лицом к лицу заставляют более внимательно присмотреться к этому типу коммуникации. Кстати, при воздействии на противника учитывается тот факт, что перед дезертирством солдат обязательно будет обсуждать саму эту возможность со своим соседом по окопам.

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. *Бетелин, В.* Информационная безопасность в России: опыт составления карты / В. Бетелин, В. Галатенко // Jet Info № 1. — 1998. — С. 5.

4. Библиотека «ПСИ-ФАКТОРА» [Электронный ресурс]. – Электрон. текстовые дан. – Режим доступа: http://psyfactor.org/lybr.htm, свободный. – Загл. с экрана.

5. *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.

6. *Бодров, В. А.* Информационный стресс : учеб. пособие для студентов вузов / В. А. Бодров. — М. : ПЕР СЭ, 2000. – 352 с.

7. *Бурлаков, И. В.* Homo Gamer : Психология компьютерных игр / И. В. Бурлаков. – М. : Независимая фирма «Класс», 2000. – 141 с. – (Библиотека психологии и психотерапии, вып. 86).

8. *Гарфинкель, С.* Всё под контролем : Кто и как следит за тобой / С. Гарфинкель ; *пер. с англ.* В. Масянкина. — Екатеринбург : У-Фактория, 2004. – 432 с.

9. *Гафнер, В. В.* Информационная пассивность педагога / В. В. Гафнер // Народное образование. – 2005. – № 2. – С. 235–239.

10. *Гафнер, В. В.* О профессиональной компетентности учителя ОБЖ / В. В. Гафнер // ОБЖ. Основы безопасности жизни. – 2005. – № 11. – С. 31-34.

11. *Гафнер, В. В.* О профессиональной компетентности учителя ОБЖ / В. В. Гафнер // ОБЖ. Основы безопасности жизни. – 2005. – № 12. – С. 40-44.

12. *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.

13. *Гафнер, В. В.* Профессиональная деформация и компетентность педагога / В. В. Гафнер // ОБЖ. Основы безопасности жизни. – 2004. – № 10. – С. 22–24.

14. *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.

15. *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.

16. *Грачев Г. В.* Информационно-психологическая безопасность личности: состояние и возможности психологической защиты / Г. В. Грачев. – М. : Изд-во РАГС, 1998. – 125 с.

17. *Грачев, Г. В.* Личность и общество: информационно-психологическая безопасность и психологическая защита / Г. В. Грачев. — М. : ПЕР СЭ, 2003. – 304 с.

18. *Грачев Г. В.* Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия / Г. В. Грачев, И. К. Мельник. – М. : Алгоритм, 2002. – 288 с.

19. *Гриняев, С. Н.* Поле битвы – киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны / С. Н. Гриняев. — Мн. : Харвест, 2004. – 448 с.

20. *Дмитриев, А. В.* Слухи как объект социологического исследования / А. В. Дмитриев // Социс. – 1995. – № 1. – С. 5– 11.

21. *Днепров, А. Г.* Защита детей от компьютерных опасностей (+ CD) / А. Г.Днепров. – СПб. : Питер, 2008. – 192 с.

22. Доктрина информационной безопасности Российской Федерации // Указ Президента РФ № Пр–1895 от 9.09.2000.

23. *Доценко, Е. Л.* Психология манипуляции: феномены, механизмы, защита / Е. Л. Доценко. — М. : Речь, 2004. – 304 с.

24. *Дубин, Б. В.* Слухи как социально-психологический феномен / Б. В. Дубин, А. В. Толстых // Вопросы психологии. – 1993. - № 3. – С. 15-31

25. *Загородников, С. Н.* Основы информационного права : учеб. пособие для студентов вузов / С. Н. Загородников, А. А. Шмелев. — М. : Акад. Проект : Парадигма, 2005. – 192 с.

26. Информационная безопасность России / Ю. С. Уфимцев, Е. А. Ерофеев и др. — М. : «Экзамен», 2003. – 560 с.

27. 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.

28. Информационно-психологическая и психотронная война : хрестоматия. — Мн. : Харвест, 2003. – 432 с.

29. *Кара-Мурза, С.* Манипуляция сознанием / С. Кара-Мурза. — М. : Эксмо, 2005. – 832 с.

30. *Караяни, А. И.* Слухи как средство информационно - психологического противодействия / А. И. Караяни // Психологический журнал. – 2003. – № 6. – Том 24.

31. *Карпов, А. В.* Психология групповых решений / А. В. Карпов. - М. ; Ярославль, 2000. – 532 с.

32. *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.

33. *Козлов, В. Е.* Теория и практика борьбы с компьютерной преступностью / В. Е. Козлов. — М. : Горячая линия-Телеком, 2002. – 336 с.

34. *Колесникова, Т. И.* Психологический мир личности и его безопасность / Т. И. Колесникова. — М. : ВЛАДОС-ПРЕСС, 2001. – 176 с.

35. *Колин, К. К.* Социальная информатика : учеб. пособие для студентов вузов / К. К. Колин. — М. : Акад. Проект : Фонд «Мир», 2003. – 432 с.

36. Концепция национальной безопасности Российской Федерации // Указ Президента РФ № 1300 от 17.12.1997.

37. *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.

38. *Корнилова, Т. В.* Психология риска и принятия решений / Т. В. Корнилова. – М. : Аспект Пресс, 2003. – 286 с.

39. *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.

40. *Крысько, В. Г.* Секреты психологической войны (цели, задачи, методы, формы, опыт) / В. Г. Крысько. — Мн. : Харвест, 1999. – 448 с.

41. *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.

42. *Лисичкин, В. А.* Третья мировая (информационно-психологическая) война / В. А. Лисичкин, Л. А. Шелепин. — М. : Институт социально-политических исследований АСН, 2000. – 304 с.

43. *Макаренкова, В.* Видеоигры в информационной и психологической борьбе / В. Макаренкова // «Зарубежное военное обозрение». – 2005. – № 2.

44. *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.

45. *Мельникова, А. А.* Язык и национальный характер. Взаимосвязь структуры языка и ментальности / А. А. Мельникова. – СПб. : Речь, 2003. – 320 с.

46. Методика информационной безопасности / Ю. С. Уфимцев, В. П. Буянов и др. — М. : Издательство «Экзамен», 2004. – 544 с.

47. *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.

48. *Моляков, А.* Особенности проявления паники в условиях экологического бедствия / А. Моляков // Психологический журнал. – 1992. – № 2. – Том 13.

49. *Назаретян, А. П.* Агрессивная толпа, массовая паника, слухи / А. П. Назаретян. - СПб. : Питер, 2004. – 192 с.

50. *Нарицын, Н. Н.* Азбука психологической безопасности / Н. Н. Нарицын. — М. : Издательство «Русский журнал», 2000. – 224 с.

51. *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.

52. *Номоконов, В. А.* Глобализация информационных процессов и преступность [Электронный ресурс] / В. А. Номоконов. – Электрон. текст. дан. – Режим доступа: http://www.crime-research.ru/library/nomokon.htm, свободный. – Загл. с экрана.

53. Об авторском праве и смежных правах // Закон Российской Федерации № 5351-1 от 9.07.1993.

54. Об информации, информационных технологиях и о защите информации // Закон Российской Федерации № 149-ФЗ от 27.07.2006.

55. О государственной тайне // Закон Российской Федерации № 5485–1 от 21.07.1993.

56. *Одинцов, А. А.* Экономическая и информационная безопасность : справ. : учеб. пособие для студентов вузов / А. А. Одинцов. — М. : Экзамен, 2005. – 576 с.

57. Одинцов, А. А. Экономическая и информационная безопасность предпринимательства : учеб. пособие для студентов вузов / А. А. Одинцов. — М. : Академия, 2006. – 336 с.

58. *Оганджанян, Ш.* Чем промывают мозги / Ш. Оганджанян // Всё ясно. – 2006. – № 4 (62). – С. 39-41.

59. Основы информационной культуры : учеб.–метод. пособие / *авт.-сост.* В. И. Золотарева [и др.]. – М. : МИФИ, 2005. – 128 с.

60. *Олпорт, Г.* Становление личности: избранные труды / Г. Олпорт. – М. : Смысл, 2002.

61. Патентный закон // Закон Российской Федерации № 3517-1 от 23.09.1992.

62. *Плаус, С.* Психология оценки и принятия решений / С. Плаус. — М. : Информационно-издательский дом «Филинъ», 1998. – 368 с.

63. *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.

64. *Почепцов, Г. Г.* Информационные войны / Г. Г. Почепцов. — М. : «Рефл-бук» ; К. : «Ваклер», 2001. – 576 с.

65. *Почепцов, Г. Г.* Психологические войны / Г. Г. Почепцов. — М. : «Рефл-бук» ; К. : «Ваклер», 2001. – 528 с.

66. 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.

67. Психология экстремальных ситуаций / *сост.* А. Е. Тарас, К. В. Сельченок. – М. : АСТ, Мн. : Харвест, 2001. – 480 с.

68. *Райнер, П.* Застывший взгляд / П. Райнер. – М.: evidentis, 2003. – 224 с.

69. Растим здоровых, умных, добрых: воспитание младшего школьника : пособ. для средн. и высш. педагогич. учебн. заведений / *сост.* Л. В. Ковинько. — М. : Академия, 1996. – 288 с.

70. Реклама: внушение и манипуляция : учеб. пособие / сост. Д. Я. Райгородский. — Самара : БАРАХ-М, 2001. –752 с.

71. *Розен, Э.* Анатомия слухов: маркетинговые приемы / Э. Розен. – СПб. : Питер, 2006. – 240 с.

72. *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.

73. *Светлакова, Н. Б.* Реклама, которая вас убивает / Н. Б. Светлакова. – М. : Вече, 2007. – 176 с.

74. *Синельников, В. В.* Таинственная сила слова. Формула любви. Как слова воздействуют на нашу жизнь / В. В. Синельников. – М. : ЗАО Центрполиграф, 2006. – 255 с.

75. *Спенсер, Д.* «Да» или «Нет» / Д. Спенсер. — СПб. : Питер Пресс, 1996. – 128с.

76. *Столяренко А. М.* Экстремальная психопедагогика / А. М. Столяренко. – М. : ЮНИТИ-ДАНА, 2002. – 608 с.

77. *Тоффлер Э.* Третья волна. — М.:АСТ, 2004. — 783с.

78. *Тоффлер, Э.* Шок будущего. — М.:АСТ, 2004. — 557 с.

79. *Харрис, Р.* Психология массовых коммуникаций / Р. Харрис. — СПб. : Прайм-ЕВРОЗНАК, 2002. – 448 с.

80. *Черноушек, М.* Психология жизненной среды / М. Черноушек ; *пер. с пол.* И. И. Попа. – М. : Мысль, 1989. - 176 с.

81. *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.

82. *Шнайер, Б.* Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер. — СПб. : Питер, 2003. – 368 с.

83. *Щербаков, А. Ю.* Введение в теорию и практику информационной безопасности / А. Ю. Щербаков. — М. : издатель Молгачева С. В., 2001. Нечаев В. В., Дарьин А. В. 352 с.

84. *Эмото, М.* Послания воды: Тайные коды кристаллов льда / М. Эмото; *пер. с англ.* О. Горбунова. — М. : ООО Изд-во «София», 2006. – 96 с.

85. *Эриксен, Т. Х.* Тирания момента. Время в эпоху информации / Т. Х. Эриксен ; *пер. с норв.* – М. : Издательство «Весь Мир», 2003. – 208 с.

86. *Ярочкин, В. И.* Система безопасности фирмы / В. И. Ярочкин. — М. : Ось-89, 2003. -352 с.

87. *Ярочкин, В. И.* Информационная безопасность : учеб. для студентов вузов / В. И. Ярочкин. — М. : Акад. Проект, 2008. — 544 с.

88. Язык наш поводырь наш в рай или ад : сб. статей / *под ред.* Г. Емельяненко. — СПб.: Изд-во Л.С. Яковлевой, 2001. – 336 с.

89. Jet Info, информационный бюллетень [Электронный ресурс]. – Электрон. текстовые дан. – Режим доступа: http://www.jetinfo.ru, свободный. – Загл. с экрана.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Утверждаю
Заместитель Министра образования и науки
Российской Федерации
А. Г. Свинаренко

«31» января 2005 г.
Номер государственной регистрации
715 пед/сп (новый)

Государственный образовательный стандарт Высшего профессионального образования

Специальность 050104.65 «Безопасность жизнедеятельности» Квалификация учитель безопасности жизнедеятельности

Вводится в действие с момента переутверждения
вместо ранее утвержденного (14.04.2000 г., № 379пед/сп)
(выписка)

Москва 2005

ТРЕБОВАНИЯ К ОБЯЗАТЕЛЬНОМУ МИНИМУМУ СОДЕРЖАНИЯ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ПОДГОТОВКИ ВЫПУСКНИКА ПО СПЕЦИАЛЬНОСТИ 050104.65 «БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ»

Индекс	Наименование дисциплин и их основные разделы	Всего часов
ДПП	**Дисциплины предметной подготовки**	**4334**
ДПП.Ф.00	**Федеральный компонент**	**3934**
ДПП.Ф.16	**Информационная безопасность** Понятие информационной безопасности. Место информационной безопасности в системе национальной безопасности РФ. Основы государственной политики обеспечения информационной безопасности. Международная деятельность по обеспечению информационной безопасности. Законодательство в области информационной безопасности. Основные факторы и ключевые проблемы информационной безопасности. Основы защиты деловой информации и сведений, составляющих служебную, коммерческую, государственную тайну. Защита интеллектуальной собственности. Методы и средства защиты электронной информации. Информационные технологии и здоровье. Негативные последствия глобальной информатизации общества, расширение средств массовой информации и рекламы, их дестабилизирующее воздействие на человека.	**140**

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 ч в неделю, для младшего школьника – 3 ч, включая просмотры и в выходные дни, для подростка – не более 5 ч. 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 она 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.

З**ащита 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
Часть 2

Редактор М. А. Ли-Буланкова

Подписано в печать 01.07.09. Формат 60x90/16.
Бумага для множ. ап. Гарнитура Times New Roman.
Печать на ризографе. Усл. печ. л. 12,3 Уч.-изд. л.
Тираж 500 экз. Заказ 2858

Оригинал-макет отпечатан в отделе множительной техники
Уральского государственного педагогического университета
620017, г. Екатеринбург, просп. Космонавтов, 26.
E-mail: uspu@uspu.ru
E-mail: uralfbg@mail.ru
www.bezopasnost.edu66.ru