ЗДОРОВЬЕ И БЕЗОПАСНОСТЬ ДЕТЕЙ В МИРЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНТЕРНЕТ

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКТ

Москва
СОЛОН-ПРЕСС
2010

УДК 621.396.218
ББК 32.884.1
346

Авторы:
Л. Н. Горбунова (руководитель авторского коллектива),
Л. А. Аникова, А. М. Семибратов, Н. К. Смирнов,
Е. В. Сорокина, Т. М. Третьяк

346 Здоровье и безопасность детей в мире компьютерных технологий и Интернет. Учебно-методический комплект. — М.: СОЛОН-ПРЕСС, 2010. — 176 с.: ил.

ISBN 978-5-91359-076-3

Программа «Здоровье и безопасность детей в мире компьютерных технологий и Интернета» разработана с учетом потребностей образовательных учреждений в области безопасной работы в Интернете. Она ориентирована на руководителей учреждений общего образования, на школьных учителей и методистов, которые заинтересованы в расширении своих компетенций в области применения ИКТ и безопасной работы в сети Интернет. Программа может быть использована, как в учреждениях дополнительного профессионального образования, так и в системе методической работы с практическими работниками образования Методическое приложение к программе рекомендуется использовать при организации просветительской работы с родителями школьников.

К книге прилагается **компакт-диск**, на котором размещен текст книги в формате PDF, нормативные документы, презентация по безопасности, интерактивный курс по безопасности и полезные ссылки на вспомогательные материалы.

ISBN 978-5-91359-076-3

Методические рекомендации к программе повышения квалификации педагогических кадров «Здоровье и безопасность детей в мире компьютерных технологий и Интернета»

Методические рекомендации разработаны в целях оказания помощи специалистам, реализующим программу повышения квалификации «Здоровье и безопасность детей в мире компьютерных технологий и Интернета». Их подготовка обусловлена тем, что, несмотря на обилие разнообразной информации по проблеме безопасного поведения в Интернете, профилактике заболеваний и сохранению здоровья в новых средах, насыщенных компьютерами и средствами ИКТ, она не систематизирована для решения педагогических задач в практике дополнительного профессионального педагогического образования и для просветительской работы с общественностью.

Методические рекомендации содержат материалы, раскрывающие основное содержание тем, представленных в модулях программы, и служат ориентиром в многообразии информации, содержащейся в уже изданных книгах, в Интернет-источниках по проблематике программы. Назначение методических рекомендаций состоит в том, чтобы выступить информационным, библиографическим, дидактическим навигатором, чтобы помочь преподавателям правильно расставить акценты в организации, содержании и технологиях образовательного процесса.

Предлагаемые материалы не носят исчерпывающего характера, что связано с ожиданием творческого подхода к реализации программы со стороны ее реализаторов — преподавателей учреждений дополнительного профессионального образования, региональных учебных центров Microsoft «Академия учителей».

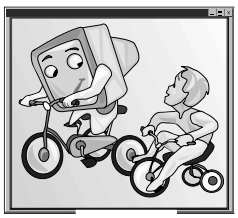
В книге использованы рисунки «5000 забавных изображений» www.cdboom.com.

Модуль 1
ПСИХИЧЕСКОЕ И ФИЗИЧЕСКОЕ ЗДОРОВЬЕ ДЕТЕЙ ПРИ РАБОТЕ ЗА КОМПЬЮТЕРОМ

Тема 1.1
КОМПЬЮТЕРЫ И ФИЗИЧЕСКОЕ ЗДОРОВЬЕ ДЕТЕЙ

Повсеместная информатизация и компьютеризация общества, позволяющая современному человеку идти в ногу со временем, отрицательно влияет на соматическое и психическое здоровье взрослых, а еще больше — детей. Минимизация вредного воздействия компьютера на детский организм становится одной из важных задач, стоящих перед современной школой. Выдвижение проблемы профилактики нарушений здоровья школьников при работе с компьютером в число приоритетных задач социального развития обусловило актуальность теоретической и практической разработки указанной проблемы. В разработке стратегии компьютерного обучения должно быть предусмотрено профилактическое направление, включающее преодоление факторов риска и активное воспитание обучающихся в гигиеническом режиме.

Сегодня представить будущее без компьютера невозможно. Работа на нем обучает детей новому, более простому и быстрому способу получения и обработки информации. А умение найти необходимый для деятельности материал и эффективно его обработать ускоряет и оптимизирует процесс мышления. Компьютер может стать помощником в интеллектуальном развитии ребенка, освоении им профессии, а может разрушить здоровье и привести к социальной дезадаптации.



Компьютер стимулирует мыслительные процессы ребенка, компьютерные игры позволяют ребенку рассмотреть не только единичное понятие или конкретную ситуацию, но и получить обобщенные представления обо всех похожих ситуациях или предметах, т. е. у детей развиваются важнейшие операции мышления — обобщение и классификация. В виртуальной игре формируется понимание ребенком уровневой организации окружающего мира (реальные предметы и картинки, схемы, символы), развивается знаковая функция сознания, предоставляющая возможность мыслить без опоры на внешние предметы. Компьютерные игры облегчают процесс перехода психического действия из внешнего плана во внутренний, способствуют формированию произвольного, осмысленного запоминания, внимания, развивают зрительно-моторную координацию ребенка. Компьютер развивает множество интеллектуальных навыков.

Однако все же не следует переходить грань разумного в использовании компьютера — и в учебной деятельности, и в работе, и в организации своего досуга. Это предупреждение обусловлено тем, что длительная работа за компьютером, что подтверждено многочисленными исследованиями, негативно сказывается на многих функциях организма человека: высшей нервной деятельности, эндокринной, иммунной и репродуктивной системах, на зрении и костно-мышечном аппарате. Названные проблемы, относящиеся к соматическим, отражаются и на психическом состоянии пользователя компьютерной техникой.

Конечно, в период школьной жизни ученика именно от учителя зависит то, какое влияние на здоровье учащихся оказывают процесс обучения и внутришкольная среда. Использование новых технических средств обучения, с одной стороны, повышает наглядность обучения и создает условия для сохранения работоспособности. С другой стороны, по сравнению с обычными уроками увеличивается объем информации, получаемой учащимися. И хотя форма подачи информации с применением ТСО более наглядна, возросший объем информации увеличивает напряжение в работе, темп работы, приводит к возрастанию нагрузки на зрительный анализатор. Даже не очень продолжительная работа на ПК (не более 1 часа) вызывает у 73 % подростков общее и зрительное утомление, в то время как обычные учебные занятия вызывают усталость только у 54 % подростков. Нагрузка на глаза при работе с ПК существенно отличается от нагрузки при других видах зрительной работы. Кроме того, увеличивается статическая нагрузка и снижается двигательная активность. Еще один фактор — нервно-эмо-

циональное напряжение. Общение с компьютером, особенно с игровыми программами, сопровождается сильным нервным напряжением, поскольку требует быстрой ответной реакции. Ребенок испытывает своеобразный эмоциональный стресс, а кратковременная сильная концентрация внимания вызывает у него сильное выраженное утомление. Бурно распространяющаяся компьютеризация принесла с собой так называемый «компьютерный зрительный синдром»: миллионы людей — и взрослых, и детей — стали жаловаться на ухудшение зрения. Неблагоприятное воздействие условий работы на ПК может быть уменьшено за счет установления регламента продолжительности работы школьников с компьютерами, рационального кондиционирования воздуха, ведения регулярных занятий физической культурой, специальных упражнений для профилактики зрительного утомления.

Организационно-педагогические условия осуществления образовательного процесса, как и технологии работы учителя на уроке, составляют сердцевину здоровьесберегающих образовательных технологий. Большая часть этих условий регламентированы в СанПиНах, но приоритет компетенции педагогов здесь бесспорен. Основные объекты внимания — учебная нагрузка, создание условий для получения учащимися достаточной физической нагрузки, грамотное использование технических средств обучения, содействие рациональной организации режима дня школьников.

По характеру действия здоровьесберегающие технологии, применяемые при организации работы школьника на компьютере, могут быть подразделены на следующие группы: защитно-профилактические; компенсаторно-нейтрализующие; стимулирующие; информационно-обучающие.

К группе защитно-профилактических технологий относятся приемы, методы, направленные на защиту ребенка от неблагоприятных для здоровья воздействий, связанных с работой на компьютере (воздействие электромагнитного излучения, неправильное расположение монитора, длительность работы на компьютере и ряд других). Это, в частности, выполнение санитарно-гигиенических требований, регламентированных СанПиНами.

При использовании *компенсаторно-нейтрализующих технологий* ставится задача восполнить недостаток того, что требуется организму для полноценной жизнедеятельности, или хотя бы частично нейтрализовать неблагоприятное воздействие статичности уроков, недостаточность физической нагрузки при длительной работе за компьютером. Это может быть, например, проведение физкультурных пауз, зрительной гимнастики.

Стимулирующие приемы и методы позволяют активизировать функции организма, например, проведение физкультминуток.

Информационно-обучающие здоровьесберегающие технологии обеспечивают формирование у школьников необходимого уровня грамотности для эффективной заботы о своем здоровье и соблюдения оптимальных условий для работы на компьютере. Посредством этих технологий учащиеся получают представление об основных правилах работы с компьютером, с правилами техники безопасности, с санитарно-гигиеническими нормами, которые необходимо не только знать, но и соблюдать, чтобы снизить вредное воздействие на зрение.

Тема 1.2
ГИГИЕНИЧЕСКИЕ ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ЗАНЯТИЙ С ИСПОЛЬЗОВАНИЕМ НОВЫХ ИНФОРМАЦИОННО-КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Использование новых информационных технологий в дошкольном образовательном учреждении создает специфический микроклимат окружающей среды, характеризующийся такими физическими факторами, как шум, вибрация, электромагнитное поле, статические электричество и др. Изменяется температура, влажность и химический состав воздуха.

Более того, процесс восприятия материала требует от дошкольника более значительного, чем при других методах обучения, зрительного, эмоционального, умственного, статического напряжения.

Задача педагога, проводящего занятия с использованием технических средств обучения, — снять или свести до минимума их отрицательное влияние на здоровье дошкольника.

Гигиенические нормы и правила внедрения в образовательный процесс компьютеризации содержат требования:

1. К помещениям, где находятся компьютеры
2. К оборудованию мест для занятий
3. К режиму занятий и отдыха при работе.

Педагогу, проводящему занятие с использованием компьютерных технологий, нужно не только хорошо изучить данные гигиенические требования, но и уметь проверять соответствие имеющихся в его распоряжении компьютеров перечисленным параметрам, осуществляя таким образом постоянный контроль за работой

Гигиенические требования к состоянию воздушной среды (по Н.Т. Лебедевой)

Физические показатели	
Температура	18, 20, 22
Относительная влажность, %	65, 58, 52
Содержание легких ионов, 1/куб. см	1500—3000
Химический состав	
Аммиак	0,2 мг/куб.м
Диоксид углерода	0,1 %
Озон	0,03 мг/куб.м
Фенол	0,003 мг/куб. м
Формальдегид	0,01 мг/куб.м
Хлористый винил	0,05 мг/куб.м
Шум и вибрация	
Уровень шума	Не более 50 дБ
Вибрация на рабочем месте (виброскорость)	79—67 Гц
Естественное освещение	
Ориентация освещения	Север, северо-восток
Соотношение яркостей в рабочей зоне (экран—стол)	3 : 1
Солнцезащитные жалюзи	Солнечные лучи не должны попадать на экран
Освещенность стола	Не более 600 лк
Искусственное освещение	
Коэффициент пульсации светильников	Не более 10 %
Включение света	Раздельно по рядам
Освещенность	
Экран	Не более 300 лк
Клавиатура	Не более 400 лк
Стол	Не более 400 лк
Классная доска	Не более 500 лк

компьютерной техники и средств ТСО. Не реже двух раз в год (в зимний и весенний периоды) работа кабинетов должна контролироваться врачами соответствующих служб. Такое обследование сопровождается лабораторными анализами воздушной среды, ее химических и физических показателей.

Гигиенические требования к оформлению и размещению различных ТСО

Экран монитора телевизора	Клавиатура	Оформление изображения на экране
Расстояние 0,6—0,7 м от ребенка	Клавиши светло-серого цвета с матовой поверхностью	Размер символов на высоте не менее 3,1—3,8 мм
Антибликовое покрытие	Наклон клавиатуры 12—10°	Контраст между яркостью символов и фона не ниже 80 %
Рентгеновское излучение не более 10,8 мкР/ч		Изображение стабильно, без мерцаний и бликов

Обязанности медицинских работников образовательных учреждений, использующих информационные технологии, не ограничиваются контролем за выполнением гигиенических требований к помещениям, оборудованию техникой, а включают еще и контроль за мебелью.

Чтобы сохранить здоровье учащихся, кроме выполнения требований к помещениям, технике, мебели, нужно использовать такой режим работы, который соответствовал бы функциональным возможностям детей старшего дошкольного и школьного возраста.

К сожалению, часто недооценивается значимость санитарных норм и правил устройства оборудования, режима работы, содержания компьютерных программ, необходимые методики, рекомендации, позволяющие беречь здоровье детей в условиях компьютерного обучения.

По данным материалов обобщения педагогического опыта педагогов, применяющих информационные технологии, наиболее часто допускаемыми нарушениями в образовательных учреждениях являются:

- использование видеомониторов, не отвечающих гигиеническим требованиям;
- отсутствие в помещениях кондиционеров;
- применение бытовых вентиляторов вместо специальной вентиляционной системы.

Часты следующие нарушения режима занятий:

- нет перерывов либо они недостаточны для проветривания и уборки помещения;
- увеличена продолжительность работы воспитанников на компьютерах;
- игнорируются физкультминутки.

Особенно опасен следующий факт: интерес детей к работе с компьютерами настолько маскирует утомление, дети, подростки настолько увлекаются, что не замечают признаков утомления, продолжают занятия и, в результате, наносят существенный вред своему здоровью. Как результат — мы получаем появление психосоматических расстройств, невротических реакций и распространенность проявлений стресса.

Педагог должен быть особенно внимательным к учащимся, уметь выявлять признаки утомления и дифференцировать для учащихся учебную нагрузку.

Достаточно грамотно поступают педагоги, которые осуществляют не только компьютеризацию учебного процесса, но и оценку состояния здоровья воспитанников, их функциональных возможностей с помощью компьютера.

Важнейший показатель эффективности занятий с использованием информационных технологий — режим учебных занятий. Длительность работы с компьютером зависит от индивидуально-возрастных особенностей занимающихся.

Таким образом, используя в образовательном процессе современные информационные технологии, педагог должен помнить о необходимости сохранения здоровья воспитанников, руководствуясь следующими направлениями в своей деятельности:

1. Знать санитарно-гигиенические нормы и правила устройства оборудования.

2. Составлять правила использования помещений ТСО с учетом санитарных правил и условий конкретного образовательного учреждения.

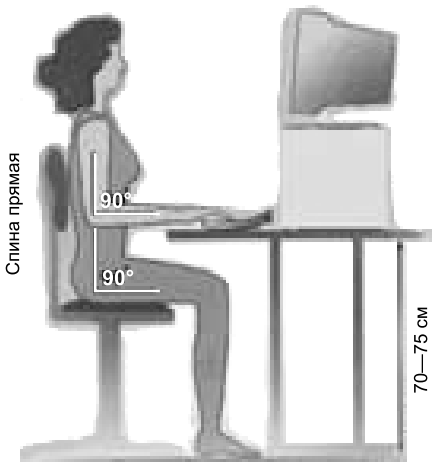
3. Внедрять компьютеризированную диагностику состояния здоровья школьников.

Рабочее место

Кроме всего, важно знать, как правильно организовать рабочее место. Сделать это не трудно, а сохранению здоровья ребенка помочь может. Так, мебель должна соответствовать его росту.

Стул должен быть обязательно со спинкой. Сидеть ребенок должен на расстоянии не менее 50—70 см от компьютера (чем дальше, тем лучше), упираясь взором перпендикулярно в центр экрана. Посадка прямая или слегка наклоненная вперед, с небольшим наклоном головы. Чтобы обеспечить устойчивость посадки, ребенок должен сидеть на стуле, опираясь на 2/3—3/4 длины бедра. Между корпусом тела и краем стола сохраняется свободное пространство не менее 5 см. Руки свободно лежат на столе. Ноги согнуты в тазобедренном и коленном суставах под прямым углом и располагаются под столом на соответствующей подставке.

Стол, на котором стоит компьютер, следует поставить в хорошо освещенное место, но так, чтобы на экране не было бликов. Помните, занятия на компьютере принесут пользу, если вы прислушаетесь к нашим рекомендациям и будете их выполнять. От этого зависит здоровье вашего ребенка.



Рост ребенка в см	Стол Высота поверхности над полом, мм	Стул Высота сидения над полом, мм
90—100	420	240
101—115	460	260
116—130	520	300

Тема 1.3
ПРОФИЛАКТИКА НАРУШЕНИЙ ОСАНКИ И ЗРЕНИЯ ПРИ РАБОТЕ ЗА КОМПЬЮТЕРОМ

Работа человека, сидящего за компьютером, — одна из самых напряженных и утомительных. В некоторых странах она внесена в список наиболее вредных для здоровья. Наибольшие функциональные изменения в организме отмечаются со стороны органов зрения, дыхания, костномышечной и нервно-психической системы.

О здоровье ребенка взрослые обязаны подумать еще до того, как ребенок приступил к занятиям с использованием компьютера. Поэтому педагог должен быть достаточно компетентным в вопросах возрастных особенностей своих воспитанников. Важно предупредить любое отклонение в состоянии здоровья ребенка, если таковое может случиться при использовании конкретных методов и приемов обучения.

Основные направления профилактики нарушений здоровья детей при работе за компьютером следующие.

- Ограничение количества времени, проводимого детьми за компьютером (3—4-летнему малышу в день в общей сложности можно пребывать перед монитором тридцать—сорок минут, разделив их на три-четыре сеанса по 10 минут, а для младших школьников это время может быть увеличено до полутора-двух часов);
- Чередование компьютерных занятий и физической активности, не требующей напряжения зрения (прогулка, игра в мяч на воздухе или поход в магазин), проведение физкультминуток и физкультпауз;
- Использование упражнений, снижающих зрительное утомление, например, слежение за объектами, движущимися в поле зрения, или концентрация зрения на удаленных предметах;
- Попеременное использование работы с текстовым документом и игр, в которых присутствуют движущиеся объекты, чередование аркадных игр, требующих быстрой мышечной и зрительной реакции, с какими-нибудь головоломками, логическими заданиями;
- Применение разного рода тренажеров, установленных под рабочим столом — педалей, пневмоковриков;
- Подбор стула, соответствующего росто-возрастным показателям ребенка;

- Принятие мер по уменьшению отражений от монитора (например, выключение верхнего освещения, задергивание штор на окнах, поворот монитора таким образом, чтобы ни прямо перед ним, ни сзади не было ярких источников света, установление специального антибликового экрана);
- Контроль позы ребенка, формирование привычки сидеть ровно и смотреть прямо на монитор;
- Использование упражнений с помощью кистевых пружинных или резиновых эспандеров; гимнастики, направленной на снятие утомления в кистях рук и предплечьях, проведение точечного массажа.

Профилактика нарушений осанки при работе за компьютером

Осанка является комплексным показателем состояния здоровья детей, и безобидные функциональные нарушения могут привести к стойким деформациям опорно-двигательного аппарата.

Известно, что на рост, развитие, укрепление здоровья и формирование осанки оказывают влияние условия окружающей среды, т. е. условия, в которых развивается и воспитывается ребенок. Поэтому родители, родственники, сотрудники дошкольных и школьных учреждений должны постоянно следить за формированием осанки у детей, строго контролировать позу детей при сидении, стоянии, ходьбе. Важное значение имеют своевременное полноценное питание, свежий воздух, массаж, гимнастика, закаливание, подбор мебели в соответствии с длиной тела, оптимальная освещенность. Поддержание правильной позы требует систематичности и повторяемости. В то же время в рамках многообразия задач, решаемых на уроке, существует постоянная опасность упустить из внимания моменты формирования осанки школьника. При этом следует признать, что уроки физической культуры не решают проблему формирования осанки.

Особенно портит осанку неправильная поза при письме, чтении, просмотре телевизора, работе с компьютером. Что же нужно знать, чтобы все-таки избежать печальных последствий агрессивной школьной среды, компьютерного господства?

Конструкция позвоночного столба позволяет ему, сохраняя гибкость и подвижность, выдерживать ту же нагрузку, которую может выдержать в 18 раз более толстый бетонный столб. Позвоночный столб отвечает за сохранение осанки, служит опорой для тка-

ней и органов, а также принимает участие в формировании стенок грудной полости, таза и брюшной полости. Каждый из позвонков, составляющих позвоночный столб, имеет внутри сквозное позвоночное отверстие. Позвоночные отверстия составляют позвоночный канал, содержащий спинной мозг, который таким образом надежно защищен от внешних воздействий.

Масса и размеры позвонков увеличиваются по направлению от верхних к нижним: это необходимо, чтобы компенсировать возрастающую нагрузку, которую несут нижние позвонки. Помимо утолщения позвонков, необходимую степень прочности и упругости позвоночнику обеспечивают несколько его изгибов, лежащих в сагиттальной, т. е. боковой плоскости. Четыре разнонаправленных изгиба, чередующиеся в позвоночнике, расположены парами: изгибу, обращенному вперед (лордозу), соответствует изгиб, обращенный назад (кифоз). Благодаря такой конструкции позвоночник работает подобно пружине, распределяя нагрузку равномерно по всей своей длине.

Всего в позвоночном столбе 32—34 позвонка, разделенных межпозвоночными дисками и несколько различающихся своим устройством.

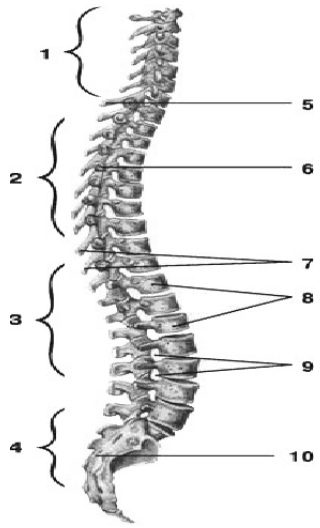


Рис. 1. Позвоночный столб (вид справа): 1 — шейный лордоз; 2 — грудной кифоз; 3 — поясничный лордоз; 4 — крестцовый кифоз; 5 — выступающий позвонок; 6 — позвоночный канал; 7 — остистые отростки; 8 — тело позвонка; 9 — межпозвоночные отверстия; 10 — крестцовый

Однако и такая замечательная «конструкция» требует бережного обращения. В противном случае могут возникнуть неприятности в виде нарушений осанки. Нарушения осанки делятся на 2 группы:

1) изменение физиологических изгибов в сагиттальной (перед-не-задней) плоскости;

2) искривление позвоночника во фронтальной плоскости (сколиозы).

Особого внимания требуют нарушения осанки в сагиттальной плоскости.

Различают следующие варианты нарушения осанки в сагиттальной плоскости, при которых происходит изменение правильных соотношений физиологических изгибов позвоночника:

а) «сутуловатость» — увеличение грудного кифоза в верхних отделах при сглаживании поясничного лордоза;

б) «круглая спина» — увеличение грудного кифоза на всем протяжении грудного отдела позвоночника;

в) «вогнутая спина» — усиление лордоза в поясничной области;

г) «кругло-вогнутая спина» — увеличение грудного кифоза и увеличение поясничного лордоза;

д) «плоская спина» — сглаживание всех физиологических изгибов;

е) «плоско-вогнутая спина» — уменьшение грудного кифоза при нормальном или несколько увеличенном поясничном лордозе.

Обычно различают 3 степени искривлений позвоночника (сколиоза) в сагиттальной плоскости. Чтобы определить, является ли искривление уже установившимся, стойким, — ребенка просят выпрямиться:

- деформация 1 степени — искривление позвоночника выравнивается до нормального положения при выпрямлении;
- деформация 2 степени — отчасти выравнивается при выпрямлении ребенка или при висе на гимнастической стенке;
- деформация 3 степени — искривление не меняется при висе или выпрямлении ребенка.

Дефекты осанки во фронтальной плоскости не подразделяются на отдельные виды. Для них характерно нарушение симметрии между правой и левой половинами туловища; позвоночный столб представляет собой дугу, обращенную вершиной вправо или влево; определяется асимметрия треугольников талии, пояса верхних конечностей (плечи, лопатки), голова наклонена в сторону. Симптомы нарушения осанки могут быть выявлены в различной степени от чуть заметных до резко выраженных.

Боковое искривление позвоночника при функциональных нарушениях осанки может быть исправлено волевым напряжением мускулатуры или в положении лежа.

Сколиоз

Сколиоз на начальной стадии развития процесса (1 ст.), как правило, характеризуется теми же изменениями, что и нарушение осанки во фронтальной плоскости. Но, в отличие от нарушений осанки, при сколиозе, кроме бокового искривления позвоночника, наблюдается скручивание позвонков вокруг вертикальной оси. Об этом свидетельствует наличие реберного выбухания по задней поверхности грудной клетки (а при прогрессировании процесса формирование реберного горба) и мышечного валика в поясничной области. На более позднем этапе развития сколиоза происходит развитие клиновидной деформации позвонков, расположенных на вершине дуги искривления позвоночника. Диагноз сколиоза выставляется врачом-ортопедом на основании клинического и рентгенологического обследования.

Профилактика нарушений осанки у обучающихся начальных классов

Уже в дошкольный период позвоночник ребенка начинает испытывать повышенные нагрузки: как правило, современные родители стараются водить своих малышей на подготовительные занятия. И начиная с 5—6 лет, хотя бы по 2 часа 2—3 раза в неделю, малыш «сидит за партой». А мебель (столы и стульчики) чаще не приспособлена для еще маленьких учеников. В результате перегружается спина и устают глаза.

В домашней обстановке будущие первоклашки регулярно занимаются совершенствованием полученных навыков: пишут, читают, рисуют и т. д. Грамотно созданное «рабочее место» крайне необходимо первокласснику. Именно в период начала регулярных занятий позвоночник ребёнка сам «ищет» для себя удобную позу... Удобную, но НЕПРАВИЛЬНУЮ! Если родители своевременно не примут меры, способствующие выработке правильной осанки, то последствия неизбежны и не всегда поправимы. Увы, медицина не

победила окончательно такую проблему, как «сколиоз», и споров на тему методов лечения предостаточно. А вот меры профилактики давно известны.

Одна из них — своевременная и правильная организация рабочего места школьника, способствующая закреплению навыков правильной осанки.

Нарушения осанки при работе за компьютером

Осанка — это положение, которое принимает тело, когда человек сидит за компьютером. Правильная осанка необходима для профилактики заболеваний шеи, рук, ног, спины. Нас, конечно же, беспокоит та сидячая поза, которая увеличивает статическую нагрузку и снижает и без того низкую двигательную активность современного ребенка. Необходимо так организовать рабочее место ребенка, чтобы осанка была оптимальной, что снизит риск нарушений и отклонений в состоянии здоровья и развитии растущего организма дошкольника.

При проведении первого занятия с использованием компьютера можно вместе с воспитанниками сформулировать инструкцию правильной посадки за столом с компьютером. При работе за компьютером лучше всего сидеть на 2,5 см выше, чем за обычным столом. Голову нужно держать ровно по отношению к обоим плечам, голова не должна наклоняться к одному плечу. При взгляде вниз голова должна находиться точно над шеей, а не наклоняться вперед. К характеристикам неправильного положения тела при работе за компьютером можно отнести следующее:

1. *Сгорбленное положение* (увеличивает и без того большую нагрузку на позвоночник, приводит к чрезмерному растяжению мышц, поддерживающих осанку).

2. *Голова выдвинута вперед* (такая осанка часто возникает по следующим причинам: глядя на экран монитора, ребенок напрягается, что заставляет его вытягивать шею вперед; сидя в такой позе, напряжения мышц у основания головы и шеи могут привести к следующим нарушениям: головные боли, боль в шее, боль в руках и кистях).

3. *Сутулость* (линия плеча располагается не точно над линией бедер и под линией ушей; сутулость вызывает чрезмерную нагрузку на плечевые сухожилия, что приводит к напряжению мышц плеча. Сутулость может приводить к развитию: синдрома запястного канала, синдрома ущемления плеча).

Для улучшения осанки можно использовать специальные упражнения, которые помогают поддерживать хорошую физическую форму. Например: сидя, предплечья лежат на подлокотниках, а кисти находятся под крышкой стола ладонями вверх. Надавив ладонями на внутреннюю поверхность крышки стола, напрягать мышцы предплечья, осуществляющие это движение. В этом положении следует оставаться в течение 10 секунд. Повторять не менее 10 раз.

Полезно!
Инструкция по правильной посадке за компьютером

1. Сядьте прямо.
2. Спину держите ровно, корпус разверните строго к монитору (нельзя сидеть вполоборота).
3. Ноги не скрещивайте, поставьте обе ступни твердо на пол или на подножку.
4. Поясница слегка выгнута, опирается на спинку кресла.
5. Расслабьте корпус и ноги, вам должно быть удобно сидеть.
6. Расслабьте плечи, руки расслабленно положите на стол (или на клавиатуру с мышью), расслабьте пальцы.
7. Линия плеча должна располагаться прямо над линией бедер.
8. Предплечья можно положить на мягкие подлокотники на такой высоте, чтобы запястья располагались чуть ниже, чем локти.
9. У рук всегда должна быть опора, чтобы они не находились на весу. Руки должны удобно располагаться по сторонам.
10. Руки выпрямите более чем на половину (угол в локте должен быть больше 90 градусов).
11. Локти согнуты и находятся примерно в 3 см, от корпуса.
12. Клавиатуру поместите ниже локтей (по возможности) или на их уровне.
13. Голову держите прямо, по желанию — с небольшим наклоном вперед.

Внимание! Компьютерный зрительный синдром

С началом «эры компьютеризации» было отмечено специфическое зрительное утомление у детей и взрослых, работающих на компьютерах, получившее общее название «компьютерный зрительный синдром» (CVS — Computer Vision Syndrome). Зрительная система человека приспособленна для восприятия объектов в отраженном свете. При работе на компьютере часами у глаз не бывает необходимых фаз расслабления, глаза напрягаются, их работоспо-

собность снижается. Очень часты жалобы на затуманенное зрение, трудности при переносе взгляда с ближайших на дальние и с дальних на ближние предметы, кажущееся изменение окраски предметов, их двоение, неприятные ощущения в области глаз — чувство жжения, «песка», покраснение век, боли при движении глаз.

«Компьютерный зрительный синдром» обусловлен следующими особенностями работы за компьютером и погрешностями в этой работе:

- свечением и мерцанием монитора;
- постоянным переводом глаз с клавиатуры на монитор;
- использованием устаревшей техники;

Каковы основные симптомы данного расстройства? Это:

- быстрая утомляемость глаз;
- сухость, покраснение, резь в глазах;
- головная боль;
- болезненные ощущения в области спины, шеи, плеч;
- слезоотделение;
- подрагивание век.

Почему компьютерный зрительный синдром связан с детским возрастом? Дело в том, что именно дети достаточно много времени проводят за играми у компьютера. Выдерживая большие, длительные и высокие нагрузки, дети часто не обращают внимание на усталость глаз, даже если она уже наступила. К сожалению, повсеместно для дошкольников используются «взрослые» мониторы меньших размеров.

Предупредить переутомление и все негативные моменты занятий за компьютером все-таки можно, если соблюдать все гигиенические требования к процессу обучения за компьютером, ограничивать длительность занятий, проводить гимнастику для глаз (офтальмотренаж), правильно обустроить рабочее место, следить за правильной посадкой, использовать только качественные программы, способствующие возрасту ребенка.

Детские психологи утверждают, что для любого человека и в первую очередь для детей, условно время отдыха, проведенное за играми на компьютере, можно определить как его возраст полных лет, приравненный к минутам, увеличенный в два—три раза, причем время отдыха от компьютера должно быть в два—три раза больше времени, проведенного за компьютером. Например, если ребёнку 6 лет, то играть на компьютере ему желательно не более

12—18 минут с перерывом на один час, а также не играть перед сном.

Экран видеомонитора должен находится на уровне глаз или чуть ниже. На расстоянии не ближе 50 см. Ребенок, носящий очки, должен заниматься за компьютером в них. Недопустимо использование одного компьютера для одновременного занятия нескольких ребят.

Чтобы указанные нарушения здоровья не возникли, необходимо соблюдать гигиенические требования (см. ниже), а если симптомы нарушений здоровья, отклонения и заболевания уже возникли, необходимо срочно обратиться к врачу.

Профилактика нарушений зрения

Гимнастика для глаз не только обеспечивает улучшение кровоснабжения тканей глаза, повышает силу, эластичность и тонус глазных мышц и нервов, снимает переутомление зрительного аппарата, но и, совершенствуя координацию движений глаз, повышает способность зрительного восприятия и оценки объектов окружающего пространства, корректирует функциональные дефекты зрения.

Полезно!
Упражнения профилактики нарушений зрения при работе за компьютером

1. Плотно закройте глаза руками так, чтобы через них не проходил свет. Следите при этом за тем, чтобы посадка была удобной. Особое внимание — на спину и шею, они должны быть прямыми и расслабленными. Закрыв глаза, попытайтесь увидеть перед глазами абсолютно чёрный цвет. Скорее всего, постоянно будут возникать цветные полоски, ромбики и кляксы. Чем чернее будет цвет, тем лучше расслаблены глаза. Многие из людей со слабой близорукостью могут добиться полного восстановления зрения сразу после выполнения этого упражнения.

2. Закрыв глаза, глядя сквозь веки на солнце (или на яркую лампу), поворачивайте глаза вправо-влево, делая круговые движения. После окончания упражнения крепко сожмите веки на несколько секунд. Упражнение носит скорее не расслабляющий, а возбуждающий характер, поэтому после него рекомендуется делать упражнение № 1.

Комплекс упражнений для снижения утомления глаз

- Сидеть с закрытыми глазами, расслабив мышцы лица, 10—15 с.
- Выполнить движение глазными яблоками; 1 — вправо — вверх; влево — вверх; вправо — вниз; влево — вниз; 18—20 с.
- Закрыть глаза и выполнить самомассаж надбровных дуг и нижней части глазниц, делая пальцами легкие круговые поглаживающие движения от носа наружу 20—30 с. Затем посидеть спокойно с закрытыми глазами 10—15 с.
- Сидеть с закрытыми глазами. Не открывая глаз, круговыми движениями глазными яблоками, по 2—3 раза в каждую сторону.
- 1 — с напряжением закрыть (зажмурить) глаза. 2 — раскрыть глаза и посмотреть вдаль. Повторить 3—5 раз. Посидеть с закрытыми глазами 10—15 с.
- Сидеть в расслабленном состоянии с закрытыми глазами 10—15 с.
- Смотреть вдаль 2—3 с. 2 — перевести взгляд на кончик пальца, поставленного перед глазами на расстоянии 25—30 см, и смотреть на него 3—5 с. Повторить 10—12 раз.
- Крепко зажмурить глаза на 3—5 с, а затем открыть на 3—5 с. Повторить 6—8 раз.
- Закрыть глаза и выполнить круговые движения глазными яблоками вправо и влево 15—20 с.
- Закрыть глаза и выполнить круговые движения глазными яблоками вправо и влево 15—20 с.
- Закрыть глаза, подушечками трех пальцев каждой руки легко надавливать на верхнее веко 2—3 с. Затем снять пальцы с века и посидеть с закрытыми глазами 2—3 с. Повторить 3—4 раза.
- 15 колебательных движений глазами по горизонтали справа — налево, слева — направо.
- 15 колебательных движений глазами по вертикали вверх — вниз, вниз — вверх.
- 15 вращательных движений глазами слева — направо.
- 15 вращательных движений глазами справа — налево.
- 15 вращательных движений глазами в правую, затем в левую стороны — «восьмерка».

Комплекс упражнений по методу Г.А. Шичко

1. Пальминг

Центр ладони должен быть над центром глазного яблока.

Основание мизинца (и правой, и левой руки) — на переносице, как мостик очков. Ладошки на глазах должны лежать так, чтобы ни единой дырочки не было, чтобы глаза находились в кромешной тьме. Локти поставить на стол, сесть поудобнее. Спина прямая, голову не наклонять. Под ладошками темно. Можно представить себе приятную картину. В какое-то мгновение начнет казаться, что кто-то вас раскачивает, значит, пальминг можно заканчивать.

2. Вверх—вниз. Влево—вправо

Двигать глазами вверх — вниз, влево — вправо. Зажмурившись, снять напряжение, считая до десяти.

3. Круг

Представить себе большой круг. Обводить его глазами сначала по часовой стрелке, потом против часовой стрелки.

4. Квадрат

Предложить детям представить себе квадрат. Переводить взгляд из правого верхнего угла, в левый нижний, в левый верхний, в правый нижний. Еще раз одновременно посмотреть в углы воображаемого квадрата.

В ходе проведения урока, на переменах и после уроков детей надо стимулировать к периодическому выполнению упражнений, способствующих преодолению гиподинамии, напряжения, «зажатости» мышц, эмоциональному раскрепощению, т. е. к разминкам.

На эффективность проведения разминки влияет использование разных компонентов, которые помогут проводить комплекс живо, эмоционально, интересно. Музыкальное сопровождение комплекса упражнений останется в памяти воспитанников и будет способствовать наиболее яркому восприятию движений, помогающих восстановлению организма детей после занятий на компьютере.

Для занятий с дошкольниками рекомендуются двигательно-игровые упражнения с выраженным эмоциональным компонентом.

Изменение работоспособности и функционального состояния ребенка

Определенная последовательность режимных моментов занятия предусматривает динамику изменений функционального состояния организма ребенка и его работоспособности:

I период (врабатывания) совпадает с организационным моментом и характеризуется всплеском функциональных изменений, предшествующих началу работы (до 5—7 мин), несогласованностью действий, отвлеченностью внимания (действия педагога должны способствовать успешной адаптации школьников к учебной деятельности);

II период (оптимальной работоспособности) включает наиболее трудные фрагменты занятия (длительность активного внимания и работоспособности детей 15 минут с начала занятия);

III период (пониженной работоспособности — стадия компенсированного утомления) совпадает с моментом закрепления полученных знаний.

На сроки наступления и длительность каждого периода влияют различные факторы:

- возраст детей, их общий эмоциональный настрой;
- время суток и количество занятий;
- характер и длительность выполняемой работы, чередование различных видов учебной деятельности;
- уровень трудности учебного материала;
- статические и динамические компоненты занятия.

Все занятия должны включать физкультурные «минутки» (1—2 минуты) и физкультурные паузы (3—4 минуты) для повышения внимания, умственной работоспособности и эмоционального тонуса. Кроме того, они помогают уменьшить статическую нагрузку на позвоночник и предупредить нарушение осанки.

Физкультминутки на занятиях с детьми школьного и дошкольного возраста

Физкультурно-спортивные минутки представляю собой выполнение упражнений традиционной гимнастики под счет, где каждое упражнение рассчитано для определенной группы мышц (бег, прыжки, приседания, ходьба и т. д.):

- Основная стойка. Руки через стороны вверх, подняться на носки, подтянуться; вернуться в исходное положение (и.п.).
- Руки к плечам. Локти прижаты к туловищу. Вращение рук вперед, вращение рук назад.
- Ноги на ширине плеч, руки на поясе. Наклоны вперед, руки в стороны; вернуться в и.п.
- Присед на носках, руки на коленях. 3 прыжка на месте в приседе, выпрямиться.

- Основная стойка. Выпад правой ногой вперёд, руки вверх, в стороны; вернуться в и.п. То же левой ногой.
- Стойка ноги врозь, руки в стороны. Наклониться вперед, расслабить мышцы, уронить руки вниз и потрясти ими; вернуться в и.п.

Двигательно-речевые физкультурные минутки предполагают речевое сопровождение выполнения упражнений. Подготовка двигательно-речевых минуток развивает творческие способности самого педагога, способствует развитию интереса учеников к изучению того или иного учебного материала.

Комплексы физкультурных минуток подбираются в зависимости от вида занятия, его содержания. Упражнения должны быть разнообразны, так как однообразие снижает интерес к ним, а следовательно, их результативность.

На каждом занятии следует проводить по две физкультминутки. Темп медленный и средний.

В физкультурные минутки включают обычно не менее трех упражнений.

Первое — типа «подтягивания» — воздействует на позвоночник и грудную клетку (выпрямляющее), второе — для ног и третье — для туловища. Упражнения для рук отдельно не проводятся, их следует сочетать с другими упражнениями. В тех случаях, когда физкультминутка проводится на занятиях информатики, следует в сочетании с другими упражнениями проводить упражнения для пальцев рук.

Дети должны понимать значение физкультминуток и сознательно выполнять включенные в них упражнения. Педагог проводит с детьми краткую беседу, разъясняет значение упражнений и порядок проведения физкультминуток. В определенный момент, когда педагог сочтет необходимым провести физкультурную минутку, он объявляет: «Физкультурная минутка». По этому сигналу дети готовятся к выполнению упражнений.

Важно запомнить несколько «**золотых правил**» при работе за компьютером, которые помогут избежать неприятностей для здоровья и получить от занятий максимум удовлетворения.

Золотые правила при работе за компьютером

Правило первое: перед работой за компьютером обязательно сделай разминку.

Правило второе: когда работаешь, сиди расслабленно.

Правило третье: чаще меняй позу, делай перерывы в работе.

В среднем, раз в 10 минут рекомендуется отвлечься от работы, сделать 1—2 упражнения — простых и привычных. В том числе, из числа обозначенных выше.

Правило четвертое: пальцы должны быть легкими и расслабленными.

Очень важно не допустить перегрузку суставов кистей рук. Нервные окончания подушечек пальцев как бы разбиваются от постоянных ударов по клавишам, возникают онемение, слабость, в подушечках бегают мурашки. Это может привести к повреждению суставного и связочного аппарата кисти, а в дальнейшем заболевания кисти могут стать хроническими.

Правило пятое: закончил занятие — сделай разминку.

Цель проведения разминки — обеспечить восстановление после завершения занятий, когда значительную нагрузку испытывали органы зрения, опорно-двигательный аппарат, мышцы туловища, особенно спины, находящиеся в статическом состоянии мышцы кисти работающей руки.

Исходя из этого, для разминки составляют комплекс, включающий в себя 3—4 простых упражнения для больших групп мышц (ног, рук, плечевого пояса, туловища), активизирующие дыхание и кровообращение. Выполняются они в течение 1,5—2 минут.

Общеразвивающие, корригирующие и дыхательные упражнения должны быть детям хорошо знакомы. Выполнение комплексов упражнений с пособиями или дидактическим инвентарем повышает интерес к их выполнению, улучшает качество выполнения, способствует формированию правильной осанки.

Детям можно предложить упражнения с такими предметами и природными материалами, как флажки, кубики, ленточки, мячики, эспандеры, природный материал (шишки, желуди, орехи).

Упражнения выполняются сидя и стоя. Исходное положение для ног (обычно — стойка, ноги на ширине ступни параллельно) должно быть удобным, обеспечивая устойчивое положение и способствуя равномерному распределению тяжести тела.

Особенно важно обращать внимание детей на то, что, выполняя упражнения, включенные в комплекс разминки после занятий, нужно правильно сочетать движения с ритмом дыхания, не задерживая его. Чтобы научить детей правильно дышать при выполнении упражнений, предложите им при опускании рук вниз, при приседаниях, наклонах произносить звуки или слова. Напри-

мер, при наклоне вперед протяжно произнести звук «ш-ш-ш» — как сдувается лопнувший шарик и т. д.

Правило шестое: при работе на компьютере необходимо постоянно заботиться о зрении.

Проверочные вопросы к модулю 1

1. Какую опасность для здоровья человека представляет работа на компьютере?
2. Какое правильное положение тела при работе на компьютере?
3. Какие упражнения помогают предупредить нарушения осанки при работе на компьютере?
4. Как уберечь зрение при работе на компьютере?
5. Какие упражнения помогают уберечь зрение при работе на компьютере?
6. Какие требования предъявляются к помещению, в котором проходит работа на компьютере?
7. Какие требования предъявляются к воздушной среде помещения, в котором проходит работа на компьютере?
8. Чем опасно увлечение компьютерными играми?
9. Как правильно и без ущерба для здоровья пользоваться Интернетом?
10. Как эффективно отдыхать после работы на компьютере?
11. Какие возрастные особенности детей необходимо учитывать, допуская их к работе на компьютере?
12. Перечислите «золотые правила» при работе на компьютере.

Литература

1.Агабабян Н.В., Любимова С.В. Использование здоровьесберегающих технологий при проведении занятий по информатике с детьми. Тамбов, 2008.

2. Баловсяк Н. Компьютер и здоровье. СПб, 2008.

3. КиберМама. Ру: статьи для родителей — URL: http://www.cybermama.ru

4. Колосков А. Боль в руках — профессиональный недуг компьютерщиков // Физкультура и спорт. 2003. № 12.

5. Кучма В.Р. Теория и практика гигиены детей и подростков на рубеже тысячелетий. М., 2001.

6. Кудряшова Н. Наедине с компьютером // Физкультура и спорт. 2004. № 5.

7. Ковалько В.И. Здоровьесберегающие технологии: школьник и компьютер: 1—4 классы. М., 2007.

8. Поляков С.Д., Хрущев С.В., Корнеева И.Т. и др. Мониторинг и коррекция физического здоровья школьников: Методическое пособие. М., 2006.

9. Профилактика нарушений зрения при работе с компьютером: Методические рекомендации // Тамбовский областной ИПК. Тамбов, 2008.

10. Передерин В. Компьютерная болезнь // Будь здоров! 2004. № 4.

11. Окулова Е. Ребенок в «заэкранье» // Наука и жизнь. 2005. № 5.

12. Сидорова А. Влияние компьютерных игр на поведение подростков // Воспитание школьников. 2007. № 7.

13. Синельников Р. Д. Атлас анатомии человека. Т. I. М., 2006.

14. Смирнов Н.К. Здоровьесберегающие образовательные технологии и психология здоровья в школе. М., 2005.

Модуль 2
СОЦИАЛЬНЫЙ, ЭМОЦИОНАЛЬНЫЙ И ЛИЧНОСТНЫЙ АСПЕКТЫ ЗАНЯТИЙ ДЕТЕЙ НА КОМПЬЮТЕРЕ

Тема 2.1
РАЗВИТИЕ ИНТЕЛЛЕКТА И СТИЛИ ОБУЧЕНИЯ В ЦИФРОВОМ МИРЕ

Развитие детей в современном мире, в котором широко распространены информационные технологии, когда компьютер становится неотъемлемой частью жизни почти каждого человека, может быть нарушено неправильным использованием этих технологий. Между девятью и двенадцатью годами происходит всплеск развития предлобной части коры головного мозга, подготовка к взрослому поведению. Значительное количество времени, проводимое с банальной, жестокой или социально изолирующей компьютерной технологией и программами, искажает этот процесс. С другой стороны, правильное использование технологии в этом возрасте может способствовать развитию. Юные подростки должны совершить крупные эмоциональные скачки в развитии морального мышления: им особенно необходимы чувства социальной связности, целостные ощущения и опыт в области искусства и гуманитарных наук, хорошие модели системы ценностей и нравственные отношения. И хотя иногда поведе-

ние подростков предполагает обратное, им все еще требуются близкие и заботливые отношения с ответственными и отзывчивыми взрослыми. Не позволяйте компьютерной деятельности заменить это критическое — и подчас болезненное — обучение. Чувство изолированности может вызывать у юных подростков склонность к депрессии, заниженной самооценке и антисоциальному поведению.

Подросткам более старшего возраста требуется много жизненного опыта, но новые пути созревания нервной системы делают их более подготовленными к использованию новых технологий. Хотя созревание лобной доли заканчивается не раньше двадцати лет (возможно, даже тридцати или больше), это возраст, когда социально обоснованное использование компьютерного обучения (например, совместная работа со сверстниками над гипермедийным проектом или языком программирования) может очень многое предложить подросткам.

Эмоциональный и исполнительный аспекты развития мозга могут быть более других подвержены вредному воздействию компьютера. Давайте поближе рассмотрим две стороны эмоционального интеллекта и определим, как компьютерная техника и технология могут способствовать или вредить развитию.

Память

Предлобная и лимбическая части мозга связаны с навыками памяти. Один вид памяти, «оперативная память», действует, будто рабочий стол для удержания вещей, требующий моментального и непосредственного внимания. Как у рабочей поверхности, у оперативной памяти есть ограничения: одной из причин того, что пожилые люди забывают взять ключи от машины, если они думают о списке покупок, является то, что в стареющем мозгу оперативная память начинает ухудшаться.

Во время развития оперативная память постепенно возрастает в объеме и эффективности, и подростки учатся удерживать в уме достаточное количество альтернатив, чтобы проводить сравнения, понимать математическую задачу и делать записи на лекции. У детей, которые имеют в школе плохую успеваемость или связанные с учебой проблемы, часто бывают трудности с оперативной памятью, соответствующей их возрасту.

Каковы будут последствия для оперативной памяти человека, если дети проводят очень много времени, не отрываясь, играя в

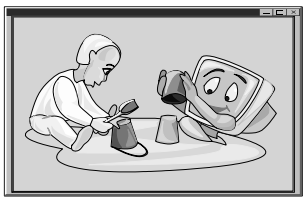
компьютерные игры, вместо использования своего потенциала памяти и воображения? Мы этого не знаем, но если компьютер станет основной деятельностью, то для тренировки растущего человеческого мозга может остаться очень мало места.

Приобретенные эмоции

Даже мозг взрослых иногда идет на поводу у их эмоций или импульса. У всех нас крупные дозы нейрохимических веществ и гормонов буквально «меняют ум» перед лицом страха, волнения или возбуждения. Мозжечковая миндалина, масса серого вещества в основании мозга, может бессознательно регистрировать эмоции страха; мозг и тело реагируют на угрозу, но человек не осознает своих собственных физических реакций. Дети даже более чувствительны, не всегда зная, что для них лучше, поэтому многие компьютерные игры могут оказывать более глубокое воздействие, чем осознает игрок. Повторяющиеся ощущения формируют устойчивые модели, которые, в конечном счете, могут оказаться губительными.

Например, мозг «прошит» производством ответной реакции на страх от внезапных громких шумов, а также соревнования или насилия, по мере того как миндалины, вырабатывающие адреналин, выбрасывают в систему «боевые» химические вещества (например, адреналин), учащая ритм сердцебиений и подготавливая мышцы. Эта гиперактивность адреналиновой реакции, которая сопровождает компьютерные игры, при повторяющихся действиях будет становиться укоренившейся физической привычкой. Измерения кровяного давления, сердечного ритма и даже колебаний мозга во время виртуального взаимодействия отражают те же значения, которые появляются в реальной жизненной ситуации, — только бессознательно.

Все последствия подобного постоянного предпочтения примитивных «боевых» реакций не известны, но они могут приучить мозг к потребности в острых ощущениях или хронически повлиять на кровяное давление. Некоторые люди в силу своих конституционных особенностей могут быть больше подвержены риску, чем другие. Как следует из некоторых исследований, если такие занятия на компьютере также приводят в бездействие предлобную часть коры головного

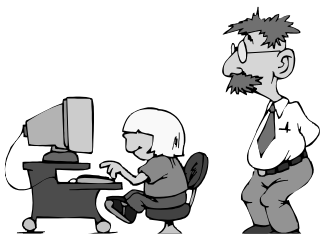


мозга, мы должны обратить на это особое внимание, так как ребенок с ленивой или неразвитой исполнительной системой может столкнуться со множеством проблем.

Влияние видеоигр на развитие интеллекта

Перейдем к рассмотрению влияния видеоигр, компьютерных игр на развитие интеллекта. Ролевая компьютерная игра — это простой и доступный способ моделирования другого мира или таких жизненных ситуаций, в которых человек никогда не был и не будет в реальности. Это простой способ пожить в другой жизни, где нет проблем, нет работы, на которую нужно ходить каждый день, нет хлопот по зарабатыванию денег на жизнь и т. д. В этом смысле может показаться, что ролевые компьютерные игры служат средством снятия стрессов, снижения уровня депрессии, т. е. своего рода терапевтическим методом. Однако использование ролевых игр в таком качестве под вопросом, хотя и представляется вполне возможным. На практике же люди обычно злоупотребляют этой возможностью ухода от реальности, теряют чувство меры, играя длительное время. Вследствие этого возникает опасность не временного, а полного отрешения от реальности, образование очень сильной психологической зависимости от компьютера.

Процесс благотворного влияния ролевых 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. 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. Один компьютерный аддикт, который увлекается в основном играми типа 3D-Action («трехмерное действие», вид «из глаз»), сказал: «Когда я встаю из-за компьютера и выхожу на улицу, мне не хватает оружия, которое есть у меня в игре. Без него я чувствую себя беззащитным, поэтому стараюсь побыстрее прийти домой и снова сесть играть».



Т.е. мы видим, что постоянный уход от реальности приводит к усилению этого стремления, к появлению устойчивой потребности бегства от реальности. Здесь мы находим аналогии с наркотиками и наркотической зависимостью: с каждой принятой дозой сила зависимости увеличивается; с каждым часом игры зависимость от нее усиливается, и вскоре для человека становится невозможным обходиться без компьютерной игры.

Родители часто спрашивают, что могут компьютерные игры сделать с интеллектом их детей. Могут ли они формировать полезные навыки, о которых мы еще не знаем? Конечно, это зависит от того, как их использовать. У игр могут быть какие-то подкупающие черты в зависимости от их содержания и от того, позволено ли им отбирать драгоценное время, отведенное для развития традиционных академических, социальных или личностных умений.

Игры могут развивать определенные формы наглядно-пространственного мышления, хотя мы пока еще не знаем, как эти умения будут соотноситься с требованиями школьного обучения.

Но мы знаем, что компьютерные игры захватывают, увлекают игрока и как таковые оказывают намного более сильное воздействие (плохое или хорошее), чем телевидение. Во-вторых, некоторые игры улучшают определенные визуально-пространственные навыки, например, навыки, необходимые для управления самолетом с приборной доски или точного нахождения цели. Однако понятие «визуально-пространственные навыки» охватывает обширный круг способностей, которые нам еще только предстоит определить и понять. Поисковая умственная установка игроков может оказаться особенно ценной для свободного решения задач, но в то же время возможно, что игры, допускающие наличие только одного верного решения, будут подавлять мышление.

Различные виды инструментальных средств с разными техническими требованиями развивают разные виды интеллекта. В случае с видеоиграми визуальное перспективное, графическое и пространственное представление может привести к новым открытиям или новым формам мышления, даже с использованием картинок для передачи звука.

В то же время, когда мы подключаем детей к все более реалистичным компьютерным программам, психологическое расстояние между ребенком и компьютером сокращается. В частности, если содержание плохо подобрано, как, например, в играх, где нужно

убить первым, чтобы выжить, такой опыт может негативно сказаться на поведении и мировоззрении ребенка («Это жестокий мир, где я никому не могу доверять!»), а также на его познавательных способностях.

Так означают ли положительные результаты некоторых исследований, что нам стоит засадить детей за компьютерные игры? Как и большая часть жизненного опыта, необходимого для развивающегося ума, компьютерные игры нужно «отпускать» только в разумных «дозах» и на соответствующем возрастном этапе — в такой обстановке, где взрослые могут всерьез контролировать использование компьютерных средств и программ. Так как программисты знают, как сделать игры столь психологически захватывающими (даже своего рода наркотиком), у них есть власть, которая выходит за рамки большинства детских игр. Невозможно сказать, какие игры и в каких количествах подходят для определенного ребенка, но что бы вы ни делали, убедитесь, что у ребенка формируется свое мировоззрение, свое собственное мнение.

Приведем некоторые советы о том, как выбрать игру для ребенка, как приучить его разумно тратить время на игру и т. д.

Советы по использованию видеоигр:

- Просмотрите и критически оцените содержание игры: наличие насилия, антисоциальных посылок, половых стереотипов и других существенных, на ваш взгляд, моментов.
- Обсудите содержание игры с ребенком; выскажите свою зрелую точку зрения по вышеперечисленным вопросам. Можно подтолкнуть ребенка к нахождению правильных ответов, не становясь при этом деспотом (например: «Ты бы действительно сделал что угодно, чтобы выиграть?»; «В жизни есть что-то более важное, чем победа?»).
- Домашнее задание и домашние обязанности должны стоять на первом месте.
- Разработайте в семье разумные ограничения времени, проводимого за видеоиграми.
- Не позволяйте кибермирам заменить реальное общение или физические ощущения.
- Внимательно следите за возникновением симптомов «отстраненного» поведения, которые могут указывать на редкие случаи возникновения приступов, вызванных видеоиграми.
- Ищите для ребенка игры, которые поощряют чтение и нахождение оригинальных решений вместо запоминания определенной последовательности действий.

Тема 2.2
ВЛИЯНИЕ КОМПЬЮТЕРА НА ВНИМАНИЕ, МОТИВАЦИЮ

Дети обладают разными способностями концентрировать внимание, не замечать посторонних раздражителей и обращать внимание на самое важное. У некоторых детей могут быть проблемы с вниманием, но опыт и ощущения, полученные во время критических периодов, также могут повлиять на эту систему. Программисты, создающие программное обеспечение, точно знают, как удержать внимание детей с помощью захватывающей и зрительно отвлекающей информации. Чтобы понять, насколько пагубно это может быть, рассмотрим, как развивается система внимания.

Первым формируется *выборочное внимание* — способность контролировать концентрацию мозга, критический период которого приходится на возраст *до семи лет*. У детей, чей ум кажется «неспокойным», которые без разбора реагируют на незначительные шумы, зрительные образы или мысли, еще не сформировано выборочное внимание. Другие могут казаться отрешенными или отвлеченными большую часть времени. Слишком сильная «бомбардировка» чувствительных центров может сместить установки нормальных уровней. Дети из семей, где происходит много скандалов и ссор или постоянно присутствуют громкие шумы от телевизора, учатся очень эффективно переставать обращать внимание на человеческие голоса. И действительно, учителя полагают, что повышенная реакция в виде «отключения» мозга, ослепленного СМИ, является одной из причин растущей эпидемии нарушений внимания.

Второй аспект внимания, называемый *организацией ответной реакции,* быстрее развивается в позднем детстве, в течение особенно чувствительного периода *с семи до девяти лет*. По мере того как мозг учится контролировать область своей концентрации, он должен научиться составлять план и действовать в соответствии с ним организованно и эффективно.

Многие детские компьютерные программы управляют избирательным вниманием и организацией ответной реакции ребенка. В реальном мире, выполняя проект, домашние обязанности, занимаясь хобби или выполняя долговременное домашнее задание, ребенок должен самостоятельно концентрироваться на значимых материалах и целях во время организации ка-

кой-либо ответной реакции. Он должен продумать последовательность действий и контролировать выполняемый проект. Когда ребенок «исследует» предварительно организованную компьютерную среду или выполняет действия согласно программе-симулятору со стратегиями, которые осуществляются методом проб и ошибок, формирования ответной реакции практически не требуется. С другой стороны, некоторые компьютерные действия требуют проявления самоорганизованности: например, сбор данных и затем составление электронных таблиц или баз данных, планирование и внедрение гипермедийной презентации.

Устойчивое внимание и способность оставаться сосредоточенным формируется, главным образом, начиная с *одиннадцати лет*. Теперь мозг может сосредоточиваться на проблеме, даже если материал не очень интересный. Устойчивое внимание, или сосредоточенность, пожалуй, больше других видов внимания ставится под угрозу в информационной культуре. Мы должны убедиться, что ребенок является инициатором концентрации внимания, что он не находится в зависимости от стимулов компьютерной программы.

Последний вопрос касается «разносторонних детей», чьи системы внимания позволяют им (или даже требуют от них) делать одновременно более одного действия. В гипермедийном мире этот тип интеллекта может стать все более адаптационным — пока он предоставляет достаточно внимания для выполнения какого-либо задания. Так как многие дети с нарушениями внимания могут оставаться «приклеенными» к экрану в течение длительного времени, их занятия на компьютере должны должным образом контролироваться, и некоторые исследователи уже изучают этот вопрос. Предполагается, что компьютеры со временем проложат новые пути развития полезных умственных навыков. Больше всего мы хотим, чтобы молодежь сама управляла своим умом, не была рассеянной и подверженной воздействию любого проходящего импульса или ощущения.

Если следить за ребенком, контролировать его время, проводимое за компьютером, использовать различные приемы, компьютер не будет негативно влиять на здоровье ребенка. Дадим несколько полезных рекомендаций по улучшению внимания у ребенка.

Практические рекомендации по улучшению внимания

1. В отношении маленьких детей обратите особое внимание на программное или мультимедийное обеспечение, которое чрезмерно воздействует на органы чувств: громкие, ошеломляющие шумы или движения, кричаще-яркие цветовые эффекты.

2. Убедитесь, что ваш ребенок получает достаточно физических упражнений. В школе настаивайте на необходимости физкультпауз во время длительных занятий за компьютером.

3. Не позволяйте времени, проводимому у экрана, нарушать режим сна: недостаток сна может привести к появлению симптомов, имитирующих синдром дефицита внимания.

4. Беспокойство или депрессия также приводят к снижению внимания. Настаивайте на занятиях с программами, подходящими ребенку по возрасту.

5. Наблюдайте за ребенком. Спросите себя:

- Кто управляет его вниманием?
- Кто формирует его ответы?
- Кто в действительности контролирует ситуацию? Если это не ребенок, выбросите программу.

6. Покажите ребенку, как рассказывать о своих планах и обсуждать стратегии перед запуском программы.

Использование компьютеров для повышения мотивации

Джулиан Роттер, который разработал в 1960-х г знаменитую шкалу «Точка контроля», позже писал, что «недостаток внутренней ключевой точки контроля переходит в потерянную связь между усилием и результатом; дети с плохой успеваемостью не научились справляться с трудной работой».

Мотивация — вероятно, самая значимая составляющая будущего успеха. Хорошо известно, что адекватные уровни трудности задачи и ее сложность могут стимулировать интерес; в свою очередь, мотивированный ребенок чувствует себя достаточно уверенно и готов приниматься за решение новых задач. Компьютеры могут повысить мотивацию, если они смогут индивидуализировать степень сложности урока и предложить подходящую ответную реакцию. Они не должны использовать задачу и ее сложность, чтобы занимать мозг банальными вещами, как это происходит во множестве игр, предположительно предназначенных для обучения. Когда компьютерные игры изымают из обучения человеческое общение и эмоциональный аспект, они, в конечном счете, снижают мотивацию.

Дети приходят в этот мир с достаточной для учебы мотивацией, но она зиждется на поддержке. Если ребенок узнает, что это просто здорово — стараться и добиваться успеха, он будет жаждать сделать большее. Если, с другой стороны, у него развивается чув-

ство, что его собственные усилия неэффективны или не требуются, он может потерять этот важный стимул к достижению успеха.

Когда со временем ребенок присоединится к рядам рабочей силы, ему понадобится достаточная мотивация для самостоятельной работы и частого переоснащения. Для выполнения этих требований психологи выделили два признака мотивации, которые должны появляться к восьми—девяти годам: 1) сильное чувство индивидуальности, иногда называемое «автономией» или «внутренней точкой контроля»; 2) достижение целей обучения, а не целей выполнения задания. Какое воздействие компьютеры оказывают на эти мотивационные характеристики?

Самостоятельные люди мотивированы, так как они чувствуют себя способными на многое и обладают внутренней мотивацией — они хотят лично прочувствовать радость успеха. Рассмотрим компьютер как один из факторов, влияющих на мотивацию.

Влияние компьютера на внимание, мотивацию.

1. *Позвольте ребенку быть активным участником, а не просто нажимать кнопки.* Предложенный ребенку разумный выбор в установленных пределах формирует схему внутреннего контроля. Хорошее программное обеспечение предлагает реальный выбор («Как бы вы закончили рассказ?»), а не просто банальные альтернативы («Выберите оружие для поражения пришельца»).

2. *Избегайте программ, которые предлагают «награду» за выполнение задания,* особенно простого. Подчеркивайте, что нужно получать удовольствие, используя свой ум для решения проблем, и радоваться успеху. Самый верный способ погасить мотивацию — это распределять внешние «награды» за то, что ребенок и так считает безумно интересным (например, создание рисунка, решение головоломки или решение математической задачки).

3. *Исправляющие ответы* развивают умственные навыки и уверенность, помогая ученикам понять ошибку и подсказывая, как ее исправить. Например, вместо простого ответа «правильно» или «неправильно», электронные репетиторы должны помогать ученикам понять, «почему» и «как» решить проблему. Если программа также может помочь ученику самому поразмышлять или оценить стратегии в перспективе, это даже лучше. Иначе ребенку понадобится живой помощник.

4. *Выработайте у ребенка понятие, что обучение является интересным занятием от природы, а не чем-то скучным, за что необходимо поощрять извне.* Такие поощрения, как предоставление проблем или заданий более высокого уровня сложности, когда ребенок справился с легкими, часто повышают степень мотивации. Программы такого типа могут повысить уверенность ученика в себе и помочь научиться брать на себя конструктивные интеллектуальные риски.

5. *Хорошо разработанные гипермедийные программы могут повышать мотивацию,* особенно у детей с более выраженными зрительными или кинестетическими стилями обучения.

6. *Проверьте, требует ли программа стандартных ответов* или она позволяет ребенку проявить оригинальное мышление. Можно ли придумать решение, которое не предвидели даже программисты? Всегда предпочтительнее программы, которые поощряют творческое мышление.

7. *Лишенный индивидуальности компьютер может помочь нерешительным ученикам* принимать рискованные решения в процессе обучения, так как здесь их никто не будет высмеивать или критиковать. Он может поощрять учеников более старшего возраста, которые уже чувствуют себя растерянными или сбитыми с толку прошлыми неудачами.

8. *Заставляйте ребенка брать на себя реальную ответственность.* Не позволяйте ребенку уверовать, что компьютер делает за него всю работу, или обвинять его в ошибках. Раннее и среднее детство закладывают важные основы для развития самостоятельности, а слишком много времени, проводимого за компьютером, может помешать этому, прежде чем родители осознают, что происходит.

Тема 2.3
НЕГАТИВНОЕ ВОЗДЕЙСТВИЕ КОМПЬЮТЕРА НА ПСИХИЧЕСКОЕ ЗДОРОВЬЕ ДЕТЕЙ

За последние два десятилетия собран большой объем данных негативных последствий информатизации и влияния компьютеризации, особенно на детей, их психологическое здоровье.

Однако это не единственный вариант такого — такого рода достаточно много. В психологических работах, посвященных последствиям компьютеризации, предметом исследования часто оказываются навыки, конкретные действия, отдельные психические

процессы. В то же время проблемам генерализации, глобальных личностных изменений уделяется еще недостаточно внимания. При этом вопросы, связанные с данной темой, изучаются в основном в теоретическом плане, экспериментальных исследований проведено крайне мало.

Применение информационных технологий при конкретных действиях или видах деятельности может оказывать влияние на разные виды деятельности и даже на всю личность в целом. Воздействие процессов информатизации на деятельность может происходить и прямо, через трансформацию и опосредование самой деятельности и появление новых ее видов, связанных с информационными технологиями, и косвенно, через многократное опосредование некомпьютеризированных видов деятельности. Такое косвенное многократное опосредование может происходить, например, при просмотре фильмов, созданных с помощью компьютерной графики. При этом компьютеризированная деятельность может оказывать воздействие на другие виды деятельности поразному. Характерно и то, что одни преобразования накладываются на другие, приводя и к нейтрализации психологических последствий информатизации, и к их увеличению.

Распространяющиеся глобальные преобразования психических явлений могут приводить к изменению всей мотивационно-личностной сферы субъекта, которое может носить и выраженный негативный характер. Примерами такого негативного изменения личности могут служить: увлечения компьютерными играми, Интернетом, программированием и информационными технологиями в целом (т.н. хакерство). Все эти виды увлечений при разной феноменологии имеют близкие психологические механизмы и особенности. Многие исследователи считают, «что механизм формирования игровой зависимости основан на частично неосознаваемых стремлениях, потребностях: уход от реальности и принятие роли». Эти механизмы работают независимо от сознания человека и характера мотивации игровой деятельности, включаясь сразу после знакомства человека с ролевыми компьютерными играми и начала более или менее регулярной игры в них. То есть независимо от того, чем руководствуется человек и что им движет, когда он первое время начинает играть в компьютерные игры, включаются механизмы формирования зависимости, и в дальнейшем та потребность, на которой основан превалирующий ме-

ханизм, принимает первостепенное значение в мотивации игровой деятельности.

Рассмотрим некоторые механизмы ухода от реальности.

Уход от реальности

Основой механизма ухода от реальности является потребность человека в «отстранении» от повседневных хлопот и проблем, своеобразная трансформация потребности в сохранении энергии. Мы употребляем термин «уход от реальности», а не «уход от социума», о котором упоминают некоторые авторы работ по сходной тематике. Дело в том, что мы имеем в виду не просто среду, общество, социум, а объективную реальность в целом. Уйти от социума можно посредством самых разнообразных способов, включая неролевые компьютерные игры. Однако уйти от реальности можно только лишь «погрузившись» в другую реальность — виртуальную.

Психологические аспекты механизма основаны на естественном стремлении человека избавиться от разного рода проблем и неприятностей, связанных с повседневной жизнью. Ролевая компьютерная игра — это простой и доступный способ моделирования другого мира или таких жизненных ситуаций, в которых человек никогда не был и не будет в реальности. В этом смысле может показаться, что ролевые компьютерные игры служат средством снятия стрессов, снижения уровня депрессии, т. е. своего рода терапевтическим методом. Однако использование ролевых игр в таком качестве под вопросом, хотя и представляется вполне возможным. На практике же люди обычно злоупотребляют этим способом ухода от реальности, теряют чувство меры, играя длительное время. Вследствие этого возникает опасность не временного, а полного отрешения от реальности, образование очень сильной психологической зависимости от компьютера.

Процесс благотворного влияния ролевых 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. Остальная часть пирамиды потребностей сдвинута в виртуальную

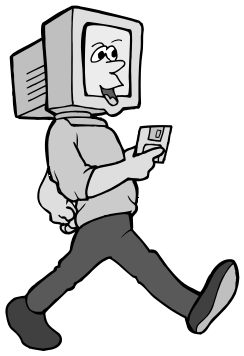
реальность и удовлетворяется там. Реальный мир начинает казаться чужим и полным опасностей, потому что человек не может в реальном мире делать все то, что ему дозволено в виртуальном.

В последнее время мы часто можем слышать новый термин «Синдром компьютерного стресса». У людей, которые целый день работают за компьютером, отмечаются нарушения памяти, бессонница, ухудшение зрения, головные боли, хроническая усталость, депрессивное состояние. У них могут возникнуть даже проблемы в общении с друзьями и близкими...

Можно говорить о двух сторонах в психологическом изучении взаимодействия человека и компьютера: с одной стороны, необходимо изучение вопроса о том, как усовершенствовать работу человека с компьютером и какие проблемы при этом возникают, а с другой стороны, важно исследовать, как изменяется сам человек, приспособившись к работе в новой знаковой среде. Изучение психологических последствий применения информационных технологий относится именно ко второму кругу психологических проблем в этой области.

Большое количество психологических исследований было проведено в рамках проблематики освоения человеком новых технологий. Так, были изучены феномены потребности в «общении» с компьютером при работе пользователя и особенности такого общения, например, потребность в антропоморфном интерфейсе и эмоционально окрашенной лексике, феномен персонификации компьютера, а также различные формы компьютерной тревожности. В более поздних работах на данную тему эти феномены были отнесены к проявлению тенденции субъекта к неосознаваемому уподоблению себя компьютеру, сравнению собственных интеллектуальных способностей и возможностей системы.

Вторая сторона взаимодействия человека с компьютером — проблема психологических последствий информатизации — заслуживает не меньше внимания. Указания на негативные последствия применения информационных технологий можно найти и в письме Министерства образования РФ «Об информационной культуре», в котором говорится об опасности аутизации детей и подростков в результате чрезмерного увлечения информационными технологиями.



Виртуальная деятельность может и напрямую влиять на психику ребенка, способствовать возникновению маниакальной зависи-

мости от Интернета или от игр. При сильном увлечении компьютерными играми ребенок склонен полностью посвящать себя игре, исключая любую иную деятельность, игра для него становится самоцелью. Компьютерные игры становятся мощнейшим дезадаптирующим фактором. Ребенок уже не может жить без них, не может самостоятельно справиться с патологическим влечением.

Можно выделить следующие признаки, характерные для игромани, как разновидности зависимого поведения:

- постоянная вовлеченность, увеличение времени, проводимого в ситуации игры;
- изменение круга интересов, постоянные мысли об игре, преобладание в воображении ситуаций, связанных с игровыми комбинациями;
- персонификация компьютера;
- появление «теории игры»;
- состояние психологического дискомфорта, раздражительности, беспокойства через короткие промежутки времени после игры с труднопреодолимым желанием возобновить игровую деятельность;
- увеличение частоты участия в игре;
- снижение способности сопротивляться соблазну; вытеснение прежних мотивов, нежелание учиться и вообще посещать школу и т. д.

Осознание важности данной проблемы ставит новые задачи перед педагогами, социальными работниками, психологами, руководителями учебных учреждений, медиками. Выше перечисленным специалистам необходимо реализовать действенную систему профилактики, сформировать личность ребенка, обладающую разносторонними интересами, умеющую успешно адаптироваться к социуму, преодолевать критические жизненные ситуации, уверенно взаимодействовать с окружающими людьми.

Эффективной моделью профилактики компьютерной зависимости может стать обучение социальноважным навыкам. Жизненными навыками обозначают способность к адаптивному и позитивному поведению, позволяющую индивиду эффективно удовлетворять свои потребности и решать возникающие проблемы. В частности, жизненные навыки — это комплекс физиологических возможностей и навыков межличностного взаимодействия, которые помогают людям принимать продуманные решения, урегулировать проблемы, конструктивно разрешать конфликты, критично и творчески мыслить, эффективно общаться, строить здоровые взаимоотношения и продуктивно управлять своей жизнью.

Хорошие результаты дает организация деятельности, альтернативной зависимому поведению. Данная форма работы основана на представлениях о том, что аномальные проявления формируются в случае дефицита позитивных моделей поведения (например, пребывание в Интернете может повышать самооценку или помогать вхождению в референтную группу). Альтернативными формами активности являются: познание (путешествия), испытание себя (походы в горы, спорт с риском), значимое общение, любовь, творчество, деятельность (в том числе профессиональная).

В семейном воспитании данная форма профилактики может быть реализована через вовлечение ребенка в различные виды активности — спорт, искусство, познание, формирование позитивных потребностей личности, устойчивых интересов, способности любить и быть любимым, умений найти себе занятие и выбрать привлекательную деятельность.

Эффективна профилактика, направленная на активизацию личностных ресурсов. Занятия спортом, творческое самовыражение, участие в группах общения и личностного роста, арттерапия — все это способствует раскрытию внутреннего потенциала, активизирует личностные ресурсы и обеспечивает устойчивость индивида к негативному влиянию виртуальной реальности.

В настоящее время в работе с ребенком с выраженной предрасположенностью к зависимому поведению часто используется *интегративный подход,* предполагающий комбинацию взаимодополняющих методов и приемов. Интегративный подход также определяет сочетание различных форм работы. Например, для подростка, склонного к компьютерной зависимости, может быть адекватной следующая схема психологической помощи: индивидуальная коррекция — семейное консультирование — групповая психотерапия.

Профилактика зависимого поведения — это работа с нарушенной социальной адаптацией, поэтому изменение деструктивного поведения возможно только через включение личности в поддерживающие и конструктивные социальные системы.

Приводят ли жестокие игры к агрессивному поведению?

С тех пор, как существуют компьютерные игры, содержащие элементы насилия, агрессии и т. п., в СМИ периодически появляются сообщения о трагедиях, разыгравшихся на почве фанатичного увлечения виртуальными играми. Более того, с определенной периодичностью власти различных стран предпринимают ограни-

чительные меры, касающиеся продажи, выпуска и распространения агрессивных электронных игр. Вот некоторые примеры подобных случаев.

Двое американских подростков протащили в школу самодельные гранаты и убили двенадцать одноклассников, учителя, ранили еще несколько человек. Потом и себя отправили в мир иной. При проведении расследования была обнаружена видеозапись, сделанная незадолго перед кровавым походом в школу. Один из «карателей» сказал, глядя в камеру, что задуманное ими будет «чем-то вроде стрелялки Doom».

Профессора психологии Крейг Андерсон и Карэн Дил утверждали: дети видят все больше жестокости в современном мире. Виноваты в этом телевидение, кино и компьютерные игры. В статье утверждалось, что существует связь между жестокостью компьютерных игр и агрессивным поведением подростков, что может привести к преступлениям и убийствам. В обращении к Сенату США К. Андерсон сказал: «Хотя в области исследования поведенческих особенностей есть много сложностей, одну простую и ясную вещь нужно знать всем: компьютерные игры увеличивают жестокость и насилие. Наше исследование показало: влияние на агрессивность поведения у жестоких компьютерных игр даже серьезнее, чем у жестоких телепередач и фильмов».

26 апреля 2002 года Роберт Штайнхойзер убил 17 и ранил 7 человек в гимназии имени Гуттенберга, город Эрфурт, Германия. Роберт плохо учился, не ладил с учителями. 14 из 17 убитых — учителя. При опросах свидетелей, в частности, выяснилось, что подросток играл в Counter-Strike. Авторитетная газета «Франкфуртер Альгемайне Цайтунг» вышла со статьей «Программы для бойни», в которой писалось: «убийца тренировался с помощью компьютерных игр». При этом в Германии ни в одном магазине вы не найдете, например, Quake III. Они запрещены законом.

Любопытна точка зрения отечественного эксперта В. Морозовой, заведующей детским психотерапевтическим отделением Тюменского Центра психического здоровья. Она полагает, что сами по себе компьютерные игры никакой опасности не представляют: «На настоящем этапе развития человечество пользуется виртуальными играми, и это нормально. Другое дело, сколько этому занятию времени посвящается. Вопрос не в том, играет ли ребенок на компьютере, а в том, есть ли у него в реальной жизни друзья, какие-то достижения. Компьютер — это мир фантазий. А для любого нормального человека, который чувствует себя успешным, реальность важнее и нужнее любой самой привлекательной иллю-

зии. Если у ребенка хорошие отношения с родителями, ему есть чем заняться, то ему уже не хочется лежать и смотреть телевизор. Но когда он ноет: “Что бы мне поделать... Не знаю, чем заняться...”, и вы, желая отвязаться, включаете ему мультик, для такого компьютерные игры в дальнейшем будут опасны».

Стресс при работе с компьютером. Способы его профилактики и коррекции

Деятельность в системах «человек — компьютер» связана с периодическим, иногда довольно длительным и интенсивным воздействием (или ожиданием воздействия) экстремальных значений профессиональных, социальных, экологических факторов, которое сопровождается негативными эмоциями, перенапряжением физических и психических функций, деструкцией деятельности. Наиболее характерным психическим состоянием, развивающимся под влиянием указанных факторов у человека, является психологический стресс. Развитие стресса в экстремальных условиях, связанных с компьютерной деятельностью, может быть связано также с возможностью, ожиданием, угрозой воздействия разнообразных раздражителей физико-химической, психологической (личностной), организационной и, прежде всего, профессиональной природы. На этом основании данное состояние можно считать типичной формой информационного стресса. С другой стороны, особенности механизмов регуляции этого психического состояния позволяют отнести его к категории психологического стресса.

Информационный стресс по своей природе является разновидностью профессионального (рабочего) стресса. Стресс может быть вызван факторами, связанными с эмоциональной перегрузкой человека при работе с компьютером. Факторы информационного стресса следующие.

Стресс может возникнуть в результате плохих физических условий, например, отклонений в температуре помещения, плохого освещения или чрезмерного шума. Неправильные соотношения между полномочиями и ответственностью, плохие каналы обмена информацией в организации и необоснованные требования сотрудников друг к другу тоже могут вызвать стресс. Идеальным будет такое положение, когда производительность находится на возможно более высоком уровне, а стресс — на возможно более низком. Чтобы достичь этого, необходимо научиться справляться со стрессом в самих себе.

Под воздействием стресса организм человека испытывает стрессовое напряжение. Рассмотрим различные состояния человека, которые могут сигнализировать о наличии в организме внутреннего напряжения. Сознательная оценка способна перевести эти сигналы из сферы эмоциональной (чувства) в сферу рациональную (разум) и тем самым ликвидировать нежелательное состояние.

Приведем признаки стрессового напряжения (по Шефферу):

- Невозможность сосредоточиться на чем-то.
- Слишком частые ошибки в работе.
- Ухудшается память.
- Слишком часто возникает чувство усталости.
- Очень быстрая речь.
- Мысли часто улетучиваются.
- Довольно часто появляются боли (голова, спина, область желудка).
- Повышенная возбудимость.
- Работа не доставляет прежней радости.
- Потеря чувства юмора.
- Резко возрастает количество выкуриваемых сигарет.
- Пристрастие к алкогольным напиткам.
- Постоянное ощущение недоедания.
- Пропадает аппетит, вообще потерян вкус к еде.
- Невозможность вовремя закончить работу.

Если мы обнаружили у себя признаки стрессового напряжения организма, то необходимо внимательно изучить его причины.

Каждый человек должен сам проводить анализ своего состояния и выявлять причины стрессового напряжения, возможно, характерные только для его организма (с точки зрения его личных ощущений). Предрасположенность к стрессовому напряжению можно определить также с помощью различных тестов.

Возникает вопрос — как человеческий организм может противостоять стрессу и управлять им? Рассмотрим возможные реакции организма на стресс и основные способы борьбы со стрессом: — релаксацию; — концентрацию; — ауторегуляцию дыхания. Как человеческий организм реагирует на стресс? Каковы возможные реакции организма человека на стресс?

1. *Неблагоприятные факторы (стрессоры),* к которым относится и работа с компьютером, вызывают реакцию стресса, т. е. стресс. Человек сознательно или подсознательно старается приспособиться к совершенно новой ситуации. Затем наступает выравнивание, или адаптация. Человек либо обретает равновесие в создавшейся

ситуации и стресс не дает никаких последствий, либо не адаптируется к ней — это так называемая маладаптация (плохая адаптация). Как следствие этого могут возникнуть различные психические или физические отклонения. Иными словами, стресс либо достаточно долго продолжается, либо возникает довольно часто. Причем частые стрессы способны привести к истощению адаптационной защитной системы организма, что, в свою очередь может стать причиной психосоматических заболеваний.

2. *Пассивность.* Она проявляется у человека, адаптационный резерв которого недостаточен и организм не способен противостоять стрессу. Возникает состояние беспомощности, безнадежности, депрессии. Но такая стрессовая реакция может быть преходящей. Две другие реакции активные и подчинены воле человека.

3. *Активная защита от стресса.* Человек меняет сферу деятельности и находит что-то более полезное и подходящее для достижения душевного равновесия, способствующее улучшению состояния здоровья (спорт, музыка, работа в саду или огороде, коллекционирование и т. п.).

4. *Активная релаксация (расслабление),* которая повышает природную адаптацию человеческого организма — как психическую, так и физическую. Эта реакция наиболее действенная. Попытаемся объяснить, что происходит в организме во время стресса. В нормальных условиях в ответ на стресс у человека возникает состояние тревоги, смятения, которое является автоматической подготовкой к активному действию: атакующему или защитному. Такая подготовка осуществляется в организме всегда, независимо от того, какой будет реакция на стресс — даже тогда, когда не происходит никакого физического действия. Импульс автоматической реакции может быть потенциально небезопасен и приводит организм в состояние высшей готовности. Сердце начинает биться учащенно, повышается кровяное давление, мышцы напрягаются. Вне зависимости от того, серьезна ли опасность (угроза жизни, физическое насилие) или не очень (словесное оскорбление), в организме возникает тревога и в ответ на нее — готовность противостоять.

Автоматическая реакция тревоги состоит из трех последовательных фаз (согласно теории Г. Селье): импульс—стресс—адаптация. Иными словами, если наступает стресс, то вскоре стрессовое состояние идет на убыль — человек так или иначе успокаивается. Если же адаптация нарушается (или вообще отсутствует), то возможно возникновение некоторых психосоматических заболеваний или расстройств. Следовательно, если человек хочет направить

свои усилия на сохранение здоровья, то на стрессовый импульс он должен осознанно отвечать релаксацией. С помощью этого вида активной защиты человек в состоянии вмешиваться в любую из трех фаз стресса. Тем самым он может помешать воздействию стрессового импульса, задержать его или (если стрессовая ситуация еще не наступила) ослабить стресс, предотвратив тем самым психосоматические нарушения в организме. Активизируя деятельность нервной системы, релаксация регулирует настроение и степень психического возбуждения, позволяет ослабить или сбросить вызванное стрессом психическое и мышечное напряжение. Так что же такое релаксация?

Релаксация — это метод, с помощью которого можно частично или полностью избавляться от физического или психического напряжения. Релаксация является очень полезным методом, поскольку овладеть ею довольно легко — для этого не требуется специального образования и даже природного дара. Но есть одно непременное условие — мотивация, т. е. каждому необходимо знать, для чего он хочет освоить релаксацию.

Методы релаксации нужно осваивать заранее, чтобы в критический момент можно было запросто противостоять раздражению и психической усталости. При регулярности занятий релаксационные упражнения постепенно станут привычкой, будут ассоциироваться с приятными впечатлениями, хотя для того, чтобы их освоить, необходимо упорство и терпение.

Средства снятия стресса

Снять отрицательные последствия стресса помогут:

1) разрядка эмоций: если нельзя проявить эмоции сразу, то можно это осуществить после события, в одиночестве. Выразите вслух или письменно (главное — чтобы чувства были облечены в слова) все, что вы хотите или хотели сказать;

2) плач: если хочется плакать — плачьте. Особенно это касается мужчин. В нашей культуре считается, что настоящий мужчина не должен плакать. Эту мысль внушают мальчикам с раннего детства, однако слезы приносят облегчение и снижают боль;

3) теплый душ: теплая вода действует расслабляюще на мышцы, тем самым снимая напряжение. Струи воды способствуют также релаксации (расслаблению) путем легкого массирующего действия;

4) физические упражнения;

5) релаксация через расслабление мышц;

6) переключение с неприятных событий на то, что приносит покой, радость, а иногда и просто позволяет не думать о том, что произошло. Это могут быть ваши увлечения, физическая активность, музыка;

7) дыхательные упражнения;

8) умение жить настоящим моментом, делать упор в ощущениях «на здесь и сейчас», а не проигрывать вновь и вновь прошлые события и ожидать плохого.

ПРАКТИЧЕСКАЯ ЧАСТЬ МОДУЛЯ 2

Игры и упражнения на снижение агрессии и ослабление негативных эмоций, возникших при работе с компьютером

«Брыкание»

Участники разбиваются на пары. Один лежит на полу, другой стоит напротив. По команде стоящий наваливается руками на согнутые в коленях ноги лежащего. Лежащий сопротивляется «нападению» и при этом громко кричит: «Нет!» Упражнение длится 2—3 минуты, затем пары меняются ролями.

Предостережение:

1. «Нападающий» давит только руками, а не телом.
2. Защищающийся брыкается только ногами, без помощи рук.

«Жужжа»

«Жужжа» сидит на стуле с полотенцем в руках. Все остальные бегают вокруг нее, строят рожицы, дразнят, дотрагиваются до нее, щекочут. «Жужжа» терпит, но когда ей все это надоедает, она вскакивает и начинает гоняться за «обидчиками» вокруг стула, стараясь отхлестать их полотенцем по спинам.

Замечание: взрослый следит за формой выражения «дразнилок». Они не должны быть обидными и болезненными.

Игры-освобождения, снимают напряженность и отрицательные эмоции:

УПРАЖНЕНИЕ 1. «ВИДЕОКАМЕРА»

Для того чтобы снять остро-эмоциональное напряжение, перед упражнением «Видеокамера» проведите кратковременное занятие на релаксацию (упражнение «Пресс»). Когда вы почувствуете не-

которое успокоение, попробуйте представить историю развития ваших конфликтных взаимоотношений в виде своеобразного сценария: когда вы впервые увидели человека, с которым у вас впоследствии возникли осложнения в отношениях, каково было ваше первое впечатление. Какие общие дела и занятия вас с ним объединяли, с какого момента отношения стали портиться, что вы делали и говорили, что он делал и говорил и т. п. Представьте также, что все эти ситуации в их реальной последовательности, вы снимаете на видеокамеру. При этом, следовательно, вы детально воспроизводите обстановку и условия каждой из этих ситуаций, других его участников, динамику развития конфликта и его апогей.

Время этого упражнения не ограничено. Вы сами почувствуете, когда начнете «отходить» от конфликтной ситуации и относиться к ней более спокойно.

УПРАЖНЕНИЕ 2. «МОЙ ВРАГ — МОЙ ДРУГ»

Это упражнение поможет вам принципиально (от отрицательного к положительному) изменить отношение к человеку, с которым у вас напряженные взаимоотношения.

Представьте себе своего обидчика. Возьмите лист бумаги и постарайтесь описать его внешний вид, т. е. составить словесный портрет. Старайтесь фиксировать прежде всего симпатичные детали его внешности. Прочитайте то, что написали. Если вы соскользнули на описание отрицательных внешних данных этого человека, вычеркните их. Затем на втором листе опишите качества характера своего партнера по конфликту. Опирайтесь на то, что в нем хорошего, не разрешайте себе описывать отрицательные свойства его личности. Если все же это произошло, при повторном чтении второй страницы вычеркните их.

На третьем листке опишите взаимодействие с этим человеком, опять-таки опираясь на позитивные моменты в его поведении. В связи с этим попробуйте проанализировать свое собственное поведение. Вы почувствуете, как что-то изменилось к лучшему в вашем отношении к этому человеку, а теперь на основе вашего измененного отношения выстройте другую линию вашего поведения: «Мне надо сделать все по-другому»...

УПРАЖНЕНИЕ 3. «ТЕЛЕПАТИЯ»

Группа участников разбивается на пары. Это можно сделать как на основе симпатий участников, так и на основе выборной системы (например, «Считалочка»).

В каждой паре участники садятся лицом друг к другу и договариваются, кто из них будет ведущим, а кто ведомым. Ведущий начинает «передавать» какой-нибудь образ или мысль: он сосредотачивается и в течение 4—5 минут внушает их своему партнеру, принимающему. Задача последнего — понять или почувствовать то, о чем думает ведущий.

Игра имеет несколько ограничений.

Нельзя использовать слова и вспомогательные средства: рисунок, жесты.

После того, как передача образа состоялась, принимающий рассказывает ведущему, что он понял.

УПРАЖНЕНИЕ 4. «ОТГАДАЙ»

Цель игры состоит в отгадывании человека, которого загадала группа. Все участники садятся в круг; по желанию выделяется ведущий. Он выходит из комнаты, а группа в его отсутствие выбирает человека из числа оставшихся в комнате. Когда ведущий заходит в комнату, он начинает спрашивать у каждого участника по отдельности: с каким, например, животным ассоциируется у вас этот человек, или с каким временем года, или с каким цветом.

Задача ведущего состоит в том, чтобы отгадать этого человека, причем после того, как он отгадает этого человека, он должен сказать, какая именно характеристика способствовала его выводу, и пояснить, почему.

УПРАЖНЕНИЕ 5. «ФОТОГРАФИЯ»

Возьмите в руки какую-нибудь фотографию незнакомого человека (знакомого кому-нибудь из членов группы), вглядитесь в его лицо, обратите внимание на его одежду, позу, постарайтесь определить род занятий, стиль жизни, придумайте биографию этого человека.

Потом обсудите это в группе.

Тест «Шкала оценки личностной тревожности (ЛТ)» (по Ч. Спилбергеру и Ю. Л. Ханину)

Оцените, как часто в последнее время вы испытываете каждое из приведенных в шкале состояний, с помощью баллов: 1 — почти никогда; 2 — иногда; 3 — часто; 4 — почти всегда.

1. Я испытываю удовольствие.
2. Я обычно быстро устаю.

3. Я легко могу заплакать.

4. Я хотел бы быть таким же счастливым, как другие.

5. Нередко я проигрываю из-за того, что недостаточно быстро принимаю решения.

6. Обычно я чувствую себя бодрым.

7. Я спокоен, хладнокровен и собран.

8. Ожидаемые трудности обычно очень тревожат меня.

9. Я слишком переживаю из-за пустяков.

10. Я вполне счастлив.

11. Я принимаю все слишком близко к сердцу.

12. Мне не хватает уверенности в себе.

13. Обычно я чувствую себя в безопасности.

14. Я стараюсь избегать критических ситуаций и трудностей.

15. У меня бывает хандра.

16. Я доволен.

17. Всякие пустяки отвлекают и волнуют меня.

18. Я так сильно переживаю свои разочарования, что потом долго не могу о них забыть.

19. Я уравновешенный человек.

20. Меня охватывает сильное беспокойство, когда я думаю о своих делах и заботах.

Данный текст является надежным и информативным способом самооценки уровня тревожности в данный момент (реактивной тревожности как состояния и личностной тревожности как устойчивой характеристики человека).

Сумма баллов 46 и более — высокая тревожность.

Под тревожностью понимается особое эмоциональное состояние, выражающееся в повышенной эмоциональной напряженности, сопровождающейся страхами, беспокойством и опасениями, которые препятствуют нормальной деятельности или общению с людьми. Тревожность — важное и довольно устойчивое персональное качество человека.

Под личностной тревожностью понимается индивидуальная черта, отражающая предрасположенность человека к эмоциональным отрицательным реакциям на различные жизненные ситуации, несущие в себе угрозу для его «Я» (самооценки, уровня притязаний, отношения к себе и т. п.). Личностная тревожность — это стабильная склонность реагировать на подобные социальные ситуации повышением тревоги и беспокойства.

Используемые литература и ресурсы

1. Беки Уорли. Интернет: реальные и мнимые угрозы/ Пер. с англ. — М.: КУДИЦ-ОБРАЗ, 2004. — 320 с.

2. Будунов Г.М. Компьютерные технологии в образовательной сфере: «за» и «против». — М.: АРКТИ, 2006. — 192 с.

3. Леонова А.Б., Чернышева О.Н. Психология труда и организационная психология: Современное состояние и перспективы: Хрестоматия. — М., 1995—386 с.

4. Митина Л.М., Митин Г.В., Анисимова О.А. Профессиональная деятельность и здоровье педагога. — М.: Академия, 2005. — 363 с.

5. Стресс жизни: Сборник./ Составители: Л. М. Попова, И. В. Соколов. (О. Грегор. Как противостоять стрессу. Г. Селье. Стресс без болезней.) — Спб, ТОО «Лейла», 1994. — 384 с.

6. Соболева А. Е., Емельянова Е.Н. Диагностика развития: внимания, памяти, мышления [Электрон. ресурс] «Психологический центр Адалин» — 2009. — Режим доступа: http://adalin.mospsy.ru/l_04_00/l040217.shtml

7. Интернет-СМИ «Ваш личный Интернет» [Электронный ресурс]. — URL: http://contentfiltering.ru/

Модуль 3
ИНФОРМАЦИОННАЯ ЭТИКА И ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 3.1
ИНФОРМАЦИОННАЯ ЭТИКА И ПРАВО

Информационная безопасность

Безопасность — это не только наука, которую надо изучать, не только мастерство, секреты которого надо постигать, но это и культура, которую надо воспитывать.

Безопасность является той сферой, с которой любой человек сталкивается на протяжении всей жизни, в той или иной форме, на том или ином участке профессиональной деятельности. Организация защиты не может быть уделом только профессионалов. Те, кто выступает в качестве пользователей, исполнителей, носителей защищаемых сведений, в отношении которых осуществляется физическая охрана, должны разбираться в вопросах безопасности не хуже тех, кто ее обеспечивает.[1]

В.Даль указывал, что безопасность есть отсутствие опасности, сохранность, надежность. По С.Ожегову, безопасность — это «состояние, при котором не угрожает опасность, есть защита от опасности». Сегодня появилось множество других определений безопасности, авторы которых исходят из разных критериев. Также полагают, что «безопасность есть состояние, тенденции развития (в том числе латентные) и условия жизнедеятельности социума, его структур, институтов и установлений, при которых обеспечивается сохранение их качественной определенности с объективно

обусловленными инновациями и свободное, соответствующее собственной природе и ею определяемое функционирование».

Начнем изучение этой темы с определений в терминологии информационной безопасности.

Информационная безопасность — механизм защиты, обеспечивающий:

- конфиденциальность: доступ к информации только авторизованных пользователей;
- целостность: достоверность и полноту информации и методов ее обработки;
- доступность: доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

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

Исходя из Доктрины информационной безопасности Российской Федерации, следует, что:

- Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.
- Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.
- Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Информационная безопасность достигается путем реализации соответствующего комплекса мероприятий по управлению инфор-

мационной безопасностью, которые могут быть представлены политиками, методами, процедурами, организационными структурами и функциями программного обеспечения.

Основными составляющими и аспектами информационной безопасности (которые не следует отождествлять с информационной безопасностью в целом) являются:

- Защита информации (в смысле охраны персональных данных);
- Компьютерная безопасность или безопасность данных;
- Защищенность информации и поддерживающей инфраструктуры от случайных и преднамеренных воздействий;
- Информационно-психологическая удовлетворенность потребностей граждан и защищенность от негативных информационно-психологических и информационно-технических воздействий.

При анализе проблематики, связанной с информационной безопасностью, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что ***информационная безопасность*** есть составная часть информационных технологий — области, развивающейся беспрецедентно высокими темпами. Здесь важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие жить в темпе технического прогресса.

Угрозы информационной безопасности

Под ***угрозой (threat)*** понимаются характеристики, свойства системы и окружающей среды, которые в соответствующих условиях могут вызвать появление опасного события.

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***.

Существует три разновидности угроз:

1. ***Угроза нарушения конфиденциальности*** заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Она имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в вычислительной системе или передаваемой от одной системы к

другой. Иногда, в связи с угрозой нарушения конфиденциальности, используется термин «утечка».

2. ***Угроза нарушения целостности,*** которая включает в себя любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую. Когда злоумышленники преднамеренно изменяют информацию, говорится, что целостность информации нарушена. Целостность также будет нарушена, если к несанкционированному изменению приводит случайная ошибка программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, санкционированным изменением является периодическая запланированная коррекция некоторой базы данных).

Целостность информации — это существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию). Чаще субъектов интересует обеспечение более широкого свойства — достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, т. е. ее неискаженности.

3. ***Угроза отказа служб,*** возникающая всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным — запрашиваемый ресурс никогда не будет получен, или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В этих случаях говорят, что ресурс исчерпан.

Доступность информации — свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.

Исходя из Доктрины информационной безопасности Российской Федерации, угрозы информационной безопасности Российской Федерации подразделяются на **следующие виды**:

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

- угрозы информационному обеспечению государственной политики Российской Федерации;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Уровни информационной безопасности

В деле обеспечения информационной безопасности успех может принести только комплексный подход. Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих **уровней:**

- законодательного;
- административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
- процедурного (меры безопасности, ориентированные на людей);
- программно-технического.

Направления защиты компьютерной информации

Основными целями и направлениями защиты данных провозглашаются предотвращение потери и искажения данных, несанкционированного использования, угрозы безопасности человеку и государству, защита прав субъектов информатизации. Защита должна производиться как в интересах держателей информации (собственников, владельцев, пользователей), так и людей, имеющих непосредственное отношение к ним (авторов, пациентов медицинских учреждений, коммерсантов и т. д.).

Основными направлениями защиты информации являются правовая, организационная и инженерно-техническая защиты информации как выразители комплексного подхода к обеспечению информационной безопасности.

Средствами защиты информации являются физические средства, аппаратные средства, программные средства и криптографические методы.

Электронно-цифровая подпись

Электронно-цифровые подписи обеспечивают защиту аутентификации и целостности электронных документов. Они могут использоваться при необходимости контроля с целью удостоверения, кто подписал электронный документ, а также при проверке, было ли содержание подписанного документа изменено. Рассмотрим подробнее нормативный документ об электронно-цифровой подписи. 10 января 2002 года Президентом был подписан закон «Об электронной цифровой подписи» номер 1-ФЗ (принят Государственной Думой 13 декабря 2001 года). Его роль поясняется в статье 1:

1. Целью настоящего Федерального закона является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

2. Действие настоящего Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях. Действие настоящего Федерального закона не распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

Закон вводит следующие основные понятия (Статья 3):

- ***Электронный документ*** — документ, в котором информация представлена в электронно-цифровой форме.

- ***Электронная цифровая подпись*** — реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.
- ***Владелец сертификата ключа подписи*** — физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).
- ***Средства электронной цифровой подписи*** — аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.
- ***Сертификат средств электронной цифровой подписи*** — документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.
- ***Закрытый ключ электронной цифровой подписи*** — уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.
- ***Открытый ключ электронной цифровой подписи*** — уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

- ***Сертификат ключа подписи*** — документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.
- ***Подтверждение подлинности электронной цифровой подписи в электронном документе*** — положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.
- ***Пользователь сертификата ключа подписи*** — физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи.
- ***Информационная система общего пользования*** — информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.
- ***Корпоративная информационная система*** — информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Согласно Закону, **электронная цифровая подпись в электронном документе равнозначна собственноручной подписи** в документе на бумажном носителе при одновременном соблюдении следующих **условий**:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;

- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Закон определяет **сведения**, которые должен содержать **сертификат ключа подписи**:

- уникальный регистрационный номер сертификата ключа подписи, даты начала и окончания срока действия сертификата ключа подписи, находящегося в реестре удостоверяющего центра;
- фамилия, имя и отчество владельца сертификата ключа подписи или псевдоним владельца. В случае использования псевдонима запись об этом вносится удостоверяющим центром в сертификат ключа подписи;
- открытый ключ электронной цифровой подписи;
- наименование средств электронной цифровой подписи, с которыми используется данный открытый ключ электронной цифровой подписи;
- наименование и местонахождение удостоверяющего центра, выдавшего сертификат ключа подписи;
- сведения об отношениях, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

Цифровые подписи могут применяться для любой формы документа, обрабатываемого электронным способом, например, при подписи электронных платежей, денежных переводов, контрактов и соглашений. Цифровые подписи могут быть реализованы при использовании криптографического метода, основывающегося на однозначно связанной паре ключей, где один ключ используется для создания подписи (секретный/личный ключ), а другой — для проверки подписи (открытый ключ). Необходимо с особой тщательностью обеспечивать конфиденциальность личного ключа, который следует хранить в секрете, так как любой имеющий к нему доступ может подписывать документы (платежи, контракты), тем самым фальсифицируя подпись владельца ключа. Кроме того, очень важна защита целостности открытого ключа, которая обеспечивается при использовании сертификата открытого ключа

Следует уделять внимание выбору типа и качеству используемого алгоритма подписи и длине ключей. Необходимо, чтобы криптографические ключи, используемые для цифровых подписей, отличались от тех, которые используются для шифрования. При использовании цифровых подписей необходимо учитывать требования всех действующих законодательств, определяющих условия, при которых цифровая подпись имеет юридическую силу.

Может потребоваться наличие специальных контрактов или других соглашений, чтобы поддерживать использование цифровых подписей в случаях, когда законодательство в отношении цифровых подписей недостаточно развито. Необходимо воспользоваться консультацией юриста в отношении законов и нормативных актов, которые могут быть применимыми в отношении предполагаемого использовании организацией цифровых подписей.

Тема 3.2
ОСНОВНЫЕ ЗАКОНЫ РОССИИ В ОБЛАСТИ КОМПЬЮТЕРНОГО ПРАВА

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Самое важное (и, вероятно, самое трудное) на законодательном уровне — создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом развития современного общества, в частности, информационных технологий. Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это может привести к снижению информационной безопасности.

Законодательство в сфере информационной безопасности в Российской Федерации начало развиваться только в начале девяностых годов прошлого столетия. Ряд законодательных актов довольно долго действовал в старых редакциях, часть документов утратили свою самостоятельность и были включены в Гражданский кодекс РФ. В рамках данной темы дается возможность проследить судьбу некоторых актуальных документов.

Одним из основных законов Российской Федерации является **Конституция**, принятая 12 декабря 1993 года.

В соответствии со статьей 24 Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 — право на знание достоверной информации о состоянии окружающей среды.

Статья 23 Конституции гарантирует право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, статья 29 — право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к *средствам защиты информации.*

В **Уголовном кодексе Российской Федерации** Глава 28 носит название «Преступления в сфере компьютерной информации», которая содержит три статьи:

- Статья 272. Неправомерный доступ к компьютерной информации;
- Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;
- Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Статья 272 УК РФ описывает ситуации неправомерного доступа к охраняемой законом компьютерной информации лицом или группами лиц, повлекшие за собой уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. Здесь описаны штрафные и уголовные меры за содеянное.

Статья 273 УК РФ знакомит с мерами пресечения действий в отношении создания программ для ЭВМ или внесения изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети и т. д.

Статья 138 УК РФ защищает конфиденциальность персональных данных и предусматривает наказание за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

В области информационной безопасности законы реально преломляются и работают через нормативные документы, подготовленные соответствующими ведомствами. В этой связи интересны руководящие документы, выпущенные Федеральной службой по

техническому и экспортному контролю Российской Федерации, определяющие требования к классам защищенности средств вычислительной техники и автоматизированных систем. Особенно можно выделить документ по межсетевым экранам, вводящий в официальную сферу один из самых современных классов защитных средств.

В информационном обществе нормативно-правовая база должна быть согласована с международной практикой. Особое внимание следует обратить на то, что желательно привести российские стандарты и сертификационные нормативы в соответствие с международным уровнем информационных технологий вообще и информационной безопасности в частности. Есть целый ряд оснований для того, чтобы это сделать. Одно из них — необходимость защищенного взаимодействия с зарубежными организациями и зарубежными филиалами российских компаний. Второе (более существенное) — доминирование аппаратно-программных продуктов зарубежного производства.

На законодательном уровне должен быть решен вопрос об отношении к таким изделиям. Здесь необходимо выделить два аспекта: независимость в области информационных технологий и информационную безопасность. Использование зарубежных продуктов в некоторых критически важных системах (в первую очередь, военных) может представлять угрозу национальной безопасности (в том числе информационной безопасности), поскольку нельзя исключить вероятности встраивания закладных элементов. В то же время, в подавляющем большинстве случаев потенциальные угрозы информационной безопасности носят исключительно внутренний характер. В таких условиях незаконность использования зарубежных разработок (ввиду сложностей с их сертификацией) при отсутствии отечественных аналогов затрудняет (или вообще делает невозможной) защиту информации без серьезных на то оснований.

Проблема сертификации аппаратно-программных продуктов зарубежного производства действительно сложна, однако, как показывает опыт европейских стран, решить ее можно. Сложившаяся в Европе система сертификации по требованиям информационной безопасности позволила оценить операционные системы, системы управления базами данных и другие разработки американских компаний. Вхождение России в эту систему и участие российских специалистов в сертификационных испытаниях в состоянии снять имеющееся противоречие между независимостью в области информационных технологий и информационной безопасностью без какого-либо ущерба для национальной безопасности.

Подводя итог, можно наметить следующие основные направления деятельности на законодательном уровне:

- разработка новых законов с учетом интересов всех категорий субъектов информационных отношений;
- обеспечение баланса созидательных и ограничительных (в первую очередь преследующих цель наказать виновных) законов;
- интеграция в мировое правовое пространство;
- учет современного состояния информационных технологий.

Предлагаем ознакомиться с некоторыми важными нормативно-правовыми документами в области информационных технологий и информационной безопасности более подробно.

Закон «О правовой охране программ для электронных вычислительных машин и баз данных» (от 23.09.1992г. № 3523—1). Закон «Об авторском праве и смежных правах» (от 09.07.1993г. № 5351—1 с последующим изменением и дополнением). Четвертая часть Гражданского кодекса РФ (от 18.12.2006г № 230-ФЗ). Федеральный закон «О введении в действие части четвертой Гражданского кодекса РФ» (от 18.12.2006г. № 231-ФЗ)

Два важных документа — Закон «О правовой охране программ для электронных вычислительных машин и баз данных» (от 23.09.1992 г. № 3523—1) и Закон «Об авторском праве и смежных правах» (от 09.07.1993г. № 5351—1) были введены в действие с целью регулирования правовых норм в отношении авторского права и охране программ для ЭВМ. Законы работали самостоятельно до 1 января 2008 года, в связи с введением в действие ФЗ «О введении в действие части четвертой гражданского кодекса РФ» (от 18.12.2006 г. № 231-ФЗ).

Четвертая часть гражданского кодекса РФ (от 18.12.2006 г. № 230-ФЗ), в текстах которого прописаны нормы правовой охраны программ для ЭВМ и баз данных, затрагивает права на результаты интеллектуальной деятельности и средства индивидуализации (к которым и относятся программы для ЭВМ и базы данных); авторское право; права, смежные с авторскими; патентное право и т. д. Отсюда можно узнать, как используется авторское право, как оно действует, какие есть ограничения в использовании авторских прав, как составляются договора и документы по авторскому праву и охране программ для ЭВМ, какие санкции могут применяться относительно неправомерного использования авторского права и т. д.

Закон «О государственной тайне» (от 21.07.1993г. № 5485—1 с последующим изменением и дополнением)

Рассмотрим подробнее закон «О государственной тайне» (от 21.07. 1993г. № 5485—1 с последующим изменением и дополнением). Закон регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в Законе «О государственной тайне» (с изменениями и дополнениями от 6 октября 1997 года). В нем ***гостайна*** определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Согласно данному Закону, ***средства защиты информации*** — это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну; средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Законодательство Российской Федерации о государственной тайне основывается на Конституции Российской Федерации, Законе Российской Федерации «О Безопасности» и включает в себя настоящий закон, а также положения других актов законодательства, регулирующих отношения, связанные с защитой государственной тайны.

Федеральный закон «О связи» (от 07.07.2003г. № 126-ФЗ с последующим изменением и дополнением)

Данный Федеральный закон впервые был принят в редакции от 16.02.1995г. за номером 15-ФЗ. В настоящее время имеют дело с редакцией от 07.07.2003г. № 126-ФЗ с последующим изменением и дополнением. Закон устанавливает правовые основы деятельности в области связи на территории Российской Федерации и на находящихся под юрисдикцией Российской Федерации территориях, определяет полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи.

Целями настоящего Федерального закона являются:

- создание условий для оказания услуг связи на всей территории Российской Федерации;

- содействие внедрению перспективных технологий и стандартов;
- защита интересов пользователей услугами связи и осуществляющих деятельность в области связи хозяйствующих субъектов;
- обеспечение эффективной и добросовестной конкуренции на рынке услуг связи;
- создание условий для развития российской инфраструктуры связи, обеспечения ее интеграции с международными сетями связи;
- обеспечение централизованного управления российским радиочастотным ресурсом, в том числе орбитально-частотным, и ресурсом нумерации;
- создание условий для обеспечения потребностей в связи для нужд государственного управления, обороны страны, безопасности государства и обеспечения правопорядка.

Статья 63 «Тайна связи» Главы 9 «Защита прав пользователей услугами связи» затрагивает проблему конфиденциальности передаваемой информации операторами связи.

Федеральный закон «Об информации, информационных технологиях и защите информации» (от 27.07.2006г. № 149-ФЗ)

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон «Об информации, информатизации и защите информации» от 20 февраля 1995 года номер 24-ФЗ (принят Государственной Думой 25 января 1995 года). В настоящее время его название видоизменено и звучит следующим образом — «Об информации, информационных технологиях и защите информации». Закон в обновленном виде действует с 27 июля 2006г. за номером 149-ФЗ.

Настоящий Федеральный закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

В нем даются основные определения и намечаются направления развития законодательства в данной области.

Приведем основные определения согласно статье 2:

1) **информация** — сведения (сообщения, данные) независимо от формы их представления;

2) **информационные технологии** — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) **информационная система** — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) **информационно-телекоммуникационная сеть** — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

5) **обладатель информации** — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

6) **доступ к информации** — возможность получения информации и ее использования;

7) **конфиденциальность информации** — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

8) **предоставление информации** — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9) **распространение информации** — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10) **электронное сообщение** — информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11) **документированная информация** — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию — или в установленных, законодательством Российской Федерации случаях ее материальный носитель;

12) **оператор информационной системы** — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации прописаны в статье 3. Правовое регулирование отношений, возни-

кающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

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

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Статья 16 носит название «Защита информации» и затрагивает следующие аспекты:

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

А Статья 17 предусматривает ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.

Исходя из того, что практические умения и навыки по указанным выше вопросам представляется целесообразным формировать в условиях, приближенных к жизненным, наиболее подходящим средством для этого являются ситуационные задачи, т. е. задачи, которые формулируются в виде описания жизненных ситуаций.

Для закрепления вышеизложенного материала предлагается проанализировать эти ситуации, выявить в них моменты правонарушений, обосновав выдержками из упомянутых выше нормативных документов, и по необходимости сделать выводы.

ПРАКТИЧЕСКАЯ ЧАСТЬ МОДУЛЯ 3

Ситуационные задачи

Задача 1. Гражданин Серебренников разработал в соавторстве с гражданином Семеновым информационно-справочную систему «Энциклопедия. Животные Крайнего Севера». Финансовую поддержку программных разработок вышеупомянутым гражданам оказал гражданин Андреев. Граждане Серебренников и Семенов 13.05.06 оформили свое авторство на данную информационную систему. В марте 2006 г. данный программный продукт был выпущен под авторством гражданина Андреева.

Имеет ли место в данной ситуации нарушение авторского права граждан Серебренникова и Семенова?

Решение. В данной ситуации есть нарушение авторского права граждан Серебренникова и Семенова, так как налицо факт выпуска программы для ЭВМ под чужим именем, что противоречит ст. 20 закона «О правовой охране программ для ЭВМ и баз данных».

Задача 2. Сотрудник Научно-исследовательского института приборостроения скопировал схемы, чертежи и графики прибора с целью продажи этой информации зарубежной фирме-производителю. Правомерно ли это?

Решение. Действия указанного лица в данной ситуации квалифицируются как противоправные на основании ст. 272, п. 2 УК РФ, так как очевиден факт превышения служебных полномочий и неправомерный доступ к компьютерной информации.

Задача 3. Определите, будет ли электронная подпись равнозначной собственноручной подписи, если подтверждена подлинность электронной цифровой подписи в электронном документе.

Решение. Электронная подпись не будет равнозначной собственноручной подписи только лишь при подтверждении подлинности электронной цифровой подписи в электронном документе, так как на основании ст. 4, п. 1 закона «Об электронной цифровой подписи» этого условия недостаточно.

Задача 4. Гражданин В. А. Мельников, автор и правообладатель электронной энциклопедии «Вокруг света», планировал сотрудничать с компанией «Видеотех», занимающейся тиражированием программных продуктов. Экземпляр электронной энциклопедии был передан в компанию для ознакомления. При этом договор о передаче компании «Видеотех» имущественных прав на программу составлен не был. В. А. Мельников предъявил судебный иск к компании «Видеотех», которая осуществила выпуск данного программного продукта. Какое решение вынесет суд и почему?

Решение. В данной ситуации суд вынесет решение в пользу гражданина Мельникова, так как имеет место быть нарушение его авторского права. Такое решение будет вынесено на основании соответствующей статьи ГК РФ, ввиду того, что налицо факт выпуска программы для ЭВМ без разрешения правообладателя.

Задача 5. Будет ли удовлетворен иск компании «Интермедиа» о привлечении к уголовной ответственности гражданина Р. И. Сизова и выплате им фирме денежной компенсации, если он внедрил в компьютерную сеть компании программу, действие которой заключается в уничтожении исполняемых файлов в какой-либо компьютерной сети? Функционирование данной программы принесло убытки различным организациям на общую сумму 670 000 рублей.

Решение. Судебный иск компании «Интермедиа» о привлечении к уголовной ответственности гражданина Р. И. Сизова и выплате им данной компании денежной компенсации будет удовлетворен, так как действия гражданина Р. И. Сизова в данной ситуации квалифицируются как противоправные на основании ст. 273, п. 2 УК РФ, ввиду того, что налицо распространение, вредоносных программ для ЭВМ, которое привело к тяжким последствиям.

Вопросы

1. Зачем нужны законодательные акты в информационной сфере?
2. Какой закон регламентирует права авторов программ и баз данных?
3. Какой закон регламентирует вопросы защиты информационных ресурсов? На какой закон вы сошлетесь, если вам будет нанесен ущерб путем использования информации, касающейся вашей частной жизни?
4. Какие действия уголовный кодекс классифицирует как преступления в компьютерной информационной сфере?
5. Появилось ли у вас желание после прочтения этого параграфа заняться производством и распространением компьютерных вирусов?
6. Какими положениями определяется правовой режим информационных ресурсов?

7. Какое условие является обязательным для включения информации в информационные ресурсы?
8. Когда документ приобретает юридическую силу?
9. Чем может подтверждаться юридическая сила документа, помимо собственноручной подписи?
10. Какими могут быть информационные ресурсы?
11. При каких условиях физические, юридические лица могут быть собственниками информационных ресурсов?
12. При каких условиях РФ и субъекты РФ могут быть собственниками информационных ресурсов?
13. При каких условиях государство имеет право выкупа документированной информации у физических и юридических лиц?
14. Имеет ли право собственник информационных ресурсов, принадлежащих к государственной тайне, распоряжаться ими? Если да, то на каких условиях?
15. Создает ли право собственности на средство обработки информации право собственности на информационные ресурсы?
16. Как подразделяются государственные информационные ресурсы?
17. По какой статье финансируется деятельность по формированию, накоплению и использованию информационных ресурсов?
18. Какие противоправные действия с компьютерной информацией со стороны граждан РФ отражены в УК РФ?
19. Какое наказание предусматривает УК РФ за несанкционированный доступ к компьютерной информации, совершенный гражданином РФ, в результате которого произошли уничтожение, блокирование, модификация и (или) копирование информации?
20. Какое наказание предусматривает УК РФ за несанкционированный доступ к компьютерной информации, совершенный гражданином РФ, в результате которого произошел сбой в работе ЭВМ, системы ЭВМ или их сети?
21. Какое наказание предусматривает УК РФ за несанкционированный доступ к компьютерной информации, совершенный по предварительному сговору граждан РФ, в результате которого произошли уничтожение, блокирование, модификация и (или) копирование информации?
22. Какое наказание предусматривает УК РФ за несанкционированный доступ к компьютерной информации, совершенный по предварительному сговору граждан РФ, в результате которого произошел сбой в работе ЭВМ, системы ЭВМ или их сети?

Используемые литература и ресурсы

1. Доктрина информационной безопасности Российской Федерации. (Утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г., № Пр-1895) [Электронный ресурс]. — URL: http://www.scrf.gov.ru/documents/5.html

2. Галатенко В.А. Основы информационной безопасности. Дистанционный курс (с)INTUIT.ru: Интернет-Университет Информационных Технологий — дистанционное образование, 2003—2008 [Электронный ресурс]. — URL: http://www.intuit.ru/

3. Партыка Т.Л., Попов И.И. Информационная безопасность: Учебное пособие, изд. 3-е, испр., доп. — М.: ФОРУМ, 2008. — 432 с.: ил. — (Профессиональное образование).

4. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. изд. 3-е — М.: Академический Проект — 2006. — 544 с.

5. Федеральный закон «Об электронной цифровой подписи» [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=72518;div=LAW;mb=LAW;opt=1;ts=AB736230098ADC672E8227AAFB97B9A8

6. Электронно-цифровая подпись — Что это такое? [Электронный ресурс]. — URL: http://www.digitalsign.ru/

7. Национальный стандарт РФ. ГОСТ Р ИСО/МЭК 17799—2005 Информационная технология. Практические правила управления информационной безопасностью. ISO/IEC 17799:2000 Information technology — Code of practice for information security management (IDT) Издание официальное. Москва. Стандартинформ, 2006.

8. ГОСТ Р 50922—2006 Государственный стандарт Российской Федерации. Защита информации. Основные термины и определения — сайт Федерального агентства по техническому регулированию и метрологии [Электронный ресурс]. — URL: http://protect.gost.ru/v.aspx?control=8&baseC=6&page=0&month=6&year=2008&search=50922&RegNum=1&DocOnPageCount=15&id=121129&pageK=E10BFA12-ED02-4212-8D58-3F1D91F314A0

9. Попов В.Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности. — М.: Финансы и статистика, 2005. — 176 с.

10. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учебное пособие — М.: Инфра-М, 2001. — 301 с.

11. Безбогов, А.А. Методы и средства защиты компьютерной информации: учебное пособие / А.А. Безбогов, А.В. Яковлев, В.Н. Шамкин. — Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006. — 196 с.

12. Федеральный закон «О введении в действие части четвертой Гражданского кодекса РФ» [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=83483;fld=134;dst=100052

13. Федеральный закон «О государственной тайне» [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=89782

14. Федеральный закон «О связи» [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=76690

15. Федеральный закон «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=61798

16. Федеральный закон «О безопасности» [Электронный ресурс]. — URL: http://base.garant.ru/10136200.htm

17. Уголовный кодекс Российской Федерации [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=93431

18. Конституция Российской Федерации [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=2875

19. Официальный сайт Федеральной службы по техническому и экспортному контролю [Электронный ресурс]. — URL: http://www.fstec.ru/_razd/_ispo.htm

20. Блохина Е.В. Лекция по теме: «Правовые основы использования Интернет-ресурсов. Авторские права. Поиск информации в Интернете» [Электронный ресурс]. — URL: http://festival.1september.ru/articles/412857/

21. Расторгуев С.П. Основы информационной безопасности // Информатика и образование. — 2007. — № 8.

22. Семенова З.В. Углубленное изучение темы «Защита данных в информационных системах» // Информатика и образование. — 2004. — № 1.

23. Черкашина И. Ф. Изучение темы «Информационная безопасность» в курсе информатики // Информатика и образование. — 2007. — № 9.

24. Бачило И.Л. О законодательстве в информационной сфере отношений. [Электронный ресурс]. — URL: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/a11ec0af30c1cc6ec3256c4f00312cfb

25. Ефимова Л. Проблемы правовой защиты детей от информации, приносящей вред их здоровью и развитию, распространяемой в сети Интернет [Электронный ресурс]. — URL: http://www.medialaw.ru/publications/zip/156—157/1.htm

Модуль 4
БЕЗОПАСНОСТЬ ДЕТЕЙ В ИНТЕРНЕТЕ

Тема 4.1
ОПАСНОСТИ, С КОТОРЫМИ ДЕТИ МОГУТ СТОЛКНУТЬСЯ В СЕТИ

Существует немало серьезных рисков, с которыми дети сталкиваются онлайн. Например, получая доступ к неподходящей информации на сайтах, посвященных преступной деятельности, или заходя на сайты, подвергающие риску их конфиденциальность. Хотя нашу озабоченность, в первую очередь, вызывает порнографический и иной контент сексуальной направленности, распространены другие виды неприемлемой доступной информации, которая может быть столь же вредной для наших детей.

Риск получения ребенком доступа к неподходящей информации включает в себя:

- доступ к информации, которая может быть не подходящей для детей вообще;
- сайты, посвященные продаже контрабандных товаров или другой незаконной деятельности;
- сайты, подвергающие риску конфиденциальность посетителей;
- сайты, размещающие изображения порнографического или иного неприемлемого сексуального контента, к которым дети могут легко получить доступ;
- сайты с рекламой табака и алкоголя;
- сайты, посвященные изготовлению взрывчатых веществ;

- сайты, пропагандирующие наркотики;
- сайты, пропагандирующие насилие и нетерпимость;
- сайты, публикующие дезинформацию;
- сайты, где продают оружие, наркотики, отравляющие вещества, алкоголь;
- сайты, позволяющие детям принимать участие в азартных играх онлайн;
- сайты, на которых могут собирать и продавать частную информацию о самих детях и их семье.

Для детей эти риски могут оказаться намного опаснее, чем, например, столкновение с откровенно сексуальным контентом. Кроме того, дети могут выдать информацию о кредитной карте родителя или ее пароль (а также любые другие пароли), выдать личную информацию о родителях и своей семье, купить вещи без Вашего ведома, нарушить авторские права, совершить компьютерные преступления, а также получить доступ, передать или стереть личные файлы. В некоторых случаях они, возможно, даже не знают, что совершают это. Наконец, существует риск атаки личного компьютера вирусами или хакерами.

Существует несколько типов рисков, с которыми дети могут встретиться, пользуясь Интернетом:

1. Дети могут получить доступ к неподходящей их возрасту информации. К ней относятся: порнография, дезинформация, обман, пропаганда ненависти, нетерпимости, насилия, жестокости.

2. Дети могут получить доступ к информации, совершить действия и купить товары, потенциально опасные для них. Существуют сайты, предлагающие инструкции по изготовлению взрывчатых веществ, продающие оружие, алкоголь, отравляющие и ядовитые вещества, наркотики, табачные изделия, а также сайты, предлагающие принять участие в азартных онлайн играх.

3. Дети могут быть подвержены притеснениям со стороны других пользователей сети (чаще всего злоумышленниками оказываются другие дети), которые грубо ведут себя в Интернете, пишут оскорбления и угрожают. Дети также могут загрузить себе на компьютеры вирусы или подвергнуться нападению хакеров.

4. Дети могут выдать важную и личную информацию, заполняя анкеты и принимая участие в онлайн конкурсах и, в результате, стать жертвой безответственных торговцев, использующих нечестные, запрещенные маркетинговые методы.

5. Дети могут стать жертвами обмана при покупке товаров через Интернет, а также выдать важную финансовую информацию

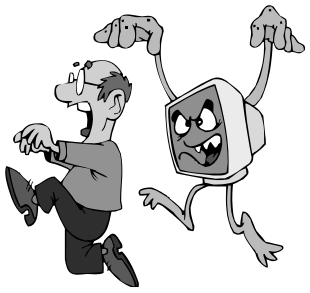
другим пользователям (например, номер кредитной карточки, пин-коды и пароли).

6. Дети могут стать жертвой киберманьяков, ищущих личной встречи с ребенком.

Тема 4.2
БЕЗОПАСНОЕ ОБЩЕНИЕ ДЕТЕЙ В ИНТЕРНЕТЕ

Если ребенок только начал общение с Интернетом, необходимо познакомить его с практическими способами безопасной работы в Интернете. Противостояние угрозам из Интернета включает два основных момента: во-первых, находясь в Интернете, не нужно терять бдительности и поддаваться ухищрениям злоумышленников, реализующих атаку на локальный компьютер. Во-вторых, необходимо построить защиту компьютера, которая будет включать в себя надежное приложение-антивирус, а также новейшую версию браузера для работы в Интернете с предварительно настроенными параметрами безопасности. Приведем некоторые рекомендации, которым необходимо следовать:

- Работу с электронной почтой лучше всего осуществлять с помощью почтовых сервисов Web-сайтов, которые выполняют антивирусную проверку почтовых сообщений.
- Можно использовать «временный» адрес электронной почты: спамеры эффективно собирают адреса электронной почты из всех видов источников, поэтому будет лучше использовать такие адреса, от которых вы готовы избавиться через 6 месяцев или через год, если объем спама станет большим.
- Запомните, что если вы используете почтовый клиент, никогда не конфигурируйте его на автоматическое открытие почтовых вложений. Любое послание от любого лица может содержать вложение самого опасного характера, поскольку его может послать кто угодно, в том числе вирус, заразивший компьютер отправителя.



- Обычно предпочтительнее выступать на форумах с модераторами — такими, где определенному человеку (именуемому «модератор») поручено следить за поведением уча-

стников и реагировать на плохое поведение и появление плохих личностей.

- Знайте, что специфика общения в Интернете такова, что она имеет тенденцию притягивать негатив. Будьте очень рассудительны в том, как вы описываете вещи, следите за языком, который может непреднамеренно передавать враждебность. Поддержание собственной безопасности в Интернете означает защиту самого себя от непреднамеренного провоцирования ссор и злой воли.
- Используйте в письмах шаблонные приветствия и благодарности, которые вставляются в начало или конец каждого послания. Ведь электронное послание лишь создается в сети — прочитает его все равно живой человек.
- Непосредственно перед отправкой специалисты советуют всегда производить контрольное прочтение. Таким образом можно убедиться, что приложены все файлы, а в сообщении все же написано то, что запланировано.
- Следите за поведением своего компьютера, когда посещаете Web-сайты. Если компьютер начинает проявлять подозрительную активность или процессор по непонятным причинам начнет перегружаться, проверьте с помощью диспетчера задач, что у вас запущено. Настораживать должны непонятные сообщения, некорректное и нелогичное поведение браузера и т. п. В крайнем случае, прервите соединение.

В снтернете также широко распространены службы для мгновенного обмена сообщениями и онлайн-общения (Windows Live Messenger, ICQ, IRC, чаты). Эти службы также могут таить в себе опасности при их использовании детьми, поэтому необходимо придерживаться некоторых правил.

Общение с помощью IRC (ретранслируемый Интернет-чат)

С помощью IRC (система диалогового общения по Интернету) в Интернете можно проводить беседы в режиме реального времени. Эта система предоставляет более широкий выбор возможностей, чем простой чат. Для подключения к необходимым каналам

(дискуссионным группам или комнатам) необходима отдельная программа — клиент IRC. С помощью IRC можно одновременно общаться на нескольких каналах, а также вести личные беседы между двумя людьми. В IRC применяются те же правила безопасного использования, что и для чатов.

Мгновенный обмен сообщениями (Windows Live Messenger, ICQ и т. п.)

Так же, как и чаты, программы мгновенного обмена сообщениями позволяют общаться в режиме реального времени. Разница заключается в том, что пользователь может выбирать человека, с которым он хочет пообщаться. В программе отображаются те друзья, которые в настоящее время находятся в Интернете. Для участия в личной беседе можно пригласить одного или нескольких друзей. Кроме того, можно обмениваться файлами, например, фотографиями, музыкальными файлами или видеоклипами, играть в игры или совершать голосовые или видеовызовы.

Технология программ мгновенного обмена сообщениями подвержена тем же рискам, что и электронная почта с чатом. Пользователь может открыть вложение или ссылку, содержащую вирус, шпионскую программу или непригодный для детей материал. Общение в Интернете с человеком, которого вы знаете в жизни, гораздо безопаснее. Общение с помощью программ мгновенного обмена сообщениями всегда является личным, и пользователь может контролировать не только то, с кем и как он разговаривает, но и время разговора.

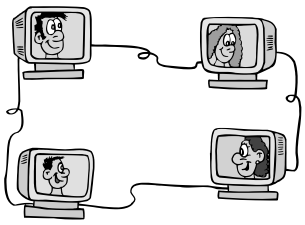
Общение в чатах

Для общения в Интернете также используют чаты. Чатом называется открытая дискуссионная группа в Интернете, в которой можно общаться с другими людьми в режиме реального времени, используя псевдоним. Чатам и группам чатов часто присваиваются названия на основе темы или возрастной группы. В обсуждении может участвовать множество пользователей, но также возможно личное общение между двумя пользователями. Общение в чатах предполагает собственный язык, этикет и даже культуру. Родителям было бы полезно знать о таких протоколах чатов. Рекомендуется выяснить это у своего ребенка.

Что такое безопасный чат?

Человек, с которым происходит общение, в значительной степени определяет, насколько безопасной и приятной для вас является атмосфера в чате. Как правило, степень безопасности чата, в котором общается ребенок, можно определить по трем основным вопросам. Иногда в чатах работают добровольные модераторы, которые предотвращают случаи неуместного общения и могут заблокировать доступ в чат для хулиганов и других нарушителей порядка. Если контроль не осуществляется, в чате по крайней мере должна иметься кнопка для связи с администратором. Для детей предпочтительны контролируемые чаты; уровень безопасности также повышается, если беседы сохраняются.

Инструкции по безопасному общению в чатах



Дети, которые общаются в чатах, должны знать, как делать это безопасным образом. Каждый должен помнить о следующих внутренних правилах чата.

1. Не доверяйте никому вашу личную информацию.
2. Сообщайте администратору чата о проявлениях оскорбительного поведения участников.
3. Если вам неприятно находиться в чате, покиньте его.
4. Если вам что-то не понравилось, обязательно расскажите об этом родителям.
5. Будьте тактичны по отношению к другим людям в чате.

Личная беседа

При знакомстве с новым человеком в интерактивной дискуссионной группе, возможно, захочется перейти от общения в общественном чате к более личной беседе с глазу на глаз. Например, можно начать беседу в общей комнате чата, а затем перейти к общению с помощью программы мгновенного обмена сообщениями или переписке по электронной почте. При использовании этих средств можно по-прежнему обеспечить защиту своей личности путем использования псевдонима (например, псевдоним01@домен.ru). Кроме того, проще предоставить такой тип адреса на слу-

чай, если новым контактом окажется человек, с которым необходимо будет прекратить общение. Рекомендуется наставить детей, чтобы они отказывались от участия в личных интерактивных беседах с людьми, которых они не знают в жизни.

Встреча с собеседниками из Интернета

Если ребенок общается в Интернете с новым человеком, возможно, ему/ей захочется лично встретиться с этим другом. Даже если дружба через Интернет поддерживалась в течение некоторого времени, эту встречу стоит воспринимать с осторожностью. Несмотря на то, что большинство встреч друзей по Интернету являются веселыми и безопасными мероприятиями, к сожалению, иногда они могут оставить неприятные впечатления. К счастью, случаи подобного рода крайне редки. Если встреча запланирована, настоятельно рекомендуется сопровождение ребенка родителем или другим взрослым, которому ребенок доверяет, а также проведение встречи в общественном месте.

Интернет-этика

Если вы хотите, чтобы дети стали ответственными пользователями, объясните им фундаментальные правила поведения в сети:

- Узнайте правила прежде, чем что-нибудь сказать или сделать. Некоторые чаты и форумы имеют специальные правила, поясняющие, что Вы можете и не имеете права говорить или делать. Так как некоторые люди критически относятся к тем, кто нарушает правила, знание правил может избавить вас и вашего ребенка от ненужного дискомфорта.
- Думайте прежде, чем что-либо напечатать. Удостоверьтесь, что вы говорите приемлемые вещи, которые не приведут к разгоревшемуся конфликту. Единственное, в чем вы можете не сомневаться, — это в том, что все, сказанное вами в Интернете, может вернуться и неотступно преследовать вас.

- Не относитесь критически к другим, особенно к новичкам, даже если они нарушают правила. Если вы должны помочь кому-то или испра-

вить кого-то, сделайте это по электронной почте, а не на общественном форуме (например, в чате). Помните, что и вы когда-то были новичком.

- Не тратьте время других пользователей впустую. Не посылайте цепочку электронных писем, не передавайте киберслухи, не разыгрывайте других, не рассылайте спам.
- Защищайте личную жизнь и личную информацию других пользователей. Не публикуйте в онлайне чей-либо адрес электронной почты без разрешения владельца. Вместо этого можно использовать опцию «Отправить по электронной почте». Не используйте без разрешения чужой пароль.
- Не присваивайте вещи, не платя за них (в основном это касается условно-бесплатного программного обеспечения).

Как не следует вести себя в сети

- Печатать ЗАГЛАВНЫМИ БУКВАМИ, что может рассматриваться как крик, провоцирующий спор или конфликт.
- Размещать ложную информацию или грубые высказывания о другом человеке.
- Отправлять большие вложенные файлы, не спросив разрешения у получателя.
- Обращаться к другим в чате по их настоящему имени.
- Рассылать электронную почту рекламного содержания людям, которых Вы не знаете (что является разновидностью спама).
- Отклоняться от темы разговора на форуме.
- Не дожидаться своей очереди или не следовать правилам чата или форума.

Безопасность работы в форумах

При работе в различного рода форумах в Интернете необходимо соблюдать все те же самые правила защиты, исходя из того, что вы находитесь на потенциально опасном ресурсе. Как и на любом другом потенциально опасном ресурсе, не рекомендуется сообщать о себе любые персональные данные.

Практический совет:

Разделите форумы, которые вы посещаете, минимум на две категории: доверенные и недоверенные. Вы можете использовать

для каждой из этих групп одно и то же имя пользователя и пароль для простоты запоминания.

Если вы создаете свой форум, то необходимо его защитить максимально доступными средствами от злоумышленников. Одно из самых важных правил — это аутентификация на форуме. При аутентификации оставлять сообщения на форуме смогут только зарегистрированные пользователи. Это хороший способ защиты, но недостаточный. Также необходимо включать премодерацию на сайте, в результате которой сообщения предварительно просматриваются владельцем (администратором) форума и только после подтверждения печатаются на форуме.

Тема 4.3
ФЕНОМЕН «ИНТЕРНЕТ-ЗАВИСИМОСТИ». ПРОФИЛАКТИКА ИНТЕРНЕТ-ЗАВИСИМОСТИ У УЧАЩИХСЯ

Интернет-зависимость психологи сравнивают с любой другой формой зависимости. Замените слово «компьютер» словами «наркотические вещества» или «алкоголь» — и вы поймете, что Интернет-одержимость вписывается в рамки классического определения зависимости. Она предлагает способ убежать от реальности, приятные чувства и альтернативную реальность, которая маскирует депрессию или беспокойство. Она также может вызвать изменения в нормальном функционировании мозга, стимулируя центры удовольствий.

Социальные контакты в Интернете представляют большую опасность, чем телевидение, так как предлагают общение с другими людьми. Притворяясь новыми личностями, люди могут начать верить, что их любят и заботятся о них за их новые обличия. Людям нужны друзья, они испытывают потребность принадлежности. Без подобных отношений они могут испытывать серьезные личные и социальные проблемы. Однако способность находить общий язык с людьми вне круга семьи должна воспитываться. Помимо того, что искусственные кибермиры предлагают легкую альтернативу, они являются также соблазнительной заменой, особенно для юных подростков, чья застенчивость может осложнить их социальные отношения.

Интернет захватывает ребенка целиком, не оставляя ему ни времени, ни сил на другие виды деятельности, на упорядочивание жизни собственной становящейся личности.

В настоящее время интенсивно обсуждается феномен «зависимости от Интернета», или «Интернет-аддикции» (Internet Addiction Disorder, или IAD). Исследователи исходят из возможности развития зависимости (аддикции) не только от вводимых в организм материальных сущностей, но и от производимых субъектом действий и сопровождающих их эмоций. Эта зависимость возникает посредством общения через Интернет, образуется благодаря его свойствам и характеристикам — тому, чего нет в других формах коммуникаций. Симптоматика зависимости от Интернета не всегда отделена от симптоматики «технологической зависимости» или, например, «зависимости от компьютеров», поскольку любое увлечение человека в крайней свой форме дает определенные основания говорить об аддикции.

Мы рассматривали такой аспект IAD, как общение с помощью Интернета (ведь общение в Интернете обладает неповторимыми свойствами). Оно полностью анонимно, демократично, доступно и массово. Это чрезвычайно привлекательно. Что может приводить к Интернет-зависимости в таких условиях — отсутствие навыков коммуникативной компетентности при общении оффлайн, «яркая» индивидуальность, ограниченные возможности для общения (инвалидность, например). Дети ждут очередного сеанса связи, чтобы снова поговорить с «друзьями» из Интернета. Что их привлекает в этом? Таким образом они удовлетворяют потребности, которые невозможно реализовать вне Интернета. Однако отсутствие клинических исследований, посвященных феномену Интернет-зависимости, некачественные опросники и анкеты по этому вопросу не позволяют говорить о заболевании, а вот заявлять о таком феномене, исследовать его и оказывать психологическую помощь подверженным ему людям — вполне актуально. Приведем поведенческие характеристики, которые могут быть отнесены к этому синдрому:

- экономический аспект: неспособность и нежелание отвлечься даже на короткое время от работы в Интернете; досада и раздражение, возникающие при вынужденных отвлечениях, и навязчивые размышления об Интернете в такие периоды; стремление проводить за работой в Интернете все увеличивающиеся отрезки времени и неспособность спланировать время окончания конкретного сеанса работы; побуждение

тратить на Интернет все больше денег, не останавливаясь перед влезанием в долги;

- межличностный аспект: готовность лгать друзьям и членам семьи, преуменьшая длительность и частоту работы в Интернете, способность и склонность забывать при работе в Интернете о домашних делах и учебе, важных личных встречах, пренебрегая занятиями; стремление и способность освободиться на время работы в Интернете от ранее возникнувших чувств вины или беспомощности, от состояний тревоги или депрессии, обретение ощущения эмоционального подъема и своеобразной эйфории; нежелание принимать критику подобного рода образа жизни; готовность мириться с потерей друзей и круга общения из-за поглощенности работой в Интернете;
- аспект здоровья: резкое сокращение длительности сна, избегание физической активности, пренебрежение личной гигиеной, постоянное забывание о еде;
- за проявлениями зависимости от Интернета нередко скрываются другие аддикции либо психические отклонения;
- расширение симптоматики, преувеличение количества потенциальных пациентов, шумиха в прессе удобны на данный момент специалистам по психическому здоровью и исследователям этого феномена.

Феномен зависимости от Интернета постоянно изменяется вместе со стремительным развитием Интернета и заслуживает досконального изучения. Такой феномен может проявить себя в школе, где появился Интернет. В таком случае школьная психологическая служба должна быть готова заранее, то есть мы считаем, что необходимы профилактические меры по предупреждению Интернет-зависимости.

О профилактике Интернет-зависимости

Существует «группа риска» среди учащихся, которые могут быть подвержены «Интернет-зависимости». Они интровертированы, необщительны или не имеют коммуникативных навыков, умны. Их легко отличить по поведению: они погружены в себя, много фантазируют, держатся в стороне от одноклассников, иногда не успевают по предметам.

В результате дети, обладающие индивидуальной внутрипсихологической способностью или умением преодолевать стрессовые ситуации, трансформировать их в различного рода поисковую ак-

тивность, значительно более устойчивы ко всякого рода аддикциям. Профилактическая программа направлена не только на эту группу, но и на всех учащихся школы, она универсальна.

Психиатр Иван Голдберг, создатель интерактивной группы поддержки Интернет-зависимых людей, предложил пять советов для преодоления этой зависимости.

Преодоление Интернет-зависимости

1. Признайте свою зависимость. «Патологическое использование компьютера» можно распознать по «симптомам» навязчивой потребности, пропущенным урокам и встречам, забытой и несделанной домашней работе, потере контакта с друзьями и родственниками.

2. Определите проблемы, лежащие в основе зависимости. В зависимости от возраста человека, такие моменты, как неуверенность в будущем, трудность успевать в школе или проблемы социальных отношений, могут подвигнуть ребенка на побег в гостеприимные виртуальные миры.

3. Решайте реальные проблемы. Стараясь избежать стрессовых ситуаций, мы только усложняем их. Вы можете найти репетитора, который поможет с домашним заданием, поможет начать решать социальные трудности, написать о том, что вас «гложет», или даже обратиться к специалисту.

4. Контролируйте работу на компьютере. Совсем не обязательно полностью выключать его — можно просто ограничить время нахождения в Интернете. В зависимости от возраста родители или сам учащийся могут взять на себя эту ответственность. Все виды деятельности должны быть выстроены по их приоритетности. Общение в Интернете не должно происходить до выполнения домашней работы или других обязанностей.

5. Проводите различие между интерактивной фантазией и полезным использованием Интернета.

Тема 4.4
ТЕХНОЛОГИИ БЕЗОПАСНОЙ РАБОТЫ В СЕТИ

Залогом безопасной работы в сети Интернет является соблюдение основных правил и рекомендаций, таких как грамотное посещение сайтов и проверка почты. Особенно это становится акту-

альным при работе на общедоступном компьютере. Безопасность при навигации по сайтам и по приему почты будет достигнута при соблюдении следующих рекомендаций:

1. Не ходите на незнакомые сайты.

2. Если ходите, то выключайте (на всякий случай) поддержку языка Java и использование cookies.

3. Если к вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на макровирусы.

4. Если пришло незнакомое вложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину в вашей программе чтения почты. Бывали случаи рассылки вирусов, а также вскрытия крупнейших узлов бесплатной почты. Так что не исключено, что с адреса вашего знакомого может прийти вирус.

5. Никогда не посылайте никому свой пароль.

6. Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв. А еще лучше сгенерируйте его специальной программой или попросите сделать это своего провайдера.

Пять советов по безопасности при работе на общедоступном компьютере

1. *Не сохраняйте свои учетные данные для входа в систему.* После завершения работы на Web-узле обязательно пользуйтесь функцией завершения сеанса работы с Web-узлом. Просто закрыть окно обозревателя или ввести другой адрес недостаточно. Многие программы (особенно программы для обмена мгновенными сообщениями) имеют функцию автоматического входа в систему, сохраняющую имя пользователя и пароль. Отключите эту функцию, чтобы никто, кроме вас, не смог войти в систему.

2. *Не оставляйте без присмотра компьютер с важными сведениями на экране.* Закончив работу на общедоступном компьютере, воспользуйтесь функцией выхода из системы во всех программах и закройте все окна, в которых могут отображаться конфиденциальные данные.

3. *Заметайте свои следы.* В Internet Explorer и других Web-обозревателях сохраняются сведения о паролях пользователя и всех посещенных им Web-страницах, даже если он закрыл их и вышел из системы.

4. *Опасайтесь подглядывания через плечо.* Работая на общедоступном компьютере, следите за мошенниками, которые подгляды-

вают через плечо, как вы вводите секретные пароли, чтобы потом получить доступ к вашим данным.

5. *Не вводите важные сведения на общедоступном компьютере.*

Эти меры обеспечат некоторую защиту от хакеров-любителей, которые могут воспользоваться компьютером после вас. Однако профессиональный мошенник может установить на общедоступном компьютере специализированное программное обеспечение, которое будет записывать каждое нажатие клавиши, а затем отправлять ему эту информацию по электронной почте.

ПРАКТИЧЕСКАЯ ЧАСТЬ МОДУЛЯ 4

Тест на определение Интернет-зависимости: тест Кимберли Янг. (http://www.psyhelp.ru/texts/iad_test.htm)

Для выявления Интернет-зависимости ответьте на следующие вопросы:

Часть 1

1. Часто ли вы замечаете, что проводите онлайн больше времени, чем намеревались?
2. Часто ли вы пренебрегаете домашними делами, чтобы провести больше времени в сети?
3. Часто ли вы предпочитаете пребывание в сети интимному общению с партнером?
4. Часто ли вы заводите новые знакомства с пользователями Интернета, находясь онлайн?
5. Часто ли окружающие интересуются количеством времени, проводимым вами в сети?
6. Часто ли страдают ваши успехи в учебе или работе, так как вы слишком много времени проводите в сети?
7. Часто ли страдает ваша производительность труда из-за увлечения Интернетом?
8. Часто ли вы занимаете оборонительную позицию и скрытничаете, когда вас спрашивают, чем вы занимаетесь в сети?

9. Часто ли вы блокируете беспокоящие мысли о вашей реальной жизни, утешительными мыслями об Интернете?

10. Часто ли вы обнаруживаете себя предвкушающим, как вновь окажетесь в Интернете?

11. Часто ли вы ощущаете, что жизнь без Интернета скучна, пуста и безрадостна?

12. Часто ли вы ругаетесь, кричите или иным образом выражаете свою досаду, когда кто-то пытается отвлечь Вас от пребывания в сети?

13. Часто ли вы пренебрегаете сном, засиживаясь в Интернете допоздна?

14. Часто ли вы предвкушаете, чем займетесь в Интернете, находясь оффлайн, или фантазируете о пребывании онлайн?

15. Часто ли Вы говорите себе «еще минутку», находясь онлайн?

16. Часто ли терпите поражение в попытках сократить время, проводимое в сети?

17. Часто ли вы пытаетесь скрыть количество времени, проводимое вами в сети?

18. Часто ли вы выбираете провести время в Интернете, вместо того, чтобы выбраться куда-либо с друзьями?

19. Часто ли вы испытываете депрессию, подавленность или нервозность, будучи вне сети, и отмечаете, что это состояние проходит, как только вы оказываетесь онлайн?

Часть 2

1. Чувствуете ли вы эйфорию, оживление, возбуждение, находясь за компьютером?

2. Требуется ли вам проводить все больше времени за компьютером, чтобы получить те же ощущения?

3. Чувствуете ли вы пустоту, депрессию, раздражение, находясь не за компьютером?

4. Случалось ли вам пренебрегать важными делами, в то время как вы были заняты за компьютером, но не работой?

5. Проводите ли вы в сети больше 3 часов в день?

6. Если вы в основном используете компьютер для работы, участвуете ли в рабочее время в чатах или обнаруживаете себя на не связанных с работой сайтах более, чем дважды в день?

7. Качаете ли Вы файлы с порносайтов?
8. Считаете ли вы, что с человеком легче общаться онлайн, нежели лично?
9. Говорили ли вам друзья или члены семьи, что вы слишком много времени проводите онлайн?
10. Мешает ли вашей деловой активности количество времени, проводимое в сети?
11. Бывало ли такое, что ваши попытки ограничить время, проводимое в сети, оказывались безуспешными?
12. Бывает ли так, что ваши пальцы устают от клавиатуры или щелканья кнопкой мыши?
13. Случалось ли вам лгать на вопрос о количестве времени, проводимом в сети?
14. Был ли у Вас хоть раз «синдром карпального канала» (онемение и боли в кисти руки)?
15. Бывают ли у вас боли в спине чаще, чем 1 раз в неделю?
16. Бывает ли у вас ощущение сухости в глазах?
17. Увеличивается ли время, проводимое вами в сети?
18. Случалось ли вам пренебречь приемом пищи или есть прямо за компьютером, чтобы остаться в сети?
19. Случалось ли вам пренебречь личной гигиеной, например, бритьем, причесыванием и т. п., чтобы провести это время за компьютером?
20. Появились ли у вас нарушения сна и/или изменился ли режим сна с тех пор, как вы стали использовать компьютер ежедневно?

ПРАКТИЧЕСКИЕ РАБОТЫ

ПРАКТИЧЕСКАЯ РАБОТА № 1
Установка фильтрации. Фильтрация TCP/IP

В системе Windows 2000/XP имеется средство защиты компьютера от нежелательного IP-трафика — фильтрация TCP/IP

Фильтрация TCP/IP — это мощное средство противодействия хакерским атакам, позволяющее защитить компьютер от сетевого трафика, несущего потенциальную угрозу компьютерной системе.

При использовании фильтрации TCP/IP пакет принимается на обработку, если он удовлетворяет следующим условиям:

- является пакетом ICMP;
- TCP-порт назначения присутствует в списке допустимых TCP-портов;
- UDP-порт назначения присутствует в списке допустимых UDP-портов;
- IP-порт назначения присутствует в списке допустимых IP-портов.

Для указания допустимых портов TCP и UDP, а также протоколов IP, выполните следующее:

1. Выполните команду **Пуск/Настройка/Сетевые подключения —** на экране отобразится окно Сетевые подключения (рис.)

2. Щелкните правой кнопкой мыши на **Подключение по локальной сети** и в отобразившемся контекстном меню выберите команду **Свойства (**рис. 1).

3. Выберите **Протокол Интернета (TCP/IP)** и щелкните по кнопке **Свойства** (рис. 2).

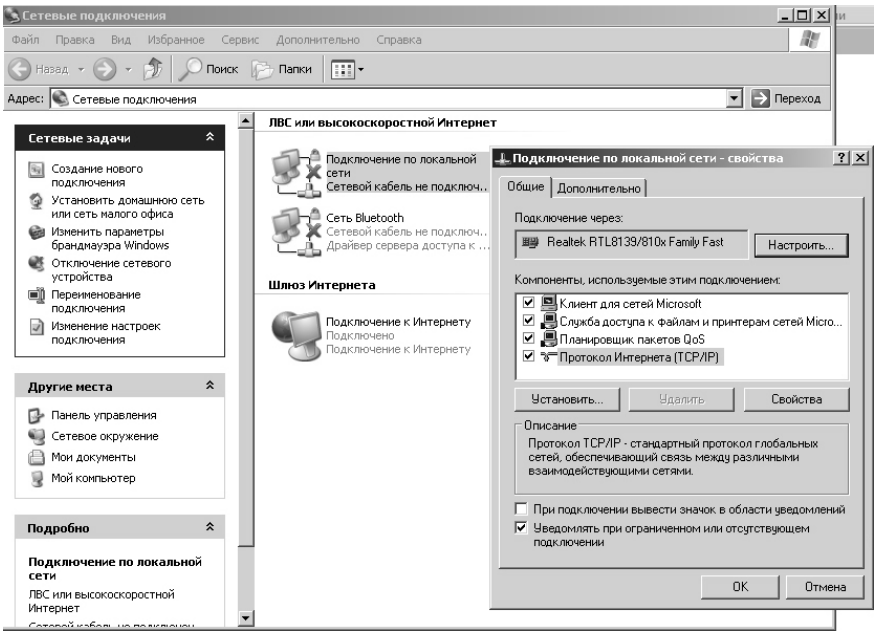


Рис. 1

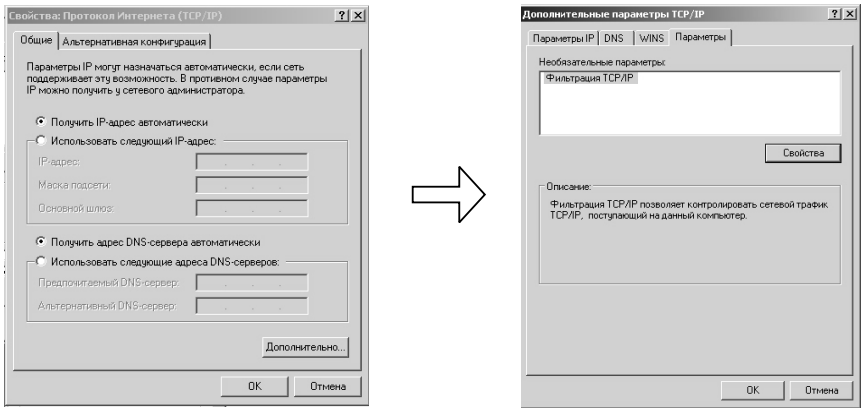


Рис. 2

4. В окне Свойства: **Протокол Интернета (TCP/IP)** щелкните на кнопке **Дополнительно** и откройте вкладку **Параметры**.

5. В списке «Необязательные параметры» содержатся два элемента: IP-безопасность и Фильтрация TCP/IP. Выберите пункт «Фильтрация TCP/IP» и щелкните на кнопке «Свойства» (рис. 3). В отобразившемся окне **Фильтрация TCP/IP** отметьте флажок **Задействовать фильтрацию TCP/IP (все адаптеры)**.

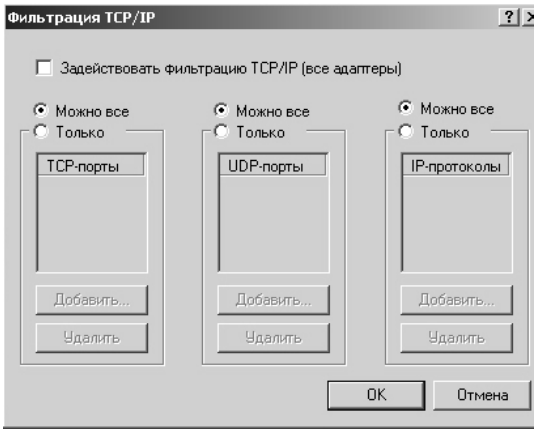


Рис. 3

Эта мера защиты системы Windows 2000/XP является первоочередной при подключении к Интернету.

ПРАКТИЧЕСКАЯ РАБОТА № 2
Установка безопасной работы и обеспечение конфиденциальности и надежности с помощью Internet Explorer 8 (http://www.microsoft.com/rus/windows/internet-explorer/)

Internet Explorer 8 — последняя версия популярного обозревателя, привычного для большинства пользователей. Она удобна в использовании, упрощает и ускоряет работу в Интернете, а также обеспечивает более высокую степень конфиденциальности и безопасности в отличие от ранних версий.

Быстрота. Новые страницы и вкладки открываются в обозревателе Internet Explorer 8 гораздо быстрее, чем раньше, а сбои происходят реже. С его помощью можно без труда получать доступ к любым нужным сведениям: одним щелчком открывать веб-почту, любимые новостные узлы и другие веб-службы.

Простота. Количество действий, необходимых для выполнения многих типичных задач, сокращено, а также автоматизирован доступ к обновлениям данных в реальном времени. Кроме того, можно отслеживать сведения о любимых спортивных командах, прогнозы погоды и новости с помощью одного щелчка мыши.

Повышенная конфиденциальность. При работе в Интернете обеспечивается защита личных и конфиденциальных данных.

Повышенная безопасность. Обозреватель защищает компьютер от вредоносных программ и упрощает определение потенциально опасных веб-узлов.

УПРАЖНЕНИЕ 1
Установка Internet Explorer 8

1. Нажмите кнопку Загрузить на странице (http://www.microsoft.com/downloads/details.aspx?FamilyID=341c2ad5—8c3d-4347—8c03—08cdecd8852b&displaylang=ru), чтобы начать загрузку, выберите язык в раскрывающемся списке **Выбор языка** и нажмите кнопку **Перейти**.

2. Выберите один из указанных ниже вариантов.

- Чтобы немедленно начать установку, нажмите кнопку **Запустить**.
- Чтобы сохранить загруженный файл и установить его позднее, нажмите кнопку **Сохранить**.
- Чтобы отменить установку, нажмите кнопку **Отмена**.

Автоматическое восстановление после сбоев

Разделение вкладок

Что бы ни случилось в одной из вкладок, открытой в Internet Explorer 8, другие вкладки будут продолжать работать независимо.

Новому браузеру не страшны сбои на страницах: если вкладка неожиданно закрывается, она автоматически перезагрузится и вернет вас на просматриваемый веб-сайт.

Улучшенная функция удаления истории просмотра

Теперь удаление истории просмотра, файлов cookies и временных файлов происходит отдельно от сайтов, добавленных в «Избранное».

Благодаря сохранению настроек и файлов cookies переход на проверенные сайты осуществляется быстрее и безопаснее.

УПРАЖНЕНИЕ 2
Работа с фильтром SmartScreen браузера IE 8

Новый фильтр SmartScreen браузера IE 8 помогает защититься от скрытой установки вредоносных программ, которые могут повредить, передать злоумышленникам или уничтожить ваши доку-

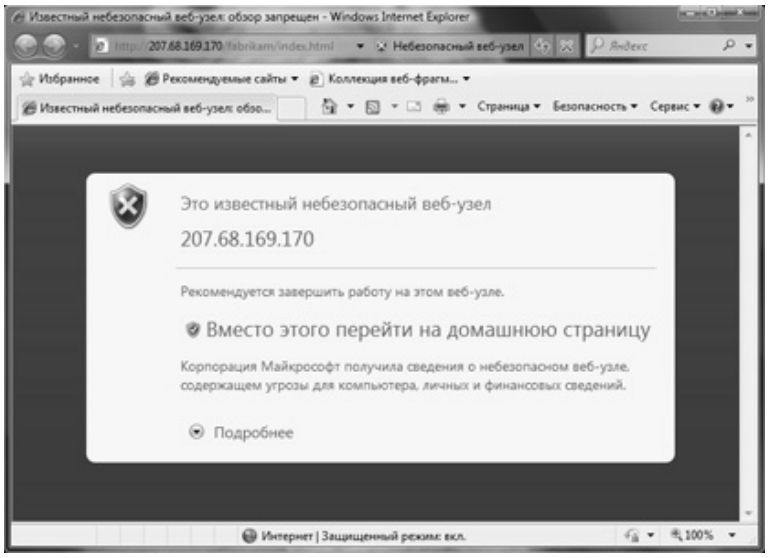


Рис. 4

менты, ценные файлы, рабочие и семейные архивы, использовать ваши персональные данные или просто нарушить работу компьютера в целом.

Фильтр SmartScreen способен обучаться, получая от пользователей информацию о мошеннических веб-сайтах. Вы и сами можете внести собственный вклад в повышение безопасности Интернета, сообщая о подозрительных сайтах — со SmartScreen это делается одним кликом.

При любой опасности SmartScreen покажет вам предупреждающее сообщение и предложит альтернативные варианты действий — покинуть сайт или продолжить просмотр на свой страх и риск.

SmartScreen также сообщит о попытках загрузить потенциально опасные программы. Он заметит их не только на странице, но и за ее пределами, на связанных с ней ссылках (рис. 4).

УПРАЖНЕНИЕ 3
Работа в режиме InPrivate

Проверяя сообщения электронной почты, вы вряд ли хотите, чтобы эта информация была доступна кому-либо еще. Функция просмотра InPrivate в Internet Explorer 8 не позволяет браузеру сохранять историю просмотра, временные Интернет-файлы, введенные в формы данные, файлы cookies, имена пользователей и пароли. В защищенном режиме InPrivate вы не оставляете никаких сведений о веб-страницах, которые посещали или искали с Internet Explorer 8.

Чтобы включить режим просмотра InPrivate, откройте новую вкладку и щелкните «Просмотреть в режиме InPrivate» или выберите эту функцию, нажав кнопку «Безопасность», расположенную в правом верхнем углу окна браузера.

После этого Internet Explorer 8 запустит новый сеанс браузера, во время которого не будут сохраняться никакие сведения, в том числе история поиска и сведения о просмотренных веб-страницах. Чтобы завершить сеанс просмотра InPrivate, просто закройте окно браузера (рис. 5).

Фильтрация InPrivate

Современные веб-сайты наполняются содержимым из множества источников. Пользователи зачастую и не подозревают, что некоторое содержимое — изображения, реклама, аналитические

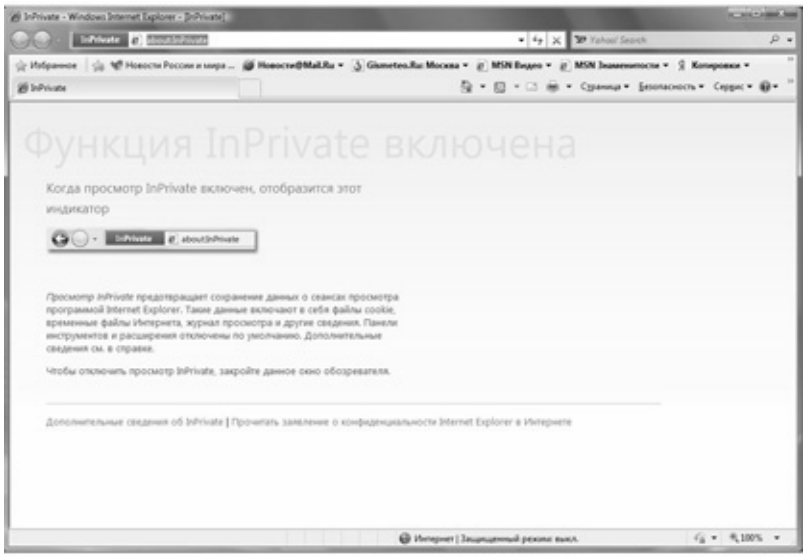


Рис. 5

данные — предоставлено сторонними веб-сайтами и что некоторые из них могут отслеживать перемещение пользователей в Интернете. Фильтрация InPrivate предоставляет пользователю новый уровень контроля и право выбора информации, которая будет использоваться веб-сайтами для отслеживания его перемещений в Интернете. По вашему желанию, она будет обнаруживать и блокировать на странице все содержимое, относящееся к сторонним сайтам, повышая безопасность и конфиденциальность пользования Интернетом.

По умолчанию фильтрация InPrivate отключена. Ее необходимо включать каждый раз при запуске браузера.

Чтобы включить InPrivate, в меню «Безопасность» выберите «Фильтрация InPrivate».

Для управления параметрами фильтрации в меню «Безопасность» выберите «Параметры фильтрации InPrivate».

Чтобы завершить сеанс просмотра InPrivate, просто закройте окно браузера.

Примечание. Повышение уровня безопасности в Интернете с помощью Internet Explorer версии 8 можно провести с помощью XSS-фильтра (http://blogs.technet.com/swi/archive/2008/08/19/ie-8-xss-filter-architecture-implementation.aspx).

ПРАКТИЧЕСКАЯ РАБОТА № 3
Удаление сведений о паролях пользователя и всех посещенных им веб-страницах

УПРАЖНЕНИЕ 1
Отключение функции сохранения паролей

Перед открытием веб-страниц в обозревателе Internet Explorer отключите функцию сохранения паролей.

1. В обозревателе Internet Explorer откройте меню **Сервис** и выберите пункт **Свойства обозревателя.**

2. Откройте вкладку **Содержание** и нажмите кнопку **Автозаполнение.**

3. Снимите оба флажка, имеющие отношение к паролям.

УПРАЖНЕНИЕ 2
Удаление временных файлов Интернета и очистка журнала

Завершив работу на общедоступном компьютере, удалите все временные файлы и очистите журнал пользования Интернетом.

1. В обозревателе Internet Explorer откройте меню **Сервис** и выберите пункт **Свойства обозревателя**.

2. На вкладке **Общие** в разделе **Временные файлы Интернета** нажмите кнопку **Удалить файлы**, а затем **Удалить «Cookie»**.

3. В разделе **Журнал** нажмите кнопку **Очистить журнал**.

УПРАЖНЕНИЕ 3
Удаление прочих файлов, сохраненных корпоративными порталами, например, Sharepoint Portal Server

Если для просмотра внутренних документов компании вы пользуетесь корпоративным веб-узлом, то можете непреднамеренно сохранить важные документы на общедоступном компьютере.

1. Удалите все файлы из временной папки своей учетной записи пользователя, находящейся по следующему пути: C:\Documents and Settings\имя_пользователя\Local Settings\Temp.

2. Если в компании используется сервер Microsoft Office SharePoint Portal Server, очистите временную папку (My Documents\ SharePoint Drafts).

ПРАКТИЧЕСКАЯ РАБОТА № 4
Настройка параметров безопасности Web-браузера

Настройка системы безопасности Web-браузера.

1. Для настройки параметров безопасности браузера Internet Explorer версии 5 и выше запустите приложение и выберите команду меню **Сервис/Свойства обозревателя**. В отобразившемся окне **Свойства обозревателя** выберите вкладку **Безопасность** (рис. 6).

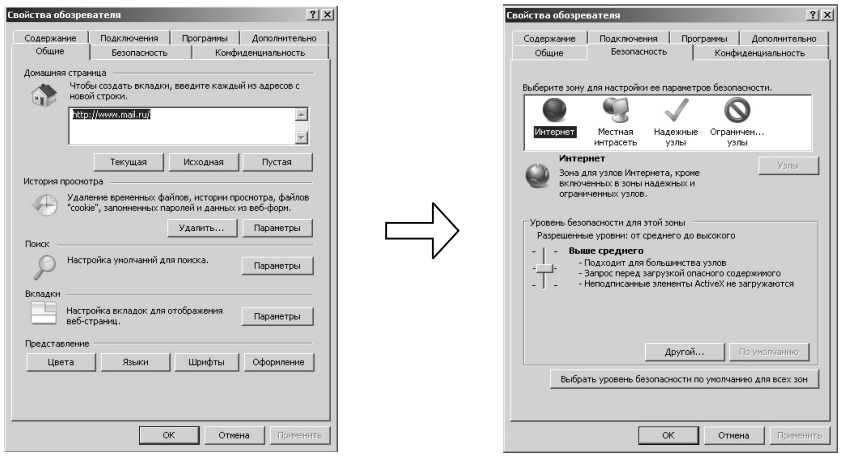


Рис. 6

2. Для настройки параметров безопасности Интернета выполните следующее:

- Щелкните на пиктограмме **Интернет** сверху вкладки **Безопасность** и либо воспользуйтесь предварительно настроенными уровнями безопасности, либо создайте свои правила безопасности.
- Для выбора предварительно настроенного уровня безопасности передвиньте ползунковый регулятор в разделе **Уровень безопасности** для этой зоны в нужную позицию; по умолчанию для браузера Internet Explorer установлен уровень выше среднего, пригодный для посещения большинства сайтов (рис. 7).

3. Для создания списка ненадежных сайтов выполните следующие действия:

- На вкладке **Безопасность** окна **Свойства обозревателя** щелкните на пиктограмме **Ограниченные узлы**. Щелкните мышью на кнопке **Узлы**; отобразится окно **Ограниченные узлы** (рис. 8).

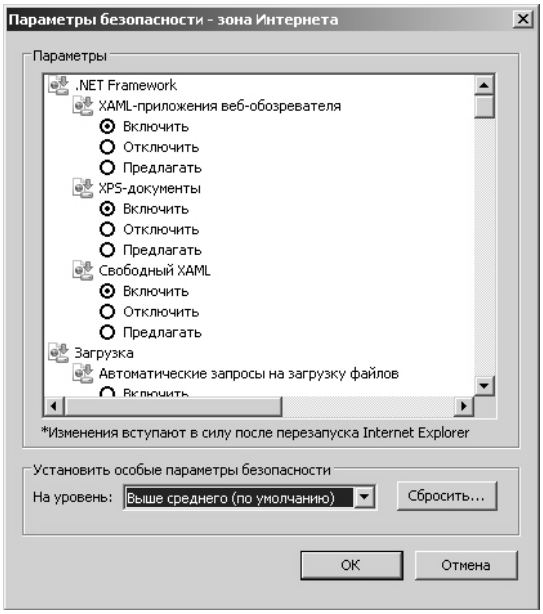


Рис. 7

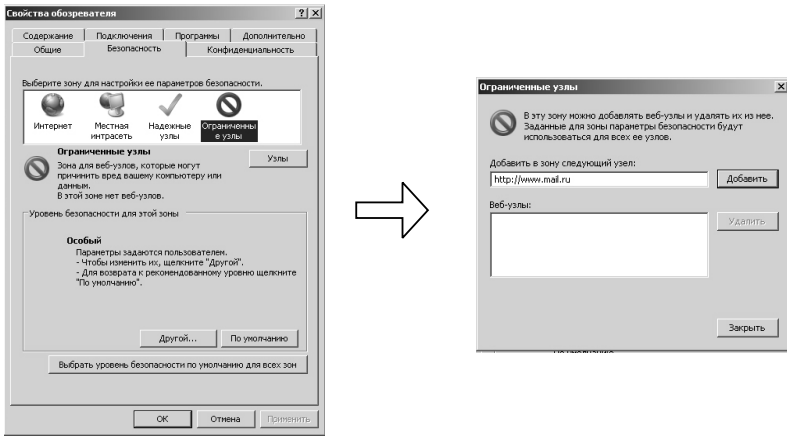


Рис. 8

Введите в поле **Добавить узел** в зону адрес ненадежного Web-сайта и щелкните на кнопке **Добавить**. Адрес отобразится в списке **Web-узлы**. Для удаления Web-сайта из списка ненадежных

узлов выберите адрес узла из списка **Web-узлы** и щелкните мышью на кнопке **Удалить**.

После создания списка ненадежных Web-сайтов щелкните на кнопке **ОК** вернитесь во вкладку **Безопасность**.

ПРАКТИЧЕСКАЯ РАБОТА № 5

Активация функции Родительского Контроля (Parental Control) в Microsoft Windows 7

Операционная система Microsoft Windows 7 содержит мощный и современный инструмент контроля над работой детей за компьютером — Родительский Контроль (Parental Control). Используя функционал Родительского Контроля в Windows 7, можно полностью контролировать, как члены семьи используют компьютер в целом и ресурсы сети Интернет.

Примечание. Полезные ресурсы:
www.microsoft.ru/protect, www.microsoft.ru/security

Для того, чтобы активировать функцию родительского контроля в Windows 7:

1. Нажмите **Панель управления / Учетные записи пользователей и семейная безопасность/ Родительский контроль**. Щелкните на учетную запись пользователя, чью работу за компьютером вы хотели бы контролировать. Если учетной записи нет, щелкните **Создать новую учетную запись** (рис. 9).

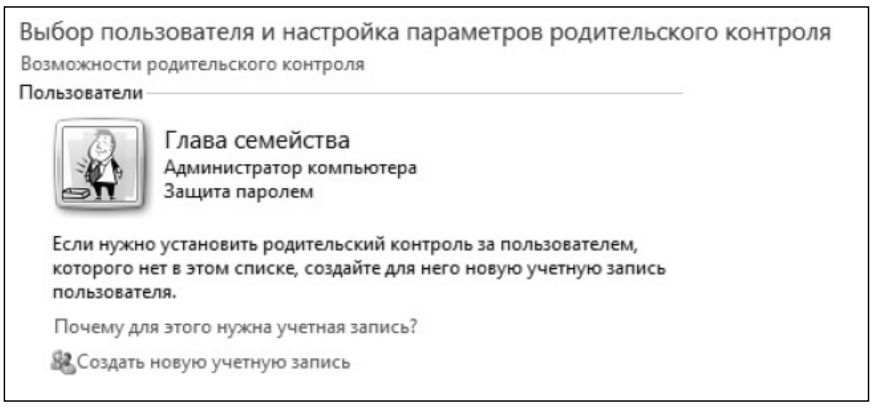


Рис. 9

2. В появившемся окне в настройке **Родительский контроль** выберите **Включить, используя текущие параметры**. Теперь вы можете установить ограничения по времени использования компьютера, а также играм и программам, которые можно запускать (рис. 10).

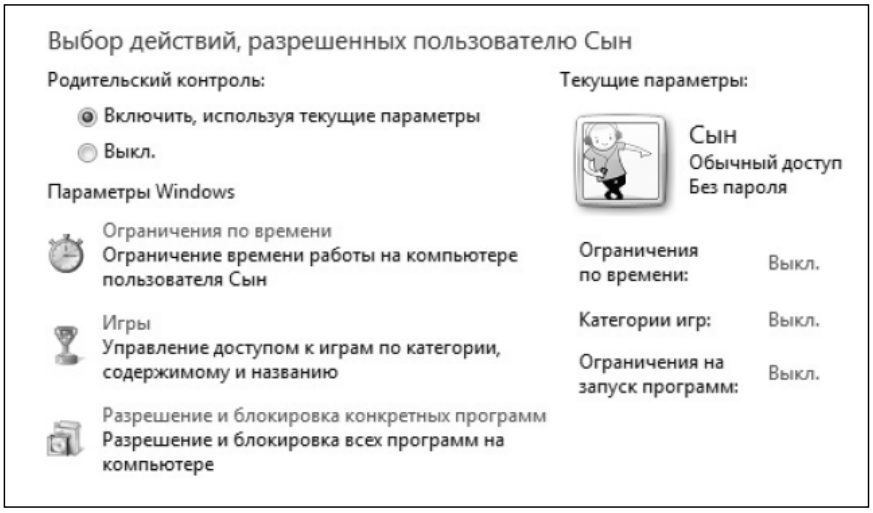


Рис. 10

3. Для того, чтобы установить ограничения времени использования компьютера, щелкните **Ограничения по времени,** в появившемся расписании выделите мышкой дни и часы, в которые разрешается использовать компьютер. Позже вы можете отредактировать выбранное расписание (рис. 11).

4. Для того, чтобы установить ограничения по категориям игр, щелкните **Игры**. В открывшемся окне выберите, может ли пользователь запускать игры. Если выбрано **Да**, то доступно две настройки: **Задать категории для игр** и **Запрещение и разрешение игр**. Щелкните **Задать категории для игр**. Здесь вы можете выбрать, в игры с какой оценкой может играть пользователь. Также можно разрешить или запретить игры, категория которых не указана (рис. 12).

5. Для того, чтобы разрешить или блокировать конкретную программу, щелкните **Разрешение и блокировка конкретных программ.** Если выбрать пункт «**...**может работать только с разрешенными программами», то в окне ниже появится список программ. Галочками необходимо отметить разрешенные программы. Добавить программу к списку можно кнопкой **Обзор**.


Задание времени, в которое Сын сможет работать на компьютере
Выделите курсором время, когда работа за компьютером будет запрещена или разрешена.
Час
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
понедельник
вторник
среда
четверг
пятница
суббота
воскресенье
Разрешено
Запрещено

Рис. 11

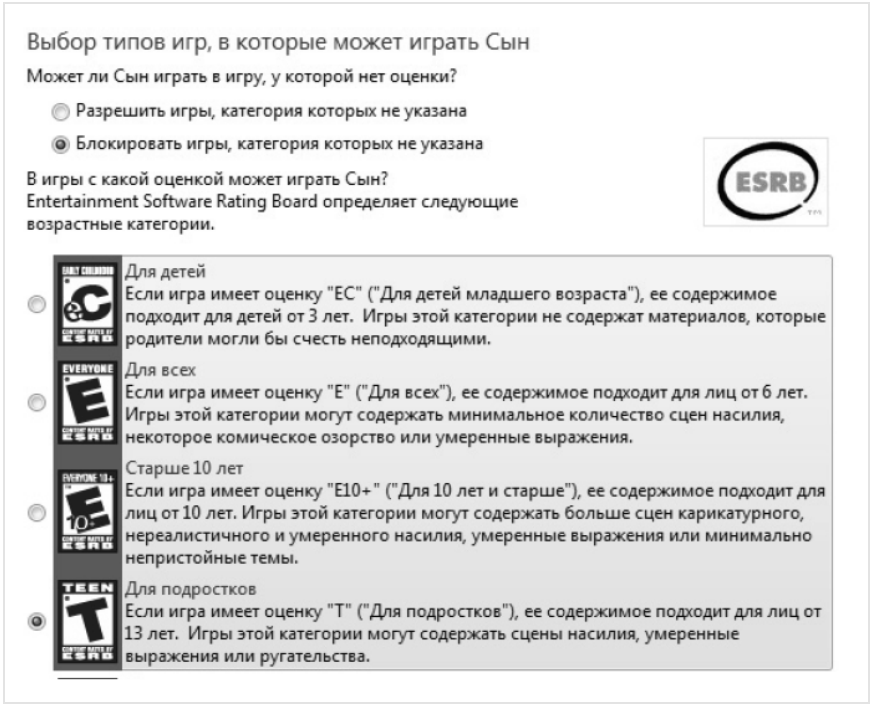

Выбор типов игр, в которые может играть Сын
Может ли Сын играть в игру, у которой нет оценки?
Разрешить игры, категория которых не указана
Блокировать игры, категория которых не указана
В игры с какой оценкой может играть Сын?
Entertainment Software Rating Board определяет следующие возрастные категории.
ESRB
Для детей
Если игра имеет оценку "EC" ("Для детей младшего возраста"), ее содержимое подходит для детей от 3 лет. Игры этой категории не содержат материалов, которые родители могли бы счесть неподходящими.
Для всех
Если игра имеет оценку "E" ("Для всех"), ее содержимое подходит для лиц от 6 лет. Игры этой категории могут содержать минимальное количество сцен насилия, некоторое комическое озорство или умеренные выражения.
Старше 10 лет
Если игра имеет оценку "E10+" ("Для 10 лет и старше"), ее содержимое подходит для лиц от 10 лет. Игры этой категории могут содержать больше сцен карикатурного, нереалистичного и умеренного насилия, умеренные выражения или минимально непристойные темы.
Для подростков
Если игра имеет оценку "T" ("Для подростков"), ее содержимое подходит для лиц от 13 лет. Игры этой категории могут содержать сцены насилия, умеренные выражения или ругательства.

Рис. 12

6. Чтобы ограничить детей — пользователей компьютера от просмотра веб-сайтов сомнительного содержания, необходимо загрузить пакет **Семейная безопасность** с веб-узла http://download.live.com/familysafety, следуя инструкциям на указанной странице. Выберите компонент **Семейная безопасность** и нажмите **Установить**. После установки появится приветственное окно **Windows Live**! Если у вас нет LiveID, то вы можете его создать, нажав на кнопку **Зарегистрироваться**. Запустите программу **Семейная безопасность**. Для этого щелкните **Все программы/Windows Live/Семейная безопасность Windows Live.** В появившемся окне **Фильтр Семейной безопасности Windows Live** щелкните **Добавить членов семьи и управлять ими на этом компьютере**. Введите свой идентификатор Windows Live ID и пароль. Поставьте галочку в поле **Контроль учетной записи** напротив имени необходимого пользователя. Нажмите **Далее,** в появившемся окне в выпадающем списке **Пользователи Семейной безопасности** выберите пункт **Добавить** и нажмите кнопку **Сохранить**. В следующем окне будут показаны итоговые результаты. По умолчанию применяется базовый веб-фильтр и включается создание отчетов о действиях. Для того, чтобы изменить эти параметры, необходимо зайти на сайт http://familysafety.live.com и, выбрав нужного пользователя, настроить необходимые параметры согласно подсказкам, указанным на странице.

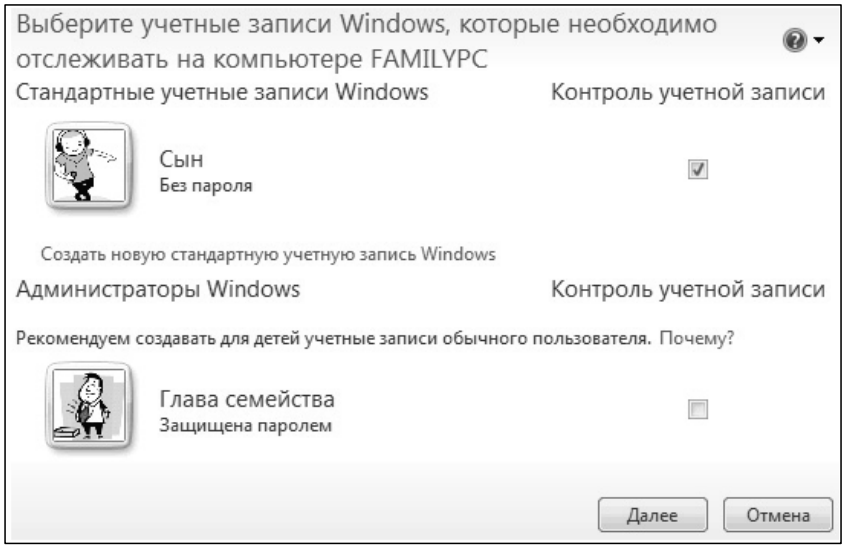


Рис. 13

Используемые литература и ресурсы

1. Галатенко В.А. Основы информационной безопасности. [Текст] 4-е изд. учеб. пособие, ВУЗ // — М: Издательство Бином. Лаборатория знаний, Интуит, 2008—205 с.

2. Глушаков С.В. Секреты хакера: защита и атака [Текст] / С.В. Глушаков, М.И. Бабенко, Н.С. Тесленко. — изд. 2-е, доп. и перераб. — М: АСТ: АСТ МОСКВА; Владимир: ВКТ, 2009. — 544 с. — (Учебный курс).

3. Ленков С.В., Перегудов Д.А, Хорошко В.А. Методы и средства защиты информации. В 2 томах. Том 1. Несанкционированное получение информации [Текст] // — М: Издательство: Арий, 2008 г. 464 с.

4. Прохода А. Н. Обеспечение Интернет-безопасности. Практикум: Учебное пособие для вузов. [Текст] // — М.: Горячая линия — Телеком, 2007. — 180 с: ил.

5. Основы безопасности детей и молодежи в Интернете — интерактивный курс по Интернет-безопасности. Владельцами авторских прав на сайт являются проект Финский день информационной безопасности и WSOYpro [Электронный ресурс]. — URL: http://laste.arvutikaitse.ee/rus/html/copyright.htm

6. Безопасность детей в Интернете. Nachalka.com 2008 [Электронный ресурс]. — URL: http://www.nachalka.com/bezopasnost

7. Безопасность дома [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/default.mspx

8. Евтеев Леонид. Безопасность ребенка в Интернете. Инновационная образовательная сеть «Эврика» — Пермь, 2009. [Электронный ресурс]. — URL: http://www.diaghilev.perm.ru/class/sobr4—2.htm

9. Кимберли Янг. Тест на Интернет-зависимость / Перевод теста, выполненный и адаптированный В.А.Буровой/ Клиника СПО Центр — М: 2009 [Электронный ресурс]. — URL: http://www.psyhelp.ru/texts/iad_test.htm

10. Барбара Гутман, Роберт Бэгвилл. Политика безопасности при работе в Интернете — техническое руководство. CIT Forum 2009 [Электронный ресурс]. — URL: http://www.citforum.ru/internet/security_guide/index.shtml

Модуль 5
ТЕХНОЛОГИИ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ РАЗРУШЕНИЯ И НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Тема 5.1
ЦЕЛИ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ. УРОВНИ И МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Целью совершения любого преступления является удовлетворение корыстных целей человека или группы людей, как то материальных, моральных, психических и так далее. Преступления в информационной сфере затрагивают различные аспекты: это и получение информации нелегальным путем (в том числе и с использованием детей), распространение в Интернете материалов порнографического типа (в том числе и детской порнографии), мошенничество в Интернете и т. д.

Основные понятия в области защиты информации от разрушения и несанкционированного доступа рассмотрим исходя из **ГОСТ Р 50922—2006.** Настоящий стандарт устанавливает основные термины с соответствующими определениями, применяемые при проведении работ по стандартизации в области защиты информации. Термины данного стандарта рекомендуется использовать в правовой, нормативной, технической и организационно-распорядительной документации, научной, учебной и справочной литературе.

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

Примечание: собственниками информации могут быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защита информации — деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защита информации от утечки — защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами.

Примечание: заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защита информации от несанкционированного воздействия — защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия — защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных не целенаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от разглашения — защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа — защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Примечание: заинтересованными субъектами, осуществляющими несанкционированный доступ к защищаемой информации, могут быть государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Цель защиты информации: заранее намеченный результат защиты информации.

Примечание: результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Эффективность защиты информации — степень соответствия результатов защиты информации цели защиты информации.

Показатель эффективности защиты информации — мера или характеристика для оценки эффективности защиты информации.

Норма эффективности защиты информации — значение показателя эффективности защиты информации, установленное нормативными и правовыми документами.

Замысел защиты информации — основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

Система защиты информации — совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

Техника защиты информации — средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Объект защиты информации — информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

Способ защиты информации — порядок и правила применения определенных принципов и средств защиты информации.

Оценка соответствия требованиям по защите информации — прямое или косвенное определение степени соблюдения требований по защите информации, предъявляемых к объекту защиты информации.

Средство защиты информации — техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Средство контроля эффективности защиты информации — средство защиты информации, предназначенное или используемое для контроля эффективности защиты информации.

В связи с тем, что информация является предметом собственности (государства, коллектива, отдельного лица (субъекта)), то неизбежно возникает проблема угрозы безопасности этой информации, заключающейся в неконтролируемом ее распространении, в хищении, несанкционированном уничтожении, искажении, передаче, копировании, блокировании доступа к информации. Следовательно, возникает проблема защиты информации от утечки и несанкционированных воздействий на информацию и ее носители, а также предотвращения других форм незаконного вмешательства в информационные ресурсы и информационные системы. В связи с чем, понятие ***«Защита информации»*** становится основополагающим (ключевым) понятием и рассматривается как деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Значимость защиты информации увеличивается в связи с возрастанием возможностей иностранных разведок за счет совершенствования технических средств разведки, приближения этих средств к объектам разведки (носителям информации) вследствие развертывания инспекционной деятельности, создания совместных предприятий и производств, сокращения закрытых для иностранцев зон и городов.

Определившись с терминологией защиты информации, переходим на рассмотрение уровней и мер защиты информации. Можно выделить три основных уровня защиты информации. Например, применительно к общеобразовательному учреждению они выглядят следующим образом:

- защита информации на уровне рабочего места ученика и учителя;
- защита информации на уровне компьютерного класса;
- защита информации на уровне образовательного учреждения.

Защита информации на этих различных уровнях будет иметь как общие способы, так и специальные способы, зависящие от уровня.

Одним из способов (мер) по защите информации являются программные средства защиты. В настоящее время создано большое количество операционных систем, систем управления базами данных, сетевых пакетов и пакетов прикладных программ, уже включающих в себя разнообразные средства защиты информации.

С помощью программных средств защиты решаются следующие задачи информационной безопасности:

- контроль загрузки и входа в систему с помощью персональных идентификаторов (имя, код, пароль и т. п.);
- разграничение и контроль доступа субъектов к ресурсам и компонентам системы, внешним ресурсам;
- изоляция программ процесса, выполняемого в интересах конкретного субъекта, от других субъектов (обеспечение работы каждого пользователя в индивидуальной среде);
- управление потоками конфиденциальной информации с целью предотвращения записи на носители данных несоответствующего уровня (грифа) секретности;
- защита информации от компьютерных вирусов;
- стирание остаточной конфиденциальной информации в разблокированных после выполнения запросов полях оперативной памяти компьютера;
- обеспечение целостности информации путем введения избыточности данных;
- автоматический контроль над работой пользователей системы на базе результатов протоколирования и подготовка отчетов по данным записей в системном регистрационном журнале.

Методы обеспечения защиты информации могут быть разные, но основные из них следующие:

- препятствие;
- управление доступом;
- маскировка;
- регламентация;
- принуждение и побуждение.

Тема 5.2
УСТАНОВКА ПАРОЛЕЙ НА ПК И ПАПКИ. МЕРЫ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОЧТОЙ

Для разграничения доступа на одном компьютере современные операционные системы позволяют разграничивать доступ к информации и другим частям операционной системы (сервисы, программы и т. д.) с помощью учетных записей с задаваемыми правами доступа. На ОС по умолчанию представлены две учетные записи: администратор (полный доступ), гость (минимальный доступ). Также существует такое понятие, как группы пользователей — это

некий набор предустановленных прав, которые можно назначать пользователям. Для того чтобы однозначно авторизовать того или иного пользователя, применяются пароли. Это может быть применимо для ограничения и контроля деятельности работы детей на домашнем компьютере.

С помощью этого же механизма также регламентируется доступ к файловой системе, в частности, к папкам. Необходимым условием работы любого компьютера в сети является установка на нем персонального межсетевого экрана с функцией анализа активности программного обеспечения. По тому же принципу, но более сложными механизмами, связанными с централизованным администрированием, реализуется разграничение прав доступа в доменной структуре учреждения, например, школы.

Самым распространенным путем утечки информации является электронная почта. В настоящее время злоумышленники активно развивают методы социального инжиниринга, которые позволяют проникнуть даже на самый защищенный пользовательский компьютер.

Социальная инженерия — технология использования человеческого фактора для взлома информационной безопасности. Именно человек является наиболее слабым звеном в системах защиты. Один из приемов использования социальной инженерии — методика введения пользователя в заблуждение путем сообщения ему важных для него данных, оказывающихся на самом деле ложными.

Пример подобной методики — фишинг. Фишинг — вид онлайнового мошенничества, целью которого является получение идентификационных данных пользователей. Для этого рассылаются электронные письма от имени популярных брендов и вставляются в них ссылки на фальшивые сайты. Оказавшись на таком сайте, пользователи рискуют сообщить информацию конфиденциального характера.

Злоумышленники рассылают письма с троянскими программами, которые были спрятаны под фотографиями. Для заманивания пользователей на сайты-ловушки текст письма составляется так, чтобы у читающего не возникло сомнения в правдивости написанного.

Основой защиты от таких атак является, как ни странно, «обучение» пользователей. Необходимо информировать пользователей об этом виде угроз.

Для борьбы с фишинг-атаками используются средства контентной фильтрации, такие, как системы контроля электронной почты, фильтры, обеспечивающие фильтрацию сообщений Ин-

тернет-пейджеров. Антивирусная фильтрация и проверка на наличие шпионских программ позволяют значительно снизить уровень воздействия фишинг-атак на сеть. Целью многих подобных атак является установка на компьютере пользователя троянцев или программ-шпионов, дающая возможность злоумышленникам получить доступ к персональным данным пользователя.

Большинство клиентских почтовых программ использует протоколы POP3 и IMAP4 для подключения к пользовательскому почтовому ящику и считывания почты и протокол SMTP — для отправки писем. Веб-доступ к почтовым ящикам осуществляется по протоколу HTTP.

Для обеспечения защиты при приеме и передаче почтовых сообщений рекомендуется использовать *протокол SSL (Secure Sockets Layer)*.

Программа Microsoft Outlook, например, для работы с почтовым сервером Exchange использует *протокол RPC,* включающий в себя встроенные механизмы обеспечения безопасности канала.

При работе с электронной почтой следует обязательно пользоваться современными антивирусными программами и, желательно, средствами защиты от нежелательной почты — *спама*.

Тема. 5.3
БЕЗОПАСНОСТЬ РАБОТЫ В ЛОКАЛЬНОЙ СЕТИ

Рассмотрим безопасность в локальной сети исходя из требований Национального стандарта согласно ГОСТу Р ИСО/МЭК 17799—2005. Для этого вводятся такие понятия, как управление сетевыми ресурсами, средства контроля сетевых ресурсов, контроль сетевого доступа, политика в отношении использования сетевых служб.

Управление сетевыми ресурсами

Цель: обеспечение безопасности информации в сетях и защиты поддерживающей инфраструктуры.

Средства контроля сетевых ресурсов

Для обеспечения требуемого уровня безопасности компьютерных сетей и его поддержки требуется комплекс средств контроля. Руководители, отвечающие за поддержку сетевых ресурсов, долж-

ны обеспечивать внедрение средств контроля безопасности данных в сетях и защиту подключенных сервисов от неавторизованного доступа. В частности, необходимо рассматривать следующие меры и средства управления информационной безопасностью:

- следует распределять ответственность за поддержание сетевых ресурсов и компьютерных операций;
- следует устанавливать процедуры и обязанности по управлению удаленным оборудованием, включая оборудование, установленное у конечных пользователей;
- если необходимо, специальные средства контроля следует внедрять для обеспечения конфиденциальности и целостности данных, проходящих по общедоступным сетям, а также для защиты подключенных систем.

Контроль сетевого доступа

Цель: защита сетевых сервисов.

Доступ как к внутренним, так и к внешним сетевым сервисам должен быть контролируемым. Это необходимо для уверенности в том, что пользователи, которые имеют доступ к сетям и сетевым сервисам, не компрометируют их безопасность, обеспечивая:

- соответствующие интерфейсы между сетью организации и сетями, принадлежащими другим организациям, или общедоступными сетями;
- соответствующие механизмы аутентификации в отношении пользователей и оборудования;
- контроль доступа пользователей к информационным сервисам.

Политика в отношении использования сетевых служб

Несанкционированные подключения к сетевым службам могут нарушать информационную безопасность целой организации. Пользователям следует обеспечивать непосредственный доступ только к тем сервисам, в которых они были авторизованы. Контроль доступа, в частности, является необходимым для сетевых подключений к важным или критичным приложениям или для пользователей, находящихся в зонах высокого риска, например, в общественных местах или за пределами организации вне сферы непосредственного управления и контроля безопасности со стороны организации.

Следует предусматривать меры безопасности в отношении использования сетей и сетевых сервисов.

При этом должны быть определены:

- сети и сетевые услуги, к которым разрешен доступ;
- процедуры авторизации для определения, кому, к каким сетям и сетевым сервисам разрешен доступ;
- мероприятия и процедуры по защите от несанкционированного подключения к сетевым сервисам.

Необходимо, чтобы эти меры согласовывались с требованиями в отношении контроля доступа.

Рассматривая работу в локальных сетях, необходимую для обеспечения безопасности в школе и дома, остановимся на вопросах основ безопасности при работе в сетях, принципах построения защищенных операционных систем (ОС), основных угрозах при работе в сети, основных мерах безопасности при работе в сети.

Основы безопасности при работе в сетях

В современном информационном мире, когда все компьютеры, объединенные в локальную сеть, имеют доступ в Интернет, актуальными становятся вопросы защиты от взлома злоумышленниками.

Рассмотрим основные принципы построения защищенных операционных систем:

- все современные ОС являются *многопользовательскими* — они рассчитаны на работу в системе (в том числе одновременную) нескольких пользователей;
- чтобы отличить одного пользователя от другого, применяются *учетные записи* (accounts) с уникальными *именами* и *паролями*;
- учетные записи различаются *уровнем полномочий (привилегий, прав)* — набором действий, которые обладатель данной учетной записи может выполнять в системе. Обычно учетные записи разделяют на *административные,* обладающие максимальными привилегиями, и *пользовательские,* набор полномочий для которых позволяет нормально работать в системе, но не разрешает выполнять какие-либо критичные с точки зрения безопасности данных операции, например, форматировать разделы жесткого диска или менять настройки сети.

  В различных версиях ОС Windows дополнительно существуют учетные записи с уровнем прав, средним между административным и пользовательским (участники группы «Опытные пользователи»), а также обладающие минимальными

полномочиями *гостевые учетные записи* (участники группы «Гости», включая встроенную учетную запись «Гость»).

Кроме того, существует два типа учетных записей — *локальные* из базы данных конкретного компьютера с ОС Windows, и *глобальные учетные записи в домене,* которые хранятся на контроллерах домена (подробнее о них будет сказано далее);

- для входа в компьютер обязательно нужно указать имя и пароль учетной записи, зарегистрированной в системе. Следует подчеркнуть, что понятие «вход в систему» подразумевает не только непосредственный доступ, но и другие возможности работы с компьютером, например, *сетевой* или *терминальный* вход, для которых также требуются пользовательские имя и пароль.

  В операционных системах Windows допускается также сетевой вход без указания имени и пароля *(анонимный* вход); такие подключения используются при некоторых взаимодействиях в сетях Microsoft;
- после входа в систему (интерактивного, сетевого и т. д.) пользователь получает доступ к ресурсам того компьютера, в который он вошел (например, доступ к локальным файлам или каталогам). Уровень доступа при этом определяется *списком разрешений,* т. е. возможных действий, которые данный пользователь может осуществлять с защищенным объектом. Например, один пользователь может изменить или удалить файл, другой — только прочитать его, а третьему вообще будет отказано в доступе к этому файлу.

Основные угрозы при работе в сети

Угроз, поджидающих пользователей при подключении компьютера к сети, довольно много. Мы приведем только основные из них:

- *«взлом» компьютера* обычно производится с целью захвата контроля над операционной системой и получения доступа к данным;
- *повреждение системы* чаще всего организуется, чтобы нарушить работоспособность (вызвать отказ в обслуживании — «Denial of Service») каких-либо сервисов или компьютера (чаще сервера) целиком, а иногда — даже всей сетевой инфраструктуры организации;
- *кража данных* из-за неправильно установленных прав доступа, при передаче данных или «взломе» системы позволяет

получить доступ к защищаемой, часто — конфиденциальной информации со всеми вытекающими отсюда неприятными для владельца этих данных последствиями;
- *уничтожение данных* имеет целью нарушить или даже парализовать работу систем, компьютеров, серверов или всей организации.

Атаки на компьютеры или серверы, вирусы, «черви», шпионские и «троянские» программы — все это злонамеренное ПО пишется для того, чтобы осуществить в той или иной степени перечисленные выше угрозы.

Основные меры безопасности при работе в сети

Меры безопасности при работе в сети довольно просты. Их можно сформулировать в виде следующего набора правил:
- отключайте компьютер, когда вы им не пользуетесь. Как любят говорить эксперты по компьютерной безопасности, «самым защищенным является выключенный компьютер, хранящийся в банковском сейфе»;
- своевременно обновляйте операционную систему. В любой ОС периодически обнаруживаются так называемые *«уязвимости»*, снижающие защищенность вашего компьютера. Наличие уязвимостей нужно внимательно отслеживать (в том числе читая «компьютерную» прессу или информацию в Интернете), чтобы вовремя предпринимать меры для их устранения.

Рекомендации по защите компьютеров

Для ОС Windows корпорацией Microsoft создан специальный веб-узел Windows Update, обратившись к которому (например, с помощью программы WUPDMGR.EXE или команды **Windows Update** или **Центр обновлений** в меню **Пуск),** нетрудно просмотреть и скачать список обновлений, рекомендуемых для вашего компьютера:
- используйте ограниченный набор хорошо проверенных приложений, не устанавливайте сами и не разрешайте другим устанавливать на ваш компьютер программы, взятые из непроверенных источников (особенно из Интернета). Если приложение больше не нужно, удалите его;
- без необходимости не предоставляйте ресурсы своего компьютера в общий доступ. Если же это все-таки потребова-

лось, обязательно настройте минимально необходимый уровень доступа к ресурсу только для зарегистрированных учетных записей;

- установите (или включите) на компьютере персональный межсетевой экран (брандмауэр). Если речь идет о корпоративных сетях, установите брандмауэры как на маршрутизаторах, соединяющих вашу локальную сеть с Интернетом, так и на всех компьютерах сети;
- обязательно установите на компьютер специализированное антивирусное и «антишпионское» программное обеспечение. Настройте его на автоматическое получение обновлений как минимум один раз в неделю (лучше — ежедневно или даже несколько раз в день);
- даже если вы единственный владелец компьютера, для обычной работы применяйте пользовательскую учетную запись: в этом случае повреждение системы, например, при заражении вирусом, будет неизмеримо меньше, чем если бы вы работали с правами администратора. Для всех учетных записей, особенно административных, установите и запомните сложные пароли.

Сложным считается пароль, содержащий случайную комбинацию букв, цифр и специальных символов, например, jxglrg$N. Разумеется, пароль не должен совпадать с именем вашей учетной записи.

Пароль в виде случайной последовательности символов нелегко запомнить, поэтому часто используют следующую технику — пароль набирается в английской раскладке русскими буквами. Например, слово «Пароль» тогда будет выглядеть как «Gfhjkm». Однако этот способ следует применять с осторожностью — взломщики давно имеют целые словари подобным образом преобразованных слов, так что желательно вставлять в такие пароли специальные символы и цифры.

Пароли для доступа в различные системы должны быть разными. Недопустимо использовать один и тот же пароль для администрирования вашего компьютера и для входа, например, на игровой веб-сайт;

- при работе с электронной почтой никогда сразу не открывайте вложения, особенно полученные от неизвестных отправителей. Сохраните вложение на диск, проверьте его антивирусной программой и только затем откройте. Если есть такая возможность, включите в вашей почтовой программе защиту от потенциально опасного содержимого и отключите поддержку HTML;

- при работе с веб-сайтами соблюдайте меры разумной предосторожности: старайтесь избегать регистрации, не передавайте никому персональные сведения о себе и внимательно работайте с Интернет-магазинами и другими службами, где применяются онлайновые способы оплаты с помощью кредитных карт или систем типа WebMoney, Яндекс-Деньги и т. д.;
- при проведении оплаты убедитесь, что соединение защищено шифрованием с помощью технологии Secure Sockets Layer (SSL) — в этом случае адресная строка обязательно должна начинаться с «https://»;
- перечисленные выше меры лишь повышают общую защищенность системы и данных, но не дают никакой гарантии от их повреждения или даже полной потери. Поэтому обязательно следует создавать резервные копии системы и данных на съемном жестком диске или на DVD-RW — это позволит вам легко восстановить их в случае утери. При этом одну копию имеет смысл хранить вне дома, например, в сейфе;
- исключительно важную роль играет обучение всех пользователей основам безопасной работы в сетях — как в домашних, так и в корпоративных, — ведь нарушение правил одним пользователем ставит под угрозу всю систему защиты.

Защита локальной сети и данных актуальна на всех уровнях корпоративной инфраструктуры, т. к. затрагивает безопасность серверов и рабочих станций. Microsoft предлагает целостное решение по построению информационной системы, основанной на серверной платформе Windows Server 2008 R2 и рабочих станциях Windows Vista и Windows 7.

В систему защиты сети и данных от несанкционированного доступа входят следующие технологии:

- Система управления доступом.
- Система аудита.
- Система аутентификации пользователей.
- Аутентификация с использованием смарт-карт.
- Политика на ограничение использования программ.
- Служба управления правами.
- Центр сертификации.
- Встроенные средства шифрования.
- Шифрующая файловая система EFS.
- Поддержка протокола IPSec.
- Безопасность беспроводных соединений.
- Организация виртуальных частных сетей (VPN).

Для защиты компьютеров дома или в сети можно использовать брандмауэр.

Брандмауэр — это программное или аппаратное обеспечение, которое блокирует атаки хакеров и не позволяет вирусам и вирусам-червям попасть на компьютер через Интернет.

Если компьютер используется дома, включение брандмауэра —эффективный и важный этап его защиты. Если сеть развернута дома, необходимо защитить каждый входящий в нее компьютер. Для защиты сети служит аппаратный брандмауэр, например, маршрутизатор. Кроме того, на каждом компьютере следует установить программный брандмауэр для блокировки распространения вируса в случае, если один из компьютеров все же будет заражен.

Если компьютер используется в сети школы или другой организации, то соблюдайте политику, заданную администратором сети. Администраторы могут настраивать все компьютеры в сети так, что включить брандмауэр нельзя, пока они подключены к сети. В этом случае о необходимости включения брандмауэра на конкретном компьютере можно узнать у администратора сети.

Брандмауэр входит в состав большинства операционных систем Windows, начиная с Windows XP.

ПРАКТИЧЕСКАЯ ЧАСТЬ МОДУЛЯ 5

Практическое задание

Настройка локальной сети школы с учетом требований по минимизации угроз информационной безопасности.

Рекомендации:

- определите периметр локальной сети и средства его защиты;
- разделите ЛВС на несколько физических и/или логических сегментов (компьютеры администрации, методические объединения, компьютерные классы, библиотека и т. д.);
- выделите общие и разделенные (тематические, групповые и т. д.) информационные ресурсы ЛВС (папки: общие, метод. объединений, компьютерных классов; почтовый сервер; база данных библиотеки; принтеры и т. д.);
- выделите ответственных (собственников) информационных ресурсов и выработайте совместно с ними процедуру предоставления доступа к их ресурсам;

- выделите критичные информационные ресурсы и учебные процессы, тесно интегрированные с информационными технологиями (компьютеры и файлы администрации и т. д.);
- выделите особо уязвимые компоненты (компьютерные классы, точки доступа WiFi, удаленный доступ и т. д.);
- определитесь с необходимыми средствами защиты каждого из компонентов (не забудьте о резервном копировании и централизованном обновлении);
- максимально документируйте все ваши действия, создавайте и актуализируйте схемы;
- разработайте документы, содержащие хотя бы общие планы действий для разных экстренных ситуаций (вирусное заражение, удаление файлов с отчетами с сетевого диска секретариата, недоступность ресурсов Интернета с рабочего места завуча и т. д.);
- совместно с другими преподавателями выработайте модель общения с учениками в разнообразных нестандартных ситуациях, связанных с использованием информационных технологий (ученик скопировал на общий ресурс фотографии с неприличным содержанием, ученик пытается использовать ПО для получения пароля администратора системы и т. д.).

Вопросы

1. Можно ли сообщить хорошо успевающему ученику пароль администратора домена?
2. Стоит ли использовать один пароль для разных информационных систем и почему?
3. Какие преимущества дает централизованное администрирование компьютеров и серверов (домен)?
4. Сколько резервных копий критичных данных нужно иметь и где их хранить?
5. Доступ к каким категориям ресурсов сети Интернет необходимо блокировать в соответствии с законодательством РФ?
6. На всех ли компьютерах можно разрешить использовать внешние устройства (флешки, фотоаппараты, смартфоны и т. д.) и почему?
7. Стоит ли разрешать неконтролируемое подключение мобильных устройств (КПК, смартфонов, ноутбуков и т. д.) к ЛВС школы?
8. Правильно ли располагать компьютеры классов информатики и компьютеры администрации в одном сегменте?
9. Какие действия вы предпримете, если заподозрите что в вашей сети появились зараженные компьютеры?

10. Нужно ли контролировать посещение учениками ресурсов социальных сетей и форумов и в каком объеме (запретить все, разрешить только «доверенные ресурсы», журналировать все действия учеников на этих ресурсах и т. д.)?
11. Использовать в работе школы или нет ЭЦП и если использовать, то для каких целей?

Используемые литература и ресурсы

1. Сайт Федерального агентства по техническому регулированию и метрологии ГОСТ Р 50922—2006 ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Защита информации. Основные термины и определения [Электронный ресурс]. — URL: http://protect.gost.ru/v.aspx?control=8&baseC=6&page=0&month=6&year=2008&search=50922&RegNum=1&DocOnPageCount=15&id=121129&pageK=E10BFA12-ED02—4212—8D58—3F1D91F314A0

2. Основы компьютерных сетей: Учебное пособие. — 3-е изд., испр. и доп. — М.: БИНОМ. Лаборатория знаний, 2007. — 160 с.

3. Национальный стандарт Российской Федерации. ГОСТ Р ИСО/МЭК 17799—2005 Информационная технология. Практические правила управления информационной безопасностью. ISO/IEC 17799: 2000 Information technology — Code of practice for information security management (IDT) Издание официальное. Москва Стандартинформ 2006

4. Защитите свой компьютер: брандмауэр, безопасность при работе в Интернете. Что такое брандмауэр? [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/computer/basics/firewall.mspx

5. Защитите свой компьютер: брандмауэр, безопасность при работе в Интернете. Выберите оптимальный брандмауэр для своей версии системы Windows [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/computer/firewall/using.mspx —

6. Взлом и защита локальной сети [Электронный ресурс]. — URL: http://virusinfo.info/showthread.php?t=29760

Модуль 6
КОМПЬЮТЕРНЫЕ ВИРУСЫ И СРЕДСТВА ЗАЩИТЫ

Тема 6.1
ОБЗОР И СПОСОБЫ КЛАССИФИКАЦИИ КОМПЬЮТЕРНЫХ ВИРУСОВ

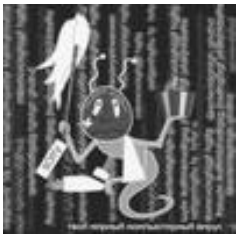
Способы распространения вирусов

Для того чтобы персональные компьютеры дома или локальная сеть в образовательном учреждении не оказались под угрозой заражения вирусами, необходимо представлять не только что это такое и к каким последствиям это может привести, но и быть осведомленными в вопросах борьбы с вирусами. Ознакомимся с тем, что представляют из себя вирусы.

Вирусы — это фрагменты программного кода, которые видоизменяют другие программы на компьютере при приведении их в действие. Они могут распространяться как вложения в электронные письма, храниться на сайтах ваших коллег и друзей по интересам и ждать, когда вы их скачаете, или же храниться на сайтах, принимая вид полезных файлов.

Прежде чем вирус нанесет вред, он должен начать работать. Например, кто-то присылает вам вирус, а вы, не зная того, сохраняете его как вложение в электронное письмо, и он «поселяется» на вашем жестком диске; но пока он не начал работать, вы не заражены.

Наиболее распространенный способ заставить вирус работать — сделать двойной



щелчок и открыть файл, содержащий спрятанный в нем вирус. Зараженный файл может быть чем угодно — от картинки до музыки и даже setup-файлом для новых программ, скачанных вами из Интернета.

Было время, когда открытие зараженного вложения было единственным способом заставить скрытую программу-вирус работать, но писатели вирусов отладили этот процесс так, что некоторые вирусы начинают работать автоматически. В 2005—2006 году в Microsoft была внедрена методика написания безопасного для атак кода, до сих пор не применяемая большинством других разработчиков.

История вредоносных программ

Мнений по поводу рождения первого компьютерного вируса очень много. Нам доподлинно известно только одно: на машине Чарльза Бэббиджа, считающегося изобретателем первого компьютера, вирусов не было, а на Univax 1108 и IBM 360/370 в середине 1970-х годов они уже были.

Обратимся к истории массовых вирусных атак. Когда и с чего это все началось? В 1988 году произошла первая массовая компьютерная эпидемия — эпидемия червя Морриса, и Американская ассоциация компьютерного оборудования объявила 30 ноября международным Днем защиты информации (Computer Security Day).

Несмотря на это, сама идея компьютерных вирусов появилась значительно раньше. Отправной точкой можно считать труды Джона фон Неймана по изучению самовоспроизводящихся математических автоматов. Эти труды стали известны в 1940-х годах. А в 1951 г. знаменитый ученый предложил метод, который демонстрировал возможность создания таких автоматов. Позднее, в 1959 г., журнал «Scientific American» опубликовал статью Л. С. Пенроуза, которая также была посвящена самовоспроизводящимся механическим структурам. В отличие от ранее известных работ, здесь была описана простейшая двумерная модель подобных структур, способных к активации, размножению, мутациям, захвату. Позднее по следам этой статьи другой ученый — Ф.Ж. Шталь — реализовал модель на практике с помощью машинного кода на IBM 650.

Необходимо отметить, что с самого начала эти исследования были направлены отнюдь не на создание теоретической основы

для будущего развития компьютерных вирусов. Наоборот, ученые стремились усовершенствовать мир, сделать его более приспособленным для жизни человека. Ведь именно эти труды легли в основу многих более поздних работ по робототехнике и искусственному интеллекту. И в том, что последующие поколения злоупотребили плодами технического прогресса, нет вины этих замечательных ученых.

В 1962 г. инженеры из американской компании Bell Telephone Laboratories — В. А. Высотский, Г. Д. Макилрой и Роберт Моррис — создали игру «Дарвин». Игра предполагала присутствие в памяти вычислительной машины так называемого супервизора, определявшего правила и порядок борьбы между собой программ-соперников, создававшихся игроками. Программы имели функции исследования пространства, размножения и уничтожения. Смысл игры заключался в удалении всех копий программы противника и захвате поля битвы.

На этом теоретические исследования ученых и безобидные упражнения инженеров ушли в тень, и совсем скоро мир узнал, что теория саморазмножающихся структур с не меньшим успехом может быть применена и в несколько иных целях (по материалам сайта http://www.viruslist.com/ru/viruslist.html).

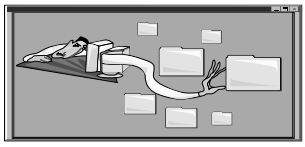
От истории перейдем к вирусной терминологии, владение которой поможет ориентироваться в компьютерном мире и находить правильные методы защиты от проникновения вирусов в домашние и школьные компьютеры.

Вирусная терминология

Познакомьтесь с некоторыми из терминов, обычно используемых в разговоре о вирусах, такими, как: вредоносный код, вирус, червь, антивирусная программа и база, уязвимость, программы удаленного администрирования, клавиатурные шпионы. А также рассмотрим некоторую классификацию вирусов.

Вредоносный код. Любая часть компьютерного кода, обычно программа, которая может нанести вред или отрицательно воздействовать на компьютер.

Вирус. Программа, которая заражает компьютер и изменяет другие программы (включая операционную систему).



Червь. Тип вируса, который может распространяться, не заражая отдельные программы или файлы. Большинство

червей распространяется по электронной почте или через компьютеры, объединенные в сеть.

Антивирусная программа. Антивирусный сканер или программа, которая оценивает данные на жестком диске или входящие данные и определяет, не содержат ли они компьютерные вирусы.

Антивирусная база. База данных известных вирусов, которую имеет любая компания, производящая антивирусные программы. База данных вирусов обновляется по мере того, как появляются и распространяются новые вирусы. Технические характеристики каждого вируса использованы как критерии, по которым антивирусный сканер оценивает файлы, выполняя поиск зараженных файлов.

Уязвимость. Любая ошибка или ряд особенностей, которые дают хакеру или вирусу возможность недозволенного входа в машину. Когда разработчикам программ становится известно об уязвимостях, они выпускают патчи, которые пользователи должны скачать и установить, чтобы ликвидировать уязвимость.

Программы удаленного администрирования (Backdoor' Trojans). Программы, которые прячутся на вашем компьютере, пытаясь избежать обнаружения во время совершения несанкционированных действий.

Клавиатурные шпионы. Это программы, записывающие щелчки мыши, нажатия клавиш и иногда скриншоты во время работы на компьютере. Они создают запись событий, которая может быть послана по электронной почте или прочитана злоумышленниками, если они имеют непосредственный доступ к вашему компьютеру.

Классификация вирусов

Операционная система или приложение может подвергнуться вирусному нападению в том случае, если она имеет возможность запустить программу, не являющуюся частью самой системы. Данному условию удовлетворяют все популярные «настольные» операционные системы, многие офисные приложения, графические редакторы, системы проектирования и прочие программные комплексы, имеющие встроенные скриптовые языки.

Если операционная система существует в единичных экземплярах, то вероятность ее злонамеренного использования близка к нулю. Если же производитель системы добился ее массового распространения, то очевидно, что рано или поздно хакеры и вирусописатели попытаются использовать ее в своих интересах. Чем популярнее операционная система или приложение, тем чаще она

будет являться жертвой вирусной атаки. Практика это подтверждает — распределение количества вредного программного обеспечения для Windows и Linux практически совпадает с долями рынка, которые занимают эти операционные системы.

По масштабу вредных воздействий, которые могут нанести вирусы, их можно разделить на 4 группы (рис. 1).

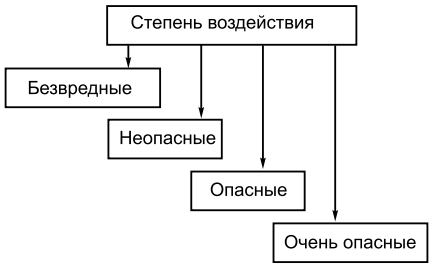


Рис. 1

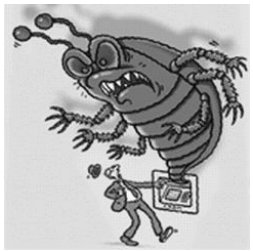
Безвредные уменьшают свободную область на диске за счет своего размножения.

Неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках.

Действия таких вирусов проявляются в каких-либо графических или звуковых эффектах. Но даже если в алгоритме вируса не найдено ветвей, наносящих ущерб системе, этот вирус нельзя с полной уверенностью назвать безвредным, так как проникновение его в компьютер может вызвать непредсказуемые и порой катастрофические последствия.

Опасные вирусы, которые могут привести к различным нарушениям в работе компьютера.

Очень опасные, воздействие которых может привести к безвозвратной потере программ, уничтожению данных, стиранию информации в системных областях диска.



В настоящее время известны тысячи компьютерных вирусов, которые можно классифицировать по следующим признакам (рис. 2).

В зависимости от **среды обитания** вирусы можно разделить на сетевые, файловые, загрузочные (рис. 3).

Сетевые вирусы распространяются по различным компьютерным сетям. Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

Файловые вирусы внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE, и активируются при их запуске. Находятся в оперативной памяти до выключения компьютера.

Рис. 2

Рис. 3

Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record). При загрузке операционной системы с зараженного диска внедряются в оперативную память и ведут себя как файловый вирусы.

Макровирусы — являются макрокомандами, которые заражают файлы документов Word, Excel, находятся в оперативной памяти до закрытия приложения.

Драйверные вирусы — заражают драйверы устройств компьютера или запускают себя путем включения в файл конфигурации дополнительной строки.

Вирус не может содержаться в ASCII-текстах, графических или звуковых файлах, т. к. он является программой и требует исполнения своего кода.

Самые распространенные вирусы

На сегодняшний день очень популярными являются вирусы, которые называют червями.

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. Некоторые черви обладают также свойствами других разновидностей вредоносного программного обеспечения, например, содержат троянские функции или способны заражать выполняемые файлы на локальном диске, т. е. имеют свойство троянской программы. Троянские программы осуществляют различные не санкционированные пользователем действия, например, сбор информации и передачу ее злоумышленнику, 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.

Сведения о самых распространенных угрозах и потенциально нежелательных программах можно всегда найти на портале Центра Microsoft по защите от нежелательных программ (http://www.microsoft.com/rus/protect/products/computer/malwareprotectioncenter.mspx). А также специалисты «Лаборатории Касперского» постоянно информируют о новых угрозах, новых появившихся вирусах (*http://www.securelist.com/ru/descriptions)*.

Макровирусы

Переходя к рассмотрению макровирусов, особое внимание обратим на вирусы, распространяющиеся по глобальной сети через электронную почту и телеконференции.

Итак, основным источником вирусов на сегодняшний день является глобальная сеть Интернет. Наибольшее число заражений вирусом происходит при обмене письмами в форматах Word/Office. Особо широкое распространение в последнее время получили макровирусы.

Макровирусы — программы, написанные на языке макропоследовательностей программ Microsoft Word и Excel. Макровирусы записываются в документы и шаблоны документов Word и Excel. Открыв документ, зараженный макровирусом, вы заразите стандартный шаблон документов, находящийся на вашем компьютере, а через него все документы, которые будете открывать в дальнейшем. Уже существует множество разновидностей макровирусов — от достаточно безобидных до удаляющих системные и программные файлы и форматирующих жесткий диск. Пользователь зараженного макровирусом редактора, сам того не подозревая, рассылает зараженные письма адресатам, которые, в свою очередь, отправляют новые зараженные письма, и т. д.

Нередки случаи, когда зараженный файл-документ или таблица Excel по причине недосмотра попадает в списки рассылки коммерческой информации какой-либо крупной компании. В этом случае страдают сотни или даже тысячи абонентов таких рассылок, которые затем разошлют зараженные файлы десяткам тысяч своих абонентов.

Файл-серверы «общего пользования» и электронные конференции также служат одним из основных источников распространения вирусов. Практически каждую неделю приходит сообщение о том, что какой-либо пользователь заразил свой компьютер вирусом, который был снят с BBS, FTP-сервера или получен из какой-либо электронной конференции.

Теперь обратимся к такому понятию, как **«цикл функционирования вируса»**.

В цикле функционирования или существования любого вируса можно выделить три этапа.

Первый этап: вирус находится в **неактивном состоянии**. В этом состоянии он внедрен в тело исполняемого файла или находится в загрузочном секторе диска и «ждет» своего часа. Именно в неактивном состоянии вирусы переносятся вместе с программами или дискетами от одного ПК к другому. Для того чтобы он начал свою работу, необходимо запустить исполняемый файл или загрузиться с зараженной дискеты. В этот момент **активизируется вирус**, кото-

рый либо **создает резидентную** в памяти **программу**, способную порождать копии или производить какие-то разрушительные действия, либо **немедленно приступает к работе.**

Если вирус создал резидентную программу, то ее активизация осуществляется различными способами — все зависит от фантазии автора вируса.

Второй этап жизнедеятельности вируса — это этап активного размножения, поэтому вирусная программа стремится максимально скрыть от пользователя ПК результаты своей деятельности.

Третий этап: после того как заражено достаточно много файлов, наступает этап, связанный с внешними проявлениями работы вируса. Ваш компьютер вдруг начнет вести себя странно: зазвучит музыкальная фраза или начнут «сыпаться» символы на экране дисплея. Некоторые вирусы к этому моменту могут уже безвозвратно нарушить файловую структуру.

Методы борьбы с вирусами

Защита информации от преднамеренного искажения или уничтожения — это защита от вирусов. Здесь эффективен комплекс мер, включающий в себя профилактические (использование антивирусных программ) и общие методы защиты.

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов.

Вот несколько основных признаков того, что компьютер может быть заражен вирусом:

- Компьютер работает медленнее, чем обычно.
- Компьютер перестает отвечать на запросы и часто блокируется.
- Каждые несколько минут происходит сбой и компьютер перезагружается.
- Компьютер самопроизвольно перезагружается и после этого работает со сбоями.
- Установленные на компьютере приложения работают неправильно.
- Диски или дисководы недоступны.
- Не удается выполнить печать.
- Появляются необычные сообщения об ошибках.
- Открываются искаженные меню и диалоговые окна.

Это типичные признаки заражения. Однако они характерны и для неполадок программного обеспечения или оборудования, не имеющих ничего общего с вирусами. Пока на компьютере не запущено **средство удаления вредоносных программ Microsoft** и не установлена последняя версия **антивирусного программного обеспечения**, соответствующего отраслевым стандартам, нельзя с уверенностью сказать, заражен ли компьютер вирусом.

Одним из основных методов борьбы с вирусами является, как и в медицине, своевременная профилактика. Компьютерная профилактика предполагает соблюдение небольшого числа правил, которые позволяют значительно снизить вероятность заражения вирусом и потери каких-либо данных. Если компьютер не защищен при подключении к Интернету, хакеры могут получить доступ к личным сведениям пользователя. Они могут установить программный код, который уничтожит файлы или вызовет сбои в работе, либо использовать компьютер для атак на другие домашние или офисные компьютеры, подключенные к Интернету.

Для того чтобы не подвергнуть компьютер заражению вирусами и обеспечить надежное хранение информации, необходимо соблюдать следующие правила:

1. При переносе на свой компьютер файлов в архивированном виде проверяйте их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами.

2. Всегда защищайте свои носители информации от записи при работе на других компьютерах, если на них не будет производиться запись информации.

3. Обязательно делайте архивные копии ценной для вас информации.

4. Используйте **брандмауэр Интернета**. Брандмауэр — это программное или аппаратное обеспечение, которое блокирует атаки хакеров и не позволяет вирусам и вирусам-червям попадать на компьютер через Интернет. Если вы пользуетесь компьютером дома или на малом предприятии, применение брандмауэра — самое эффективное и важное действие по защите компьютера. Очень важно включить брандмауэр и антивирусную программу *до* подключения к Интернету.

5. Посетите **Центр обновления Microsoft** и включите функцию **автоматического обновления**. (Если на компьютере установлен пакет Office 2003 или Office XP, он будет обновляться автоматически. Если используется более ранняя версия пакета Microsoft Office, посетите **Центр загрузки Office**.)

6. Подпишитесь на получение **стандартного антивирусного программного обеспечения** и регулярно обновляйте его.

7. Никогда не открывайте вложения в сообщениях электронной почты, полученных от незнакомых людей.

8. Не открывайте также вложенные файлы в сообщениях, полученных от знакомых, если характер содержимого точно не известен. Отправитель может и не подозревать о наличии вируса в сообщении.

9. Чтобы наверняка не заразиться макровирусом, на вкладке **Общие параметры настройки** диалогового окна **Параметры**, вызываемого командами **меню Сервис/Параметры** Word и Excel, воспользуйтесь пунктом **Защита от вирусов в макросах.**

10. При попытке открыть документ, содержащий автоматически выполняющуюся макропоследовательность, программа предупредит об этом и предложит отменить выполнение подозрительного макроса, который может оказаться макровирусом.

Портал Центра Microsoft по защите от нежелательных программ (Microsoft Malware Protection Center, MMPC)

Это интерактивный веб-портал, который содержит сведения о новых угрозах безопасности компьютера и мерах борьбы с ними. Этот портал служит для сообщения пользователям результатов исследований Центра по защите от нежелательных программ в области вредоносных программ и мер борьбы с ними.

Портал Центра Microsoft по защите от нежелательных программ включает приведенные ниже разделы и сведения:

- Энциклопедия вредоносных программ. Здесь можно узнать о конкретном вирусе или другой угрозе с помощью функции поиска в энциклопедии.
- Описание способа отправки образцов для испытаний. В этом разделе можно отправить файлы, которые, по вашему мнению, могут быть заражены вредоносными или нежелательными программами. Специалисты Центра проведут анализ этих файлов и на вашу электронную почту будут высланы результаты анализа файлов.

- Новейшие сигнатуры вирусов для **Защитника Windows.** Вредоносные программы постоянно меняются. Здесь можно получить мгновенный доступ к новейшим описаниям угроз.
- Сведения о самых распространенных угрозах и потенциально нежелательных программах, предоставленные пользователями, которые сообщают о них в Центр MMPC, а также по сведениям, полученным от продуктов по обеспечению безопасности компании Microsoft, таких как **средство удаления вредоносных программ**, **Защитник Windows**. В этом разделе можно получить новейшие сведения о десяти самых распространенных категориях угроз, про которых сообщают пользователи. Каждая угроза сопровождается ссылкой для отображения дополнительных сведений.

Тема 6.2
АНТИВИРУСНЫЕ И АНТИШПИОНСКИЕ ПРОГРАММЫ

Ничто не может гарантировать полную безопасность компьютера. Чтобы повысить защиту компьютера и снизить вероятность заражения вирусами, используйте **брандмауэр** (система Windows XP с пакетом обновления 2 (SP2) содержит брандмауэр, который по умолчанию включен), регулярно обновляйте систему, своевременно обновляйте **антивирусное программное обеспечение** и следуйте основным рекомендациям.

Антишпионские программы помогают защитить компьютер от всплывающих окон, снижения производительности и угроз безопасности, вызванных программами-шпионами и другими нежелательными программами.

Для обнаружения, удаления вирусов и защиты от них разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными.

Корпорация Microsoft предлагает несколько продуктов для защиты компьютера от вирусов и программ-шпионов. Ниже приведена таблица продуктов и их функций (рис. 4).

Для защиты от программ-шпионов и других нежелательных программ используйте **Защитник Windows**. Он включает систему наблюдения, которая обеспечивает защиту в режиме реального времени, предоставляя рекомендации при обнаружении программ-шпионов и сводя к минимуму нарушения работы. Защитник

Название продукта	Устранение программ-шпионов и других нежелательных программ		Устранение вирусов и вредоносных программ		Проверка по расписанию	Без дополнительной оплаты
	Проверка и удаление	Защита	Проверка и удаление	Защита		
Защитник Windows	✓	✓			✓	✓
Средство проверки безопасности Windows Live OneCare	✓		✓			✓
Средство удаления вредоносных программ			✓			✓
Windows Live OneCare	✓	✓	✓	✓	✓	

Рис. 4

Windows входит в состав системы Windows Vista и бесплатно доступен пользователям Windows XP с пакетом обновления 2 (SP2).

Средство удаления вредоносных программ

Средство удаления вредоносных программ для систем Microsoft Windows проверяет компьютеры на наличие некоторых распространенных вредоносных программ и удаляет их в случае обнаружения.

Программа Windows Live Messenger и средство проверки безопасности Windows Live OneCare можно использовать для удаленного обнаружения и решения практически любых проблем: от устранения вирусов до фрагментации жесткого диска.

Средство проверки безопасности Windows Live OneCare

Веб-служба, которая обеспечивает работоспособность компьютера с помощью бесплатных средств проверки, удаляющих нежелательные программы. Наборы средств безопасности **Windows Live OneCare** работают практически без вмешательства пользователя. Полезные функции Windows Live OneCare:

- Регулярный поиск вирусов: чтобы защитить компьютер от **вирусов, вирусов-червей и программ-троянов**, служба Windows Live OneCare автоматически проверяет файлы и папки,

включая вложения сообщений электронной почты, при их открытии.

- Постоянное отслеживание работы брандмауэра: служба Windows Live OneCare представляет собой двусторонний управляемый брандмауэр, который контролирует исходящий и входящий трафик. Кроме того, для обеспечения защиты брандмауэр регулярно обновляется.
- Улучшенная защита от программ-шпионов: антишпионская технология Windows Live OneCare защищает компьютер от программ-шпионов, тайно отслеживающих действия пользователя, и помогает бороться со всплывающими окнами, отрицательно влияющими на безопасность и производительность компьютера.
- Простое резервное копирование и восстановление: служба Windows Live OneCare позволяет создавать копии важных файлов и документов и сохранять их на DVD- и компакт-дисках или внешнем жестком диске на случай чрезвычайных происшествий. Резервные копии можно создавать вручную, а также автоматически с помощью данной службы, не беспокоясь о регулярном резервном копировании файлов и документов. Служба Windows Live OneCare также позволяет восстановить резервные копии файлов на компьютере при сбоях системы.
- Постоянное обновление: служба Windows Live OneCare обновляется автоматически, поэтому на компьютере всегда используются последние версии антивирусных и антишпионских программ и брандмауэра, что обеспечивает защиту от новейших угроз.

Служба Windows Live OneCare не только помогает защитить компьютер, но и обеспечивает его бесперебойную работу. Чтобы узнать о других возможностях Windows Live OneCare, прочтите **обзор службы Windows Live OneCare**.

В дополнение к перечисленным выше продуктам также возможно использование бесплатной антивирусной программы **Microsoft Security Essentials (MSE)**. Это программа, предназначенная для полноценной защиты домашних компьютеров в режиме реального времени от основных видов вредоносного ПО (вирусов, руткитов, программ-шпионов и т. д.). Она доступна всем пользователям лицензионной операционной системы Windows (рис. 5).

Любое количество копий антивирусной программы Microsoft Security Essentials может быть установлено на компьютерах, принадлежащих вам или членам вашей семьи, при условии, что этими устройствами будут пользоваться в домашних условиях. Также

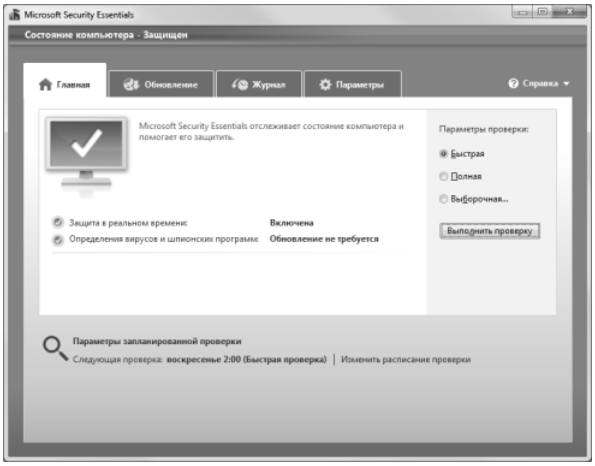


Рис. 5

разрешается использование, связанное с ведением собственного малого бизнеса из дома.

На сайте корпорации Microsoft можно найти необходимую информацию по защите и предотвращению попадания вирусов на ваш компьютер.

ПРАКТИЧЕСКАЯ ЧАСТЬ МОДУЛЯ 6

Тест «Определения вирусов»

Выберите для каждого названия вируса правильное определение

1. **Сетевые вирусы:**
   - распространяются по различным компьютерным сетям;
   - заражают драйверы устройств компьютера или запускают себя путем включения в файл конфигурации;
   - внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска;
   - внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE, и некоторые другие;
   - являются макрокомандами, которые заражают файлы документов Word, Excel.

2. Файловые вирусы:
- распространяются по различным компьютерным сетям;
- заражают драйверы устройств компьютера или запускают себя путем включения в файл конфигурации;
- внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска;
- внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE;
- являются макрокомандами, которые заражают файлы документов Word, Excel.

3. **Загрузочные вирусы:**
- распространяются по различным компьютерным сетям;
- заражают драйверы устройств компьютера или запускают себя путем включения в файл конфигурации;
- внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска;
- внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE;
- являются макрокомандами, которые заражают файлы документов Word, Excel.

4. **Макровирусы**
- распространяются по различным компьютерным сетям;
- заражают драйверы устройств компьютера или запускают себя путем включения в файл конфигурации;
- внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска;
- внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE;
- являются макрокомандами, которые заражают файлы документов Word, Excel.

5. **Драйверные вирусы:**
- распространяются по различным компьютерным сетям;
- заражают драйверы устройств компьютера или запускают себя путем включения в файл конфигурации;
- внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска;
- внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE;
- являются макрокомандами, которые заражают файлы документов Word, Excel.

Итоговый тест

Выберите один или несколько верных ответов.

Что может делать компьютерный вирус?

1) вносить изменения в работу компьютера;
2) отправлять и получать мошеннические сообщения по электронной почте;
3) приводить к частым сбоям и перезагрузке компьютера;
4) все вышеперечисленное.

Как вирус может появиться в компьютере?

1) переместиться с флеш-носителя;
2) при решении математической задачи;
3) при подключении к компьютеру модема;
4) самопроизвольно.

Компьютерным вирусом является...

1) программа проверки и лечения дисков;
2) любая программа, созданная на языках низкого уровня;
3) программа, скопированная с плохо отформатированного флеш-носителя;
4) специальная программа небольшого размера, которая может приписывать себя к другим программам, она обладает способностью «размножаться».

Заражению компьютерными вирусами могут подвергнуться...

1) графические файлы;
2) программы и документы;
3) звуковые файлы;
4) видеофайлы.

На что могут негативно повлиять вирусы?

1) подключение к Интернету;
2) программное обеспечение;
3) оборудование;
4) на все вышеперечисленное.

Какой тип файлов компьютерный вирус не только портит, но и заражает?

1) графические файлы;
2) программные файлы;

3) информационные файлы без данных;
4) медиафайлы.

Какие разновидности вирусов перехватывают обращения операционной системы к пораженным файлам?
1) троянские вирусы;
2) паразитические вирусы;
3) вирусы-черви;
4) вирусы-невидимки (стелс-вирусы).

Самые опасные вирусы, разрушающие загрузочный сектор, — это:
1) троянские вирусы;
2) паразитические вирусы;
3) вирусы-черви;
4) вирусы-невидимки (стелс-вирусы).

Основными путями проникновения вирусов в компьютер являются:
1) флеш-диски;
2) компьютерные сети;
3) больной пользователь;
4) создание файлов в Word, Excel.

Основные меры по защите информации от повреждения вирусами:
1) проверка дисков на вирус;
2) создание архивных копий ценной информации;
3) неиспользование «пиратского» программного обеспечения;
4) передача файлов только по сети.

Если есть признаки заражения вирусом, нужно:
1) проверить диск антивирусной программой;
2) отформатировать диск;
3) пригласить специалиста, чтобы изучить и обезвредить вирус;
4) скопировать свои файлы на флеш-носитель и перейти работать на другой компьютер.

В зависимости от среды обитания вирусы бывают:
1) резидентные;
2) файловые;
3) дисковые;
4) загрузочные.

ПРАКТИЧЕСКИЕ РАБОТЫ

ПРАКТИЧЕСКАЯ РАБОТА 1

Определение оптимизации времени работы антивирусной программы

На диске имеется 400 файлов, которые необходимо с помощью антивирусной программы проверить на наличие вирусов трех типов: A, B и C. Проверка файла на наличие в нем вируса A занимает 2 миллисекунды, проверка файла на вирус B или на вирус C занимает 5 миллисекунд. Антивирусная программа работает так: сначала проверяются все файлы на наличие вируса A (зараженные хоть одним вирусом файлы удаляются!), затем оставшиеся файлы проверяются на вирус B и, наконец, уцелевшие файлы проверяются на вирус C. Достоверно известно, что вирусом A заражены ровно 10 файлов, вирусом B заражено 20 файлов, а вирусом C — 30 файлов. Не исключается при этом, что некоторые файлы могут быть заражены сразу несколькими вирусами.

1) оцените общее время работы программы, определив минимально и максимально возможные значения времени (в миллисекундах), которое может быть затрачено на проверку при указанном порядке действий;

2) изменяя порядок проверок (скажем, сначала проверяем на B, затем на A, а потом на C), можно изменить и общее время. Как следует изменить порядок проверки, чтобы время работы заведомо уменьшилось?

Решение:

Порядок проверок (слева направо)	Минимальное время (мс)	Максимальное время (мс)
ABC (та, что предлаг. в условии)	4600	4650
BAC	4610	4660
ACB	4550	4600
CAB	4540	4590
CBA	4550	4590
BCA	4600	4640

Ответ: 1) $4600 \le t \le 4650$; 2) CAB или CBA.

ПРАКТИЧЕСКАЯ РАБОТА № 2

Бесплатная проверка безопасности компьютера. Настройка компьютера с помощью средства проверки безопасности Windows Live OneCare

http://onecare.live.com/site/ru-ru/tryscanner.htm

Средство проверки безопасности Windows Live OneCare — это новая служба проверки компьютера, которая помогает защищать его, удалять вирусы и поддерживать оптимальный режим работы. Она доступна бесплатно. Для последующей настройки средство проверки безопасности Windows Live OneCare можно запускать неограниченное количество раз (рис. 6).

1. Посетите веб-узел **Средства проверки безопасности Windows Live OneCare**, (http://onecare.live.com/site/ru-ru/default.htm), нажмите кнопку **Проверка всех компонентов и следуйте указаниям на экране**.

2. Средство проверки безопасности Windows Live OneCare загружается и устанавливается во время первой проверки. Оно проверяет компьютер, а затем выводит результаты и рекомендации. Для проверки наличия обновлений можно запустить средство в любое время. Обновления будут содержать новые версии средства проверки и последние сведения для распознавания (определения) вирусов, подготовленные корпорацией Microsoft.

3. Для выборочной проверки системы щелкните соответствующий значок.

	Защита. Поиск и удаление вирусов
	Очистка. Удаление нежелательных файлов с жесткого диска
	Настройка. Повышение общей производительности компьютера

Помимо трех бесплатных проверок безопасности пользователям средства проверки Windows Live OneCare доступны следующие возможности:

- получение оперативной информации об Интернет-угрозах;
- поиск в энциклопедии вирусов Microsoft Virus Encyclopedia;

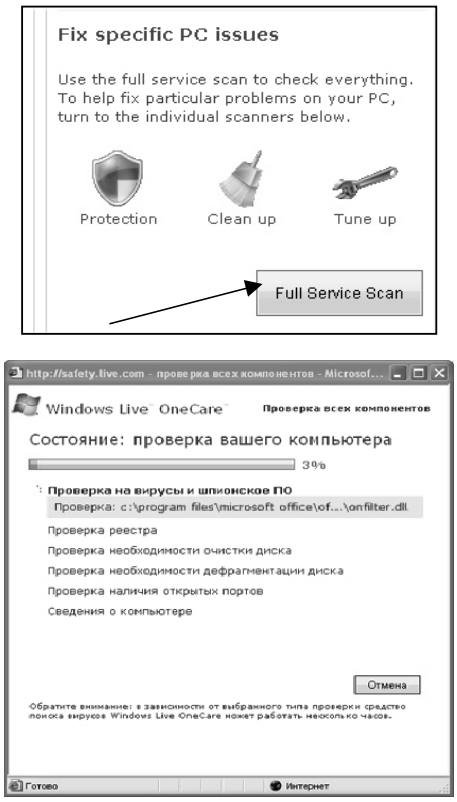


Рис. 6

- ответы на вопросы о работоспособности и безопасности компьютера;
- средства защиты, оптимизации и повышения уровня безопасности компьютера;
- средство очистки реестра, которое позволяет обнаружить и удалить недопустимые или устаревшие элементы реестра.

4. На страницу средства проверки безопасности Windows Live OneCare можно возвращаться каждый раз, когда необходимо проверить все или отдельные компоненты системы. Если нужно выполнять автоматическую проверку в фоновом режиме, подпишитесь на службу Windows Live OneCare, которая позволяет своевременно получать ясные данные об общем уровне защиты и производительности компьютера.

ПРАКТИЧЕСКАЯ РАБОТА 3
Установка и настройка антивируса Microsoft Security Essentials (MSE)

Загрузка и установка программы:

Загрузка и установка Microsoft Security Essentials очень проста и занимает всего несколько минут.

Если на вашем компьютере уже установлено антивирусное ПО, рекомендуется удалить эти программы, поскольку одновременная работа нескольких антивирусных программ может значительно снизить производительность компьютера.

Для загрузки перейдите по адресу **http://www.msantivirus.ru** и нажмите на кнопку Загрузить сейчас. В появившемся диалоге нажмите кнопку «Запустить».

По окончании загрузки вам будет предложено ознакомиться с информацией о программе, условиями лицензионного соглаше-

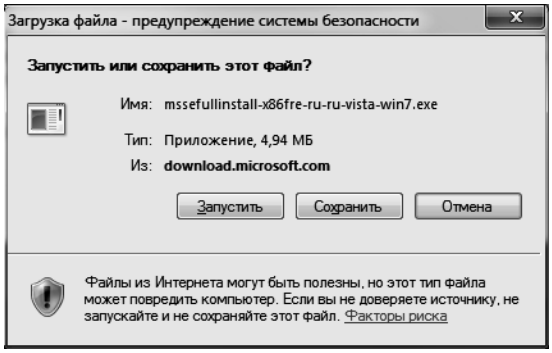


Рис. 7

Рис. 8

ния (3), проверить подлинность операционной системы Windows и завершить установку. По окончании установки нажмите кнопку «Готово».

При первом запуске основные функции программы будут заблокированы до завершения процедуры обновления.

Если у вас нет возможности произвести обновление на компьютере, на котором устанавливается антивирус (например, если компьютер заражен и блокирует доступ к сайту Microsoft для загрузки обновлений), воспользуйтесь ссылкой **http://go.microsoft.com/fwlink/?LinkID=87342** для загрузки обновлений 32-битной версии MSE.

Использование программы:

Microsoft Security Essentials автоматически обеспечивает защиту вашего компьютера от основных угроз в режиме реального времени. Зеленый индикатор MSE в области системных уведомлений свидетельствует о том, что все в порядке и можно продолжать работу.

Проверка по требованию:

MSE обеспечивает защиту в реальном времени, своевременно обнаруживая многие угрозы, однако при необходимости вы можете осуществить проверку в любой момент.

Для этого откройте окно MSE, запустив программу «Microsoft Security Essentials» из меню «Пуск» или дважды щелкнув на значке MSE в области системных уведомлений.

На вкладке «Главная» выберите необходимый уровень проверки:

- быстрая — выполняется анализ областей, заражение которых вредоносными программами, в том числе вирусами, шпионскими и нежелательными программами, наиболее вероятно;
- полная — выполняется анализ всех файлов на жестком диске и запущенных программ;

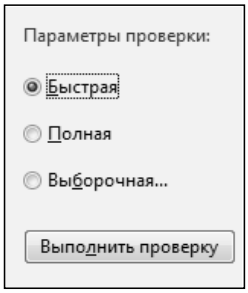


Рис. 9

- выборочная — при проверке осуществляется анализ только выбранных папок.

Нажмите кнопку «Выполнить проверку».

Если вы выбрали пункты «Быстрая» и «Полная», проверка начнется сразу же. При выборе пункта «Выборочная» вам будет предложено выбрать папки, после чего нажмите «ОК» для запуска проверки (рис. 10).

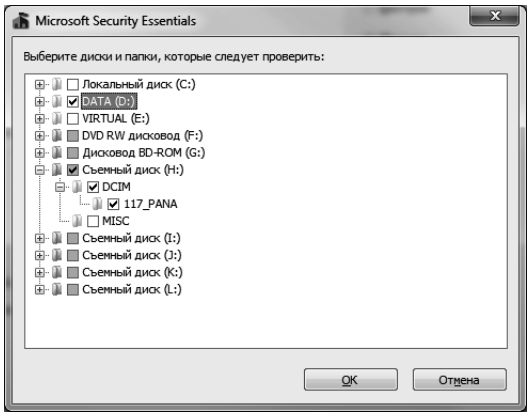
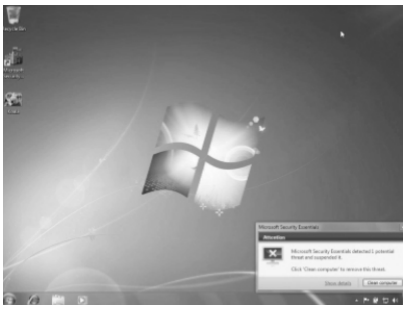


Рис. 10

Обнаружение угрозы:

Если программа обнаруживает угрозу, отображается уведомление с описанием проблемы и значок MSE меняет цвет на желтый или красный в зависимости от степени угрозы.

Красный значок обозначает «Под угрозой» и требует немедленного вмешательства. Например, если по какой-то причине антивирус был отключен, дважды щелкните по значку и нажмите кнопку «Включить».



В случае обнаружения опасности статус программы меняется на «Под угрозой», выводится уведомление и вам предлагается выбрать один из вариантов (действие по умолчанию, удалить или поместить в карантин).

Обнаруженные вирусы и описание угроз вы можете найти во вкладке «Журнал».

Управление программой:

Для того чтобы открыть окно Microsoft Security Essentials, запустите программу «Microsoft Security Essentials» из меню «Пуск» или дважды щелкните на значке MSE 

в области системных уведомлений.

Обновление:

Microsoft Security Essentials загружает и устанавливает обновления автоматически. Для того чтобы произвести обновление вручную, перейдите на вкладку «Обновление» и нажмите кнопку «Обновить».

Для загрузки обновлений вручную воспользуйтесь ссылкой **http://go.microsoft.com/fwlink/?LinkID=87342**, после чего запустите загруженный файл.

Настройка параметров:

Вы можете выполнить следующие настройки:

- Запланированная проверка — настройка расписания и объема проверки компьютера.
- Действия по умолчанию — настройка действия, отображаемого или применяемого, если MSE обнаруживает потенциальную угрозу разных уровней.
- Защита в реальном времени — включение/выключение защиты.
- Исключенные файлы и папки — исключение отдельных файлов или папок из проверки для ускорения обработки (например, архивный файл размером в несколько гигабайт).
- Исключенные типы файлов — исключение из проверки всех файлов определенного типа (например, JPEG, TXT и т. д.).
- Исключенные процессы — исключение определенных процессов (исполняемых файлов с разрешениями CMD, BAT, EXE, COM и др.).
- Дополнительные настройки — включение/выключение проверки архивных файлов, съемных носителей, создание точки восстановления системы перед очисткой компьютера, настройки прав просмотра журнала.
- Microsoft SpyNet — настройка участия в Интернет-сообществе, помогающем выбрать реакцию на потенциальную угрозу и остановить распространение вредоносных программ.

Дополнительная информация:

Ознакомиться с более подробной справкой и инструкциями на русском языке вы можете по ссылке **http://www.microsoft.com/security_essentials/support.aspx?s=1**.

ПРАКТИЧЕСКАЯ РАБОТА 4
Пример работы программы рассылки спама

Известно, что подавляющее число электронных писем представляют собой рекламные сообщения (спам).

Для автоматического выявления таких писем разрабатываются специальные программы, называемые спам-фильтрами. Один из признаков, по которому в потоке сообщений выделяются нежелательные, является рассылка идентичных сообщений большому числу пользователей.

Пытаясь затруднить работу спам-фильтров, программы рассылки спама могут несколько модифицировать рассылаемое сообщение, заменяя некоторые буквы на другие, но совпадающие с ними по написанию (например, «р» в кириллице на «p» в латинице).

Сколько разных сообщений может быть получено из текста «Погрузим ваши апельсины в бочки»?

Ответ: Каждое изменение похожего по написанию символа (а-a, е-e, о-o, р-p, с-c, у-y, в-в) приводит к удвоению числа вариантов написания всей фразы. Поэтому число возможных полученных сообщений, включая исходное, равно 2 в степени числа вхождения указанных символов в сообщение.

Замечание! Можно заметить, что при изменении размера шрифта русскую букву з можно заменить на цифру 3. Ответы, учитывающие данный вариант, будут зачтены как правильные. Однако замена букв к-k не может считаться допустимой, т. к. эти буквы все же разные по написанию.

2^8 или 2^9 с учетом буквы з

Используемые литература и ресурсы

1. Безопасность дома [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/default.mspx

2. Пять действий по защите нового компьютера перед выходом в Интернет [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/computer/advanced/xppc.mspx

3. Бесплатная проверка безопасности компьютера [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/products/computer/safetyscanner.mspx

4. Продукты и службы для обеспечения безопасности: вопросы и ответы [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/products/computer/faq.mspx

5. Защита от программ-шпионов, вирусов и нежелательных программ [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/products/computer/default.mspx

6. Учебные видеоматериалы [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/videos/default.mspx

7. Что представляет собой Windows 7 [Электронный ресурс]. — URL: http://windows.microsoft.com/ru-RU/windows7/products/what-is

8. Программа Windows Live Messenger [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/products/computer/windowslivemessenger.mspx

Приложение

«ЗДОРОВЬЕ И БЕЗОПАСНОСТЬ ДЕТЕЙ В МИРЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНТЕРНЕТА

Программа дополнительного профессионального образования (повышение квалификации)

Программа **«Здоровье и безопасность детей в мире компьютерных технологий и Интернета»** разработана с учетом потребностей образовательных учреждений в области безопасной работы в Интернете. Она ориентирована на руководителей учреждений общего образования, на школьных учителей и методистов, которые заинтересованы в расширении своих компетенций в области применения ИКТ и безопасной работы в сети Интернет. Программа может быть использована как в учреждениях дополнительного профессионального образования, так и в системе методической работы с практическими работниками образования. Методическое приложение к программе рекомендуется использовать при организации просветительской работы с родителями школьников.

Разработана при содействии Microsoft в рамках инициативы «Партнерство в образовании» (проект «Академия учителей»)

Пояснительная записка

В наши дни компьютер становится привычным элементом не только в научных лабораториях, но и дома, в школьных классах. Так, например, в Российской Федерации в настоящее время уже эксплуатируется не менее 5 млн персональных компьютеров. В Западной Европе компьютер используют свыше 60 % взрослого населения. Людей, ежедневно проводящих за компьютером по нескольку часов, становится все больше. При этом уже мало кто сомневается, что работа на персональном компьютере влияет на физическое и психологическое здоровье человека не самым лучшим образом.

Длительное пребывание у экрана, неподвижность позы пользователя ПК, электромагнитные поля и излучения, мелькание изображения на экране — все это небезвредно для здоровья. У пользователей компьютером нарушается зрение, происходит утомление мышц рук, позвоночника, наступает общая слабость. Многолетний опыт использования персональных компьютеров во всех сферах человеческой деятельности, исследования отечественных и зарубежных ученых указывают на компьютер как на объект повышенной опасности для здоровья человека.

Одновременно при масштабном проникновении Интернета в личную сферу жизни и профессиональную деятельность людей возрастает значимость проблемы защиты информации. Только в 2008 году объемы спама в месячном измерении составили почти 83 %. Становится очевидным, что условия безопасной работы, как с точки зрения здоровья, так и в аспекте информационной безопасности пользователей персональных компьютеров приобретают характер международной проблемы.

Одним из средств решения этой проблемы может стать просвещение общественности и специальная подготовка профессионалов, в первую очередь, педагогов, в сфере безопасного поведения человека, специалиста, школьника в мире компьютерных технологий и Интернета.

Предлагаемая программа повышения квалификации управленческих и педагогических кадров является ответом на вызов обозначенной выше ситуации.

В представленной программе рассматриваются здоровьесберегающие технологии, применяемые при организации работы школьника на компьютере, и основные направления профилактики нарушений здоровья детей при работе за компьютером. В ней

освещаются вопросы борьбы с вирусами и методы защиты от них с помощью антивирусных программ.

Программа курса повышения квалификации «Здоровье и безопасность детей в мире компьютерных технологий и Интернета» направлена на формирование навыков поведения в информационном обществе с целью обеспечения информационной безопасности. Она адресована различным категориям специалистов — директорам школ и заместителям директоров школ по информатизации, учителям-предметникам и педагогам дополнительного образования детей, преподавателям и тьюторам учреждений повышения квалификации.

Программа разработана на блочно-модульной основе и представляет совокупность отдельных модулей, которые могут в зависимости от желания и потребностей слушателей изучаться в различной последовательности и различной компоновке, а объем часов на изучение каждого модуля может варьироваться в зависимости от категории обучающихся. Программа снабжена приложением, включающим тестовые задания и практические работы, описание упражнений, научные, научно-популярные и публицистические тексты, которые могут использоваться для иллюстрирования ситуаций и задач, рассматриваемых в процессе повышения квалификации. Программа имеет список литературы и Интернет-источников, в том числе Web-сайтов, которые рекомендуется использовать при обучении; среди них особое место занимают Web-ресурсы Microsoft, предлагаемые для системы образования.

Программа регламентирует содержание и технологии образовательного процесса, ведущими подходами в построении которого выступают андрогогический, личностно-деятельностный и проектно-исследовательский подходы.

Результатами освоения программы являются:

- осознание обучающимися значимости проблемы и ее решения для будущего общества, образования, педагогических кадров, школьников и эмоционально-положительное отношение к предлагаемому курсу, к программе, как к потенциально эффективным инструментам решения обозначенной проблемы;
- знания в сфере проектирования безопасных информационно-методических сред образовательных учреждений, в области психолого-педагогического и здоровьесберегающего сопровождения образовательного процесса, персонала и школьников, использующих персональные компьютеры и Интернет в профессиональной, учебной и внеучебной деятельности;

- знания в области разработки программ информатизации школы с учетом соблюдения принципов безопасности информации и жизнедеятельности, здоровьесбережения участников образовательного процесса;
- опыт проектирования названных объектов, условий, программ.

В качестве продуктов, фиксирующих освоенность программы, рассматриваются проекты программ просветительской работы с родителями и общественностью, проекты учебных и методических занятий, в рамках которых рассматриваются вопросы здоровья и безопасности школьников и педагогического персонала в мире Интернета и компьютерных технологий, проекты разделов программ информатизации образовательных учреждений, информационно-методических сред, локальных вычислительных сетей школ, локальных нормативных актов, связанных с рассматриваемой проблематикой.

Продолжительность обучения в рамках данной программы повышения квалификации педагогов составляет 36—72 часа.

В качестве **реализаторов** программы рассматриваются специалисты региональных учебных центров Microsoft «Академия учителей», а также заинтересованные педагоги учреждений дополнительного профессионального педагогического образования.

Учебный план курса повышения квалификации по теме «ЗДОРОВЬЕ И БЕЗОПАСНОСТЬ ДЕТЕЙ В МИРЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНТЕРНЕТА»

Цель: повышение квалификации в области использования ИКТ для безопасной работы в Интернете.

Категория слушателей: руководители образовательных учреждений общего образования (ОУ ОО), заместители директоров по воспитательной работе (ОУ ОО), методисты региональных учреждений ДПО, специалисты РЦ, специалисты методической службы, специалисты.

Объем: 72 часа.

Вариант 1

№ п/п	Наименование разделов	Всего часов	В том числе			Формы контроля
			Лекции	Круглые столы Деловые игры Дискуссии и др.	Семинары Практические занятия Лабораторные	
I	Психическое и физическое здоровье детей при работе за компьютером	12	6	2	4	
II	Социальный, эмоциональный и личностные аспекты занятий детей на компьютере	12	6	4	2	Ролевая игра
III	Информационная этика и правовые аспекты защиты информации	12	8		4	
IV	Безопасность детей в Интернете	12	8	2	2	Ролевая игра
V	Технологии и средства защиты информации от разрушения и несанкционированного доступа	12	6		6	
VI	Компьютерные вирусы и средства защиты.	12	4		8	
	Входная диагностика					Анкетирование
	Итоговый контроль					Проекты[4]
	ИТОГО:	72	38	8	26	

Учебно-тематический план курса повышения квалификации по теме: «ЗДОРОВЬЕ И БЕЗОПАСНОСТЬ ДЕТЕЙ В МИРЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНТЕРНЕТА»

Цель: повышение квалификации в области использования ИКТ для безопасной работы в Интернете.

Категория слушателей: руководители образовательных учреждений общего образования (ОУ ОО), заместители директоров по воспитательной работе (ОУ ОО), методисты региональных учреждений ДПО, специалисты РЦ, специалисты методической службы, специалисты.

Объем: 72 часа.

Вариант 1

№ п/п	Наименование разделов и тем	Всего часов	В том числе			Формы контроля
			Лекции	Круглые столы Деловые игры Дискуссии и др.	Семинары Практические занятия Лабораторные	
I	Психическое и физическое здоровье детей при работе за компьютером	12	6	2	4	
1.1	Компьютеры и физическое здоровье детей.		2			
1.2	Гигиенические требования к организации занятий с использованием новых информационно-компьютерных технологий		2		2	
1.3	Профилактика нарушений осанки и зрения при работе за компьютером		2		2	
II	Социальный, эмоциональный и личностный аспекты занятий детей на компьютере	12	6	4	2	Ролевая игра
2.1	Развитие интеллекта и стили обучения в цифровом мире		2	2		

Продолжение табл.

№ п/п	Наименование разделов и тем	Всего часов	В том числе			Формы контроля
			Лекции	Круглые столы Деловые игры Дискуссии и др.	Семинары Практические занятия Лабораторные	
2.2	Влияние компьютера на внимание, мотивацию		2	2		
2.3	Негативное воздействие компьютера на психическое здоровье детей		2		2	
III	Информационная этика и правовые аспекты защиты информации	12	8		4	
3.1	Информационная этика и право		4		2	
3.2	Основные законы России в области компьютерного права		4	2		
IV	Безопасность детей в Интернете	12	8	2	2	Ролевая игра
4.1	Опасности, с которыми дети могут столкнуться в сети.		2			
4.2	Безопасное общение детей в Интернете		2	2		
4.3	Феномен «Интернет-заивисимости». Профилактика Интернет-зависимости у учащихся		2			
4.4	Технологии безопасной работы в сети		2		2	
V	Технологии и средства защиты информации от разрушения и несанкционированного доступа	12	6		6	
5.1	Цели совершения преступления. Уровни и меры по защите информации.		2		2	
5.2	Установка паролей на ПК и папки. Меры безопасности при работе с электронной почтой		2		2	
5.3	Безопасность работы в локальной сети		2		2	

Окончание табл.

№ п/п	Наименование разделов и тем	Всего часов	В том числе			Формы контроля
			Лекции	Круглые столы Деловые игры Дискуссии и др.	Семинары Практические занятия Лабораторные	
VI	Компьютерные вирусы и средства защиты	12	4		8	
6.1	Обзор и способы классификации компьютерных вирусов		2		4	
6.2	Антивирусные и антишпионские программы		2		4	
	Входная диагностика					Анкетирование
	Итоговый контроль					Проекты[5]
	ИТОГО:	72	34		38	

Учебный план курса повышения квалификации по теме «ЗДОРОВЬЕ И БЕЗОПАСНОСТЬ ДЕТЕЙ В МИРЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНТЕРНЕТА»

Цель: повышение квалификации в области использования ИКТ для безопасной работы в Интернете.

Категория слушателей: зам. директора по информатизации ОУ, учителя информатики и ИКТ, методисты по информатике, зам. специалистов ИКТ РЦ.

Объем: 72 часа.

Вариант 2

№ п/п	Наименование разделов	Всего часов	В том числе			Формы контроля
			Лекции	Круглые столы Деловые игры Дискуссии и др.	Семинары Практические занятия Лабораторные	
I	Психическое и физическое здоровье детей при работе за компьютером	12	6	2	4	
II	Социальный, эмоциональный и личностные аспекты занятий детей на компьютере	6	2	2	2	
III	Информационная этика и правовые аспекты защиты информации	6	4		2	
IV	Безопасность детей в Интернете	20	10	2	8	Дискуссия
V	Технологии и средства защиты информации от разрушения и несанкционированного доступа	14	8		6	
VI	Компьютерные вирусы и средства защиты	14	8		6	
	Входная диагностика					Анкетирование
	Итоговый контроль					Проекты[6]
	ИТОГО:	72	38	6	28	

Учебно тематический план курса повышения квалификации по теме: «ЗДОРОВЬЕ И БЕЗОПАСНОСТЬ ДЕТЕЙ В МИРЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНТЕРНЕТА»

Цель: повышение квалификации в области использования ИКТ для безопасной работы в Интернете.

Категория слушателей: зам. директора по информатизации ОУ, учителя информатики и ИКТ, методисты по информатике, зам. специалистов ИКТ РЦ.

Объем: 72 часа.

Вариант 2

№ п/п	Наименование разделов и тем	Всего часов	В том числе			Формы контроля
			Лекции	Круглые столы Деловые игры Дискуссии и др.	Семинары Практические занятия Лабораторные	
I	Психическое и физическое здоровье детей при работе за компьютером	12	6	2	4	
1.1	Компьютеры и физическое здоровье детей		2	2		
1.2	Гигиенические требования к организации занятий с использованием новых информационно-компьютерных технологий		2		2	
1.3	Профилактика нарушений осанки и зрения при работе за компьютером		2		2	
II	Социальный, эмоциональный и личностный аспекты занятий детей на компьютере	6	2	2	2	
2.1	Развитие интеллекта и стили обучения в цифровом мире					
2.2	Влияние компьютера на внимание, мотивацию		2			
2.3	Негативное воздействие компьютера на психическое здоровье детей			2	2	
III	Информационная этика и правовые аспекты защиты информации	6	4		2	

Окончание табл.

№ п/п	Наименование разделов и тем	Всего часов	В том числе			Формы контроля
			Лекции	Круглые столы Деловые игры Дискуссии и др.	Семинары Практические занятия Лабораторные	
3.1	Информационная этика и право		2		2	
3.2	Основные законы России в области компьютерного права		2			
IV	Безопасность детей в Интернете	20	10	2	8	Дискуссия
4.1	Опасности, с которыми дети могут столкнуться в сети.		2	2	2	
4.2	Безопасное общение детей в Интернете		2		2	
4.3	Феномен «Интернет-зависимости». Профилактика Интернет-зависимости у учащихся		2		2	
4.4	Технологии безопасной работы в сети		4		2	
V	Технологии и средства защиты информации от разрушения и несанкционированного доступа	14	8		6	
5.1	Цели совершения преступления. Уровни и меры по защите информации		2			
5.2	Установка паролей на ПК и папки. Меры безопасности при работе с электронной почтой		2		2	
5.3	Безопасность работы в локальной сети.		4		4	
VI	Компьютерные вирусы и средства защиты.	14	8		6	
6.1	Обзор и способы классификации компьютерных вирусов		4		4	
6.2	Антивирусные и антишпионские программы		4		2	
	Входная дигностика					Анкетирование
	Итоговый контроль					Проекты[7]
	ИТОГО:	72	38	6	28	

Учебный план курса повышения квалификации по теме «ЗДОРОВЬЕ И БЕЗОПАСНОСТЬ ДЕТЕЙ В МИРЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНТЕРНЕТА»

Цель: повышение квалификации в области использования ИКТ для безопасной работы в Интернете.

Категория слушателей: учителя-экспериментаторы, учителя-предметники, педагоги учреждений дополнительного образования детей.

Объем: 72 часа.

Вариант 3

№ п/п	Наименование разделов	Всего часов	В том числе			Формы контроля
			Лекции	Круглые столы Деловые игры Дискуссии и др.	Семинары Практические занятия Лабораторные	
I	Психическое и физическое здоровье детей при работе за компьютером	16	8	2	6	
II	Социальный, эмоциональный и личностный аспекты занятий детей на компьютере	14	6	2	6	
III	Информационная этика и правовые аспекты защиты информации	6	4		2	
IV	Безопасность детей в Интернете	18	8	2	8	Ролевая игра
V	Технологии и средства защиты информации от разрушения и несанкционированного доступа	10	6		4	
VI	Компьютерные вирусы и средства защиты	8	4		4	
	Входная диагностика					Анкетирование
	Итоговый контроль					Проекты[8]
	ИТОГО:	72	36	6	30	

Учебно-тематический план курса повышения квалификации по теме: «ЗДОРОВЬЕ И БЕЗОПАСНОСТЬ ДЕТЕЙ В МИРЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ИНТЕРНЕТА»

Цель: повышение квалификации в области использования ИКТ для безопасной работы в Интернете.

Категория слушателей: учителя-экспериментаторы, учителя-предметники, педагоги учреждений дополнительного образования детей.

Объем: 72 часа.

Вариант 3

№ п/п	Наименование разделов и тем	Всего часов	В том числе			Формы контроля
			Лекции	Круглые столы Деловые игры Дискуссии и др.	Семинары Практические занятия Лабораторные	
I	Психическое и физическое здоровье детей при работе за компьютером	16	8	2	6	
1.1	Компьютеры и физическое здоровье детей		4		2	
1.2	Гигиенические требования к организации занятий с использованием новых информационно-компьютерных технологий		2		2	
1.3	Профилактика нарушений осанки и зрения при работе за компьютером		2	2	2	
II	Социальный, эмоциональный и личностный аспекты занятий детей на компьютере	14	6	2	6	
2.1	Развитие интеллекта и стили обучения в цифровом мире		2		2	
2.2	Влияние компьютера на внимание, мотивацию		2		2	

Продолжение табл.

№ п/п	Наименование разделов и тем	Всего часов	В том числе			Формы контроля
			Лекции	Круглые столы Деловые игры Дискуссии и др.	Семинары Практические занятия Лабораторные	
2.3	Негативное воздействие компьютера на психическое здоровье детей		2	2	2	
III	Информационная этика и правовые аспекты защиты информации	6	4		2	
3.1	Информационная этика и право.		2		2	
3.2	Основные законы России в области компьютерного права		2			
IV	Безопасность детей в Интернете	18	8	2	8	Ролевая игра
4.1	Опасности, с которыми дети могут столкнуться в Сети		2		2	
4.2	Безопасное общение детей в Интернете		2		2	
4.3	Феномен «Интернет-зависимости». Профилактика Интернет-зависимости у учащихся			2	2	
4.4	Технологии безопасной работы в сети		4		2	
V	Технологии и средства защиты информации от разрушения и несанкционированного доступа	10	6		4	
5.1	Цели совершения преступления. Уровни и меры по защите информации		2			
5.2	Установка паролей на ПК и папки. Меры безопасности при работе с электронной почтой		2		2	
5.3	Безопасность работы в локальной сети		2		2	
VI	Компьютерные вирусы и средства защиты	8	4		4	

Окончание табл.

№ п/п	Наименование разделов и тем	Всего часов	В том числе			Формы контроля
			Лекции	Круглые столы Деловые игры Дискуссии и др.	Семинары Практические занятия Лабораторные	
6.1	Обзор и способы классификации компьютерных вирусов		2		2	
6.2	Антивирусные и антишпионские программы		2		2	
	Входная диагностика					Анкетирование
	Итоговый контроль					Проекты[9]
	ИТОГО:	72	36	6	30	

СОДЕРЖАНИЕ КУРСА

Модуль 1
Психическое и физическое здоровье детей при работе за компьютером

Тема 1.1 Компьютеры и физическое здоровье детей

Здоровьесберегающие технологии, применяемые при организации работы школьника на компьютере. Компьютерная радиация. Комплексы упражнений физкультурных минуток. Комплексы упражнений физкультурных пауз. Профилактическая гимнастика для дошкольников.

Тема 1.2 Гигиенические требования к организации занятий с использованием новых информационно-компьютерных технологий

Требования к пользователям ПЭВМ. Общие вопросы организации рабочих мест. Эргономика рабочих мест. Требования безопасности к персональным электронно-вычислительным машинам. Оценка параметров рабочих мест по антропометрическим данным человека. Освещение рабочих мест. Электробезопасность. Электромагнитные поля и излучения. Шум и вибрации.

Тема 1.3 Профилактика нарушений осанки и зрения при работе за компьютером

Основные направления профилактики нарушений здоровья детей при работе за компьютером. Проблемы осанки и опорно-двигательного аппарата. Зрение. Комплексы упражнений для глаз. Организация занятий с ПК детей школьного возраста. Организация занятий детей дошкольного возраста за игровыми комплексами на базе ПК.

Практические занятия, семинары, тренинги, консультации по разделу нацелены на диагностику профессионально-личностных особенностей педагогов, на усвоение ими теоретического материала и практических навыков в области безопасной работы на ПК как составляющей профессиональной компетентности педагога.

Литература

1. Агабабян Н.В., Любимова С.В. Использование здоровьесберегающих технологий при проведении занятий по информатике с детьми. Тамбов, 2008.

2. Баловсяк Н. Компьютер и здоровье. СПб, 2008.

3. КиберМама.Ру: статьи для родителей — URL: http://www.cybermama.ru

4. Колосков А. Боль в руках — профессиональный недуг компьютерщиков //Физкультура и спорт. 2003. № 12.

5. Кучма В.Р. Теория и практика гигиены детей и подростков на рубеже тысячелетий. М., 2001.

6. Кудряшова Н. Наедине с компьютером //Физкультура и спорт. 2004. № 5.

7. Ковалько В.И. Здоровьесберегающие технологии: школьник и компьютер: 1—4 классы. М., 2007.

8. Поляков С.Д., Хрущев С.В., Корнеева И.Т. и др. Мониторинг и коррекция физического здоровья школьников: Методическое пособие. М., 2006.

9. Профилактика нарушений зрения при работе с компьютером: Методические рекомендации // Тамбовский областной ИПК. Тамбов, 2008.

10. Передерин В. Компьютерная болезнь // Будь здоров! 2004. № 4.

11. Окулова Е. Ребенок в «заэкранье» // Наука и жизнь. 2005. № 5.

12. Сидорова А. Влияние компьютерных игр на поведение подростков // Воспитание школьников. 2007. № 7.

13. Синельников Р. Д. Атлас анатомии человека, т. I. М., 2006.

14. Смирнов Н.К. Здоровьесберегающие образовательные технологии и психология здоровья в школе. М., 2005.

Модуль 2
Социальный, эмоциональный и личностный аспекты занятий детей на компьютере

Тема 2.1. Развитие интеллекта и стили обучения в цифровом мире

Интеллект в информационном обществе. Принципы развития мозга. Влияние видеоигр на развитие интеллекта. Советы по использованию видеоигр.

Тема 2.2. Влияние компьютера на внимание, мотивацию

Влияние компьютера на внимание, мотивацию и метапознание. Компьютерная зависимость. Использование компьютеров для повышения мотивации.

Тема 2.3. Негативное воздействие компьютера на психическое здоровье детей

Воздействие компьютера на психическое здоровье детей. Уход от реальности. Признаки, характерные для игромании как разновидности зависимого поведения. Стресс при работе с компьютером. Способы его профилактики и коррекции.

Практические занятия, семинары, тренинги, консультации по разделу нацелены на усвоение слушателями теоретического материала и на развитие практических навыков в области профилактики и коррекции зависимого поведения школьников, связанного с компьютерными технологиями и Интернетом.

Литература

1. Беки Уорли. Интернет: реальные и мнимые угрозы / Пер. с англ. — М.: КУДИЦ-ОБРАЗ, 2004. — 320 с.

2. Будунов Г.М. Компьютерные технологии в образовательной сфере: «за» и «против». — М.: АРКТИ, 2006. — 192 с.

3. Леонова А.Б, Чернышева О.Н. Психология труда и организационная психология: Современное состояние и перспективы: Хрестоматия. — М., 1995—386 с.

4. Митина Л.М., Митин Г.В., Анисимова О.А. Профессиональная деятельность и здоровье педагога. — М.: Академия, 2005. — 363 с.

5. Стресс жизни: Сборник./ Составители: Л. М. Попова, И. В. Соколов. (О. Грегор. Как противостоять стрессу. Г. Селье. Стресс без болезней.) — Спб, ТОО «Лейла», 1994. — 384 с.

6. Соболева А. Е., Емельянова Е.Н. Диагностика развития: внимания, памяти, мышления [Электрон. ресурс] «Психологический центр Адалин» — 2009 — Режим доступа: http://adalin.mospsy.ru/l_04_00/l040217.shtml

7. Интернет-СМИ «Ваш личный Интернет» [Электронный ресурс]. — URL: http://contentfiltering.ru/

Модуль 3
Информационная этика и правовые аспекты защиты информации

Тема 3.1. Информационная этика и право

Информационная безопасность. Угрозы информационной безопасности. Уровни информационной безопасности. Направления защиты компьютерной информации.

Электронно-цифровая подпись.

Тема 3.2. Основные законы России в области компьютерного права

Закон «О правовой охране программ для электронных вычислительных машин и баз данных» (от 23.09.1992 г. № 3523—1). Закон «Об авторском праве и смежных правах» (от 09.07.1993 г. № 5351—1 с последующим изменением и дополнением). Четвертая часть Гражданского кодекса РФ (от 18.12.2006 г. № 230-ФЗ). Федеральный закон «О введении в действие части четвертой Гражданского кодекса РФ» (от 18.12.2006 г. № 231-ФЗ).

Закон «О государственной тайне» (от 21.07.1993 г. № 5485—1 с последующим изменением и дополнением).

Федеральный закон «О связи» (от 07.07.2003 г. № 126-ФЗ с последующим изменением и дополнением).

Федеральный закон «Об информации, информационных технологиях и защите информации» (от 27.07.2006 г. № 149-ФЗ).

Практические занятия, семинары, тренинги, консультации по разделу нацелены на усвоение слушателями теоретического материала и на формирование компетентности в области правовых аспектов информационной безопасности.

Литература

1. Доктрина информационной безопасности Российской Федерации. (Утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000г., № Пр-1895) [Электронный ресурс]. — URL: http://www.scrf.gov.ru/documents/5.html

2. Галатенко В.А.. Основы информационной безопасности. Дистанционныйкурс(с)INTUIT.ru: Интернет-Университет Информацион-

ных Технологий — дистанционное образование, 2003—2008 [Электронный ресурс]. — URL: http://www.intuit.ru/

3. Партыка Т.Л., Попов И.И. Информационная безопасность: Учебное пособие, изд. 3-е, испр., доп. — М.: ФОРУМ, 2008. — 432 с.: ил. — (Профессиональное образование).

4. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. Изд. 3-е — М.: Академический Проект — 2006. — 544 с.

5. Федеральный закон «Об электронной цифровой подписи» [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=72518;div=LAW;mb=LAW;opt=1;ts=AB736230098ADC672E8227AAFB97B9A8

6. Электронно-цифровая подпись — Что это такое? [Электронный ресурс]. — URL: http://www.digitalsign.ru/

7. Национальный стандарт РФ. ГОСТ Р ИСО/МЭК 17799—2005 Информационная технология. Практические правила управления информационной безопасностью. ISO/IEC 17799:2000 Information technology — Code of practice for information security management (IDT) Издание официальное. Москва. Стандартинформ, 2006.

8. ГОСТ Р 50922—2006 ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Защита информации. Основные термины и определения — сайт Федерального агентства по техническому регулированию и метрологии [Электронный ресурс]. — URL: http://protect.gost.ru/v.aspx?control=8&baseC=6&page=0&month=6&year=2008&search=50922&RegNum=1&DocOnPageCount=15&id=121129&pageK=E10BFA12-ED02—4212—8D58—3F1D91F314A0

9. Попов В.Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности. — М.: Финансы и статистика, 2005. — 176 с.

10. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учебное пособие — М.: Инфра-М, 2001. — 301 с.

11. Безбогов, А.А. Методы и средства защиты компьютерной информации: учебное пособие / А.А. Безбогов, А.В. Яковлев, В.Н. Шамкин. — Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006. — 196 с.

12. Федеральный закон «О введении в действие части четвертой Гражданского кодекса РФ» [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=83483;fld=134;dst=100052

13. Федеральный закон «О государственной тайне» [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=89782

14. Федеральный закон «О связи» [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=76690

15. Федеральный закон «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=61798

16. Федеральный закон «О безопасности» [Электронный ресурс]. — URL: http://base.garant.ru/10136200.htm

17. Уголовный кодекс Российской Федерации [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=93431

18. Конституция Российской Федерации [Электронный ресурс]. — URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=2875

19. Официальный сайт Федеральной службы по техническому и экспортному контролю [Электронный ресурс]. — URL: http://www.fstec.ru/_razd/_ispo.htm

20. Блохина Е.В. Лекция по теме: «Правовые основы использования Интернет-ресурсов. Авторские права. Поиск информации в Интернете» [Электронный ресурс]. — URL: http://festival.1september.ru/articles/412857/

21. Расторгуев С.П. Основы информационной безопасности // Информатика и образование. — 2007. — № 8.

22. Семенова З.В. Углубленное изучение темы «Защита данных в информационных системах» // Информатика и образование. — 2004. — № 1.

23. Черкашина И. Ф. Изучение темы «Информационная безопасность» в курсе информатики // Информатика и образование. — 2007. — № 9.

24. Бачило И.Л. О законодательстве в информационной сфере отношений. [Электронный ресурс]. — URL: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/a11ec0af30c1cc6ec3256c4f00312cfb

25. Ефимова Л. Проблемы правовой защиты детей от информации, приносящей вред их здоровью и развитию, распространяемой в сети Интернет [Электронный ресурс]. — URL: http://www.medialaw.ru/publications/zip/156—157/1.htm

Модуль 4
Безопасность детей в Интернете

Тема 4.1. Опасности, с которыми дети могут столкнуться в сети

Риск получения ребенком доступа к неподходящей информации. Типы рисков.

Тема 4.2. Безопасное общение детей в Интернете

Противостояние угрозам из Интернета. Инструкции по безопасному общению в чатах. Интернет-этика поведения в Интернете. Как не следует вести себя в Сети.

Тема 4.3. Феномен «Интернет-зависимости». Профилактика Интернет-зависимости у учащихся

Феномен «Интернет-зависимости». Профилактика Интернет-зависимости. Преодоление Интернет-зависимости.

Тема 4.4. Технологии безопасной работы в сети

Повышение уровня общей безопасности при работе в сети. Советы по безопасности при работе на общедоступном компьютере.

Практические занятия, семинары, тренинги, консультации по разделу нацелены на усвоение слушателями теоретического материала и развитие практических навыков в области обеспечения безопасной работы на ПК.

Литература

1. Галатенко В.А. Основы информационной безопасности. [Текст] 4-е изд. учеб. пособие, ВУЗ // — М: Издательство Бином. Лаборатория знаний, Интуит, 2008—205 с.

2. Глушаков, С.В. Секреты хакера: защита и атака [Текст] / С.В. Глушаков, М.И. Бабенко, Н.С. Тесленко. — изд. 2-е, доп. и перераб. — М: АСТ: АСТ МОСКВА; Владимир: ВКТ, 2009. — 544 с. — (Учебный курс).

3. Ленков С.В., Перегудов Д.А, Хорошко В.А.Методы и средства защиты информации. В 2 томах. Том 1. Несанкционированное получение информации [Текст] // — М: Издательство: Арий, 2008 г. 464 с.

4. Прохода А. Н. Обеспечение Интернет-безопасности. Практикум: Учебное пособие для вузов. [Текст] // — М.: Горячая линия—Телеком, 2007. — 180 с: ил.

5. Основы безопасности детей и молодежи в Интернете — интерактивный курс по интерент-безопасности. Владельцами авторских прав на сайт являются проект Финский день информационной безопасности и WSOYpro [Электронный ресурс]. — URL: http://laste.arvutikaitse.ee/rus/html/copyright.htm

6. Безопасность детей в Интернете. Nachalka.com 2008 [Электронный ресурс]. — URL: http://www.nachalka.com/bezopasnost

7. Безопасность дома [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/default.mspx

8. Евтеев Леонид. Безопасность ребенка в Интернете. Инновационная образовательная сеть «Эврика» — Пермь, 2009. [Электронный ресурс]. — URL: http://www.diaghilev.perm.ru/class/sobr4—2.htm

9. Кимберли Янг. Тест на Интернет-зависимость / Перевод теста, выполненный и адаптированный В.А.Буровой/ Клиника СПО Центр — М: 2009 [Электронный ресурс]. — URL: http://www.psyhelp.ru/texts/iad_test.htm

10. Барбара Гутман, Роберт Бэгвилл. Политика безопасности при работе в Интернете — техническое руководство. CIT Forum 2009 [Электронный ресурс]. — URL: http://www.citforum.ru/internet/security_guide/index.shtml

Модуль 5
Технологии и средства защиты информации от разрушения и несанкционированного доступа

Тема 5.1. Цели совершения преступления. Уровни и меры по защите информации

Цели совершения преступления. Основные понятия в области защиты информации от разрушения и несанкционированного доступа. Уровни защиты информации. Меры по защите информации.

Тема 5.2. Установка паролей на ПК и папки. Меры безопасности при работе с электронной почтой

Разграничение доступа на компьютере. Доступ к файловой системе (папкам). Утечка информации через электронную почту. Социальная инженерия. Фишинг. Меры

безопасности при работе с электронной почтой.

Тема 5.3. Безопасность работы в локальной сети

Управление сетевыми ресурсами, средства контроля сетевых ресурсов, контроль сетевого доступа, политика в отношении использования сетевых служб. Основы безопасности при работе в сетях. Принципы построения защищенных операционных систем. Основные угрозы при работе в сети. Основные меры безопасности при работе в сети.

Практические занятия, семинары, тренинги, консультации по разделу нацелены на усвоение слушателями теоретического материала и формирование компетентности в области защиты информации.

Литература

1. Сайт Федерального агентства по техническому регулированию и метрологии ГОСТ Р 50922—2006 ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Защита информации. Основные термины и определения [Электронный ресурс]. — URL: http://protect.gost.ru/v.aspx?control=8&baseC=6&page=0&month=6&year=2008&search=50922&RegNum=1&DocOnPageCount=15&id=121129&pageK=E10BFA12-ED02—4212—8D58—3F1D91F314A0

2. Основы компьютерных сетей: Учебное пособие. — 3-е изд., испр. и доп. — М.: БИНОМ. Лаборатория знаний, 2007. — 160 с.

3. Национальный стандарт Российской Федерации. ГОСТ Р ИСО/МЭК 17799—2005. Информационная технология. Практические правила управления информационной безопасностью. ISO/IEC 17799:2000 Information technology — Code of practice for information security management (IDT) Издание официальное, Москва, Стандартинформ. 2006

4. Защитите свой компьютер: брандмауэр, безопасность при работе в Интернете. Что такое брандмауэр? [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/computer/basics/firewall.mspx

5. Защитите свой компьютер: брандмауэр, безопасность при работе в Интернете. Выберите оптимальный брандмауэр для своей версии системы Windows [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/computer/firewall/using.mspx —

6. Взлом и защита локальной сети [Электронный ресурс]. — URL: http://virusinfo.info/showthread.php?t=29760

Модуль 6
Компьютерные вирусы и средства защиты

Тема 6.1. Обзор и способы классификации компьютерных вирусов

Способы распространения вирусов. История вредоносных программ. Вирусная терминология. Классификация вирусов. Самые распространенные вирусы. Цикл функционирования вируса. Ме-

тоды борьбы с вирусами. Меры защиты от проникновения и распространения вирусов.

Тема 6.2. Антивирусные и антишпионские программы

Антивирусное программное обеспечение и антишпионские программы. Продукты Microsoft для защиты от вирусов и программ-шпионов.

Практические занятия, семинары, тренинги, консультации по разделу нацелены на диагностику профессионально-личностных особенностей педагогов, на усвоение ими теоретического материала, на развитие практических навыков в области защиты от компьютерных вирусов как составляющей ИКТ компетентности педагога.

Литература

1. Безопасность дома [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/default.mspx

2. Пять действий по защите нового компьютера перед выходом в Интернет [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/computer/advanced/xppc.mspx

3. Бесплатная проверка безопасности компьютера [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/products/computer/safetyscanner.mspx

4. Продукты и службы для обеспечения безопасности: вопросы и ответы [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/products/computer/faq.mspx

5. Защита от программ-шпионов, вирусов и нежелательных программ [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/products/computer/default.mspx

6. Учебные видеоматериалы [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/videos/default.mspx

7. Что представляет собой Windows 7 [Электронный ресурс]. — URL: http://windows.microsoft.com/ru-RU/windows7/products/what-is

8. Программа Windows Live Messenger [Электронный ресурс]. — URL: http://www.microsoft.com/rus/protect/products/computer/windowslivemessenger.mspx

Содержание

Модуль 1. Психическое и физическое здоровье детей при работе за компьютером 4

Модуль 2. Социальный, эмоциональный и личностный аспекты занятий детей на компьютере 28

Модуль 3. Информационная этика и правовые аспекты защиты информации 54

Модуль 4. Безопасность детей в Интернете 77

Модуль 5. Технологии и средства защиты информации от разрушения и несанкционированного доступа 107

Модуль 6. Компьютерные вирусы и средства защиты 123

Приложение 150

Горбунова Лариса Николаевна
Аникеева Людмила Александровна
Семибратов Алексей Михайлович
Смирнов Никита Константинович
Сорокина Елена Владимировна
Третьяк Татьяна Михайловна

Здоровье и безопасность детей в мире компьютерных технологий и Интернет. Учебно-методический комплект

Ответственный за выпуск
В. Митин

Макет и верстка
С. Тарасов

Обложка
Е. Холмский

ООО «СОЛОН-ПРЕСС»
123242, Москва, а/я 20
Телефоны:
(495) 254-44-10, (499) 795-73-26
E-mail: Avtor@coba.ru

ООО «СОЛОН-ПРЕСС»
103050, г. Москва, Дегтярный пер., д. 5, стр. 2
Формат 60×88/16. Объем 11 п. л. Тираж 7000