Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

Е.В. Чернова

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

*Утверждено Редакционно-издательским советом университета
в качестве учебного пособия для студентов-социологов*

Магнитогорск
2015

УДК 004.05
ББК 3973.2

Рецензент:
Кандидат технических наук, доцент кафедры информационных технологий,
ФГБОУ ВПО «Магнитогорский государственный университет»
А.В. Меркулова

Чернова Е.В.
Информационная безопасность [Электронный ресурс] : учебное пособие для студентов-социологов / Елена Владимировна Чернова ; ФГБОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова». – Изд. 2-е, подгот. по печ. изд. 2011 г. – Электрон. текстовые дан. (1,63 Мб). – Магнитогорск : ФГБОУ ВПО «МГТУ», 2015. – 1 электрон. опт. диск (CD-R). – Систем. требования : IBM PC, любой, более l GHz ; 512 Мб RAM ; 10 Мб HDD ; MS Windows XP и выше ; Adobe Reader 8.0 и выше ; CD/DVD-ROM дисковод ; мышь. – Загл. с титул. экрана.

В учебном пособии содержится основной материал по дисциплине «Информационная безопасность» для специальности «Социология». Изложены гуманитарные аспекты обеспечения информационной безопасности личности, общества и государства. Рассмотрены негативные факторы воздействия информационных технологий на личность и общество, проблема информационно-психологической безопасности, а так же основы информационной культуры.

Настоящее пособие предназначено для студентов-социологов всех форм обучения, а также аспирантам, преподавателям высших учебных заведений, социологам и учителям социологии.

УДК 004.05
ББК 3973.2

СОДЕРЖАНИЕ

Цель курса «Информационная безопасность»

подготовка студентов по курсу «Информационная безопасность» в соответствии с требованиями «Государственного образовательного стандарта ВПО Социология».

Задачи курса:

- раскрыть ключевые аспекты в области информационной безопасности (воздействие на физическое, интеллектуальное, эмоциональное и психическое здоровье; законодательные, нормативные правовые и морально-этические нормы; механизмы защиты личности от информационных угроз и т.д.);
- раскрыть понятийный аппарат в области информационной безопасности человека и общества;
- раскрыть понятие «девиантное поведение в сфере ИКТ», его видов, особенностей, характеристик;
- подготовить к пониманию проблемы обеспечения информационно-психологической безопасности личности в информационном обществе;
- обучить применению основных методов и средств защиты информации на практике.

§1. Информационное общество

Информационное общество. Информационные революции. Критерии перехода к информационному обществу.

Понятие информационного общества

Данное понятие было введено в научный оборот Ф. Махлупом в 1962 г. в работе «Производство и распределение знания в США», положив тем самым начало изучению «экономики знаний». Впоследствии содержание данного понятия было признано весьма размытым и в некоторых отношениях не вполне корректным.

Тема «информационного общества» обрела особую актуальность в 1990-е годы с развитием «новой экономики», «экономики знания», «цифровой экономики» и т.п. Новый статус концепта «информационное общество» отразился в факте принятия «большой восьмеркой» Окинавской хартии глобального информационного общества. В Хартии этот термин был использован для обозначения цели, которая может быть достигнута в ходе глобального освоения информационно-коммуникационных технологий. Считалось, что таким образом повсюду в мире может быть обеспечен устойчивый экономический рост, повышено общественное благосостояние, укреплено социальное согласие, реализован потенциал большинства стран мира в области развития демократии и в конечном счете обеспечены транспарентное и ответственное управление в мировом сообществе, международная стабильность.

Информационное общество – социологическая и футурологическая концепция, полагающая главным фактором общественного развития производство и использование научно-технической и другой информации. Концепция информационного общества является разновидностью теории постиндустриального общества, основу которой положили З.Бжезинский, Д.Белл, О.Тоффлер.

Информационное общество – общество, в котором большинство работающих занято производством, хранением, переработкой и реализацией информации, особенно высшей ее формы – знаний.

Рассматривая общественное развитие как «смену стадий», сторонники теории информационного общества связывают его становление с доминированием «четвертого», информационного сектора экономики, следующего за сельским хозяйством, промышленностью и экономикой услуг. При этом утверждается, что капитал и труд как основа индустриального общества уступают место информации и знанию в информационном обществе. Революционизирующее действие информационной технологии приводит к тому, что в информационном обществе классы заменяются социально недифференцированными «информационными сообществами».

Усложнение индустриального производства, социальной, экономической и политической жизни, изменение динамики процессов во всех сферах деятельности человека привели, с одной стороны, к росту потребностей в знаниях, а с другой – к созданию новых средств и способов удовлетворения этих потребностей.

Информационные революции

В истории развития цивилизации произошло несколько информационных революций – преобразований общественных отношений из-за кардинальных изменений в сфере обработки информации. Следствием подобных преобразований являлось приобретение человеческим обществом нового качества.

Первая революция связана с изобретением письменности, что привело к гигантскому качественному и количественному скачку. Появилась возможность передачи знаний от поколения к поколениям.

Вторая (середина XVI в.) вызвана изобретением книгопечатания, которое радикально изменило индустриальное общество, культуру, организацию деятельности.

Третья (конец XIx в.) обусловлена изобретением электричества, благодаря которому появились телеграф, телефон, радио, позволяющие оперативно передавать и накапливать информацию в любом объеме.

Четвертая (70-е гг. XX в.) связана с изобретением микропроцессорной технологии и появлением персонального компьютера. На микропроцессорах и интегральных схемах создаются компьютеры, компьютерные сети, системы передачи данных (информационные коммуникации). Этот период характеризуют три фундаментальные инновации:

- переход от механических и электрических средств преобразования информации к электронным;
- миниатюризация всех узлов, устройств, приборов, машин;
- создание программно-управляемых устройств и процессов.

Критерии перехода к информационному обществу

В информационном обществе изменятся не только производство, но и весь уклад жизни, система ценностей, возрастет значимость культурного досуга по отношению к материальным ценностям. По сравнению с индустриальным обществом, где все направлено на производство и потребление товаров, в информационном обществе производятся и потребляются интеллект, знания, что приводит к увеличению доли умственного труда. От человека потребуется способность к творчеству, возрастет спрос на знания. Материальной и технологической базой информационного общества станут различного рода системы на базе компьютерной техники и компьютерных сетей, информационной технологии, телекоммуникационной связи.

В реальной практике развития науки и техники передовых стран в конце XX в. постепенно приобретает зримые очертания созданная теоретиками картина информационного общества. Прогнозируется превращение всего мирового пространства в единое компьютеризированное и информационное сообщество людей, проживающих в электронных

квартирах и коттеджах. Любое жилище оснащено всевозможными электронными приборами и компьютеризированными устройствами. Деятельность людей будет сосредоточена главным образом на обработке информации, а материальное производство и производство энергии будет возложено на машины.

Ряд ученых выделяют характерные черты информационного общества:

- решена проблема информационного кризиса, т.е. разрешено противоречие между информационной лавиной и информационным голодом;
- обеспечен приоритет информации по сравнению с другими ресурсами;
- главной формой развития станет информационная экономика; в основу общества будут заложены автоматизированные генерация, хранение, обработка и использование знаний с помощью новейшей информационной техники и технологии;
- информационная технология приобретет глобальный характер, охватывая все сферы социальной деятельностей человека;
- формируется информационное единство всей человеческой цивилизации;
- с помощью средств информатики реализован свободный доступ каждого человека к информационным ресурсам всей цивилизации;
- реализованы гуманистические принципы управления обществом и воздействия на окружающую среду.

Общество считается информационным, если:

- любой индивид, группа лиц, предприятие или организация в любой точке страны и в любое время могут получить за соответствующую плату или бесплатно на основе автоматизированного доступа и систем связи любую информацию и знания, необходимые для их жизнедеятельности и решения личных и социально значимых задач;

– в обществе производится, функционирует и доступна любому индивиду, группе или организации современная информационная технология;

– имеются развитые инфраструктуры, обеспечивающие создание национальных информационных ресурсов в объеме, необходимом для поддержания постоянно убыстряющегося научно-технологического и социально-исторического прогресса;

– происходит процесс ускоренной автоматизации и роботизации всех сфер и отраслей производства и управления;

– происходят радикальные изменения социальных структур, следствием которых оказывается расширение сферы информационной деятельности и услуг.

Кроме положительных моментов прогнозируются и опасные тенденции:

– все большее влияние на общество средств массовой информации;

– информационные технологии могут разрушить частную жизнь людей и организаций;

– существует проблема отбора качественной и достоверной информации;

– многим людям будет трудно адаптироваться к среде информационного общества;

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

Ближе всех на пути к информационному обществу стоят страны с развитой информационной индустрией, к числу которых следует отнести США, Японию, Великобританию, Германию, страны Западной Европы. В этих странах уже давно одним из направлений государственной политики является направление, связанное с инвестициями и поддержкой инноваций в

информационную индустрию, в развитие компьютерных систем и телекоммуникаций.

§2. Информационная культура

Информационная культура. Сетевой этикет.

Информационная культура

Информационная культура – способ жизнедеятельности человека в информационном обществе, как составляющая процесса формирования культуры человечества.

В рамках информационного подхода большинство определений подразумевает совокупность знаний, умений и навыков поиска, отбора, анализа информации, то есть всего того, что включается в информационную деятельность, направленную на удовлетворение информационной потребности. Более того, часть авторов сужает информационную культуру до рамок компьютерной грамотности.

Информационная культура – одна из граней общечеловеческой культуры или информационной компоненты человеческой культуры в целом.

В зависимости от субъекта, который выступает носителем информационной культуры, последнюю можно рассматривать на трех уровнях:

– информационная культура личности;

– информационная культура отдельных групп сообщества (определенного социума, нации, возрастной или профессиональной группы и т.д.);

– информационная культура общества в целом.

Понятие «информационная культура» включает в себя:

– культуру поиска новой информации при понимании индивидом того, что устранение информационного дефицита всегда связано со

значительными психологическими трудностями, а часто и ломкой стереотипов (современный поиск предполагает умение проанализировать свои информационные потребности, использование формальных и неформальных каналов получения информации, освоение возможностей новых информационных технологий и т.д.);

– культуру чтения и восприятия информации, понимание особенностей современных текстовых сообщений и необходимости анализа всего «документального шлейфа» изучаемого направления;

– осознание того факта, что любое профессиональное чтение есть средство получения знаний (в противовес его рассмотрению только в качестве способа устранения информационного дефицита, возникшего при решении текущих задач);

– умение перерабатывать большие массивы информации с использованием как информационных (компьютерных) технологий, так и интеллектуальных нормализованных методик (поаспектного анализа текстов, контент-анализа, классификационного и кластерного анализа и т.д.);

– умение генерировать собственные проблемно-ориентированные базы данных и вести личные поисковые системы;

– понимание важности межличностного профессионального общения для успешности любой трудовой деятельности;

– стремление к повышению уровня коммуникационной компетентности;

– воспитание в себе терпимости к чужим точкам зрения и мнениям, готовности не только получать, но и отдавать знания;

– умение находить партнеров по совместной деятельности с использованием для этого телекоммуникационных каналов связи;

– умение четко и доказательно излагать результаты собственной деятельности, в том числе, с учетом уровня подготовленности и настроя целевой аудитории;

– знание норм, регламентирующих использование интеллектуальной собственности.

Информационная культура проявляется в информационном поведении людей. Под информационным поведением мы понимаем образ действий, совокупность усилий, предпринимаемых человеком для получения-усвоения и использования-создания нового знания, его передачи и распространения в обществе.

Информационное поведение, с одной стороны, отражает активность личности как познающего субъекта, его умение ориентироваться в информационном пространстве. С другой стороны, в информационном поведении проявляется степень доступности и комфортности использования совокупных информационных ресурсов или, иными словами, те возможности, которые общество предоставляет индивиду, стремящемуся состояться как профессионалу и личности. Представляется, что в самое ближайшее время судьба каждого конкретного человека будет зависеть от того, насколько он способен своевременно находить, получать, адекватно воспринимать и продуктивно использовать новую информацию (точнее, новое знание) в своей повседневной жизни.

Культурой человек восполняет свою природную незавершенность и если природа делает человека индивидом, а общество наделяет человека социальными качествами и формирует его как личность, то культура наделяет человека уникальной индивидуальностью. Не случайно проблемы развития культуры и воздействие на это развитие различных факторов – природы, техники, политики и др. является одной из вечных проблем философской рефлексии.

Вопрос о воздействии техники на культуру приобрел особую актуальность в условиях формирования информационного общества, когда радио и телефоны, телевизоры и магнитофоны, принтеры и сканеры, калькуляторы и компьютеры, международная информационная система Интернет и специализированные Сети оказывают все возрастающее и

сложное воздействие не только на сферу материального производства, социально-политическую жизнь общества, но и на ее духовную жизнь.

От письменной культуры человечество переходит к новой - экранной - культуре. Она складывается на основе синтеза компьютера с видеотехникой. Возникает новое – экранное – мышление для которого характерно «сращение» логического и образного, понятийного и чувственно-наглядного. Основой новой культуры становится «экранная страница», которая является общечеловеческой и создает невиданные возможности общения людей. Одновременно информационная технология резко снижает возможности культурного монополизма, создавая относительно независимое множество субкультур которыми невозможно управлять из одного центра. Однако децентрализующие технические средства (книга, кассетная запись, компьютер) сопровождаются функционированием централизующих средств (газета, радио, телевидение). Это свидетельствует о противоречивом характере воздействия информационных средств на культуру и вызывает необходимость продуманного решения целого ряда вопросов этического характера.

Поэтому не удивительно, что одним из элементов новой компьютерной культуры является «компьютерная этика» – совокупность моральных принципов и норм, регулирующих отношения между людьми, сложившихся на основе их работы с компьютерами. Смена моральных норм под влиянием информационной технологии признается ныне многими исследователями. Более того, существуют попытки сформулировать определенные правила поведения при работе с компьютером. Так, к примеру, сформулировано требование: «Не делайте с помощью компьютера то, что вы сочли бы аморальными без него. Никакое действие не становится более моральным из-за того, что для его облегчения использован компьютер». Возможность такой этики обусловлена следующими обстоятельствами. Мораль предписывает какие действия следует совершать в конкретных ситуациях. Поскольку в различных областях человеческой деятельности возникают специфические и

типичные для этих областей ситуации, возникает необходимость специфических норм поведения людей, что и является основанием для возникновения прикладных этик, в том числе и компьютерной.

Что касается необходимости создания компьютерной этики, то эта необходимость вызвана в общем плане тем, что создаваемые компьютерной техникой новые ситуации часто делают морально значимым явления, которые раньше были вне поля моральных кодексов и определялись естественными закономерностями. Теперь же они, например, возможности компьютера разрешить определенные конфликтные ситуации, предугадать стихийные природные явления и др., попали в орбиту моральных оценок. Все, что связано с деятельностью компьютеров, должно находиться под строгим контролем человеческой этики. Возникает компьютерная этика, в которой внеэкономические цели часто вытесняют экономические.

Означает ли это, что компьютерные системы надо наделять моральными нормами? Большинство ученых склоняется к отрицательному ответу: моральные нормы применимы лишь к поведению людей, которые вступают между собой в определенные общественные, в том числе и моральные, отношения. Вне сферы общественных отношений, какими, к примеру, являются технические связи и функционирование искусственных систем, они не действуют. Для компьютера безразлично, какие задачи – гуманные или антигуманные – он решает. Это оценивает человек, его общественная практика, его цели и стремления, его нравственные нормы и идеалы.

Сетевой этикет

Этикет – правила хорошего тона, принятые в той или иной социальной группе. **Сетевой этикет** (Netiquette) –набор предписаний о том, как себя вести в Сети. В 1994 году, Виджиния Ши (Virginia Shea) написала книгу «Нетикет»(«Netiquette»), где были предложены 10 простых правил.

1. Помните, что Вы говорите с человеком

Не делай другим то, что не хочешь получить от них сам. Поставьте себя на место человека, с которым говорите. Отстаивайте свою точку зрения, но не оскорбляйте окружающих. В киберпространстве говорят: помните, что Вы говорите с человеком. Когда вы используете телекоммуникации, то имеете дело с экраном компьютера. Вы не можете жестикулировать, изменять тон, и выражение Вашего лица не играет никакой роли. Слова, только слова – это все, что видит Ваш собеседник. Когда вы ведете разговор – по электроной почте или в конференции – можно очень легко ошибиться в толковании слов Вашего собеседника. И, к сожалению, забыть о том, что Ваш адресат тоже человек со своими чувствами и привычками. Это парадокс. Компьютерные сети знакомят друг с другом людей, которые никогда бы не встретились в реальной жизни. Но в виртуальном пространстве Вы ощущаете в адресатах меньше человечности, чем в реальной жизни. Представьте автолюбителя на улице, который проклинает других водителей, делает неприличные жесты и вообще ведет себя, как дикарь. Обычное дело, верно? Люди, обменивающиеся сообщениями по электронной почте, часто похожи на таких автолюбителей. Многие из них никогда бы не позволили себе этого, с глазу на глаз. Но присутствие «посредника»-компьютера, считают они, допускает такое поведение. Netiquette утверждает: нет. Конечно, Вы используете сеть для свободного самовыражения. Вы знакомитесь с новыми словами и посещаете незнакомые миры. Однако, не забывайте о главном принципе сетевого этикета: всюду в Сети находятся реальные люди.

2. Придерживайтесь тех же стандартов поведения, что и в реальной жизни

В реальной жизни большинство из нас подчиняется законам, иногда из-за ограничений, иногда из-за опасений быть пойманным. В виртуальном пространстве шансы быть пойманным сравнительно невелики. Люди иногда забывают о том, что «за экраном» находится живой человек, и думают, что в Сети правила поведения не так строги, как в обычной жизни. Это

заблуждение объяснимо, но все равно – это заблуждение. Стандарты поведения могут отличаться в разных точках виртуального пространства, однако, они не более мягкие, чем в реальной жизни. Соблюдайте этику общения. Не верьте тому, кто говорит: «Вся этика здесь заключается в том, что Вы сами для себя установите». Если вы встречаетесь с проблемой этического характера в киберпространстве, подумайте, как бы Вы поступили в реальной жизни. Скорее всего, Вы быстро найдете решение. Нарушение закона – нарушение Netiquette Если кто-то нарушает закон в виртуальном пространстве, он обычно нарушает и сетевой этикет. Некоторые законы настолько туманны, что трудно себе представить, как их вообще можно исполнять. И в некоторых случаях мы по-прежнему гадаем, как закон относится к виртуальному пространству. Эта книга о хороших манерах, а не юридический справочник. Тем не менее Netiquette предполагает, что пользователям лучше оставаться в рамках закона, как в реальном, так и в виртуальном пространстве.

3. Помните, где Вы находитесь в киберпространстве

Netiquette меняется от компьютера к компьютеру. То, что без колебаний принимается в одном месте, могут посчитать за грубость в другом. Например, в конференциях, где обсуждаются телевизионные программы, разные слухи и сплетни - вполне нормальное явление. Но если вы решили вторгнуться с ними в журналистскую дискуссию, популярности это Вам не прибавит. А раз Netiquette всюду свой, то неплохо знать, где Вы находитесь в настоящий момент. Отсюда вывод: Не прыгайте наобум. Оказавшись в новой области виртуального пространства, сначала осмотритесь. Потратьте время на изучение обстановки – послушайте, как и о чем говорят люди. После этого вступайте в разговор.

4. Уважайте время и возможности других

Существует стереотип, мол, что сегодня у людей остается все меньше времени, хотя (или, быть может, поэтому?) мы тратим меньше времени на сон и изобретаем новые устройства, позволяющие сэкономить время. Когда

Вы посылаете электронную почту или отправляете сообщение в конференцию, Вы фактически претендуете на чье-то время. И тогда Вы отвечаете за то, чтобы адресат не потратил это время зря. Понятие «возможности» – очень широкое. К возможностям надо отнести и такую характеристику, как пропускная способность канала, по которому происходит связь. Для каждого участка этого канала существует ограничение по объему данных, которые могут быть переданы через него. Это верно даже для современных волоконно-оптических линий. Слово «возможности» можно уместно использовать также, говоря о физической емкости носителей информации на удаленном компьютере. И если Вы случайно отправили в одну и ту же конференцию пять одинаковых сообщений, вы потратили как время подписчиков этой конференции, так и возможности системы (ведь Вы занимали линию передачи и место на диске).

5. Сохраняйте лицо

Используйте преимущества анонимности. Я не хочу, чтобы у Вас создалось впечатление, будто Сеть – это мрачный и жестокий мир, полный людей, которые только и стремятся, что довести друг друга до инфаркта. В целом, все люди хотят, чтобы их любили. В Сети (например, в конференциях) Вы можете встретиться с теми, кого никогда бы не встретили в реальной жизни. И ни один из этих людей не видит Вас. Таким образом, никто не осудит Вас за цвет кожи, глаз, волос, за Ваш вес, возраст или манеру одеваться. Однако, Вас будут оценивать по тому, как Вы пишете. Для тех, кто находится в Сети, это имеет значение. Таким образом, правила грамматики играют важную роль. Если Вы уже давно работаете в Сети и приобрели опыт в этих вопросах, все-таки не грех совершенствоваться. В настоящее время доступно множество пособий, но, возможно, интереснее прослушать курс. Если Вы – взрослый пользователь, то, наверное, нет смысла обучаться азам грамматики в компании подростков. Вместо этого обратите внимание на специализированные курсы, которые можно найти в библиотеках.

Отдавайте себе отчет в том, что говорите. Осмысливайте содержание Вашего письма. Когда Вы хотите сказать, что-то вроде «мне кажется...» или «я слышал, что...», спросите себя – а не проверить ли еще раз правильность Ваших фактов. Недостоверная информация способна вызвать целый шквал эмоций в Сети. И если это повторяется второй и третий раз, может произойти, как в игре «испорченный телефон»: ваши слова будут искажены до неузнаваемости. (Конечно, это можно воспринять как совет не следить за своими посланиями. Но Вы отвечаете именно за то, что посылаете сами, а не за то, что потом сделали с Вашими словами). Кроме того, убедитесь, что Ваши послания ясные и логически выдержанные. Можно сочинить параграф текста, который будет безукоризненным с точки зрения грамматики, но совершенно бессмысленным. Это часто случается, если Вы хотите убедить кого-либо в Вашей правоте, используя множество сложных и длинных слов, которые Вам самому не очень-то и знакомы.

Не оскорбляйте пользователей. Наконец, будьте терпеливы и вежливы. Не употребляйте ненормативную лексику, не идите на конфликт ради самого конфликта.

6. Помогайте другим там, где Вы это можете делать

Наконец, после всех этих негативных моментов, один добрый совет. Почему задавать вопросы в виртуальном пространстве эффективно? Потому что Ваши вопросы читают многие люди, знающие на них ответ. И даже если квалифицированно ответят только несколько человек, общий объем знаний в Сети увеличится. Интернет сам по себе вырос из стремления ученых к обмену опытом. Постепенно в этот увлекательный процесс втянулись другие. Поэтому – участвуйте. Прочитав длинные списки пожеланий того, что не нужно делать, не бойтесь обмениваться своим опытом. Особенно важно обмениваться ответами на Ваши вопросы с другими пользователями. Если Вы предчувствуете, что получите массу ответов на свой вопрос или посылаете его в конференцию, которую редко посещаете – отвечайте на реплики по электронной почте, а не в конференцию. Когда вы получите все

реплики, суммируйте их и отправьте одним сообщением в конференцию. Таким образом, каждый выиграет от общения с Вами. Если Вы и сам – эксперт, то можете сделать больше. Многие люди свободно отправляют целые библиографии, от списков ресурсов по законодательству до перечней популярных книг по UNIX. Если Вы лидируете в группе, в которой отсутствует список ответов на наиболее часто задаваемые вопросы, попробуйте написать такой. Если Вы обнаружили или сами сочинили документ, который по Вашему мнению может быть интересен другим, отправьте его в конференцию. Обмен опытом - увлекательное занятие. Это древняя и славная традиция Сети.

7. Не ввязывайтесь в конфликты и не допускайте их

Флеймы (flames) – это эмоциональные замечания, часто высказанные без учета мнения других участников разговора. Это сообщения, где такт - не самое главное, а цель – вызвать реакцию пользователей: «Ну, давай, скажи, что ты на самом деле думаешь об этом?»

Запрещает ли Netiquette флеймы? Не совсем. Флеймы – тоже старая традиция Сети (а Netiquette никогда не противоречил традициям). Флеймы могуть доставлять удовольствие как сочинителям, так и читателям. А получатели флеймов часто заслуживают их.

Но Netiquette против флеймов, перерастающих в войны – серии злобных посланий, которыми обмениваются, как правило, два или три участника дискуссии. Такие войны могут буквально захватить конференцию и разрушить дружескую обстановку. Это несправедливо по отношению к другим читателям конференции. И очень скоро люди, не участвующие в дискуссии, устают от конфликтов. Фактически происходит недопустимая монополизация ресурсов.

8. Уважайте право на частную переписку

9. Не злоупотребляйте своими возможностями

Некоторые люди в виртуальном пространстве чувствуют себя профессионалами. Это асы в каждой сетевой игре, эксперты в каждом офисе и системные администраторы на каждой системе.

Обладая более широкими знаниями, чем остальные пользователи, или имея в руках более широкие полномочия, эти люди автоматически получают преимущество. Однако это вовсе не означает, что они могут им пользоваться. Например, системные администраторы не должны читать частные почтовые сообщения.

10. Учитесь прощать другим их ошибки

Каждый когда-то был новичком. И не каждый извлечет выгоду из этой книги. Поэтому когда кто-то допускает ошибку – будь это опечатка в слове, неосторожный флейм, глупый вопрос или неоправданно длинный ответ – будьте к этому снисходительны. Даже если руки чешутся ответить, подумайте дважды. Если Вы обладаете хорошими манерами, это еще не значит, что Вы имеете лицензию на преподавание этих манер всем остальным. Если же Вы решили обратить внимание пользователя на его/ее ошибку, сделайте это корректно и лучше не в конференции, а в частном письме. Дайте людям возможность посомневаться. И не будьте высокомерным и надменным. Как известно, исправления в тексте часто тоже содержат грамматические ошибки; также и указание на несоблюдение правил Netiquette, бывает, демонстрирует нарушение этого же Netiquette.

§3. Информационная безопасность

Понятие информационной безопасности. Основные составляющие информационной безопасности. Защита информации. Защищаемая информация. Вредоносное программное обеспечение.

Понятие информационной безопасности

Рассмотрим несколько определений понятия «информационная безопасность».

Доктрина информационной безопасности Российской Федерации: «под **информационной безопасностью** понимается состояние защищенности

национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства».

Закон РФ «Об участии в международном информационном обмене»: **информационная безопасность** – состояние защищенности информационной среды общества[*], обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Безопасность информации (information security) – такое состояние ее в системе обработки, когда несанкционированное получение защищаемой информации лицами и процессами, не имеющими на это специальных полномочий, становится невозможным или сводится к уровню не выше допустимого.

Информационная безопасность – защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. Поддерживающая инфраструктура: системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал.

Понятие безопасности информации тесно связано с понятием безопасность данных.

Безопасность данных – это состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их случайное или преднамеренное получение, изменение или уничтожение.

Защита данных – совокупность целенаправленных действий и мероприятий по обеспечению безопасности данных.

[*] Совокупность технических и программных средств хранения, обработки и передачи информации, а также политические, экономические и культурные условия реализации процессов информатизации

Информационная безопасность страны и ее граждан – серьезная проблема для любого государства (Рис. 1). Информация занимает в жизни каждого человека и государства в целом все более значительное место.

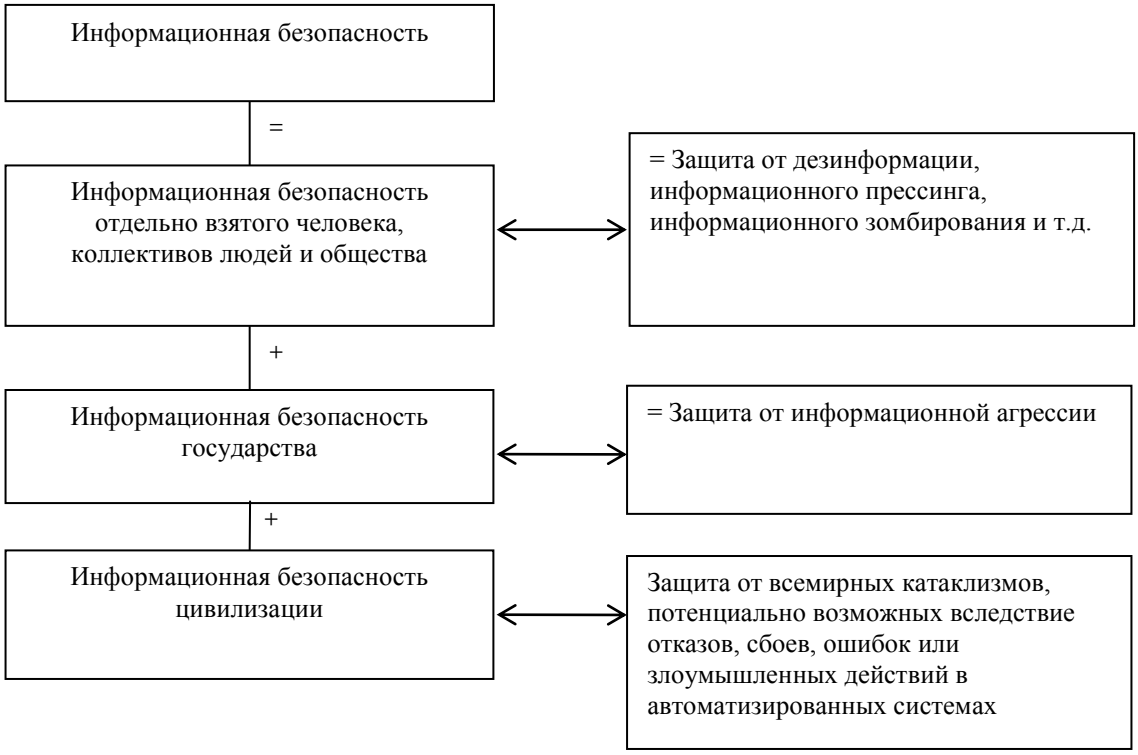


Рис. 1. Структура информационной безопасности

Дезинформация:

- заведомо ложная информация;
- намеренное искажение информации;
- введение в заблуждение ложной информацией

Информационный прессинг – использование потоков информации для оказания воздействия на формирование мнения индивида, общества

Агрессия – действие, наносящее физический вред или психическую травму окружающим людям, сопровождающееся ненавистью. В массовых социальных процессах А. проявляется в форме геноцида, террора, в этнических и идеологических столкновениях. Нередко возникает в результате стереотипного представления образа врага и негативных личных качеств – злобности, жестокости, человеконенавистничества. Устойчивая установка на агрессивное поведение может быть чертой личности. А.,

направленная на самого себя, называется *аутоагрессией* и является показателем патологических изменений личности.

Информационная агрессия – использование информационных потоков для формирование негативного мнения граждан о относительно государства, в сторону которого направлена агрессия

Характеристика составляющих информационной безопасности

Безопасность информации должна отвечать требованиям: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры (Рис. 2).

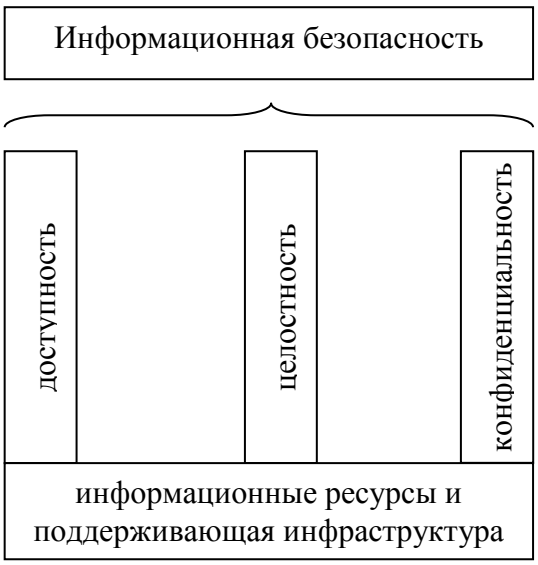


Рис. 2 Составляющие информационной безопасности

Доступность – это возможность за приемлемое время получить требуемую информационную услугу.

Доступность информации – свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

Смысл существования информационных систем – это предоставление определенных информационных услуг. Если это по каким-либо причинам становится невозможным, всем субъектам информационных отношений

наносится ущерб. Например, системы управления (производственные, транспортные), системы предоставления информационных услуг (справочные, банковские).

Под **целостностью** подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Целостность информации – ее существование в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)) (Рис. 3). Практически все нормативные документы и отечественные разработки относятся к статической целостности, хотя динамический аспект не менее важен.

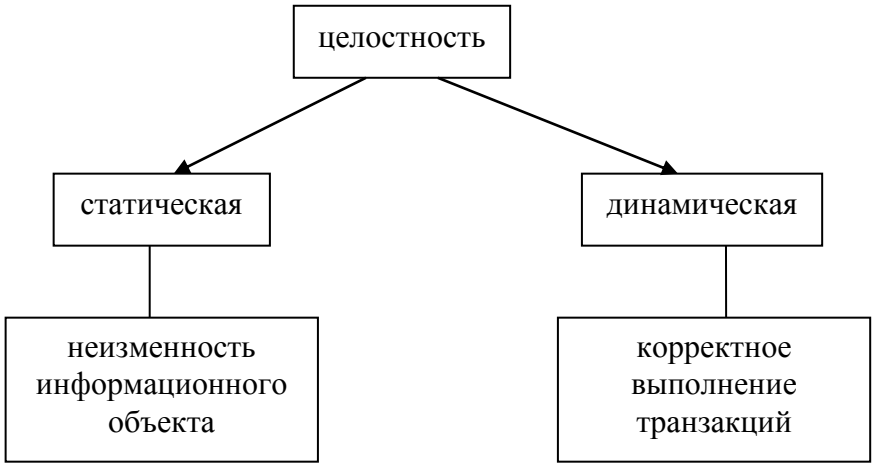


Рис. 3. Виды целостности

Целостность оказывается важнейшим аспектом информационной безопасности в тех случаях, когда информация служит «руководством к действию». Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным. Неприятно и искажение

официальной информации, будь то текст закона или страница Web-сервера какой-либо правительственной организации.

Конфиденциальность – это защита от несанкционированного доступа к информации.

Конфиденциальность информации – субъективно определяемая характеристика (свойство) информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью информационной системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.

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

Защита информации

По содержательной части защита информации рассматривается как:

– предупреждение несанкционированного доступа к информации;

– создание условий, ограничивающих распространение информации;

– ограждение права собственника на владение и распоряжение информацией;

– предотвращение утечки, хищения, утраты, несанкционированного уничтожения, копирования, модификации, искажения, блокирования, разглашения информации, несанкционированных и непреднамеренных воздействий на нее;

– сохранение полноты, надежности, целостности, достоверности, конфиденциальности информации и т.д.

Методологической основой для раскрытия сущности и определения понятия защиты информации должно быть определение понятия защита в целом, безотносительно к предмету защиты.

В толковых словарях термин защита интерпретируется двояко: как

процесс охраны, сбережения, спасения от кого, чего-нибудь неприятного, враждебного, опасного и как совокупность методов, средств и мер, принимаемых для предотвращения, предупреждения чего-то. Таким образом, содержательная часть в этих определениях по смыслу совпадает – это предотвращение, предупреждение чего-то опасного, враждебного. Если соотнести это положение с защитой информации, то самым опасным для собственника информации является нарушение установленного статуса информации, и поэтому содержательной частью защиты должно быть, предотвращение такого нарушения.

Нарушение статуса любой информации заключается в нарушении ее физической сохранности вообще либо у данного собственника (в полном или частичном объеме), структурной целостности, доступности для правомочных пользователей. Нарушение статуса конфиденциальной информации, в том числе составляющей государственную тайну, дополнительно включает в себя нарушение ее конфиденциальности (закрытости для посторонних лиц).

Вторая составляющая сущности защиты информации – способ реализации содержательной части – в толковых словарях, как уже отмечалось, представлена как процесс или как совокупность методов, средств и мероприятий.

Защита информации включает в себя определенный набор методов, средств и мероприятий, однако ограничивать способ реализации только этим было бы неверно. Защита информации должна быть системной, а в систему помимо методов, средств и мероприятий входят и другие компоненты: объекты защиты, органы защиты, пользователи информации. При этом защита не должна представлять собой нечто статичное, а являться непрерывным процессом. Но этот процесс не осуществляется сам по себе, а происходит в результате деятельности людей. Деятельность же, по определению, включает в себя не только процесс, но и цели, средства и результат. Защита информации не может быть бесцельной, безрезультатной и осуществляться без помощи определенных средств. Поэтому именно

деятельность и должна быть способом реализации содержательной части защиты.

Объединив содержательную часть защиты информации и способ реализации содержательной части, можно сформулировать следующее определение:

Защита информации – деятельность по предотвращению утраты и утечки конфиденциальной информации и утраты защищаемой открытой информации.

Цель защиты информации – желаемый результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

Концепция информационной безопасности, как система взглядов на цели, способы обеспечения безопасности информации и средства ее защиты, должна в общем виде отвечать на три простых вопроса (Рис. 4):

- Что защищать?
- От чего защищать?
- Как защищать?

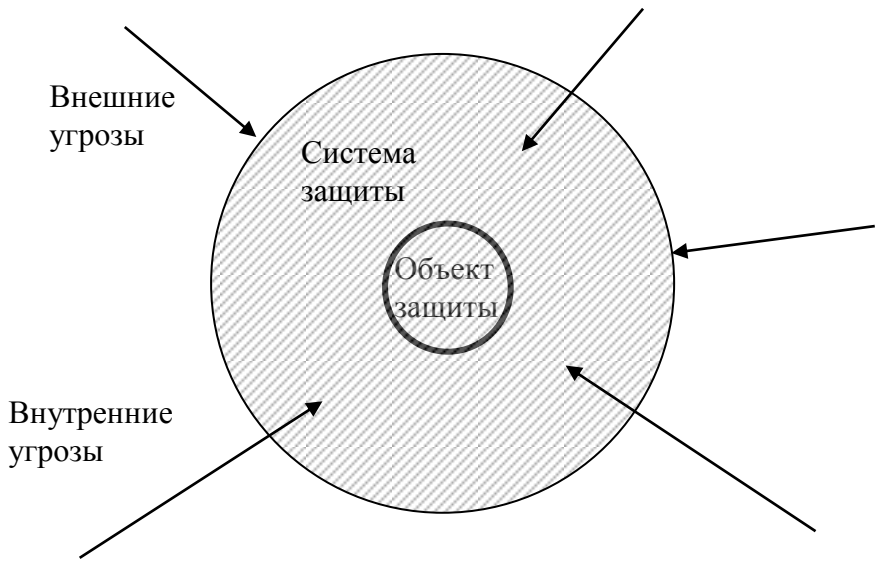


Рис. 4. Концепция информационной безопасности

С вопросом «Что защищать?» связано понятие объекта защиты.

Объект защиты – информация или носитель информации, или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации;

Объект защиты – информация, технические средства и технология ее обработки, в отношении которых необходимо обеспечить безопасность информации.

Ключевое свойство информации – ее ценность, то есть, стоимость ущерба от разрушения, потери или разглашения. Кроме того, спецификой информации является то, что она не исчезает при потреблении, не передается полностью при обмене (в отличие от денег она остается и у старого пользователя). С одной стороны, она является «неделимой», то есть имеет смысл только при достаточно полном объеме сведений, с другой стороны, качество ее повышается при добавлении новых достоверных данных, то есть можно проводить постепенное накапливание сведений и небольшими частями. Поэтому, прежде чем ответить на первый вопрос, необходимо четко разобраться, какая информация может потребовать защиты.

Следующим шагом должно стать разделение этих объектов защиты по степени ценности содержащейся в них информации и определение потенциально опасных систем, позволяющих получить к ним доступ. Поэтому все описанные средства несанкционированного съема информации привязаны к конкретному носителю, для работы с которым они предназначены. На основании вышеизложенного можно практически ответить на первый вопрос. Если хоть в общих чертах знать основные методы работы злоумышленников и возможности их аппаратуры, то это не займет много времени.

Вопрос «От чего защищать?» связан с понятием угрозы. **Угроза** – потенциальная возможность неправомерного преднамеренного или случайного воздействия, приводящее к потере или разглашению информации. Обычно выделяют внутренние и внешние угрозы.

Внешняя угроза – без доступа внутрь системы защиты.

Внутренняя угроза – имеется доступ внутрь системы защиты.

Угроза – это человек, вещь, событие или идея, которая представляет некоторую опасность для ценностей, нуждающихся в защите.

Угроза – это потенциальная возможность определенным образом нарушить информационную безопасность.

Попытка реализации угрозы называется атакой, а тот, кто предпринимает такую попытку, – **злоумышленником**. Потенциальные злоумышленники называются **источниками угрозы.**

С вопросом «Как защитить информацию?» неотъемлемо связано понятие система защиты информации.

Система защиты информации – совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Основными целями защиты информации являются:

– предотвращение утечки, хищения, утраты, искажения, подделки информации;

– предотвращение угроз безопасности личности, общества, государства;

– предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

– предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы;

– обеспечение правового режима документированной информации как объекта собственности;

– защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

– сохранение государственной тайны документированной информации в соответствии с законодательством;

– обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

В соответствии с этими целями процесс защиты информации должен обеспечить поддержание ее целостности и конфиденциальности.

Защищаемая информация

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Собственник защищаемой информации – юридическое или физическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией.

Владелец защищаемой информации – юридическое или физическое лицо, которое имеет полномочия владеть, пользоваться и распоряжаться данной информацией по договору с собственником, в силу закона или решения административных органов.

Защищают и охраняют, как правило, не всю или не всякую информацию, а наиболее важную, ценную для ее собственника, ограничение распространения которой приносит ему какую-то пользу или прибыль, возможность эффективно решать стоящие перед ним задачи.

Какую информацию относят к защищаемой?

Во-первых, секретную информацию. К секретной информации в настоящее время принято относить сведения, содержащие государственную тайну.

Во-вторых, конфиденциальную информацию. К этому виду защищаемой информации относят обычно сведения, содержащие

коммерческую тайну, а также тайну, касающуюся личной (неслужебной) жизни и деятельности граждан.

Таким образом, под *защищаемой информацией* понимают сведения, на использование и распространение которых введены ограничения их собственником.

Защищаемая информация имеет следующие отличительные признаки:

- засекречивать информацию, то есть ограничивать к ней доступ, может только ее собственник (владелец) или уполномоченные им на то лица;
- чем важнее для собственника информация, тем тщательнее он ее защищает. А для того чтобы все, кто сталкивается с этой защищаемой информацией, знали, что одну информацию необходимо оберегать более тщательно, чем другую, собственник определяет ей различную степень секретности;
- защищаемая информация должна приносить определенную пользу ее собственнику и оправдывать затрачиваемые на ее защиту силы и средства.

Таким образом, одним из основных признаков защищаемой информации являются ограничения, вводимые собственником информации на ее распространение и использование.

Вредоносные программы

К вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

Сетевые черви

Сетевой червь – независимая программа, которая размножается путем копирования самой себя из одного сетевого компьютера в другой. Обычно червь не портит данные или программы и не вызывает непредсказуемого поведения, однако может вызвать неоправданную загрузку каналов связи и памяти.

К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

- проникновения на удаленные компьютеры;
- запуска своей копии на удаленном компьютере;
- дальнейшего распространения на другие компьютеры в сети.

Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: электронную почту, системы обмена мгновенными сообщениями, файлообменные сети, LAN (Local Area Network), сети обмена данными между мобильными устройствами (телефонами, карманными компьютерами) и т.д.

Большинство известных червей распространяется в виде файлов: вложение в электронное письмо, ссылка на зараженный файл на каком-либо веб- или FTP-ресурсе в ICQ- и IRC-сообщениях, файл в каталоге обмена P2P и т.д.

Некоторые черви (так называемые «бесфайловые» или «пакетные» черви) распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и активизируют свой код.

Для проникновения на удаленные компьютеры и запуска своей копии черви используют различные методы: социальный инжиниринг (например, текст электронного письма, призывающий открыть вложенный файл), недочеты в конфигурации сети (например, копирование на диск, открытый на полный доступ), ошибки в службах безопасности операционных систем и приложений.

Некоторые черви обладают также свойствами других разновидностей вредоносного программного обеспечения. Например, некоторые черви содержат троянские функции или способны заражать выполняемые файлы на локальном диске, т.е. имеют свойство троянской программы и/или компьютерного вируса.

Классические компьютерные вирусы

Компьютерный вирус – это специально написанная, небольшая по размерам программа, которая может «приписывать» себя к другим программам («заражать» их), создавать свои копии и внедрять их в файлы, системные области компьютера и т.д., а также выполнять различные нежелательные действия на компьютере.

К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью:

– последующего запуска своего кода при каких-либо действиях пользователя;

– дальнейшего внедрения в другие ресурсы компьютера.

В отличие от червей, вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия вируса попадает на удалённые компьютеры только в том случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

– при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;

– вирус скопировал себя на съёмный носитель или заразил файлы на нем;

– пользователь отослал электронное письмо с зараженным вложением.

Некоторые вирусы содержат в себе свойства других разновидностей вредоносного программного обеспечения, троянскую компоненту уничтожения информации на диске.

Троянские программы

Название Троянский конь появилось после использования древними греками пустотелого деревянного коня с вражескими солдатами для проникновения в Трою.

Троянский конь – компьютерная программа, реализующая полезную функцию и содержащая дополнительные скрытые функции, которые тайно используют законные полномочия инициирующего процесса в ущерб безопасности.

Троян (Троянская программа) – это полезная или вроде бы полезная программа, или командная процедура, содержащая скрытый код, который при вызове выполняет некоторые нежелательные действия. Автор троянской программы может сначала создать полезную программу, интересную другим пользователям, или получить ее исходный текст, а затем добавить код, чтобы программа выполняла некоторую разрушающую функцию помимо полезной

В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера.

Данная категория вредоносных программ не является вирусом, так как они не способны самостоятельно проникать на компьютеры, а распространяются злоумышленниками «вручную» под видом «полезного» программного обеспечения. При этом наносимый вред может во много раз превышать потери от традиционной вирусной атаки, которые к тому же могут быть сведены к минимуму при помощи грамотной системы резервного копирования информации

Хакерские утилиты и прочие вредоносные программы

К данной категории относятся:

– утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);

– программные библиотеки, разработанные для создания вредоносного ПО;

– хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);

– «злые шутки», затрудняющие работу с компьютером;

– программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;

– прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам.

Например, те, кому «слабо» написать полноценный вирус, рассылают, например, письма с предупреждениями о предстоящей вирусной атаке и советуют компьютер не включать, в сеть не входить, уничтожить определенные файлы и сообщить всем знакомым и т.п.

Антивирусная защита

Защитить компьютер от вредоносных программ может только сам пользователь. Предотвратить заражение компьютера или минимизировать ущерб, если заражение все-таки произошло, можно только правильно и своевременно применяя антивирусные программы. Само по себе наличие антивирусных средств, если пользоваться ими неправильно, не гарантирует от заражения. Для надежной защиты своего компьютера выполняйте следующие правила:

– Проверяйте на вирусы все носители;

– Используйте антивирусные программы известных проверенных фирм, регулярно обновляйте их базы;

– Не выгружайте резидентную часть (монитор) антивирусной программы из оперативной памяти вашего компьютера;

– Используйте только программы и данные, полученные из надежных источников;

– Никогда не открывайте файлы, прикрепленные к электронным письмам, пришедшим от неизвестных вам отправителей, и не заходите на сайты, рекламируемые через спам-рассылки.

Антивирусная программа (**антивирус**) – программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики – предотвращения заражения файлов или операционной системы вредоносным кодом (например, с помощью вакцинации).

Хорошая антивирусная программа должна:

– Обеспечивать эффективную защиту в режиме реального времени. Резидентная часть (монитор) программы должна постоянно находиться в оперативной памяти вашего компьютера и производить проверку всех файловых операций (при создании, редактировании, копировании файлов, запуске их на исполнение), сообщений электронной почты, данных и программ, получаемых из интернета.

– Позволять проверять все содержимое локальных дисков «по требованию», запуская проверку вручную или автоматически по расписанию.

– Защищать ваш компьютер даже от неизвестных вирусов: программа должна включать в себя технологии поиска неизвестных вирусов, основанные на принципах эвристического анализа.

– Уметь проверять и лечить архивированные файлы.

– Давать возможность регулярно обновлять антивирусные базы.

Важно запомнить, что использование более чем одного антивирусного продукта для защиты в режиме реального времени может вызвать конфликты и чрезмерное использование системных ресурсов, поэтому строго рекомендуется использовать только один антивирус для защиты в режиме реального времени. С увеличением количества вредоносных программ, параллельно с антивирусами нужно иметь и другие программы для обеспечения безопасности компьютера – в первую очередь файерволлы и антишпионы.

§4. Девиантное поведение в сфере информационно-коммуникативных технологий

Понятие девиантного поведения в сфере информационно-коммуникативных технологий. Характеристика видов девиантного поведения в ИКТ-среде.

Понятие девиантного поведения в сфере ИКТ

История информатизации общества исчисляется пока десятилетиями, и еще не совсем ясно, как повлияет компьютеризация на поведение, моральные нормы, психику и жизнь будущих поколений. Развитие общества всегда базировалось на развитии человеческих сообществ. Как считает большинство ученых, первое общество появилось на нашей планете примерно 40-50 тысяч лет назад. Уже тогда человек придумал правила, регулирующие жизнь сообщества и поддерживающие его организацию. С течением времени эти правила менялись и пересматривались, противоречили друг другу, однако, всегда и везде эти правила решали единственную важнейшую задачу: что можно и что нельзя делать. «Правила устанавливали норму, нарушители демонстрировали отклонения от этой нормы». Такое поведение, нарушающее существующие правила, принято называть отклоняющимся или девиантным. **Девиантное поведение** – это целая система поступков, которые противоречат общественным правовым и нравственным нормам. Общество всегда уделяло особое внимание поведению людей, которое не соответствовало общепринятым или официально установленным социальным нормам, такое поведение осуждалось и считалось недопустимым. В широком смысле, девиантное поведение принадлежит человеку, отклонившемуся от нормы или сбившемуся с пути. Такое поведение может принимать различные формы, от отшельника-аскета до закоренелого грешника или убийцы.

Словарь психологических терминов дает следующее определение: «Девиантное поведение – поступок, действия человека, не соответствующие

официально установленным или фактически сложившимся в данном обществе нормам». С.С. Фролов определяет девиантное поведение как «поведение индивида или группы, которое не соответствует общепринятым нормам, в результате чего эти нормы ими нарушаются. Девиантное поведение – следствие неудачного процесса социализации личности: в результате нарушения процессов идентификации и индивидуализации человека, такой индивид легко впадает в состояние «социальной дезорганизации», когда культурные нормы, ценности и социальные взаимосвязи отсутствуют, ослабевают или противоречат друг другу». Е.В. Змановская предлагает следующее определение девиантного поведения – «это устойчивое поведение личности, отклоняющееся от наиболее важных социальных норм, причиняющее реальный ущерб обществу или самой личности, а так же сопровождающееся ее социальной дезадаптацией». Автор считает, что наносимый ущерб самой личности или окружающим людям, может проявляться как «дестабилизация существующего порядка, причинение морального и материального ущерба, физическое насилие и причинение боли, ухудшение здоровья».

Девиантное поведение можно условно разделить на следующие типы (рис. 5):

1. **Асоциальное поведение** – «формы социальной жизни людей, определяемые социально-негативными мотивами и приносящие неудобства или вред другим членам группы, общества». Ряд исследователей (И.П. Подласый, Е.В. Змановская и др.) относят к асоциальному поведению следующие виды: грубость, нечестность, лень, сквернословие, неуважение к старшим, бродяжничество, курение, употребление алкоголя, наркотиков, сексуальные девиации (беспорядочные половые связи, проституция, совращение, вуайеризм, эксгибиционизм и др.), вовлеченность в азартные игры на деньги, граффити, школьные прогулы, субкультурные девиации (сленг), вандализм и т.д. «Асоциальный – значит, почти граничащий с антисоциальным. Проявляется асоциальное поведение в широких пределах –

от легких, незначительных нарушений правил поведения до противоправных действий, вызванных глубокой моральной запущенностью».

2. **Делинквентное (антисоциальное) поведение** – «действия конкретной личности, отклоняющиеся от установленных в данном обществе и в данное время законов, угрожающие благополучию других людей или социальному порядку и уголовно наказуемые в крайних своих проявлениях». К проявлениям делинквентного поведения относят следующие: правонарушения, влекущие за собой уголовную или гражданскую ответственность, хулиганство, грабежи, насилие, жестокое обращение с животными и т.д. Как считает К.К. Платонов, лица с делинквентным поведением в силу индивидуально-психологических особенностей не могут предвидеть результаты своих проступков. «Такие индивиды легкомысленно, часто под влиянием внешней провокации совершают противоправное деяние, не представляя его последствий. Сила побудительного мотива к определенному действию тормозит анализ отрицательных (в том числе, и для самого человека) его последствий».

3. **Аддиктивное поведение** – «одна из форм девиантного поведения, с формированием стремления к уходу от реальности путем искусственного изменения своего психического состояния посредством приема некоторых веществ или постоянной фиксацией внимания на определенных видах деятельности», направленное на развитие и поддержание насыщенных эмоций. Основным мотивом личностей, склонных к аддиктивным формам поведения, является активное изменение не удовлетворяющего их психического состояния, которое рассматривается как «серое», «скучное», «монотонное», «апатичное». Такому человеку не удается обнаружить в реальной действительности какие-либо сферы деятельности, способные привлечь надолго его внимание, увлечь, обрадовать или вызвать иную существенную и выраженную эмоциональную реакцию. Жизнь видится ему не интересной, в силу ее обыденности и однообразности. «Аддиктивное поведение связано с желанием человека уйти из реальной жизни путем изменения состояния своего сознания».

4. **Девиантное поведение на базе гиперспособностей** – вид отклоняющегося поведения, «выходит за рамки обычного поведения человека, в подобных случаях говорят о проявлениях одаренности, таланта, гениальности в какой-либо одной из деятельностей человека». Как считает К.К. Платонов, одаренный человек часто неприспособлен к «бытовой» жизни, неспособен к правильной оценке поступков и поведения других людей, живет в своей реальности. Весь интерес такого индивидуума сосредоточен на деятельности, связанной с его способностями, не принимает активного участия во взаимодействии с окружающим миром.

5. **Патохарактерологическое поведение** – поведение, обусловленное патологическими изменениями характера, сформировавшимися в процессе воспитания.

6. **Психопатологическое поведение** – поведение, обусловленное психическими расстройствами.

Патохарактерологические и психопатологические типы поведения не рассматриваются, поскольку являются проявлением патологических изменений характера или психических заболеваний.

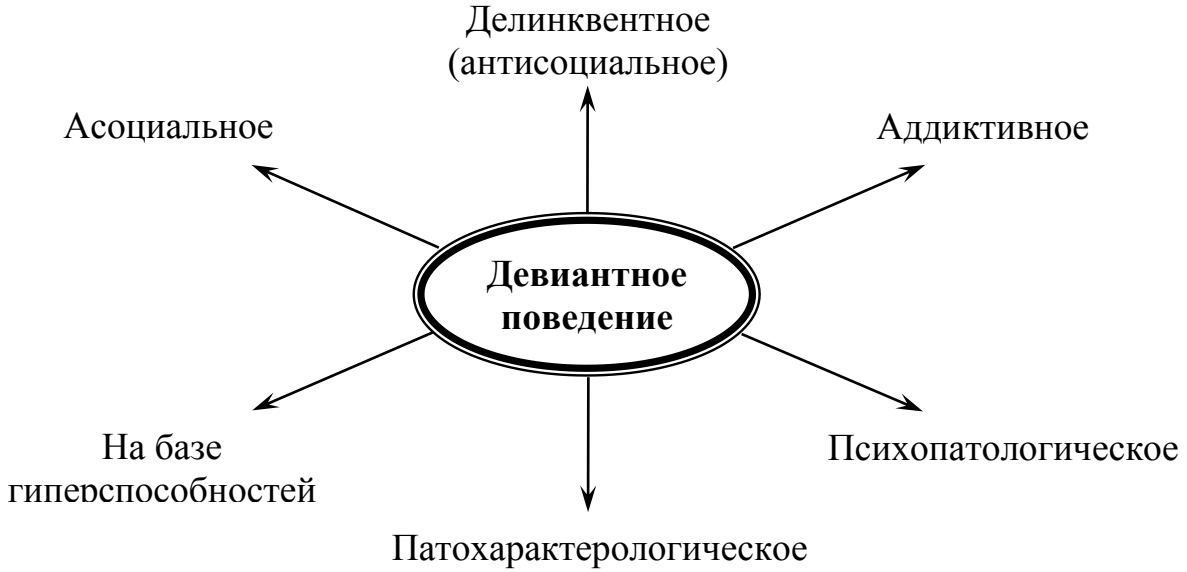


Рис. 5. Классификация девиантного поведения

Появление новой, особой среды обитания человека – виртуального пространства – привело к изменению сложившихся в обществе архетипов, моделей поведения, эстетических образов и форм социальных взаимодействий. Повсеместное внедрение ИКТ в образовательный процесс помогает молодому поколению получить навыки работы с компьютером, приобщиться к современной научной, общественной и культурной жизни. По мере освоения ИКТ существенно меняются и мотивы взаимодействия с ними: от любопытства и игры до саморазвития, самопознания, развития и тренировки определенных умений, навыков и качеств, выбора будущей профессии. Появились и новые виды девиантного поведения, характерные преимущественно для молодых пользователей компьютерных сетей.

Девиантное поведение в сфере ИКТ – вид девиантного поведения индивида (группы индивидов), представляющий систему поступков (или отдельные поступки), опосредованных применением ИКТ (либо направленных в отношении ИКТ), причиняющую ущерб (моральный, физический, экономический и иной) обществу, организациям, частным лицам или самой личности.

По аналогии с классификацией девиантного поведения, девиантное поведение в сфере ИКТ можно дифференцировать на (Рис. 6):

- асоциальное поведение: агрессивные выходки в виртуальном пространстве, увлечение виртуальным сексом, киберхулиганство;

- делинквентное (антисоциальное) поведение: диффамация[1] в киберпространстве, компьютерная преступность и кибертерроризм;

- аддиктивное поведение: Интернет-аддикция, зависимость от компьютерных игр;

- девиантное поведение на базе гиперспособностей: хакерство.

Характеристика видов девиантного поведения в ИКТ-среде

[1] Диффамация – общепринятый в большинстве стран мира юридический термин, под которым понимается правонарушение в виде распространения (произнесения слов, публикации) не соответствующих действительности фактических сведений, порочащих честь, достоинство и деловую репутацию потерпевшего.

Рис 6. Классификация видов девиантного поведения в сфере ИКТ

Асоциальное поведение в сфере ИКТ – поведение, противоречащее общественным нормам и принципам, выступающее в форме безнравственных или противоправных деяний, совершаемых с использованием ИКТ.

Какие отклонения в поведении школьников относятся к асоциальным? И.П. Подласый и Е.В. Змановская выделяют следующие: грубость, нечестность, лень, сквернословие, неуважение к старшим, воровство, хулиганство, бродяжничество, курение, употребление алкоголя, наркотиков, сексуальные девиации (беспорядочные половые связи, проституция, совращение, вуайеризм, эксгибиционизм и др.), вовлеченность в азартные игры на деньги, граффити, школьные прогулы, субкультурные девиации (сленг), вандализм и т.д.. «Асоциальный – значит, почти граничащий с антисоциальным. Схема падения от трудного к асоциальному примерно

такая: сначала появляются отдельные искажения, затем – «шатающаяся» ориентация, которая может перейти в отрицательную, и, наконец, может сформироваться устойчивая антиобщественная направленность личности. Проявляется асоциальное поведение в широких пределах — от легких, незначительных нарушений правил поведения до противоправных действий, вызванных глубокой моральной запущенностью».

Опираясь на выделенные асоциальные отклонения в поведении школьников, можно выявить следующие основные проявления асоциального поведения в сфере ИКТ: script kiddie, увлечение виртуальным сексом, киберхулиганство.

Скриптkидди (англ. script kiddie) – человек, использующий хакерские средства для взлома программ, сайтов и т.д., и не понимающий принципов их работы.

Этот термин используется для обозначения людей, не обладающих существенными познаниями в области ИКТ и просто использующих для взлома чужие хакерские утилиты. Скрипткидди чаще всего являются подростки, пользующиеся чужими программами, найденными кем-то уязвимостями, взламывающие системы с помощью написанных чужими руками эксплойтов[2]. Так как скрипткидди имеют слабые познания в сетевых технологиях, они взламывают не определенные системы, а только те, которые наименее защищены. Если взламывается веб-сайт, то зачастую подменяется главная страница сайта, на которую выкладывается любая информация, способствующая самоутверждению скрипткидди (дефейс). Одной из разновидностей скрипткидди являются так называемые «Kit clicker'ы», использующие готовые наборы кода для создания вирусов. Очень часто скрипткидди ошибочно причисляют к хакерам, однако ни скрипткидди, ни китклikеры таковыми не являются, это люди, не умеющие ни создавать соответствующие программы, ни находить уязвимости в

[2] Эксплойт (англ. exploit — использовать) — это общий термин в сообществе компьютерной безопасности для обозначения фрагмента программного кода, который, используя возможности предоставляемые ошибкой, отказом или уязвимостью, ведёт к повышению привилегий или отказу в обслуживании компьютерной системы.

существующих – они используют уже готовые программы или наборы программ, при этом абсолютно не понимая принципа их действия.

Виртуальный секс (англ. cybersex – киберсекс) – секс, представляющий собой мастурбацию перед монитором компьютера, где возбуждение приходит от созерцания эротических образов, либо в сочетании с интерактивным общением по Интернету на тему секса. Это одно из проявлений сексуальных отклонений, которое может повлечь за собой: беспорядочные половые связи, проституцию, совращение, вуайеризм, эксгибиционизм и др. По словам сексолога В. Маслова, «увлечение подростков компьютерным порно способно нанести серьезный ущерб психике, даже вызвать полное отвращение к будущей сексуальной жизни». Сексопатолог Д. Капустин считает, что «проблему виртуального секса нужно решать как можно быстрее. При помощи компьютера подростки удовлетворяют свои тайные пороки и комплексы, сознательно уходят от реальности. Просмотр порносайтов в юном возрасте снимает заложенные природой барьеры, неизбежно приводит к возникновению многочисленных извращений, ранним половым связям».

Киберхулиганство – поведение, особенно свойственное подросткам, пытающимся реализоваться за счет пострадавшего, особенно в сети (в форумах, чатах, блогах). Немалое влияние на подобное поведение оказывает и мнимая анонимность и ненаказуемость.

- проявления агрессии;
- оскорбления, использование нецензурных и бранных выражений и т.п.;
- различные хулиганские выходки;
- использование оскорбительных, вызывающих или неприличных смайликов, аватар, никнеймов (ников), картинок и фотографий, подмена IP-адресов (в локальных сетях) и т.п.

Троллинг

Размещение в сети (форумах, чатах, блогах) грубых или провокационных сообщений, которые мешают обсуждению или оскорбляют

его участников с целью привлечь внимание к персоне тролля (человека, занимающегося троллингом).

Флудерство, флужение (от англ. flood – наводнение) – размещение в сети (форумах, чатах и блогах) сообщений, занимающих большие объемы и не несущие никакой полезной информации.

Может использоваться с целью троллинга, либо от нечего делать (частный случай – технический флуд, как хакерская атака).

Флеймерство (от англ. flame – пламя; здесь – вспыхнуть, взорваться) – размещение в сети (форумах, чатах и блогах) сообщений, направленных на разжигание ссоры.

Применяется либо из соображений троллинга, либо из-за обиды на виртуального собеседника, чаще всего, «флеймить» означает «спорить не по существу, прибегать не к аргументам, а к обыденной брани».

Делинквентное (антисоциальное) поведение в сфере ИКТ – отклоняющееся поведение, представляющее собой проступок либо уголовно наказуемое деяние, совершенное посредством либо в сфере ИКТ, влекущее за собой получение выгоды и/или нанесение материального, психологического, информационного вреда жертве. К проявлениям делинквентного поведения Е.В. Змановская относит следующие: правонарушения, влекущие за собой уголовную или гражданскую ответственность, хулиганство, грабежи, насилие, жестокое обращение с животными и т.д. В целом, антисоциальное поведение направлено против существующих норм, выраженных в общественных законах.

Как считает К.К. Платонов, лица с делинквентным поведением в силу индивидуально-психологических особенностей не могут предвидеть результат проступка. «Такие индивиды легкомысленно, часто под влиянием внешней провокации совершают противоправное деяние, не представляя его последствий. Сила побудительного мотива к определенному действию тормозит анализ отрицательных (в том числе, и для самого человека) его

последствий». Делинквентное поведение может проявляться, к примеру, в озорстве и желании развлечься. К проявлениям делинквентного поведения в сфере ИКТ будем относить: диффамация, компьютерные и киберпреступления, кибертерроризм.

Диффамация в киберпространстве – анонимное распространение по компьютерным сетям заведомо ложной информации с целью нанести моральный ущерб выбранному объекту.

Кибертерроризм – «преднамеренные политически мотивированные атаки на информационные, компьютерные системы, компьютерные программы и данные, выраженные в применении насилия по отношению к гражданским целям со стороны субнациональных групп или тайных агентов».

Кибертерроризм использует открытость Интернета для дискредитации правительств и государств, размещения сайтов террористической направленности, порчи и разрушения ключевых систем путем внесения в них фальсифицированных данных или постоянного вывода этих систем из рабочего состояния, что порождает страх и тревогу, и является своего рода дополнением к традиционному виду терроризма. По мнению исследователей можно выделить два вида кибертерроризма: совершение с помощью компьютеров и компьютерных сетей террористических действий и также использование киберпространства в целях террористических групп, но не для непосредственного совершения терактов. Террористы используют Интернет как для сбора информации о предполагаемых целях, сбора денег (вплоть до вымогательства) и для обращения к массовой аудитории без цензуры и ограничений, так и для вовлечения в свои ряды соучастников (зачастую даже не подозревающих об истинных целях), информационно-психического контроля и размещения сайтов террористической направленности.

Главное в тактике кибертерроризма состоит в том, чтобы это киберпреступление имело опасные последствия, стало широко известно

населению, получило большой общественный резонанс и создавало атмосферу угрозы повторения акта без указания конкретного объекта.

Компьютерные и киберпреступления

Компьютерное преступление – это «общественно опасное действие или бездействие, которое совершается с использованием электронно-вычислительной техники или информации, и причиняет, или может причинить, вред имущественным или общественным интересам государства, а также предприятий, учреждений, организаций независимо от формы собственности, общественных формирований и граждан, правам личности».

Под **киберпреступностью** подразумевается любое противозаконное действие, возникающее «в результате использования одного или нескольких Интернет-компонентов, например, таких, как веб-сайты, форумы или электронная почта».

Преступление, совершенное в киберпространстве – это «виновное противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ». По мнению экспертов ООН, термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде. К основным видам компьютерных и киберпреступлений будем относить: крякерство; написание вредоносных программ; кардинг; фрикинг; спамерство; фишинг.

Крякерство (крякинг, крэкинг) – это взлом и изменение программ на свое усмотрение или на заказ.

Крякер, кракер (англ. cracker) – человек, занимающийся взломом защиты лицензионных программных средств.

Кряк или ***крек*** (от англ. crack) (жарг.) – специальная программа (либо файл, содержащий инструкции для такой программы), изменяющая некоторые байты в другой программе, выполняемая с целью отключения защиты от копирования или запрещение чтения системного времени (для тех программ, которые имеют демонстрационный период, в течение которого имеют полную функциональность).

Результатом работы крякера являются т. н. кряки и генераторы серийных кодов (в случае ориентации на массового пользователя), или же просто – модифицированная («крякнутая» или «взломанная») программа с нужной функциональностью.

Проблема взлома лицензионных программ появилась одновременно с самими лицензионными программами. Нежелание, либо в частности, невозможность, заплатить требуемую сумму за необходимое программное обеспечение привело к появлению такого «подвида хакеров», которые стали заниматься взломом платных программ. Либо, крякерством (также как и хакингом) занимаются из любопытства. Взламывая исходный код программы, такие люди могут на свое усмотрение: модифицировать программу (устранив какие-либо несовершенства), заставить программы решать необходимую задачу, внести какие-либо изменения, добавить особенности и т.п.

Написание вредоносных программ

Существует две различных группы вредоносных программ: для компьютера-жертвы и программы-инструменты хакеров. К вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети. Написанием

вредоносных программ в основном занимаются 4 группы людей:

– молодые люди, не нашедшие более достойного применения своих знаний, занимаются этим для самоутверждения;

– молодые люди, экспериментирующие со своими знаниями или чужими готовыми программами, чаще всего это скрипткидди;

– «профессионалы», использующие свои знания во вред, создающие вредоносные программы для достижения своих целей;

– «исследователи», изобретающие новые методы заражения, сокрытия, противодействия и т.п. ради исследования потенциальных возможностей вредоносных программ.

Кардинг (англ. carding) – использование чужой (ворованной) кредитной карты для оплаты товаров или услуг.

Кардер – человек, совершающий незаконные операции с кредитными карточками других лиц, с целью получения денег, снятых с карточки.

Кардеры делятся на 2 вида: интернет-кардеры, которые работают только с информацией, и реальные кардеры, которые работают с пластиковыми копиями кредитных карт. В настоящее время кардингом занимаются уже не отдельные мошенники, а хорошо организованные преступные сообщества. В состав таких группировок входят высоко профессиональные специалисты, они оснащены современной техникой и необходимыми документами. Выделяют следующие категории преступлений, совершаемых с использованием пластиковых (банковских) карт: злоупотребления с подлинными банковскими картами; изготовление поддельных банковских карт; сбыт поддельных банковских карт; злоупотребления с товарными чеками (слипами); использование поддельных банковских карт. Преступные сообщества очень часто привлекают к своему ремеслу новичков через Интернет: существуют специальные сайты, форумы, на которых каждый может узнать суть кардерства, какие прибыли оно может приносить, выйти на связь с профессионалами, получить полезный совет.

Фрикинг – несанкционированное получение информации (в т.ч. шпионаж) при помощи электронных устройств, а также путем несанкционированного подключения к телекоммуникационным сетям.

Фрикер – специалист в области электроники применяющий свои знания в промышленном (экономическом) шпионаже или извлекающий выгоду путем «электронного» мошенничества.

Преступная деятельность фрикеров направлена на получение кодов доступа, хищение телефонных карточек и номеров доступа с целью перенести оплату за телефонные разговоры на счет другого абонента. В частности, сейчас фрикинг в основном подразумевает под собой – разблокирование и русификация сотовых телефонов, прослушивание телефонной связи, «клонирование» телефонных номеров – когда на один номер сотового телефона подключено до 100 абонентов.

Спамерство – массовая рассылка рекламных объявлений по электронной почте без согласия на это получателей.

Спамерство активно используется как канал для различных видов мошенничества и противозаконной деятельности. Может содержать: рекламу незаконной продукции (порнография, лекарственные средства, ворованную информацию и т.д.), рекламу преступной деятельности, антирекламу (запрещенную законодательством), выманивание под различными (благотворительность, оформление документов) предлогами денег, элементы фишинга, религиозные письма или «письма счастья», вредоносные программы и т.д.

Фишинг (англ. «рыбалка») – получение конфиденциальной информации с целью использования в корыстных целях.

Сегодня существует три вида фишинга – почтовый, онлайновый и комбинированный. Первый из них самый старый. Он заключается в отправке

жертве специального письма по электронной почте с требованием выслать в ответ какие-либо данные. Под онлайновым фишингом подразумеваются аферы, когда злоумышленники копируют какие-либо сайты, чаще всего Интернет-магазины. При этом они используют похожие доменные имена и идентичный дизайн. На смену им пришел третий тип фишинга, комбинированный: создается поддельный сайт какой-либо организации, а затем на него завлекаются пользователи с помощью писем-приманок. Главная опасность комбинированного фишинга заключается в его высокой правдоподобности, никто не требует от человека отправки пароля по электронной почте. Ему всего лишь предлагают зайти на корпоративный сайт по приведенной ссылке (на самом деле это всего лишь подделка) и самому произвести необходимые операции. Иногда фишинг является обычным вымогательством.

Аддиктивное поведение в сфере ИКТ – одна из форм девиантного поведения с формированием стремления к уходу от реальности путем постоянной фиксации внимания на определенных видах деятельности, опосредованных ИКТ.

В.Д. Менделевич выделяет следующие психологические особенности лиц с аддиктивными формами поведения:

1) сниженная переносимость трудностей повседневной жизни, наряду с хорошей переносимостью кризисных ситуаций;

2) скрытый комплекс неполноценности, сочетающийся с внешне проявляемым превосходством;

3) внешняя социабельность, сочетающаяся со страхом перед стойкими эмоциональными контактами;

4) стремление говорить неправду;

5) стремление обвинять других, зная, что они невиновны;

6) стремление уходить от ответственности в принятии решений;

7) стереотипность, повторяемость поведения;

8) зависимость;

9) тревожность.

Основным мотивом личностей, склонных к аддиктивным формам поведения, является активное изменение не удовлетворяющего их психического состояния, которое рассматривается как «серое», «скучное», «монотонное», «апатичное». Такому человеку не удается обнаружить в реальной действительности какие-либо сферы деятельности, способные привлечь надолго его внимание, увлечь, обрадовать или вызвать иную существенную и выраженную эмоциональную реакцию. Жизнь видится ему не интересной, в силу ее обыденности и однообразности. Он не приемлет того, что считается в обществе нормальным: необходимости что-то делать, заниматься какой-либо деятельностью, соблюдать какие-то принятые в семье или в обществе традиции и нормы. Можно говорить о том, что у индивида с аддиктивной нацеленностью поведения значительно снижена активность в обыденной жизни, наполненной требованиями и ожиданиями. К аддиктивному поведению в сфере компьютерных технологий будем относить следующее: Интернет-аддикция и геймерство (зависимость от компьютерных игр).

Интернет-зависимость – это «навязчивое желание войти в Интернет, находясь off-line, и неспособность выйти из Интернет, будучи on-line».

Феномен «зависимости от Интернета», или «Интернет-аддикции» интенсивно обсуждается в настоящее время. В самом общем виде Интернет-зависимость определяется как «нехимическая зависимость от пользования Интернетом». Впервые данный термин предложил американский психолог доктор психологических наук Айвен Голдберг для описания непреодолимой тяги к использованию Интернета в 1996 году. Поведенчески Интернет-зависимость проявляется в том, что приоритеты в повседневной, бытовой жизни людей резко смещаются в сторону всего связанного с работой в Интернете. Порой люди настолько предпочитают жизнь в Сети, что фактически начинают отказываться от своей «реальной» жизни.

Родоначальниками психологического изучения феноменов зависимости от Интернета могут считаться два американца: психолог, профессор Питтсбургского университета К. Янг и психиатр И. Голдберг.

В 1996 г. Кимберли Янг создала опросник, определяющий степень зависимости от Интернета.

К. Янг выделила стадии зависимости от Интернета:

- на первой стадии происходит знакомство и заинтересованность Интернетом и новыми возможностями;
- на второй стадии Интернет начинает замещать значимые сферы жизни;
- на третьей стадии можно говорить о, собственно, аддикции.

По К. Янг степень аддикции определяется не количеством проведенного в Интернете времени, а суммой потерь в реальной жизни. В основном, зависимость сказывается на таких сторонах жизни, как участие в жизни собственной семьи, выполнение повседневных обязанностей, полноценный сон, чтение книг и периодики, просмотр телепередач, общение с друзьями, занятия спортом, хобби, социальные контакты. Более развернутую систему критериев наличия зависимости приводит А. Голдберг (www.psycom.net).

А.Е. Войскунский обобщил все ранее описанные поведенческие характеристики. Как он считает – «Зависимость от Интернета, или Интернет-аддикция – реально существующий феномен, но для того, чтобы считать его заболеванием, в настоящее время недостаточно клинических данных… Феномен Интернет-аддикции постоянно видоизменяется вместе со стремительным развитием Интернета и заслуживает досконального изучения» (11, 126). По его мнению, Интернет-аддикция включает в себя:

- зависимость от компьютера, т.е. пристрастие к работе с компьютером (играм, программированию или другим видам опосредствованной компьютером деятельности);

- длительная (многочасовая) навигация по сети без конкретной цели; источником удовольствия служит факт пребывания в Сети, мультимедийные формы поощрения и стимуляции посетителей сайтов либо узнавание нового в результате подобных блужданий;

- патологическая привязанность к опосредствованным Интернетом азартным играм, онлайновым аукционам и биржам или электронным покупкам;

- зависимость от «киберотношений», т.е. от социальных контактов: общения (в чатах, групповых играх и телеконференциях) и установления в ходе общения дружеских отношений или «флирта»;

- зависимость от «киберсекса», т.е. от порнографических сайтов в Интернете, от обсуждения сексуальной тематики в чатах или специальных телеконференциях «для взрослых».

Геймерство (от англ. game – игра) – зависимость от компьютерных игр, игромания; увлечение компьютерными играми и другими видами виртуальной реальности.

Геймер – (англ. жаргонизм Gamer) профессиональный игрок в компьютерные игры.

История компьютерных игр насчитывает чуть более тридцати лет. Никто и не мог предположить, что дорогие, грандиозные вычислительные машины могут быть использованы для развлечения. Первая «компьютерная» игра предположительно зародилась в недрах программируемого калькулятора и была просто сложной головоломкой. Развитие компьютерной техники повлекло за собой прогресс в области развлечений – уже в 1972 году на рынке появилась первая в мире игровая приставка (компьютер только для игр) – Odyssey компании Magnavox. С того времени разработкой игр занимались в основном энтузиасты. В 90-х годах прошлого века появляется множество игр, ставших классикой – Civilization (1991), Dune 1,2 (1992), Wolfenstein3D (1992), Doom (1993), Doom 2 (1994), War Craft (1994), War

Craft II: Tides of Darkness (1995), Full Throttle (1995), Duke Nukem 3D (1996), Command&Conquer: Red Alert (1996), Quake (1996), Quake 2 (1997), KKND (Krush, Kill 'N' Destroy) (1997), KKND 2 (1998), Star Craft (1998), Half-Life: Counter-Strike (1998) и др.

Классификация компьютерных игр

На сегодняшний день ни в отечественной, ни в западной литературе не существует четкой классификации компьютерных игр.

В игровой индустрии и среди разработчиков игр принята жанровая классификация игр: First Person Shooter («стрелялка» от первого лица), 3D-Action; Role Playing Game – RPG (ролевые игры); Real-Time Strategy (стратегии в реальном времени); Turn-Based Strategy (пошаговые стратегии); Quest[3], Adventure (приключенческие игры); Simulator (симуляторы); спортивные игры; головоломки (Puzzles); логические игры; компьютерные варианты настольных игр.

В 1988 году психолог А.Г. Шмелев предложил следующую классификацию компьютерных игр. Он выделяет несколько классов игр: стимулирующие преимущественно формальнологическое, комбинаторное мышление (компьютерные варианты шахмат и шашек); азартные игры (компьютерный покер, тотализаторы); спортивные и «конвейерные» игры (компьютерный теннис, футбол, тетрис и т.д.); военные игры и игры-единоборства (компьютерное карате и т.д.); игры типа преследование-избегание; авантюрные (приключения, аркады) игры; игры-тренажеры (управление компьютерными самолетами, автомобилями, также экономические игры).

Специалист по компьютерным играм И.В. Бурлаков в 1999 году предложил свою классификацию компьютерных игр: Дум(DOOM)-образные игры, стратегические игры, квесты, симуляторы (компьютерные игры, имитирующие управление транспортным средством), пасьянс.

М.С. Иванов предлагает следующую психологическую классификацию компьютерных игр:

[3] Quest (kwest) — англ. поиск, искомый предмет, отъезд рыцаря на поиски приключений, дознание.

I. Ролевые компьютерные игры[4]:

- игры с видом «из глаз» «своего» компьютерного героя. В играх такого типа достигается максимальный эффект «присутствия», субъективного ощущения пространства игрового мира. Специфика здесь в том, что вид «из глаз» провоцирует играющего к сильной идентификации с компьютерным персонажем, к полному вхождению в роль. При игре в такие игры наблюдается наибольшая, по сравнению с играми других типов, сила эмоциональных проявлений играющего: человек испытывает эмоции страха, если в игровом мире есть угроза его безопасности, эмоции радости, если в виртуальном мире у него что-то получилось, человек испытывает гнев, если не может выполнить какое-то задание, предусмотренное сюжетом игры и тд.

- Игры с видом извне на «своего» компьютерного героя. Отождествление себя с компьютерным персонажем носит менее выраженный характер, вследствие чего мотивационная включенность и эмоциональные проявления также менее выражены, по сравнению с играми с видом «из глаз».

- Руководительские игры. В играх этого типа играющий может выступать в роли руководителя самой различной спецификации. Это единственный класс ролевых игр, где роль не задается конкретно, а воображается играющим. Вследствие этого «глубина погружения» в игру и свою роль будет существенной только у людей с хорошим воображением. Однако мотивационная включенность в игровой процесс не менее сильна, чем в случае с другими ролевыми играми

II. Неролевые компьютерные игры.

- Аркады. Все, что нужно делать играющему - быстро передвигаться, стрелять и собирать различные призы, управляя компьютерным персонажем или транспортным средством. Эти игры в большинстве случаев весьма безобидны в смысле влияния на личность играющего, т.к. психологическая зависимость от них чаще всего носит

[4] Ролевые компьютерные игры – это игры, в которых играющий действует в моделируемом компьютером виртуальном мире, принимая на себя роль компьютерного персонажа, опосредующего эту деятельность (16).

кратковременный характер.

- Головоломки. К этому типу игр относятся компьютерные варианты различных настольных игр (шахматы, шашки, нарды и т.д.), а также разного рода головоломки, реализованные в виде компьютерных программ. Мотивация, основанная на азарте, сопряжена здесь с желанием обыграть компьютер, доказать свое превосходство над машиной.

- Игры на быстроту реакции. Сюда относятся все игры, в которых играющему нужно проявлять ловкость и быстроту реакции. Отличие от аркад в том, что они совсем не имеют сюжета и, как правило, совершенно абстрактны, никак не связаны с реальной жизнью. Мотивация, основанная на азарте, потребности «пройти» игру, набрать большее количество очков, может формировать вполне устойчивую психологическую зависимость человека от этого типа игр.

- Традиционно азартные игры. Сюда входят компьютерные варианты карточных игр, рулетки, имитаторы игровых автоматов.

Иванов так же отмечает, что «В психологическом смысле компьютерный персонаж, роль которого принял играющий, является психологической проекцией этого человека на виртуальный мир компьютерной игры».

Возникновение игровой аддикции

Психологи, исследователи феномена игровой аддикции, выделяют два основных механизма образования зависимости от компьютерных игр: потребность в уходе от реальности и в принятии роли другого. Процесс благотворного влияния компьютерных игр представляется следующим образом: человек на время «уходит» в виртуальность, чтобы снять стресс, отвлечься от проблем и т.д. А в патологических клинических случаях происходит наоборот: человек на время «выходит» из виртуальности в реальный мир, чтобы не забыть, как он выглядит, и удовлетворить физиологические потребности (Рис. 7). Остальная часть пирамиды потребностей сдвинута в виртуальную реальность и удовлетворяется там.

Реальный мир начинает казаться чужим и полным опасностей, потому что человек не может в реальном мире делать все то, что ему дозволено в виртуальном. М.С. Иванов констатирует, что использовав однажды компьютерную игру как «средство достижения того же эмоционального состояния подъема, чувства удовлетворения, которое возникает при удовлетворении высших потребностей, некоторые индивиды склонны к повторному достижению таких переживаний этим легким путем… Образуется «порочный круг» эффекта «затягивания» в компьютерную игровую деятельность». С одной стороны, данный тип зависимости отнимает значительную часть времени, выключая аддикта из активной жизни, с другой стороны, такая зависимость – явление временное, не постоянное. Чаще всего может наступить момент пресыщения компьютером и виртуальным миром, создаваемым играми, и тогда осуществляется либо переход в профессиональную сферу (киберспорт), либо интерес угасает (но всегда может возникнуть вновь, но уже к новой «игрушке»).

Рис. 7. Пирамида потребностей по А.Маслоу

Психологи-исследователи феномена игровой аддикции говорят о четырех стадиях развития зависимости (Рис. 8).

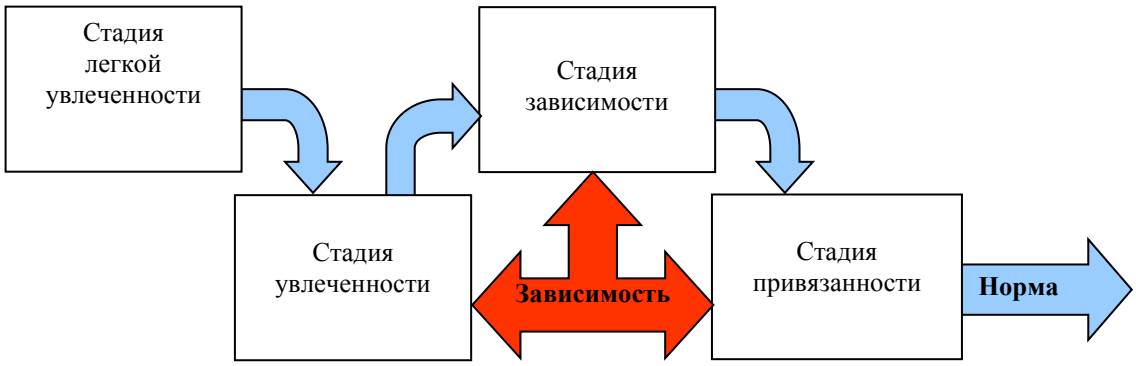


Рис. 8. Стадии развития зависимости

Стадия легкой увлеченности. Играя, человек получает удовольствие. Природа человека такова, что он стремится повторить действия, доставляющие удовольствие, удовлетворяющие потребности. Вследствие этого человек начинает играть, уже не случайным образом очутившись за компьютером, стремление к игровой деятельности принимает некоторую целенаправленность. Однако специфика этой стадии в том, что игра в компьютерные игры носит скорее ситуационный, нежели систематический характер. Устойчивая, постоянная потребность в игре на этой стадии не сформирована, игра не является значимой ценностью для человека.

Стадия увлеченности. Фактором, свидетельствующим о переходе человека на эту стадию формирования зависимости, является появление в иерархии потребностей новой потребности – участие в компьютерной игре. На самом деле стремление к игре – это потребность в бегстве от реальности. Игра в компьютерные игры на этом этапе принимает систематический характер.

Стадия зависимости. Зависимость может оформляться в одной из двух форм: социализированной и индивидуализированной. Социализированная форма игровой зависимости отличается тем, что такие люди очень любят играть совместно, играть с помощью компьютерной сети друг с другом. Игра в основном носит соревновательный характер. Эта форма зависимости менее пагубна в своем влиянии на психику человека. Индивидуализированная форма зависимости является крайней формой зависимости, когда

нарушаются не только нормальные человеческие особенности мировоззрения, но и взаимодействие с окружающим миром. Нарушается основная функция психики – она начинает отражать не воздействие объективного мира, а виртуальную реальность. Эти люди часто подолгу играют в одиночку, потребность в игре находится у них на одном уровне с базовыми физиологическими потребностями. Для них компьютерная игра – это своего рода наркотик. Если в течение какого-то времени они не «принимают дозу», то начинают чувствовать неудовлетворенность, испытывают отрицательные эмоции, впадают в депрессию. Это клинический случай, психопатология или образ жизни, ведущий к патологии.

Стадия привязанности. Эта стадия характеризуется угасанием игровой активности человека, сдвигом психологического содержания личности в целом в сторону нормы. Отношения человека с компьютером на этой стадии можно сравнить с неплотно, но крепко пришитой пуговицей. Т.е. человек «держит дистанцию» с компьютером, однако полностью оторваться от психологической привязанности к компьютерным играм не может. Это самая длительная из всех стадий – она может длиться всю жизнь, в зависимости от скорости угасания привязанности.

Девиантное поведение на базе гиперспособностей в сфере ИКТ - поведение, сопровождающееся девиациями в обыденной жизни, при особой одаренности и даже гениальности в области информационно-коммуникативных технологий.

Хакерство – ярко выраженное увлечение познанием в сфере информационных компьютерных технологий, выходящее за рамки профессиональной или учебной деятельности (и необходимости).

Хакерами (англ. hacker) в узком смысле слова называют людей, проявляющих исключительный интерес к проблематике защиты информации и применения этих знаний, как для защиты информационных систем, так и для их взлома.

Хакерство во всем мире считается у молодежи модным стилем поведения, популярность соответствующих стилей поведения возрастает. Наряду с этим, хакер – это специалист, который стремится, прежде всего, к общению с другими пользователями информационного сообщества, к выражению своих мыслей, идей в свободной, творческой атмосфере. В большинстве своем это слово не носит криминального характера – основной лозунг хакерского движения – «Информация должна быть бесплатной и общедоступной». Несмотря на достаточное разнообразие видов деятельности хакеров, различные течения внутри данной субкультуры и ее богатую историю, СМИ зачастую представляют хакеров только с негативной стороны и проецируют в общество масс-медийный «образ» хакеров. К сожалению, большая часть подростков подхватывают именно этот образ и пытаются его воплотить в реальность. Массовая культура создает образ «героя», обывательский образ подростка, который, не выходя из своей комнаты, со своего компьютера может сделать подвиг, о котором будут говорить все, и тогда он отомстит обществу взрослых и покажет ему свою индивидуальность и подростковую независимость. В качестве причин увлечения хакерством исследователи выделяют следующие:

- дезадаптация к социальной жизни, несформированность социальных привычек и умения общаться;

- деструктивные желания и склонности (стремление ломать, разрушать);

- склонность к анархии, противоправным действиям, неразвитость личностной и нравственно-правовой сфер;

- «феномен Робин Гуда» – героя, который возвращает информационно обездоленным людям забранные у них информационные ценности;

- развитие своих умений, повышение собственного мастерства и квалификации.

В исследованиях деятельности хакеров доминируют два подхода. Первый из них на основе критерия несанкционированного вторжения в

информационную систему отождествляет хакерство с преступной деятельностью. Второй подход опирается на критерий мотивации при оценке деятельности хакеров. В среде технической интеллигенции, связанной с информационными технологиями, сформировался третий подход. «Хакерство» рассматривается как исторический и социокультурный феномен, имеющий собственные специфические признаки на различных этапах своего развития.

Наиболее точно отражающим суть понятия «хакер» нам кажется высказывание начальника одного из отделов Управления «Р» Д.В. Чепчугова: «Хакеры – это не преступники, хакеры – это в большинстве талантливые ребята, а преступники те, кто вовлекает их в совершение преступления».

§5. Информационно-психологическая безопасность

Информационно-психологическая безопасность. Виды информационного манипулирования. Способы защиты.

Информационно-психологическая безопасность

Особое место в информационной сфере общества занимают индивидуальное, групповое и массовое сознание людей, которое все в большей степени подвергается агрессивным информационным воздействиям, что в ряде случаев наносит ущерб психическому и нравственному здоровью граждан, разрушает моральные нормы жизни общества, приводит к дестабилизации социально-политической обстановки. Состояние информационной среды общества оказывает весьма существенное влияние на состояние психики людей, стереотипы их поведения в обществе и личной жизни, на их моральные нормы, нравственные критерии и духовные ценности. В связи с этим в последние годы в обществе начала осознаваться новая глобальная проблема – проблема информационно-психологической безопасности.

Информационно-психологическая безопасность – состояние защищенности граждан, их отдельных групп и социальных слоев, а также населения в целом от негативных информационно-психологических воздействий.

Негативное информационно-психологическое воздействие – воздействие на человека или группу лиц (в том числе, помимо их воли), осуществляемое с использованием специальных средств и методов воздействия на психику человека и приводящее к негативным последствиям для личности, общества и государства.

Специальные средства воздействия – технические и программные средства, используемые для негативного информационно-психологического воздействия на человека или группу лиц.

Специальные методы воздействия – последовательность приемов воздействия на психику человека, применение которых приводит к негативным последствиям для личности, общества и государства.

Основные источники информационно-психологического воздействия на человека в обобщенном виде можно представить следующим образом.

– государство (в том числе иностранные), органы власти и управления и другие государственные структуры и учреждения.

– общество (различные общественные, экономические, политические и иные организации, в том числе зарубежные).

– различные социальные группы (формальные и неформальные, устойчивые и случайные, большие и малые по месту жительства, работы, учебы, службы, совместному проживанию и, проведения досуга и т.д.);

– отдельные личности (в том числе представители государственных и общественных структур, разнообразных социальных групп и т.п.).

В качестве основных средств информационно-психологического воздействия на человека в обобщенном виде выделяют:

– средства массовой коммуникации (в том числе информационные системы, например, Интернет и т.п.);

– литература (в том числе, художественная, научно-техническая, общественно-политическая, специальная и т.п.);

– искусство (в том числе, различные направления так называемой массовой культуры и т.п.);

– образование (в том числе, системы дошкольного, среднего, высшего и среднего специального государственного и негосударственного образования, система так называемого альтернативного образования и т.п.);

– воспитание (все разнообразные формы воспитания в системе образования, общественных организаций — формальных и неформальных, система организации социальной работы и т.п.);

– личное общение.

В силу индивидуально-личностных характеристик индивида, люди отличаются степенью восприимчивости к различным информационным воздействиям, возможностями анализа и оценки поступающей информации и т.д. Кроме индивидуальных особенностей есть и определенные общие характеристики и закономерности функционирования психики, которые влияют на степень подверженности информационно-психологическому воздействию и присущи большинству людей.

Основные виды информационно-психологических воздействий

- самопроизвольные воздействия, обусловленные технологическими режимами функционирования тех или иных информационных систем (например, электромагнитные излучения коммуникационной, компьютерной или же телевизионной техники);
- преднамеренные манипулятивные воздействия на личность с целью явного или скрытого побуждения к определенным действиям (нейролингвистическое программирование, виртуальная реальность и т. п.).

Так, например, информационно-психологические воздействия в политической сфере понимаются как использование дипломатических, военно-демонстрационных, экономических, политических, информационных приемов для прямого или косвенного воздействия на мнение, настроения,

чувства и, в итоге, на поведение другой стороны с целью подавить ее волю, заставить действовать под диктовку.

Информационно-психологические методы и средства психотехнологий подразделяются на открытые и скрытые, положительные и негативные и деструктивные, преследующие явные и скрытые цели.

Информационно-психологические воздействия *скрытого типа* направлены на прямую манипуляцию сознанием человека через его подсознание, путем применения скрытых психотехнологий, когда субъект воздействия не осознает факт самого воздействия. Указанные скрытые воздействия включают психотронные (техногенные) средства, а также суггестивные (внушение, массовый гипноз) и психотропные (фармакологические) воздействия, сотни видов их сочетаний.

Существуют и развиваются методы воздействия на сознание человека в присутствии логики, т.е. в обычном состоянии сознания. Воздействие здесь осуществляется скрытно путем навязывания объекту «нужной» информации на фоне потока каких-то других аудио- и видео- сообщений (суггестии).

Суггестия (внушение) – форма межличностного и межгруппового общения, при котором передача информации происходит посредством частично неосознаваемого, направленного сигнала на вербальном и/или невербальном уровнях. Отличается от убеждения сниженным уровнем критичности и потребности в верификации информации. Внушаемость, или подверженность суггестивному воздействию, зависит от состояния сознания суггерента (объекта) и внешних условий, при которых суггестия осуществляется. Так, эффективность суггестии повышается в состоянии транса, при утомлении, в условиях неопределенности, в экстремальных условиях, в толпе, при использовании СМИ. Суггестия затрагивает как нервно-психические процессы, так и социальные представления, установки, общественные нормы, ценности, мнения, а также индивидуальное самосознание. Разделяют **гетеросуггестию** – внушение, производимое другим лицом, и **аутосуггестию** – самовнушениие. Суггестия может быть прямой,

когда источник внушения осознается и прослеживается связь между ней и ее действием. И косвенной, когда внушение производится опосредованно с использованием промежуточных факторов, на которых и делается основной акцент. Эффективность косвенной суггестии выше, чем прямой.

Так, наиболее отработанным приемом акустического воздействия (суггестии) является предъявление стимулов ниже порога слышимости на фоне более громкой маскирующей информации. Такой прием легко обнаруживается. Среди наиболее перспективных методов воздействия аудиосуггестии называются спектральной маскирование и использование музыкальной информации в качестве носителя нужной информации.

Эффект воздействия существенно усиливается при комбинированном использовании различных типов внушения. Наиболее известным и простым примером такой кооперации и воздействия является комплексное использование аудио- и видеосуггестии. Уже доказано на практике, что неосознаваемая акустическая суггестия, сопровождающая зрительную осознанную информацию, может модулировать отношение субъекта к последней.

Наиболее сложной формой суггестии является нейролингвистическое программирование (НЛП), достигаемое путем долгого и кропотливого подбора «ключа» к подсознанию человека. В качестве такого «ключа» используется специально подобранный текст (так называемый нейросемантический гипертекст), содержащий наиболее значимые слова и фразы для внушаемого (суггестируемого) лица, значительной группы лиц, подразделения, региона. Наиболее вероятная область применения НЛП – средства массовой информации с ориентацией на определенный хорошо изученный контингент населения, образование, медицина, реклама

Нейролингвистическое программирование в рекламе

Сегодня нейролингвистическое программирование (НЛП) — наиболее распространенный инструмент манипулирования массовым сознанием.

Восприятие человека бывает осознанным и неосознанным. Сознание — это своеобразный буфер, который «отфильтровывает» поток получаемой информации. Кроме того, в функции сознания входит сопротивление чему-либо как ответная реакция на информацию. Если же рекламная информация составлена так, что она воспринимается не через сознание, то речь идет о программировании, или манипулировании.

Первооткрыватели НЛП проделали следующее:

1. Разбили шаблоны мышления на более простые составляющие, назвав их «репрезентативными системами», или «модальностями».

2. Посмотрели, какую последовательность этих составляющих использует усредненный человек для решения конкретной задачи или для достижения нужного ему результата.

Простые составляющие мыслительного процесса («модальности») – это обращение к зрительному и слуховому опыту и опыту ощущений. С точки зрения НЛП понятие «мы думаем» означает — мы попеременно и в разной последовательности обращаемся то к зрительным образам, которые вспоминаем или конструируем, то к звукам и словам, которые мы можем вспомнить или сконструировать, если не слышали их раньше, то к ощущениям тепла, холода и т.п. На языке НЛП «я решил познакомиться с этим человеком» означает «я *увидел* этого человека, *услышал* его голос и *почувствовал*, что он мне приятен». Такая определенная последовательность модальностей в ходе решения той или иной проблемы называется *стратегией мышления*.

С появлением НЛП специалисты по рекламе в первую очередь стали использовать стратегию мышления, приводящую к совершению «импульсивной покупки», активно применяя ее на рынке потребительских товаров. Эта стратегия представляет собой чередование зрительного образа и ощущений, другими словами – стратегия «вижу – чувствую».

В течение последних нескольких лет данную стратегию активно внедряют в массовое сознание изготовители рекламы для компании «Жиллет» - используя рекламный слоган «Вы будете выглядеть и чувствовать себя превосходно!» С помощью какой

конкретно лексики будет реализована данная стратегия, зависит лишь от словарного запаса изготовителя рекламы. Вот еще несколько показательных примеров: «Представьте себе ваши ощущения в этой ванне»; «Посмотрите, как нежно это мыло ухаживает за вашей кожей»; «Представляешь себе, мне сразу стало легче!».

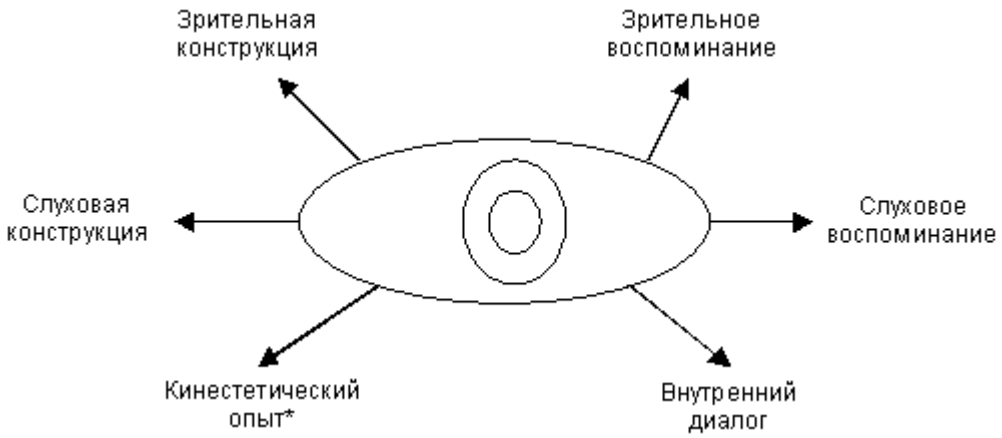
Внедрить нужную стратегию мышления можно не только посредством слогана, но и песни, стихотворения, чередования образов на экране, а если это будет сопровождаться еще и специально подобранной музыкой, то эффект удивит даже специалистов.

Следующая интересная стратегия мышления – *переход от диссоциированного образа к ассоциированному,* то есть от позиции наблюдателя к позиции участника. Сначала мы наблюдаем, как товаром пользуется персонаж рекламного ролика, затем видим товар крупным планом, как если бы мы пользовались им сами. Эта стратегия – основа подражательного поведения, которое встречается, начиная с раннего детства. В последующем многие поведенческие шаблоны мы усваиваем с помощью подобной стратегии, поскольку именно так отражается в нашем мышлении главный принцип научения: «делай, как я». Такая последовательность образов активно применяется в современной рекламе.

Возьмем хотя бы ролик по рекламе конфет «Рафаэлло». Сначала мы видим симпатичную и с привлекательной фигурой даму, которая задумчиво и очень чувственно ест конфеты, а затем – собственно товар (конфеты «Рафаэлло») крупным планом и то, как конфета сама освобождается от обертки. В другом ролике этими конфетами восхищается балерина («Это может быть только от него!»). Реклама довольно эффективна, даже несмотря на смысловую нестыковку в сюжете. Если здраво рассуждать, то конфеты профессиональной балерине может подарить разве что ее недруг, а уж никак не любимый. Следует отметить, что чувственное поедание конфет в сюжете ролика – это в основном привлечение внимания к сюжету и частично обращение к сексуальным подсознательным мотивам (что часто используется в психоаналитических технологиях). Кроме того, здесь же используется и так называемый «феномен идентификации»: потенциальной покупательнице куда приятнее ассоциировать себя с симпатичной и сексуальной девушкой, чем с чавкающей толстушкой.

Вообще основная задача любого рекламного сообщения – привлечь непроизвольное внимание к самому сообщению. Универсальными факторами, которые решают эту задачу (или, если использовать профессиональную терминологию, «стопперами»), чаще всего являются движение в поле зрения или сексуальные раздражители. Любое перемещение в поле зрения сразу же привлекает внимание; так, к магазину, который оборудован движущейся световой рекламой, подходит в полтора раза больше потребителей, чем к тому, который оборудован статичной подсветкой.

Еще одна находка НЛП, активно применяемая в рекламе, - связь направления взгляда с типом мышления в данный момент. Это знание имеет значение для производства печатной рекламы. Например, фотографию упаковки рекламируемого товара лучше помещать в верхней части плаката, а фотографию самого продукта (особенно если он съедобен) – в правом нижнем углу. Особое значение подобная технология приобретает в политической рекламе.



Конкретное направление взгляда:

• Взгляд вправо вверх: создание зрительных образов, фантазирование, ложь.

• Взгляд влево вверх: попытка вспомнить, воссоздать зрительные образы, которые либо имели место в реальности, либо были придуманы ранее.

• Взгляд вправо по горизонтали: создание слуховых образов, сочинение музыки, ложь.

• Взгляд влево по горизонтали: припоминание звуков, которые человек когда-либо слышал или придумал раньше.

• Взгляд вправо вниз: говорит о том, что человек размышляет, переживает эмоции.

• Взгляд влево вниз: внутренний диалог, анализ физических ощущений.

Когда направление взгляда меняется, изменяется и способ восприятия информации. Когда человек смотрит вверх, включаются зрительные образы; в стороны – слуховые; вниз – кинестетические – ощущение, чувствование. В процессе общения взгляд, движущийся снизу вверх, говорит о восхищении и почитании со стороны оппонента. Взгляд, идущий сверху вниз, наоборот, призван выразить критический настрой и пренебрежение.

И, наконец, рассмотрим *субмодальные стратегии*. Разделив человеческое мышление на простые составляющие — модальности, специалисты в области НЛП на этом не остановились и пошли дальше, разделив каждую модальность на субмодальности. Есть универсальные субмодальности, которые являются общими для любой модальности, — это интенсивность (яркость, громкость), распространенность (размер), местоположение и некоторые другие. Когда провели подобное дробление, оказалось, что поведение человека можно менять с не меньшей эффективностью, используя только субмодальности. Существуют три универсальные зрительные субмодальности, которые увеличивают привлекательность продукта: яркость, цветность, увеличение размера (приближение к зрителю).

Виды информационного манипулирования

Манипуляция – это вид психологического воздействия, при котором мастерство манипулятора используется для скрытого внедрения в психику адресата целей, желаний, намерений, отношений или установок, не совпадающих с теми, которые имеются у адресата в данный момент.

Манипуляция – это психологическое воздействие, нацеленное на изменение направления активности другого человека, выполненное настолько искусно, что остается незамеченным им.

В практических целях иногда удобнее пользоваться непосредственно метафорой: манипуляция – это действия, направленные на «прибирание к рукам» другого человека, помыкание им, производимые настолько искусно, что у того создается впечатление, будто он самостоятельно управляет своим поведением.

Исходя из вышесказанного, мы можем вывести определение термина

Манипулирование – это способ психологического воздействия, нацеленный на изменение направления активности других людей, осуществляемый настолько искусно, что остается незамеченным ими. Манипулирование в то же время – это такой способ применения власти, при которой обладающий ею влияет на поведение других, не объясняя им, чего он от них ожидает.

Манипуляция сознанием – это своеобразное господство над духовным состоянием людей, управление путем навязывания людям идей, установок, мотивов, стереотипов поведения, выгодных субъекту воздействия.

Выделяют 3 уровня манипулирования:

- первый уровень - усиление существующих в сознании людей нужных манипулятору идей, установок, мотивов, ценностей, норм;
- второй уровень связан с частными, малыми изменениями взглядов на то или иное событие, процесс, факт, что также оказывает воздействие на эмоциональное и практическое отношение к конкретному явлению;
- третий уровень - коренное, кардинальное изменение жизненных установок путем сообщения объекту.

Информационное манипулирование – это воздействие на индивидуальное и/или коллективное сознание и поведение, осуществляемое разнообразными информационными средствами.

Психологическая атака – метод активного воздействия на психику человека с целью отключения логического мышления: произведения положительного (отрицательного) впечатления или введения в состояние растерянности с последующим побуждением человека к нужной реакции.

*Например, в Интернет уже несколько лет распространяется следующая «просьба о помощи» (текст и номер телефона изменяются) – «4-месячному ребенку ОЧЕНЬ СРОЧНО требуется кровь 4 группы отрицательного резус-фактора. Тел. ****» или «Разошли всем, пожалуйста 12-месячному ребёнку нужна 4я (положительная) група крови. Тел. ****. попроси разослать по друзьям. Меня тоже просили разослать. Это срочно» (орфография сохранена). Звонок на указанный номер может стоить вам определенной суммы денег.*

Психологическое программирование – метод однообразного или настойчивого воздействия на психику человека с целью выработки алгоритмов его поведения и образов мышления.

Регулярная рассылка различных сообщений одной и той же тематики. Самое безобидное, например подобное сообщение «...Это денежный ангел! Перешлите это 6-ти своим хорошим друзьям и разбогатеете в течение 4-х дней. Это не шутка. Если уничтожите его – Вы будете сожалеть об этом...» (орфография сохранена).

Психологическое манипулирование – метод двойственного воздействия на психику человека, целью которого является поставить человека в положение выбора линии поведения между двумя альтернативами (между хорошим и плохим, добром и злом).

Письмо представляет собой фрагмент переписки двух человек, который якобы ошибочно был прислан сотруднику компании ("жертве"). В переписке обсуждается возможность оплаты каких-либо услуг с помощью электронных денежных средств. Один из адресатов предлагает другому оплатить услуги с помощью электронного кошелька, при этом в письме приводятся номер электронного кошелька, пароль, инструкция по

использованию. К письму прикреплен «плагин для совершения денежных операций» – троянское программное обеспечение. Таким образом, получатель попадает в положение выбора, находясь между двумя альтернативами: украсть или нет, воспользоваться чужими денежными средствами или нет.

Психологическое давление – метод внушительного воздействия на психику человека с целью принуждения его к определенным действиям.

Примеры сообщений «ICQ System (*******) В связи со сбоем работы серверов просим Вас подтвердить тот факт, что именно вы являетесь обладателем данного ICQ номера, для чего отправьте сообщение «<ваше имя и фамилия>, <пароль от данного UIN номера>» или «Здравствуйте идет перерегистрация пользователей icq если вы хотите в будущем пользаваться этим icq номером. Отправте свой Uin и пароль на этот icq номер с командой uin: parol: Эта информация строго засекреченна! Спасибо за поддержку» (орфография сохранена).

С точки зрения истории справедливо отметить, что одной из первых попыток систематизации приемов информационно-психологического воздействия на массовое сознание с помощью пропаганды, явилось описание в ряде зарубежных и отечественных источников технологии стереотипизации и «большой лжи», а также выделение следующих семи основных приемов информационно-психологического воздействия достаточно широко известных специалистам как «азбука пропаганды»:

· «Приклеивание или навешивание ярлыков» (name calling);

· «Сияющие обобщения» или «блистательная неопределенность» (glittering generality);

· «Перенос» или «трансфер» (transfer);

· «Ссылка на авторитеты», «по рекомендации», «свидетельства» или «свидетельствование» (testimonial);

· «Свои ребята» или «игра в простонародность» (plain folks);

· «Перетасовка» или «подтасовка карт» (card stacking);

· «Общий вагон», «общая платформа» или «фургон с оркестром» (band wagon)

Эти семь основных приемов в систематизированном виде были сформулированы в США в конце 30-х годов в Институте анализа пропаганды. Известно, что основой для анализа этих приемов во многом послужила практика обработки массового сознания в нацистской Германии. Они нашли широкое применение в рекламно-пропагандистских акциях и в настоящее время активно используются российскими средствами массовой коммуникации.

Содержание этих основных приемов можно коротко охарактеризовать следующим образом.

«Приклеивание или навешивание ярлыков»

Данный прием заключается в выборе оскорбительных эпитетов, метафор, названий, имен, так называемых «ярлыков», для обозначения, именования человека, организации, идеи, любого социального явления. Эти «ярлыки» вызывают эмоционально негативное отношение окружающих, ассоциируются у них с низкими (бесчестными и социально неодобряемыми) поступками (поведением) и, таким образом, используются для того, чтобы опорочить личность, высказываемые идеи и предложения, организацию, социальную группу или предмет обсуждения в глазах аудитории.

«Сияющие обобщения» или «блистательная неопределенность»

Этот прием заключается в замене названия, обозначения определенного социального явления, идеи, организации, социальной группы или конкретного человека более общим родовым именем, которое имеет положительную эмоциональную окраску и вызывает доброжелательное отношение окружающих. Он основан на эксплуатации положительных чувств и эмоций людей к определенным понятиям и словам, например, таким как «свобода», «демократия», «патриотизм», «содружество», «мир», «счастье», «любовь», «успех», «победа», «здоровье» и т.п.. Такого рода слова, несущие позитивное психоэмоциональное воздействие, применяются

для протаскивания решений и взглядов, оценок и действий, выгодных для конкретного лица, группы или организации.

«Перенос» или «трансфер»

Суть данного приема состоит в искусном, ненавязчивом и незаметным для большинства людей распространении авторитета и престижа того, что ими ценится и уважается на то, что ей преподносит источник коммуникации. Использованием «трансфера» инициируются ассоциации, формируются ассоциативные связи преподносимого объекта с кем-либо или чем-либо, имеющим ценность и значимость у окружающих. Используется также и негативный «трансфер» посредством побуждения к ассоциациям с явно отрицательными понятиями и социально неодобряемыми явлениями, событиями, действиями, фактами, людьми и т.д. Он используется для дискредитации конкретных лиц, идей, ситуаций, социальных групп и организаций.

«Ссылка на авторитеты», «свидетельства» или «свидетельствование»

Содержание этого приема заключается в приведении высказываний личностей, обладающих высоким авторитетом или же наоборот, таких, которые вызывают отрицательную реакцию у категории людей, на которых направляется манипулятивное воздействие. Используемые высказывания, обычно содержат оценочные суждения в отношении людей, идей, событий, программ, организаций и выражают их осуждение или одобрение. Таким образом, у человека, как объекта манипулятивного воздействия, инициируется формирование соответствующего отношения - эмоционально позитивного или отрицательного.

«Свои ребята» или «игра в простонародность»

Иногда также используются такие названия как «рубаха-парень», «простонародность», «простой» или «свой парень». Цель данного приема состоит в попытках установления доверительных отношений с аудиторией, как с близкими по духу людьми на основании того, что коммуникатор, его

идеи, предложения, высказывания хороши так как принадлежат простому народу. Осуществляется инициирование ассоциативных связей личности коммуникатора и его суждений с позитивными ценностями из-за их народности или принадлежности его самого к народу, как выходцу из простых, обыкновенных людей. Достаточно часто этот прием используется для создания позитивного отношения к конкретному человеку, являющемуся в данном случае объектом рекламно-информационного продвижения, пропагандистской кампании по формированию спроектированного (сконструированного) для него имиджа – «человека из народа» и, таким образом, формирование к нему доверия и позитивного отношения.

«Перетасовка» или «подтасовка карт»

Содержание данного приема заключается в отборе и тенденциозном преподнесении только положительных или только отрицательных фактов и доводов при одновременном замалчивании противоположных. Его основная цель, используя односторонний подбор и подачу фактов, свидетельств, доводов, показать привлекательность или наоборот неприемлемость какой-либо точки зрения, программы, идеи и т.п. В последнее время этот прием чаще используется в измененном виде под названием «потенцирование» или «акцентирование».

«Общий вагон», «общая платформа» или «фургон с оркестром»

При использовании данного приема осуществляется подбор суждений, высказываний, фраз, требующих единообразия в поведении, создающих впечатление, будто так делают все. Сообщение, например, может начинаться словами: «Все нормальные люди понимают, что...» или «ни один здравомыслящий человек не станет возражать, что...» и т.п. Посредством «общей платформы» у человека вызывается чувство уверенности в том, что большинство членов группы, определенной социальной общности и, в частности, с которой он себя идентифицирует или мнение которой значимо для него принимают конкретные ценности, идеи, программы, разделяют предлагаемую точку зрения. Аппеляция ко «всем», отмечает Ю.А.

Шерковин, учитывает, что люди, как правило, верят в побеждающую силу и правильность мнения большинства и поэтому, естественно, хотят быть с теми, кто его составляет. Происходит некритическое принятие излагаемых в сообщении оценок, точек зрения и т.п.

Следует отметить, что рассмотренные методы психологического воздействия могут комбинироваться, образуя тем самым новые проявления воздействия на человека.

Способы защиты личности

Человек попадает в современный мир, где действует множество манипуляторов – от недобросовестного продавца и рыночного мошенника, до целых организаций, специализирующихся на экономических аферах и политическом интриганстве, вооруженных самыми современными знаниями и мощнейшим аппаратом информационного воздействия на психику человека.

Достаточно широко известно дошедшее до наших дней латинское выражение, которое в виде краткого афоризма формулируется следующим образом: предупреждением защищен или кто предупрежден, тот вооружен. В краткой и метафорической форме оно отражает одно из необходимых условий успешной защиты – своевременное знание об опасности, которая грозит человеку, позволяет ему подготовиться к ее отражению.

Люди в различной степени подвержены психологическому воздействию, в разной мере обладают способностью отличать правду от вымысла и лжи, улавливать обман, неискренность и скрытые замыслы в действиях других людей. Одни – более проницательны, другие – менее. Считается, что проницательность не столько врожденное качество, а в большей степени формируемое, вырабатываемое с годами в процессе практической деятельности, связанной с интенсивным общением и взаимодействием с людьми, а также при обучении и проведении специальных тренинговых процедур.

Способы защиты

В 1997 г. Е.Л. Доценко выделил следующие способы защиты: бегство, замирание, прятание (уход в укрытие), встречное нападение и стремление повлиять на поведение противника. Эти способы защиты можно наблюдать практически у всех видов животных (последний, в частности, выражается в особых сигналах подчинения или в использовании разного рода хитростей). Аналогичные формы защит наблюдаются и в истории человеческих отношений, что особенно проявляется в военных действиях. Таким образом, рассмотрение эволюции способов защиты, начиная от животного мира до человека, включенного в систему социальных отношений, позволяет выделить пять основных форм защиты. К этим пяти исходным формам защиты обычно относят следующие:

1) бегство и различные его ослабленные виды - отступление, уклонение, задержки;

2) маскировка (как аналог замирания у животных и зачастую у человека, особенно при физической опасности), т.е. стремление стать незаметным для противника;

3) уход в укрытие, использование естественных и создание искусственных преград и препятствий для противника в виде стен, рвов и пр., а как облегченная модификация - использование переносимых преград: щитов, кольчуг, доспехов и т.п.;

4) нападение как активная форма защиты («лучший способ защиты – нападение»);

5) управление поведением действительного или потенциального противника, в частности, его намерениями (угрозы, задабривание, применение хитростей, обманных маневров и иных уловок).

Выделенные следующие пять исходных форм защиты: бегство, прятание (уход в укрытие), замирание (маскировка), нападение (уничтожение, изгнание) и контроль (управление) обозначаются как базовые защитные установки. Рассмотрим их подробнее:

1. *Уход* – увеличение дистанции, прерывание контакта, выход за пределы досягаемости воздействия. Проявлениями этого вида защит являются:

а) в межличностных ситуациях – смена темы беседы (на более безопасную), нежелание обострять отношения (обход «скользких тем», «острых углов»), стремление уклониться от встреч с тем, кто является источником неприятных переживаний (отказ, перенос, уклонение от встреч); избегание травмирующих ситуаций, под различными предлогами прерывание встреч, бесед и т.п.

Крайним предельным выражением данной тенденции может стать полная замкнутость, отчужденность, отказ от контактов с людьми;

б) в контакт-коммуникационных ситуациях – уход под различными предлогами (для себя и окружающих) с митингов, собраний, различных зрелищных мероприятий и т.п. или различные формы отказа от участия и присутствия на подобных мероприятиях;

в) в масс-коммуникационных ситуациях – отключение от определенных каналов средств массовой информации, от просмотра конкретных теле-радиопрограмм, отказ от чтения некоторых газет, статей, рубрик и т.п.

2. *Изгнание* (вытеснение) – увеличение дистанции, удаление, вытеснение источника воздействия.

а) в межличностных ситуациях – удаление из мест проживания, работы, отдыха (из среды обитания); выгнать из дома (смягченная форма - видеть тебя не хочу; уйди, чтобы я тебя не видел; уйди с глаз долой и т.п.), отослать куда-то под определенным предлогом (перевод, увольнение с работы и т.п.); уничижение как трансформация уничтожения в духовную форму в виде осуждения, насмешек, колкостей, унижения и т.п. (т.е. частичное уничтожение какой-либо части другого – черт характера, привычек, поступков, намерений, склонностей и т.д.); оскорбление и провоцирование конфликта, ссоры, обиды, что вынуждает источник воздействия прервать контакт, разорвать отношения, уйти и таким образом увеличить дистанцию.

Крайними формами здесь могут выступать конфликты, приводящие к физическому воздействию, например, путем драки и как предельное выражение – уничтожение источника воздействия;

б) в контакт-коммуникационных ситуациях – «захлопывание» выступающих, их прерывание, насмешки, реплики, оскорбления, свист и другие демонстрационные действия и помехи, вынуждающие коммуникатора прервать контакт и удалиться. Эти способы могут трансформироваться в такие формы, как забрасывание различными предметами и другие виды физического воздействия. Это особенно характерно для некоторых категорий участников зрелищных мероприятий и спортивных болельщиков. Они могут выскакивать на сцену, на игровое поле, пытаться физически воздействовать на артистов, игроков и спортивных судей;

в) в масс-коммуникационных ситуациях – мягкие формы аналогичны как и в случае «ухода» и представляют собой отключение от каналов информации. В предельном выражении могут трансформироваться в попытки физического уничтожения источника коммуникации. (В качестве примера может служить нападение в Москве на телецентр «Останкино» во время событий октября 1993 года).

3. *Блокировка* (ограждение, преграда) – контроль воздействия, достигающего субъекта защиты, выставление преград, ограждение психики от внешнего воздействия:

а) в межличностных ситуациях – отчужденность (официальность, ведение беседы с использованием физических разделительных преград, например, через стол, увеличение межличностного пространства), различные психологические барьеры (недоверие, настороженность, враждебность), смысловые и семантические («я вас плохо понимаю», «мне трудно понять в чем суть...» и т.п.), ролевые («я на работе», «при исполнении служебных обязанностей», «мне сейчас некогда, занят, не сейчас, потом...» и т.п.), принижение источника воздействия («непрофессионал», «слабый специалист», «несерьезный», «безответственный», «пройдоха», «все это и так

известно», «в этом нет ничего нового», «не понимает сложности ситуации», «несет чушь, бред, галиматью», «делает все только, чтобы выделиться», «гребет под себя») и т.п.;

б) в контакт-коммуникационных ситуациях – повышение негативизма, критичности, эмоциональная отчужденность, также используются психологические барьеры, принижение источника (внутреннее осмеяние, развенчание авторитета и т.п.), невнимательность (отвлечение и переключение внимания на другие объекты, не связанные с содержанием воздействия) и т.д.;

в) в масс-коммуникационных ситуациях – анналогично предыдущему пункту «б».

4. *Управление* – контроль за процессом воздействия, влияние на его характеристики и источник (воздействия):

а) в межличностных ситуациях – демонстрация угрозы (опасности); «подкуп» и стремление «умилостивить»; стать другом, членом одной общности («своих не бьют»); стремление разжалобить (плач, жалобы, ноющие интонации, вздохи, несчастный вид); ослабить или дестабилизировать активность (неожиданным отвлечением и т.п.); спровоцировать желаемое поведение (в том числе, различные приемы межличностных манипуляций как способ защиты).

Предельное выражение – психологическое и физическое подчинение другого, помыкание им (например, в тоталитарных религиозных сектах, некоторых асоциальных группировках с криминальным лидером и т.п.);

б) в контакт-коммуникационных ситуациях – возможности управления очень слабые.

В некоторых ситуациях возможно использование обратной связи как способа управления (например, в зрелищных мероприятиях выражение реакции на выступление с помощью аплодисментов, вызова на бис, различные проявления неодобрения, недовольства выступающими и т.п.);

в) в масс-коммуникационных ситуациях – управление практически невозможно.

5. *Затаивание* (маскировка) – контроль информации о самом субъекте защиты, ее искажение, сокрытие или сокращение подачи:

а) в межличностных ситуациях – масскировка, обман, сокрытие чувств, проявлений эмоций, задержка или отказ от действий, чтобы не проявлять себя (не навлекать беду);

б) в контакт-коммуникационных ситуациях – маскировка, сокрытие чувств, проявлений эмоций, задержка или отказ от действий (особенно при нахождении в толпе, чтобы не поддаться «эффекту толпы», психическому заражению и не совершить поступков, о которых потом можно будет сожалеть);

в) в масс-коммуникационных ситуациях – отсрочка реакций, поспешных выводов и оценок, задержка или отказ от действий и поступков, вызываемых информационным воздействием (для последующего рационального и взвешенного анализа с привлечением дополнительных данных).

6. *Игнорирование* – контроль информации об источнике воздействия, наличии или характере угрозы (опасности); ограничение количества такой информации или ее искаженное восприятие.

Вполне обоснованной является существующая в настоящее время точка зрения, что использование данной формы защиты оправданно, несмотря на кажущуюся, при первом взгляде, неэффективность и даже вредность для человека такого защитного механизма. Использование такой формы защиты вполне целесообразно и оправдано, если сама информация и ее распространение служат способом манипулирования личностью, или когда остальные формы защиты по каким-либо причинам не задействуются, а психики нуждается в ограждении от чрезмерного травмирования эмоциональными факторами, вызываемыми внешней информацией.

а) в межличностных ситуациях – игнорирование информации, затрудняющей или препятствующей определенной деятельности (например,

преувеличивающей силу и возможности соперника, трудности достижения поставленной цели для того, чтобы человек отказался от этого и т.п.); игнорирование информации об определенных действиях, направленных на человека со стороны источника воздействия (например, в ситуации, когда ваш руководитель, коллега или близкий человек находятся в состоянии эмоционального возбуждения и адекватно ответить ему - значит вступить в конфликт, который позднее трудно, а порой невозможно локализовать); в то же время восприятие адекватности оценки ситуации может снижаться, например, на основе стереотипизация («да он просто хулиганит», «перебесится и все будет нормально» и т.п.), умаление степени угрозы посредством объяснения позитивными намерениями источника воздействия («она желает мне добра») и т.д.;

б) в контакт-коммуникационных ситуациях – игнорирование информации, затрудняющей или препятствующей определенной деятельности или информации как средства манипулирования личностью в толпе, в массовых скоплениях людей (например, для предотвращения повышения эмоциональной восприимчивости, тревожности, внушаемости, подверженности психическому заражению; для блокировки эмоций, чувств, действий как спонтанной реакции на призывы и другие воздействия, стимулирующие проявление определенных чувств, потребностей, поведения и т.п.) и т.д.;

в) в масс-коммуникационных ситуациях – игнорирование информации как средства манипулирования личностью в различных аспектах (слухов, дезинформирования, мнимых прогнозов, конъюнктурных оценок и т.п.).

Конечно, любая обобщенная модель – это всегда лишь определенная схематизация явлений, происходящих в действительности. В нашей реальной жизни исходные формы защиты видоизменяются, образуют причудливые сочетания и комбинации в зависимости от индивидуальных особенностей людей.

§6. Информационно-психологическая безопасность в Интернет

Виды и формы общения в Интернет. Особенности и характеристики.

Способы общения в Интернете

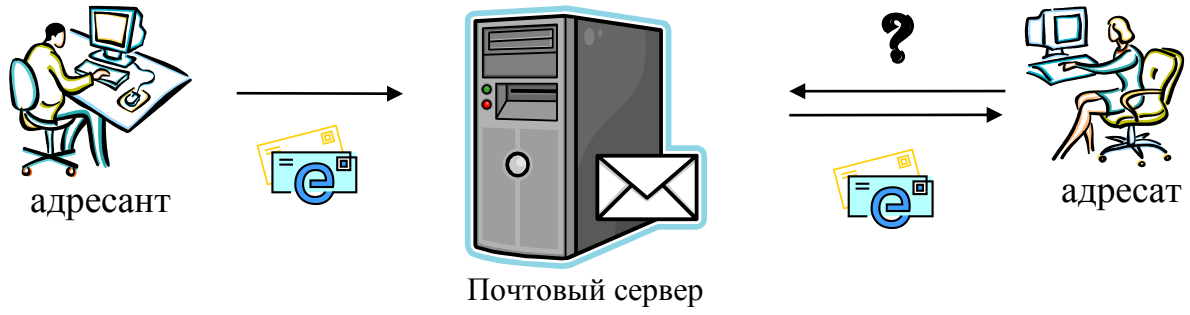
В настоящее время существует очень много способов общения в Интернете, наиболее распространенными из которых являются электронная почта, форумы, чаты, сетевые игры и социальные сети.

Электронная почта (Е-мэйл) – аналог хорошо известной системы общения через письма, отправляемые в конвертах, отличающаяся при этом тем, что письмо существует в виде электронного сообщения, которое отправляется с компьютера адресанта на почтовый сервер, а затем доставляется адресату на его почтовый ящик. Вся процедура отправки такого письма при хороших условиях занимает не более 3-5 минут.

Электронная почта – система пересылки почтовых сообщений между абонентами, одна из важнейших возможностей Интернета; также называют и сами сообщения, пересылаемые между пользователями. Пользователь имеет закрепленное за ним дисковое пространство на сервере провайдера – почтовый ящик. Благодаря уникальному адресу вся получаемая и отправляемая почта персонифицирована. Почтовая программа предоставляет сведения об отправителе, регистрирует время получения сообщения, обеспечивает сортировку большого объема почты.

Адрес электронного почтового ящика представляет собой следующее написание: имя@почтовый_сервер.код_страны (например: ivanov@mail.ru). Электронное письмо, как и обычное письмо в конверте, может содержать различные вложения в виде графических (фотографии, рисунки, картинки, схемы, таблицы), аудио (музыка, речь) и других видов файлов.

Процедура отправки обычного письма



Процедура отправки электронного письма

Электронная почта по сравнению с бумажной почтой имеет некоторые преимущества, которые состоят в следующем:

- мизерные затраты времени и денег на пересылку;
- меньшее количество требуемых данных для успешной доставки;
- возможность отправки вместе с письмом звуковых материалов;
- возможность отправки одного письма сразу нескольким адресатам;
- возможность переадресации писем и т.д.

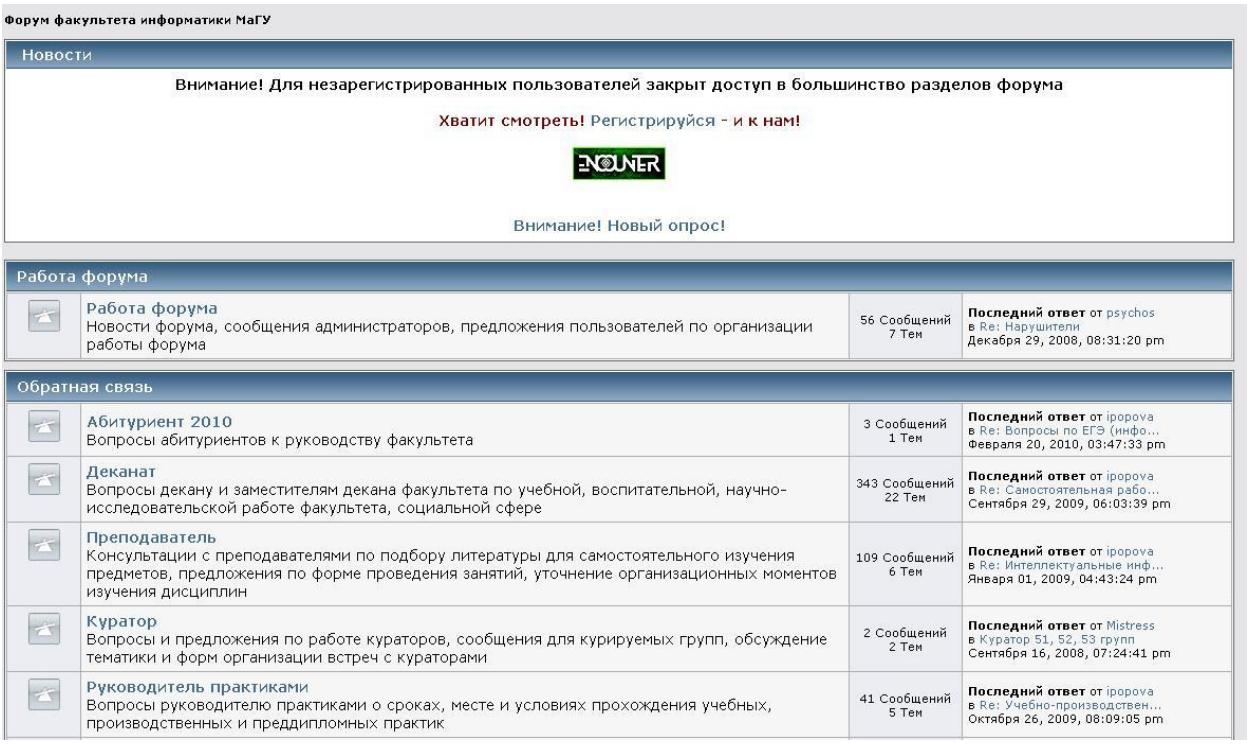
Но у Емэйл имеются и такие недостатки, как:

- необходимость наличия компьютера, выхода в Интернет, электронного почтового ящика, а также элементарных знаний по управлению программным обеспечением;

- при отправке большого числа прикрепленных файлов, либо файлов большого размера бывает целесообразнее воспользоваться обычной почтой.

Форум – организация обмена информацией и общения между большим количеством собеседников, которым небезынтересна тема обсуждения,

которая и является причиной концентрации этих людей в одном месте для вынесения её на всеобщее обсуждения. Их главное отличие состоит в том, что при организации Интернет форумов не существует строгих ограничений на контингент участников – ими могут стать любые пользователи, зарегистрированные на том или ином форуме, не существует также и временных рамок обсуждения темы – процесс продолжается до тех пор, пока тема интересна для собеседников.



Форум факультета информатики ГОУ ВПО «МаГУ»

Существуют различные по тематике, контингенту участников и преследуемым целям форумы: одни являются Интернет-аналогами ранее проводившихся собраний по каким-либо темам, требующим дальнейшего обсуждения, другие существуют для организации общения людей (как правило имеющих дружеские отношения вне Интернета, т.е. в обычной жизни), по разным причинам не способных собраться в одном месте для живого неопосредованного общения. Форумы первого типа обычно имеют научную или социально-политическую тематику и преследуют соответствующие цели, в качестве которых может выступать решение каких-либо проблем, связанных с этой тематикой. Таким форумам присущи

некоторая официальность и официально-деловой, научный или научно-публицистический стиль речи.

Форумы второго типа отличаются, прежде всего, тематикой – обсуждаться могут различные бытовые сферы жизни, общественные события или же работы творцов в области искусства (в т.ч. музыки, живописи, поэзии и прозы и т.д.), а также неофициальностью общения. Кроме того, в зависимости от контингента участников, без ограничений используются все средства языка. Общение идет преимущественно в разговорном стиле речи, но жестких рамок здесь нет. Целями можно считать получение участниками различных знаний, опыта общения, а также получение некой истины в спорах относительно того или иного явления или индивидуальных предпочтений.

Всем форумам присущи неписанные правила: обсуждение любой темы начинается с монолога автора в виде статьи (отзыва/рецензии, мнения по какой либо из интересующей многих позиции), содержащего суть проблемы и аргументированные доводы автора в пользу той или иной точки зрения. Далее к обсуждению темы с автором подключаются все заинтересованные лица. Длительность обсуждения одной темы может составлять как от нескольких часов, так до нескольких месяцев или даже лет.

Преимущества Интернет форумов перед живым общением:

– отсутствие необходимости совершать переезды к месту проведения форума – достаточно включить компьютер и набрать электронный адрес;

– колоссальная экономия времени, сил и денег при участии в форуме;

– возможность принимать участие сразу в нескольких форумах;

– отсутствие физического контакта с оппонентами исключает возможность применения физической силы в спорных ситуациях;

– период проведения форума не имеет жестких временных рамок;

Недостатки Интернет - форумов заключаются в следующем:

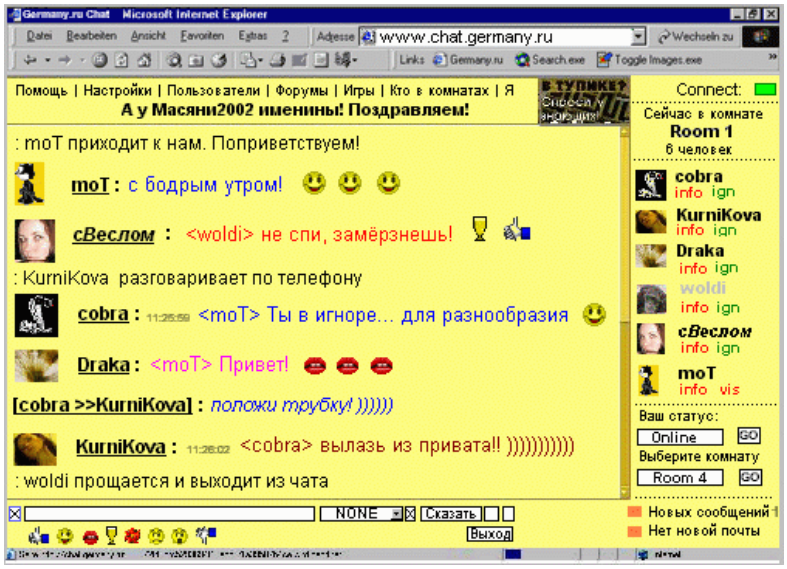
– необходимо наличие компьютера, выхода в Интернет, электронного почтового ящика, регистрации на форуме, а также элементарных знаний по использованию программного обеспечением;

– частое отсутствие визуального представления о собеседниках в виду их нежелания выставлять свои фото на всеобщее обозрение.

Обычно сообщения несут информацию «автор – тема – содержание – дата/время». Сообщение и все ответы на него образует *ветку* («тред»). Обсуждение должно соответствовать теме. Отклонение от начальной темы обсуждения часто запрещено правилами поведения форума. За соблюдением правил следит модератор – участник, наделённый возможностью удалять чужие сообщения в определённом разделе или теме, а также контролировать к ним доступ отдельных участников. На форумах может применяться чрезвычайно гибкое разграничение доступа к сообщениям. Так, на одних форумах чтение и создание новых сообщений доступны любым случайным посетителям, на других необходима предварительная регистрация (наиболее распространённый вариант) – те и другие форумы называют открытыми. Применяется и смешанный вариант – когда отдельные темы могут быть доступны на запись всем посетителям, а другие – только зарегистрированным участникам. Кроме открытых, существуют закрытые форумы, доступ к которым определяется персонально для каждого участника администраторами форума. На практике также нередко встречается вариант, когда некоторые разделы форума общедоступны, а остальная часть доступна только узкому кругу участников.

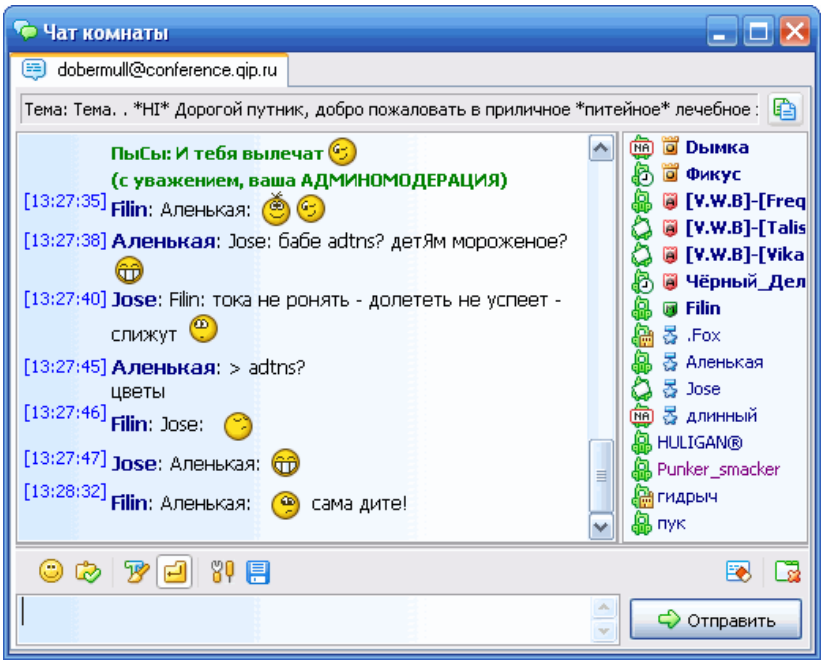
Чат (англ. *chat* – разговор) – средство общения пользователей по сети в режиме реального времени, а также программное обеспечение, позволяющее организовывать такое общение. Обычно под словом «чат» подразумевается обмен текстовыми репликами, реже используют термины **голосовой чат, видеочат** (чаще – **видеоконференция**) и т. д. Существует несколько разновидностей программной реализации чатов:

– HTTP- или веб-чаты. Такой чат выглядит как обычная веб-страница, где можно прочесть последние несколько десятков фраз, написанных участниками чата, или обрабатывается клиентом, наследующим возможности браузера. Страница чата автоматически регулярно обновляется.



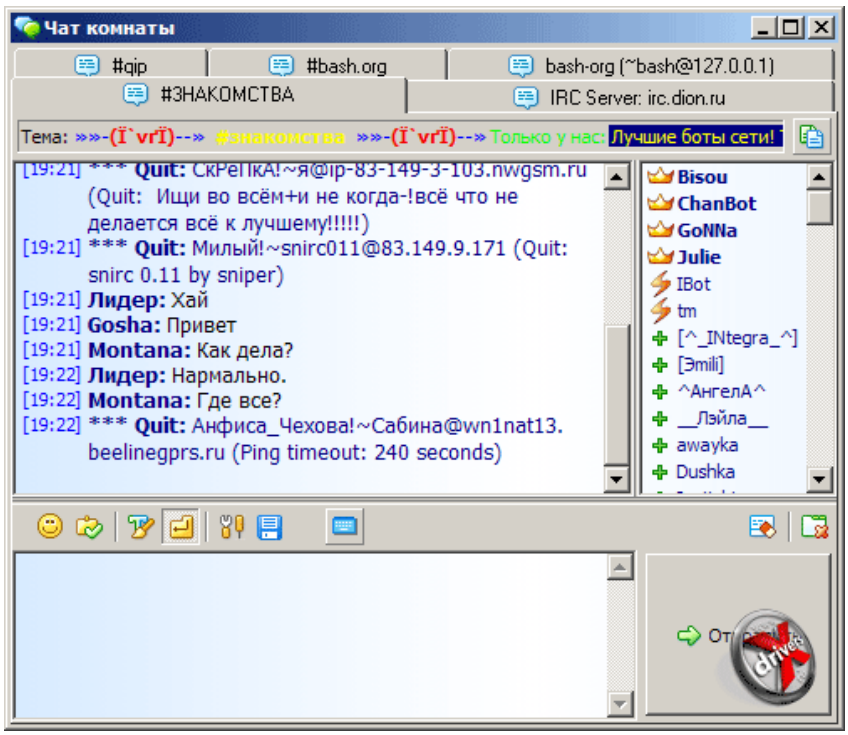
Веб-чат

– Встроенные возможности чата в IM-клиентах, «толстый клиент» (Instant messengers (IM)) – английское название класса программ, предназначенных для обмена сообщениями через Интернет в реальном времени (Служба мгновенных сообщений – Instant Messaging Service – IMS). Аббревиатура «ICQ» созвучна английской фразе «I seek you» (*я ищу тебя*, произносится *ай-сик-ю́*). В русском компьютерном сленге ICQ называют «*асей*» или «*аськой*».



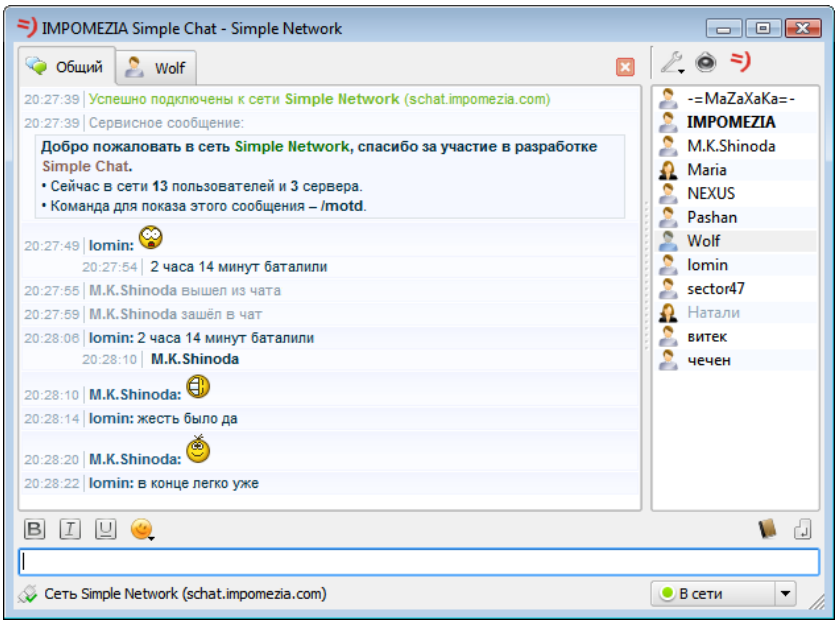
Чат в программе QIP

– IRC, специализированный протокол для чатов (Internet Relay Chat – ретранслируемый интернет-чат).



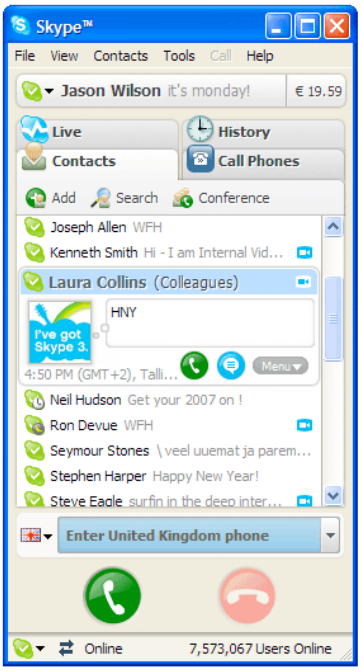
IRC-чат

– Программы-чаты для общения в локальных сетях. Часто имеют возможность передачи файлов, звука и видео.



Программа-чат

– Специализированные программы для голосовых и других видов чата.



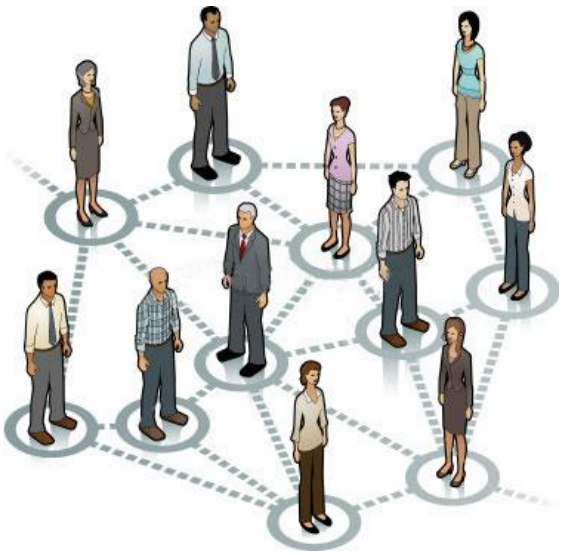
Программа Skype

Отличительной особенностью чатов является относительная кратковременность (по сравнению с форумами) каких-либо дебатов между оппонентами. Преимущества и недостатки общения в чате аналогичны преимуществам и недостаткам общения на форумах.

Многопользовательская ролевая онлайн-игра (англ. massively multiplayer online role-playing game, MMORPG) – разновидность онлайновых ролевых игр, позволяющая множеству людей одновременно играть в изменяющемся виртуальном мире через Интернет. MMORPG – это одна из разновидностей MMOG (англ. massive multiplayer online game).

Фрагмент экрана MMORPG «World of Warcraft»

Социальная сеть – социальная структура, состоящая из группы узлов, которыми являются социальные объекты, и связей между ними. В качестве узлов выступают люди или организации, а в качестве связей - их взаимоотношения. Первые социальные сети в интернете появились в конце прошлого века, но применить к ним определение, существовавшее уже в 50-х годах XX века, ученые и социологи догадались лишь несколько лет назад. По большому счету, социальная сеть в Интернете – это набор программных средств, позволяющий участникам проекта реализовывать социальные связи и взаимодействовать на их основе. Существенным отличием социальных сетей от других типов Интернет-ресурсов (не считая форумов и блогов) является то, что их содержимое (контент) создают рядовые пользователи проекта. Социальная сеть, позиционируемая как виртуальная или онлайновая структура, в большинстве своем базируется на реальных связях между людьми. Эти связи строятся по определенным признакам, все зависит от степени свободы пользователя в рамках того или иного ресурса, его предпочтений, направленности самой сети (для студентов, любителей рыбалки, топ-менеджеров, одноклассников, сотрудников корпорации), а также аудитории.



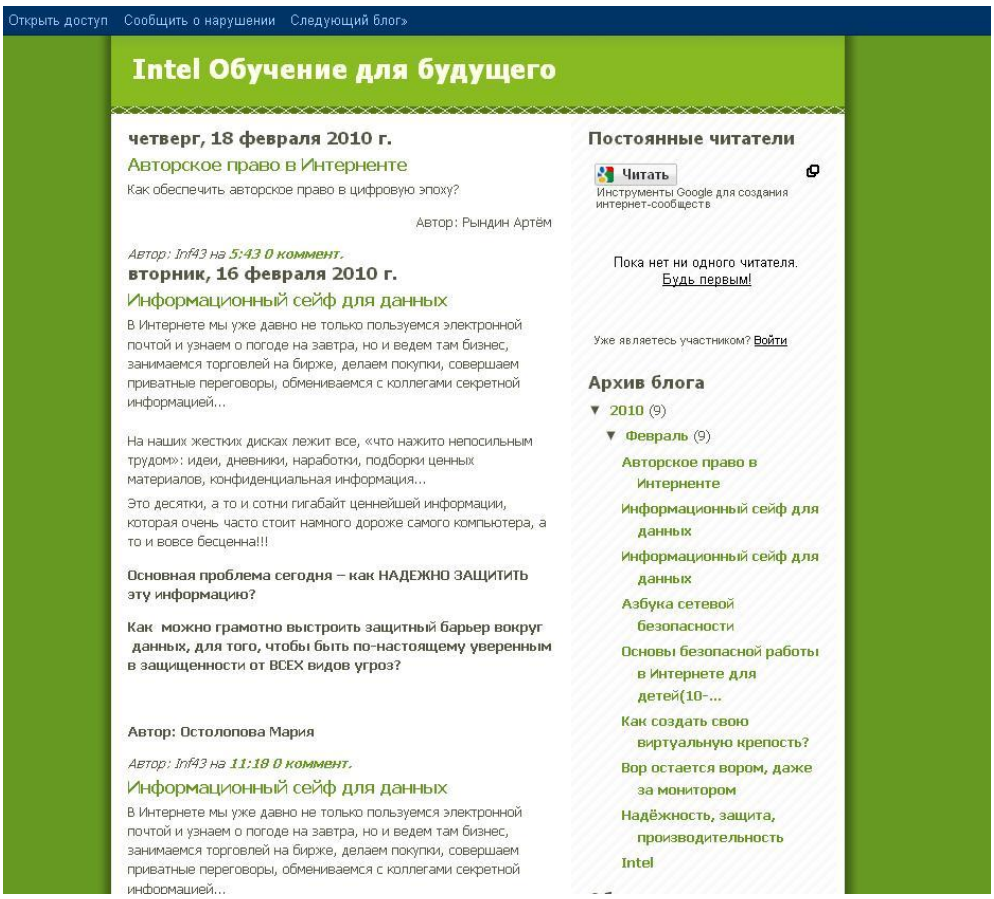
Связи между участниками социальной сети

Особенности социальных сетей:

– обязательная регистрация пользователей – для того, чтобы просмотреть данные друзей или найти человека, пользователю необходимо завести учетную запись;

– подавляющее большинство социальных сетей строятся и адаптируются под интернет-браузеры – приложения для работы в интернете. Это дает возможность человеку пользоваться услугами таких сервисов практически в любом месте, где есть подключение к интернету: на работе, дома, в учебном заведении – без необходимости установки и настройки специального программного обеспечения.

Блог (web-log) это – пополняемая через веб-интерфейс коллекция записей. Согласно определению, которое дает SlashDot, «блог – это новый, личный способ эволюции электронного сообщества. Термин «Блог» – blog – происходит от Web-logging. Он может служить примером того, как люди используют сеть для построения своей собственной среды общения». Как правило, это личные записи, содержащие аннотированные ссылки на другие ресурсы, опубликованные в сети. С этой точки зрения первый блог создал Бернерс-Ли, когда публиковал новости о развитии проекта Всемирной Паутины. Первые блоги появились еще в 1996 году, но стали заметным и популярным феноменом начиная с 1999 года. За последние несколько лет в сети появилось огромное количество сообществ, материалы которых создаются их авторами по технологии блогов. Авторы публикуют новости и комментарии к новостям. В настоящее время блоги отличает не столько структура записей, сколько простота добавления новых записей. Пользователь просто обращается к веб-серверу, проходит процесс опознания и добавляет новую запись к своей коллекции. Сервер представляет информацию как последовательность сообщений, помещая в самом верху самые свежие сообщения. Структура коллекции очень напоминает привычную последовательную структуру дневника или журнала.



Фрагмент блога http://info43intel.blogspot.com

Характерные черты блогов:

– Обратный порядок записей – самые последние свежие записи публикуются сверху. Как правило, в блоге на первой странице публикуются только последние записи, а все остальные доступны в архиве.

– Отзывы. Блог приглашает читателей писать отзывы. Приглашение к отзывам публикуется сразу же вслед за записью. В этом плане комментируемый блог похож на интернет-форум.

– Возможность объединения. Формат блога позволяет объединять содержание нескольких авторских блогов в одной странице

– Устойчивые ссылки. Каждое сообщение, опубликованное внутри блога имеет свой URL - адрес, по которому к сообщению можно обратиться.

– Редактирование при помощи обычного браузера.

Психологические особенности Интернет - общения

Электронной переписке свойственны некоторые особенности:

– общение носит межличностный или групповой характер;

– общение всегда опосредовано и дистантно (в роли посредников выступает компьютер и почтовая служба);

– по способу взаимодействия виртуальное общение может быть монологом либо диалогом;

– форма общения может быть письменная и устная (если общение идет с помощью звуковых речевых файлов, прикрепленных к письмам);

– стиль речи может быть как официально-деловой, так и любой другой, вплоть до разговорной речи и использования ненормативной лексики.

Здесь многое зависит от уровня развития собеседников, их взаимоотношений и целей, которые ими преследуются.

Все формы Интернет-общения, в связи с его опосредованностью компьютером, обладают некоторыми особенностями.

1. Анонимность – несмотря на то, что иногда есть возможность получить некоторые сведения анкетного характера и даже фотографию виртуального собеседника, это недостаточно для реального и более-менее адекватного восприятия личности. Кроме того, при виртуальном общении наблюдается скрывание или презентация ложных сведений о себе. Вследствие подобной анонимности и безнаказанности в Сети проявляется и другая особенность, связанная со снижением психологического и социального риска в процессе общения – аффективная раскрепощенность, ненормативность и некоторая безответственность участников общения. Человек в сети может проявлять и проявляет большую свободу высказываний и поступков (вплоть до оскорблений, нецензурных выражений, сексуальных домогательств), так как риск разоблачения и личной отрицательной оценки окружающими минимален.

2. Своеобразие протекания процессов межличностного восприятия в условиях отсутствия невербальной информации – как правило, сильное

влияние на представление о собеседнике имеют механизмы стереотипизации и идентификации, а также установка желаемых качеств в партнере.

3. Добровольность и желательность контактов – пользователь Интернета добровольно завязывает всевозможные контакты или уходит от них, а также может прервать их в любой момент.

4. Затрудненность эмоционального компонента общения и, в то же время стойкое стремление к эмоциональному наполнению текста, которое выражается в создании специальных значков для обозначения эмоций или в описании эмоций словами (в скобках после основного текста послания).

Набор смайлов.

5. Стремление к нетипичному, ненормативному поведению – зачастую пользователи Интернета презентуют себя с иной стороны, чем в условиях реальной социальной нормы, проигрывают нереализуемые в деятельности вне сети роли, сценарии ненормативного поведения.

В связи с рассмотренными особенностями можно сделать вывод о том, что анонимность общения влечет за собой целый ряд последствий. Так в коммуникации посредством Интернет теряют свое значение невербальные средства общения. Несмотря на то, что в текстовой коммуникации существует возможность выражать свои чувства при помощи «смайликов», физическое отсутствие участников коммуникации в акте общения приводит к тому, что чувства можно не только выражать, но и скрывать, равно, как и можно выражать чувства, которые человек в данный момент не испытывает.

В Интернете в результате физической непредставленности партнеров по коммуникации друг другу теряет свое значение целый ряд барьеров общения, обусловленных такими характеристиками партнеров по коммуникации, которые выражены в их внешнем облике: пол, возраст, социальный статус, внешняя привлекательность, коммуникативная компетентностью человека.

Другое важное следствие физической непредставленности человека в текстовой коммуникации – это возможность создавать о себе любое впечатление по своему выбору. Действительно, в текстовой коммуникации в сети Интернет люди часто создают себе так называемые «виртуальные личности», описывая себя определенным образом. Виртуальная личность наделяется именем, часто псевдонимом (который еще называют – «ник»). Существует точка зрения, согласно которой конструирование виртуальных личностей в Интернете – это отражение изменений структуры идентичности человека является отражением социальных изменений. Если человек полностью реализует все аспекты своего «Я» в реальном общении, мотивация конструирования виртуальных личностей у него, скорее всего, отсутствует, тогда общение в Интернете носит характер дополнения к основному виду общения.

Но виртуальное общение может иметь и компенсаторный, замещающий характер, это происходит в случае формирования Интернет-зависимости. Поведенчески такая зависимость проявляется в том, что люди настолько предпочитают жизнь в Интернете, что фактически начинают отказываться от своей реальной жизни, проводя до 18 часов в день в виртуальной реальности. Интернет-зависимые получают в Интернете различные формы социального признания. Их зависимость может говорить о том, что в реальной жизни социального признания они не получают, а также о том, что в реальной жизни у этой группы людей могут существовать определенные трудности в общении, которые снижают их удовлетворенность реальным общением.

Как любое сообщество, культура общения в Интернете обладает своим собственным набором ценностей, стандартов используемого языка, символов, к которому приспосабливаются отдельные пользователи. Включаясь в такую группу, человек получает возможности поддержки позитивного образа «Я» за счет позитивной социальной идентичности.

Итак, в целом можно сказать, что основными причинами обращения к Интернету, как инструменту общения может быть:

– недостаточное насыщение общением в реальных контактах – в подобных случаях пользователи быстро теряют интерес к Интернет-общению, если появляются новые возможности для удовлетворения соответствующих потребностей в реальной жизни;

– возможность реализации качеств личности, проигрывания ролей, переживания эмоций, по тем или иным причинам фрустрированных в реальной жизни - подобная возможность обусловлена особенностями общения посредством сети – анонимностью, нежесткой нормативностью, своеобразием процесса восприятия человека человеком. Желанием переживания тех или иных эмоций объясняется и стремление к эмоциональному наполнению текста.

Глоссарий

Аддиктивное поведение в сфере ИКТ – одна из форм девиантного поведения с формированием стремления к уходу от реальности путем постоянной фиксации внимания на определенных видах деятельности, опосредованных ИКТ.

Асоциальное поведение в сфере ИКТ – поведение, противоречащее общественным нормам и принципам, выступающее в форме безнравственных или противоправных деяний, совершаемых с использованием ИКТ.

Безопасность информации – такое состояние ее в системе обработки, когда несанкционированное получение защищаемой информации лицами и процессами, не имеющими на это специальных полномочий, становится невозможным или сводится к уровню не выше допустимого

Безопасность данных – это состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их случайное или преднамеренное получение, изменение или уничтожение

Блог – пополняемая через веб-интерфейс коллекция записей.

Владелец защищаемой информации – юридическое или физическое лицо, которое имеет полномочия владеть, пользоваться и распоряжаться данной информацией по договору с собственником, в силу закона или решения административных органов.

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.

Девиантное поведение в сфере ИКТ – вид девиантного поведения индивида (группы индивидов), представляющий систему поступков (или отдельные поступки), опосредованных применением ИКТ (либо направленных в отношении ИКТ), причиняющую ущерб (моральный,

физический, экономический и иной) обществу, организациям, частным лицам или самой личности.

Делинквентное (антисоциальное) поведение в сфере ИКТ – отклоняющееся поведение, представляющее собой проступок либо уголовно наказуемое деяние, совершенное посредством либо в сфере ИКТ, влекущее за собой получение выгоды и/или нанесение материального, психологического, информационного вреда жертве.

Достаточность – определяется возможностью достижения поставленной цели, при наличии доступной пользователю информации.

Достоверность – свойство информации быть правильно воспринятой; вероятность отсутствия ошибок

Доступность – это возможность за приемлемое время получить требуемую информационную услугу.

Доступность информации – свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

Защита данных – совокупность целенаправленных действий и мероприятий по обеспечению безопасности данных.

Защита информации – деятельность по предотвращению утраты и утечки конфиденциальной информации и утраты защищаемой открытой информации.

Защита информации – комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п.

Защита информации – организационные, программные и технические методы и средства, направленные на удовлетворение ограничений, установленных для типов или экземпляров данных в системе обработки данных.

Защита информации – совокупность мероприятий, обеспечивающих предупреждение несанкционированного доступа к конфиденциальной информации, к охраняемым сведениям промышленного, экономического, торгового, финансового и технологического характера.

Защита информации – деятельность собственника информации или уполномоченных им лиц по: обеспечению своих прав на владение, распоряжение и управление защищаемой информацией; предотвращению утечки и утраты информации; сохранению полноты, достоверности, целостности защищаемой информации, ее массивов и программ обработки; сохранению конфиденциальности или секретности защищаемой информации в соответствии с правилами, установленными законодательными и другими нормативными актами.

Защита информации – совокупность мероприятий, обеспечивающих предупреждение разглашения, утечки и несанкционированного доступа к конфиденциальной информации.

Защищаемая информация – любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Защищаемая информация – сведениия, на использование и распространение которых введены ограничения их собственником.

Инсайдер – любое лицо, имеющее доступ к конфиденциальной информации о делах фирмы благодаря своему служебному положению и родственным связям.

Инсайдер – член какой-либо группы людей, имеющей доступ к информации, недоступной широкой публике.

Информационная безопасность – состояние защищенности национальных интересов в информационной сфере, определяемых

совокупностью сбалансированных интересов личности, общества и государства.

Информационная безопасность – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Информационная безопасность – защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Информационная война – открытые и скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной сфере.

Информационная культура – способ жизнедеятельности человека в информационном обществе, как составляющая процесса формирования культуры человечества.

Информационное общество – общество, в котором большинство работающих занято производством, хранением, переработкой и реализацией информации, особенно высшей ее формы – знаний.

Информационная потребность – это необходимость получения информации, требуемой для решения конкретных задач, стоящих перед пользователем.

Информационно-психологическая безопасность – состояние защищенности граждан, их отдельных групп и социальных слоев, а также населения в целом от негативных информационно-психологических воздействий.

Информационные ресурсы – совокупность данных, организованных для эффективного получения достоверной 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.

Информационный терроризм – терроризм с использованием информационного оружия.

Информационные услуги – особый вид товара на информационном рынке.

Канал утечки информации – такие дестабилизирующие факторы, следствием проявления которых может быть получение (или опасность получения) защищаемой информации лицами или процессами, не имеющих на это законных полномочий.

Канал утечки информации – варианты технологии несанкционированного доступа к информации.

Канал утечки информации – физический путь от источника конфиденциальной информации к злоумышленнику, по которому возможна утечка охраняемых сведений.

Канал утечки информации – неконтролируемый физический путь от источника информации за пределы организации или круга лиц, обладающих охраняемыми сведениями, посредством которого возможно неправомерное овладение злоумышленниками конфиденциальной информацией.

Коммерческая тайна – информация, не являющаяся государственными секретами, связанная с производственной, технической, технологической информацией, управлением финансовой и другой деятельностью предприятия, разглашение (передача, утечка) которой может нанести ущерб его интересам.

Компьютерный вирус – это специально написанная, небольшая по размерам программа, которая может «приписывать» себя к другим программам («заражать» их), создавать свои копии и внедрять их в файлы, системные области компьютера и т.д., а также выполнять различные нежелательные действия на компьютере.

Компьютерная этика – совокупность моральных принципов и норм, регулирующих отношения между людьми, сложившихся на основе их работы с компьютерами.

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальная информация – информация, требующая защиты.

Конфиденциальная информация – служебная, профессиональная, промышленная, коммерческая или иная информация, правовой режим которой устанавливается ее собственником на основе законов о коммерческой, профессиональной [промышленной] тайне, государственной службе и других законодательных актов – требует защиты.

Конфиденциальность – это защита от несанкционированного доступа к информации.

Конфиденциальность информации – субъективно определяемая характеристика (свойство) информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью информационной системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.

Личная тайна – защищаемая физическим лицом информация личного характера, распространение которой может нанести моральный или материальный ущерб отдельному физическому лицу.

Многопользовательская ролевая онлайн-игра – разновидность онлайновых ролевых игр, позволяющая множеству людей одновременно играть в изменяющемся виртуальном мире через Интернет.

Надежность – свойство информации, предполагающее ее достаточную свободу от ошибок и пристрастности, а также то, что она точно представляет, что предполагалось представить.

Негативное информационно-психологическое воздействие – воздействие на человека или группу лиц (в том числе, помимо их воли), осуществляемое с использованием специальных средств и методов воздействия на психику человека и приводящее к негативным последствиям для личности, общества и государства.

Несанкционированный доступ – чтение, обновление или разрушение информации при отсутствии на это соответствующих полномочий.

Несанкционированный доступ к информации – получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения доступа...

Несанкционированный доступ к информации – преднамеренное обращение к конфиденциальной информации лицами, не имеющими права доступа к определенным сведениям.

Несанкционированный доступ к информации – неправомерный преднамеренный доступ к источникам конфиденциальной информации лицами, не имеющими права доступа к ним.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Носитель информации – материальных объект, предназначенный для хранения данных.

Носитель информации – материальные объекты, в том числе физические поля, в которых, информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, создавая тем самым возможность для ее накопления, хранения, передачи и использования.

Объект защиты – информация или носитель информации, или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Объект защиты – информация, технические средства и технология ее обработки, в отношении которых необходимо обеспечить безопасность информации.

Объем – это общее количество информации по проблеме, доступной пользователю.

Отказ – нарушение работоспособности какого-либо элемента информационной системы, приводящее к невозможности выполнения им своих функций.

Ошибка – неправильное (одноразовое или систематическое) выполнение элементом информационной системы одной или нескольких функций, происходящее вследствие специфического его состояния.

Пароль – секретная строка символов, предъявляемая пользователем компьютерной системе для получения доступа к данным и программам.

Персональные данные – сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность.

Побочные явления – электромагнитный излучения устройств информационно-вычислительных систем, внешние электромагнитные излучения, вибрации, внешние атмосферные условия и т.д.

Поддерживающая инфраструктура – системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал.

Полнота – это соотношение между имеющейся информацией по проблеме и информацией, доступной пользователю (т.е. той ее частью, которую он может получить).

Поставщики – как правило, это производители информации или ее собственники.

Потребители информации – частные лица, а также предприятия, нуждающиеся в информации для осуществления своей деятельности.

Профессиональная тайна – сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами.

Психологическая атака – метод активного воздействия на психику человека с целью отключения логического мышления: произведения положительного (отрицательного) впечатления или введения в состояние растерянности с последующим побуждением человека к нужной реакции

Психологическое давление – метод внушительного воздействия на психику человека с целью принуждения его к определенным действиям.

Психологическое манипулирование – метод двойственного воздействия на психику человека, целью которого является поставить человека в положение выбора линии поведения между двумя альтернативами (между хорошим и плохим, добром и злом).

Психологическое программирование – метод однообразного или настойчивого воздействия на психику человека с целью выработки алгоритмов его поведения и образов мышления.

Психофизическое оружие – это совокупность всех возможных методов и средств: технотронных, суггестивных, психотропных, комплексных скрытого насильственного воздействия на подсознание человека с целью модификации его сознания, поведения и физиологического состояния в нужном для воздействующей стороны направлении.

Разглашение информации – несанкционированное доведение защищаемой информации до неконтролируемого количества получателей информации.

Разглашение информации – несанкционированное ознакомление с этой информацией лиц, не имеющих законного доступа к ней, лицом, которому эти сведения были доверены или стали известны по службе или работе.

Разглашение информации – умышленное или неосторожное действие должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по работе, приведшее к не вызванному служебной необходимостью оглашению охраняемых сведений, а также передача таких сведений по открытым техническим каналам или обработка их на некатегорированных ЭВМ.

Разглашение информации – умышленные или неосторожные действия должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по службе или работе, приведшие к ознакомлению с ними лиц, не допущенных к этим сведениям.

Ресурс – запас или источник некоторых средств.

Рынок информационных услуг –совокупность экономических, правовых и организационных отношений по торговле (продаже и покупке) информационных услуг между поставщиками (продавцами) и потребителями (покупателями) и характеризуется определенной номенклатурой услуг, условиями и механизмами их предоставления и ценами.

Сбой – временное нарушение работоспособности какого-либо элемента информационной системы, следствием чего может быть неправильное выполнение им своих функций.

Сетевой червь – независимая программа, которая размножается путем копирования самой себя из одного сетевого компьютера в другой.

Сетевой этикет (Netiquette) – это набор предписаний о том, как себя вести в Сети

Система защиты информации – совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Система защиты информации – организованная совокупность органов и объектов защиты информации, используемых методов и средств защиты, а также осуществляемых защитных мероприятий.

Система защиты информации – организованная совокупность мероприятий, методов, органов и средств, создаваемых с целью защиты информации.

Служебная тайна – служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами.

Служебная тайна – информация составляет служебную...тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности;

Служебная тайна – несекретные сведения служебного характера.

Собственник защищаемой информации – юридическое или физическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией.

Социальная сеть – социальная структура, состоящая из группы узлов, которыми являются социальные объекты, и связей между ними.

Специальные средства воздействия – технические и программные средства, используемые для негативного информационно-психологического воздействия на человека или группу лиц.

Специальные методы воздействия – последовательность приемов воздействия на психику человека, применение которых приводит к негативным последствиям для личности, общества и государства.

Стихийные бедствия – пожары, наводнения, стихийные бедствия, взрывы и т.д.

Стоимость – овеществленный в товаре общественный труд, вещественное выражение общественного труда товаропроизводителей.

Троянский конь – компьютерная программа, реализующая полезную функцию и содержащая дополнительные скрытые функции, которые тайно используют законные полномочия инициирующего процесса в ущерб безопасности.

Троян (Троянская программа) – это полезная или вроде бы полезная программа, или командная процедура, содержащая скрытый код, который при вызове выполняет некоторые нежелательные действия. Автор троянской программы может сначала создать полезную программу, интересную другим пользователям, или получить ее исходный текст, а затем добавить код, чтобы программа выполняла некоторую разрушающую функцию помимо полезной.

Угроза – потенциальная возможность неправомерного преднамеренного или случайного воздействия, приводящее к потере или разглашению информации.

Угроза – это человек, вещь, событие или идея, которая представляет некоторую опасность для ценностей, нуждающихся в защите.

Угроза – это потенциальная возможность определенным образом нарушить информационную безопасность.

Угроза безопасности информации – это потенциально существующая возможность случайного или преднамеренного действия или бездействия, в результате которого может быть нарушена безопасность информации (данных).

Угроза безопасности информации – совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации, и/или несанкционированными и/или непреднамеренными воздействиями на нее.

Угроза безопасности информации – мера возможности возникновения... такого явления или события, следствием которого могут быть нежелательные воздействия на информацию: нарушение (или опасность нарушения) физической целостности, логической структуры, несанкционированная модификация (или опасность такой модификации)

информации, несанкционированное получение (или опасность такого получения) информации, несанкционированное размножение информации.

Угроза безопасности информации – потенциально существующая опасность случайного или преднамеренного нарушения безопасности информации, обусловленная особенностями ее хранения и обработки.

Угроза безопасности информации – реальные или потенциальные возможные действия или условия, приводящие к овладению, хищению, искажению, изменению или уничтожению информации.

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

Утечка информации – неконтролируемое распространение защищаемой информации;

Утечка информации – неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация доверена;

Утечка информации – бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена по службе или стала известна в процессе работы;

Утечка информации – не контролируемый выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация доверена.

Утечка информации – неправомерный выход конфиденциальной информации за пределы защищаемой зоны ее функционирования или установленного круга лиц, результатом которого является получение информации лицами, не имеющими к ней санкционированного доступа.

Уязвимость информации – событие, возникающее как результат стечения обстоятельств, когда в силу каких-то причин используемые... средства защиты не в состоянии оказать достаточного противодействия

проявлению дестабилизирующих факторов и нежелательного их воздействия на защищаемую информацию

Форум – организация обмена информацией и общения между большим количеством собеседников, которым небезынтересна тема обсуждения, которая и является причиной концентрации этих людей в одном месте для вынесения её на всеобщее обсуждения.

Целостность – актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Целостность информации – ее существование в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Цель защиты информации – желаемый результат защиты информации.

Чат – средство общения пользователей по сети в режиме реального времени, а также программное обеспечение, позволяющее организовывать такое общение.

Электронная почта – аналог хорошо известной системы общения через письма, отправляемые в конвертах, отличающаяся при этом тем, что письмо существует в виде электронного сообщения, которое отправляется с компьютера адресанта на почтовый сервер, а затем доставляется адресату на его почтовый ящик.

Этикет – правила хорошего тона, принятые в той или иной социальной группе.

Список литературы

1. Бондаренко, С.В. Некоторые аспекты функционирования виртуальных сетевых сообществ криминальной ориентации. / С.В. Бондаренко. // «Актуальные проблемы современной социологии». – РнД: Пегас, 2002. – 256 с.

2. Войскунский, А.Е. Зависимость от Интернета: актуальная проблема / А.Е. Войскунский. [Электронный ресурс] – Режим доступа: http://www.auditorium.ru/conf/psichol/belins_in.htm.

3. Войскунский, А.Е. Психологическая характеристика потенциально негативных последствий компьютерных технологий / А.Е. Войскунский // Молодежь в компьютерно-игровых и интернет-центрах. Сборник методических материалов (по итогам работы круглого стола). – М. : АРКЦентр, 2004. – с. 33-37.

4. Глушаков С.В. Антихакер / С.В. Глушаков, А.С. Сурядный, Н.С. Тесленко. – М. : АСТ МОСКВА; Владимир : ВКТ, 2008. – 501, [11] с., - ил.

5. Голубев, В. «Компьютерная преступность – проблемы и решения» / В. Голубев. [Электронный ресурс] – Режим доступа: http://www.crime-research.ru/articles/golubev_sept.

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

7. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности / А.А. Грушо, Э.А. Применко, Е.Е. Тимонина. – М. : Academia, 2009. – 272 с. (Гриф МО РФ)

8. Жичкина, А.Е. Социально-психологические аспекты общения в Интернете / А.Е. Жичкина. [Электронный ресурс] – Режим доступа: http://flogiston.ru/projects/articles/refinf.shtml.

9. Зеркина, Е.В. К вопросу о девиантном поведении школьников в сфере компьютерных технологий / Е.В. Зеркина // XVI Международная конференция-выставка «Информационные технологии в образовании» : Сборник трудов участников конференции. Часть II. – М. : «БИТ про», 2006 – 208с. – с.109-112.

10. Зеркина, Е.В. Подготовка будущих учителей к профилактике девиантного поведения школьников в сфере компьютерных технологий / Е.В. Зеркина, Г.Н. Чусавитина // Открытое образование. Проблемы и перспективы развития: Сборник научных материалов. – М. : Изд-во МГОУ, 2006. – 122с. – с. 103-108

11. Змановская, Е.В. Девиантология: (Психология отклоняющегося поведения): учеб. пособие для студ. высш.учеб. заведений / Е.В. Змановская. – 3-е изд., испр. И доп. – М. : Издательский центр «Академия», 2006. – 288 с.

12. Иванов, М.С. Психологическая характеристика ролевой компьютерной игры как особого вида деятельности / М.С. Иванов, Г.М. Авилов // Сибирская психология сегодня: Сборник научных трудов. – Кемерово : Кузбассвузиздат, 2002. – с. 41-55.

13. Кононов, А.А. Информационное общество: общество тотального риска или общество управляемой безопасности? / А.А. Кононов // Проблемы управления информационной безопасностью. – М. : 2002.

14. Короленко, Ц.П., Семь путей к катастрофе (деструктивное поведение в современном мире) / Ц.П.Короленко, Т.А.Донских. - Новосибирск, «Наука», 1990. – 224 с.

15. Кузнецов А.А. Защита деловой информации (секреты безопасности) / А.А. Кузнецов. – М. : Издательство «Экзамен», 2008. – 255, [1]с.

16. Краковский Ю.М. Информационная безопасность и защита информации : учебное пособие. – М. : ИКЦ «МарТ», Ростов н/Д : Издательский центр «МарТ», 2008. – 288 с. (серия «Учебный курс»).

17. Морозов Н.П. Защита деловой информации для всех / Н.П. Морозов, С.Б. Чернокнижный. – М. : ИД «Весь», 2003. – 160 с.

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

19. Платонов, К.К. Структуры и развитие личности/ К.К. Платонов. - АН СССР, Ин-т психологии. – М. : 1986. – 254 с.

20. Расторгуев С.П. Основы информационной безопасности / С.П. Расторгуев. – М. : Academia, 2009. – 192 с. (Гриф МО РФ)

21. Тропина, Т.Л. Киберпреступность и кибертерроризм: поговорим о понятийном аппарате / Т.Л. Тропина // Сборник научных трудов международной конференции «Информационные технологии и

безопасность». Выпуск 3. – Киев : Национальная академия наук Украины, 2003. – С. 173.

22. Фролов, С.С. Социология: Учебник. Для вузов / С.С. Фролов // Ин-т «Открытое о-во». – М. : Наука, 2004. – 256 с.

23. Яремчук С.А. Видеосамоучитель. Защита вашего компьютера (+CD). – СПб. : Питер, 2008. – 288 с. : ил.

24. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М. : Академический Проект; Фонд «Мир», 2003. – 640 с. (Гриф МО РФ)

25. Web-сервер властных структур Российской Федерации [Электронный ресурс]. – Режим доступа: www.gov.ru

26. Web-сервер Совета безопасности РФ [Электронный ресурс]. – Режим доступа: www.scrf.gov.ru

27. Web-сервер Федерального агентства правительственной связи и информации при Президенте Российской Федерации [Электронный ресурс]. – Режим доступа: www.fagci.ru

28. Web-сервер Государственной технической комиссии при Президенте Российской Федерации [Электронный ресурс]. – Режим доступа: www.infotecs.ru/gtc

29. Сервер Государственной Думы Федерального Собрания РФ [Электронный ресурс]. – Режим доступа: www.duma.gov.ru

30. Web-сервер Верховного Суда Российской Федерации [Электронный ресурс]. – Режим доступа: www.supcourt.ru

31. Web-сервер подразделения по выявлению и пресечению преступлений, совершаемых с использованием поддельных кредитных карт, и преступлений, совершаемых путем несанкционированного доступа в компьютерные сети и базы данных [Электронный ресурс]. – Режим доступа: www.cyberpolice.ru

32. Портал по информационной безопасности [Электронный ресурс]. – Режим доступа: www.infosecurity.report.ru

33. Портал по информационной безопасности [Электронный ресурс]. – Режим доступа: www.void.ru

34. Центр исследования компьютерной преступности [Электронный ресурс]. – Режим доступа: www.crime-research.ru

Учебное текстовое электронное издание

Чернова Елена Владимировна

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Учебное пособие для студентов-социологов

1,63 Мб
1 электрон. опт. диск

г. Магнитогорск, 2015 год
ФГБОУ ВПО «МГТУ»
Адрес: 455000, Россия, Челябинская область, г. Магнитогорск,
пр. Ленина 38

ФГБОУ ВПО «Магнитогорский государственный
технический университет им. Г.И. Носова»
Кафедра бизнес-информатики и информационных технологий
Центр электронных образовательных ресурсов и
дистанционных образовательных технологий
e-mail: ceor_dot@mail.ru