Концепция обучения информационной безопасности на первой ступени школьного образования

Михаил Иванович Бочаров,
доцент кафедры гуманитарных и естественно-научных дисциплин филиала государственного образовательного учреждения высшего профессионального образования «Орловская региональная академия государственной службы» в городе Липецке, кандидат педагогических наук

В СТАТЬЕ РАССМАТРИВАЮТСЯ ПОДХОДЫ К ОБУЧЕНИЮ УЧАЩИХСЯ МЛАДШИХ КЛАССОВ ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ДЛЯ ЭТОГО ПРОВОДИТСЯ АНАЛИЗ ОСОБЕННОСТЕЙ ВОСПРИЯТИЯ ИНФОРМАЦИИ ШКОЛЬНИКОМ, ВЫДЕЛЯЮТСЯ СОЦИАЛЬНЫЕ ГРУППЫ, В КОТОРЫХ ОН МОЖЕТ ОКАЗАТЬСЯ, РАССМАТРИВАЮТСЯ ВОЗМОЖНЫЕ ИСТОЧНИКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЧАЩЕГОСЯ, ХАРАКТЕРНЫЕ ДЛЯ МЛАДШЕГО ШКОЛЬНОГО ВОЗРАСТА, НА ОСНОВЕ ЧЕГО ВЫБИРАЮТСЯ АДЕКВАТНЫЕ СПОСОБЫ ОБУЧЕНИЯ ОСНОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УЧЕБНОМ ПРОЦЕССЕ.

• Информационная безопасность • Метод воспитывающих ситуаций • Контекстное обучение • Независимость от информации • Игровое моделирование •

Сущность сформированности информационной безопасности школьника состоит в умении выявлять информационную угрозу, определять степень её опасности, уметь предвидеть последствия информационной угрозы и противостоять им. Таким образом, возникает проблема педагогического осмысления развития личности школьника в современном информационном обществе и определения теоретических положений оказания помощи в противодействии информационной опасности.

Простой пример. Ребёнок находится дома один. В дверь звонит незнакомый человек и говорит: «Откройте, вам телеграмма». Конечно, можно заранее запретить ребёнку открывать дверь в этом случае. Но вряд ли это будет решением проблемы. А если за дверью говорят, что в доме пожар? Или там ближайшая соседка? Каковы должны быть действия ребёнка в этой ситуации? Как понять, ложная это информация или достоверная? Остаться дома и подвергнуть свою жизнь риску? Или быть обманутым недобросовестным человеком, желающим незаконно присвоить ценные вещи? Ответить на эти и многие другие вопросы поможет ситуационное обучение младшего школьника информационной безопасности.

В современной педагогике существует схожее понятие – «метод воспитывающих ситуаций», представляющий собой такую организацию деятельности и поведения воспитанников, в которой учащийся ставится перед необходимостью решить какуюлибо проблему, связанную с нравственным выбором, способом организации деятельности, определением социальной роли и т.д. Воспитатель специально создаёт лишь условия для возникновения ситуации. Когда у ребёнка в такой ситуации возникает проблема, и существуют условия для самостоятельного ее решения, создаётся возможность социальной пробы (испытания) как метода самовоспитания. Социальные пробы охватывают все сферы жизни человека и большинство его социальных

связей. В процессе включения в эти ситуации у детей формируется определённая социальная позиция и социальная ответственность, которая и является основой для их дальнейшего вхождения в социальную среду[1].

В педагогике профессионального образования разрабатывается теория контекстного обучения. Контекст – это система внешних и внутренних факторов и условий поведения и деятельности человека, влияющих на особенности восприятия, понимания и преобразования им мира и каждой конкретной ситуации, определяющих смысл и значение этой ситуации как целого и входящих в нее компонентов[2]. С помощью системы учебных проблем, проблемных ситуаций и задач выстраивается сюжетная канва усваиваемой профессиональной деятельности, а статичное содержание образования превращается в динамично развёртываемое. Основной единицей содержания контекстного обучения выступает проблемная ситуация, хотя и для привычных заданий находится место. Таким образом, социальное содержание «втягивается» в учебный процесс через формы совместной деятельности, предполагающие учёт личностных особенностей каждого, его интересов и предпочтений, следование нравственным нормам[3].

Ситуационное обучение младшего школьника информационной безопасности представляет собой процесс:

• формирования такой модели поведения школьника, которая способствует минимизации последствий психического, нравственного и физического воздействия в опасных для жизни ребёнка условиях и обстоятельствах средствами классификации, систематизации, моделирования в рамках учебного процесса (школы и учреждений дополнительного образования), предотвращает типовые случаи угроз информационной безопасности, в которых может оказаться ребёнок;

• контекстного обучения правилам поведения в рассматриваемых ситуациях.

Для формирования навыков безопасного поведения необходимо проанализировать различные ситуации, в которых может находиться младший школьник в процессе своей жизнедеятельности. В общем смысле под ситуациями целесообразно понимать естественные сегменты социальной жизни, для которых характерны место, время, субъекты, содержание деятельности субъектов, социальный контекст. Ситуации подразделяются на следующие виды:

• сложные (требуют интеллектуальных усилий для поиска путей преодоления препятствий);

• трудные (требуют практических усилий для преодоления препятствий, когда нет опасных и вредных факторов);

• опасные (включают факторы, при которых возможно причинение ущерба человеку, обществу);

• экстремальные (опасность столь велика, что для её преодоления человек действует на пределе возможностей);

• чрезвычайные (характерен значительный масштаб опасности, угрожающей большим группам людей);

• критические (факторы опасности невозможно устранить, и ущерб, затрагивающий существенные интересы человека, уже причинён или неизбежен)[4].

Для ситуации по обеспечению ИБ необходима профилактика, позволяющая преодолевать вредные и опасные факторы, способствующая созданию безопасных условий жизнедеятельности. В этом смысле ситуация может быть:

• информационной (на человека воздействуют сведения об опасности, оказывающие психотравмирующее влияние, провоцирующие неадекватное поведение или помогающие подготовиться к предстоящим реальным опасностям);

• игровой (опасные и вредные факторы имитируются в условиях игры);

[1] Словарь по образованию и педагогике / В.М. Полонский. М.: Высш. шк. 2004. 512 с.

[2] **Вербицкий А., Жукова Н.** Кросскультурные контексты в контекстном обучении // Высшее образование в России. 2007. № 4.
Вербицкий А.А., Дубовицкая Т.Д. Контексты содержания образования. М.: РИЦ МГОПУ им. М.А.Шолохова, 2003. 80 с. С. 4.

[3] **Вербицкий А.** Контекстное обучение в компетентностном подходе // Высшее образование в России. 2006. № 11.

[4] **Мошкин В.Н.** Воспитание культуры безопасности школьников. Монография. Барнаул: БГПУ, 2002. 310 с.

Рис. 1. Источники угроз информационной безопасности младшего школьника

• дозированной (уровень риска регулируется тренером, сотрудником службы безопасности, подростком, выбирающим себе партнёра для драки и т.д.);

• реально опасной (человек самостоятельно противостоит вредным и опасным факторам, которые влияют на него в полном объёме)[5].

Существует много способов защиты от информационного воздействия, например, в рамках западных public relation есть отдельная профессия «лечения ситуации» – spin doctor. Выделяются два варианта такой техники: подготовка ожиданий перед наступлением самого события и исправление освящения в случае, когда ситуация движется не в том направлении. Противодействие должно строиться с учетом того, что своими действиями можно усилить информационную агрессию другого. Особенно этот аспект важен при борьбе со слухами, поскольку перевод слуха из устной в официальную форму способствует его распространению, и он начинает трактоваться как правдивая информация[6].

Ситуации информационных угроз с точки зрения наиболее опасных для жизнедеятельности младшего школьника можно условно разделить на четыре группы: дома, на улице, в общеобразовательной школе, в учреждениях дополнительного образования. Так как степень свободы ребёнка младшего школьного возраста невелика в силу того, что он большую часть времени находится под присмотром взрослых, в каждой из этих групп перечислим основные ситуации и соответствующие им источники (рис. 1), несущие в себе явную или скрытую угрозу безопасности ребёнка:

• дома («Звонок в дверь», «Негативное влияние определённой литературы, отдельных ТВ программ, Интернета», «Телефонный звонок» и др.);

• на улице («Разговор с незнакомым человеком», «Разговор со сверстниками, друзьями, знакомыми о благосостоянии семьи» и др.);

[5] Там же.

[6] **Самоделова Л.А.** Изучение основ информационной безопасности в системе дополнительного образования // Автореферат диссертации на соискание ученой степени кандидата педагогических наук / М.: Институт содержания и методов обучения РАО, 2005. 17 с.

• в школе («Неадекватное поведение персонала образовательного учреждения и одноклассников по отношению к учащимся, распространение о нём и его семье негативной информации» и др.);

• в учреждениях дополнительного образования («Подверженность воздействию посторонних людей особенно при проведении экскурсий, соревнований» и др.).

Рассмотрим возможные угрозы информационного воздействия на личность младшего школьника. Средства массовой информации представляют угрозу для личности в случае многократного повторения негативной информации. При отсутствии цензуры детская литература несёт угрозу психическому и нравственному здоровью детей. Различные направления в искусстве угрожают духовному развитию личности. Неправильно организованный образовательный и воспитательный процесс может стать угрозой здоровью, духовно-нравственному состоянию ребёнка. Личное общение угрожает манипулированием сознанием человека и даже может привести к опасным физическим последствиям для здоровья ребёнка.

Чтобы быть независимым от информации, необходимо, прежде всего, обратить внимание на источник информации, достоверность информации и информационную угрозу. В качестве источников информации можно выделить следующие:

• литература и искусство (отсутствие цензуры, реклама, фильмы);

• образование и воспитание (учитель, педагог дополнительного образования, обслуживающий персонал);

• личное общение (взрослые люди, другие дети и др.) и сетевые коммуникации (телевидение, Интернет).

Попробуем классифицировать угрозы информационной безопасности с точки зрения наиболее опасных для младшего школьника:

• угрозы обмана с целью наживы и/или физического воздействия;

• угрозы нравственного и психологического воздействия;

• угроза утечки конфиденциальной информации.

Основу обучения информационной безопасности младших школьников составляют базовые умения работы с информацией для формирования которых нужно:

1) развить возможности критического мышления ребёнка (уметь анализировать ситуацию, имеющуюся информацию, сопоставлять её с ранее известной, делать выводы, сравнивать, обобщать);

2) научить выделять источник информации в сложившейся ситуации;

3) дать представления о различных видах предлагаемой информации: недостоверной, неэтичной, непристойной, деструктивной;

4) научить выделять информационную угрозу, понимать возможность её негативного воздействия (вред жизни, здоровью, учёбе, межличностному общению);

5) научить способности принимать единственно правильные решения в зависимости от сложившейся ситуации (позвонить по нужному номеру телефона, бежать, кричать, сказать взрослым и др.).

Для обеспечения безопасности младшего школьника сформируем модель ситуационного обучения информационной безопасности, в основу которой положим обучение ребёнка поведению в различных типовых ситуациях, подразумевающих информационную угрозу. Типовые ситуации разбиты на четыре группы, представляющие собой социальное окружение младшего школьника: дом и семья, вне дома и детских учреждений, школа, система дополнительного образования.

Модель основывается на психолого-возрастных особенностях восприятия информации, учитывает поведенческие особенности ребёнка в соответствующей обстановке и подразумевает анализ его социального окружения. Модель обучения младшего школьника информационной безопасности представлена на рисунке 2.

Рис. 2. Модель ситуационного обучения информационной безопасности

Представленная модель подразумевает постановку проблемных ситуаций и их разрешение посредством применения алгоритма поведения в ситуации информационной угрозы. Малых Т.А. в исследовании педагогических условий развития ИБ младшего школьника особо останавливается на нравственных аспектах в обучении ИБ и определяет «условия проведения занятий: создание реальных ситуаций, предполагающих нравственный выбор, духовно-нравственное самоопределение, наличие наглядных пособий: детской периодической литературы, компьютерных дисков, имитированных моделей сотовых телефонов и т. д.»[7].

Вопросам обеспечения информационной безопасности в школе уделяется все большее внимание, как в отечественных, так и в зарубежных исследованиях в силу стремительно возрастающего потока угроз, характерных для развивающегося информационного общества. К примеру, с 2011 года в школах Англии планируется ввести новый обязательный курс, для обучения детей безопасному поведению в Интернете. Эти уроки безопасности являются одним из составных элементов новой государственной стратегии под названием «Click Clever, Click Safe» («Кликай умно, кликай безопасно»)[8].

[7] **Малых Т. А.** Педагогические условия развития информационной безопасности младшего школьника // Диссертация на соискание ученой степени кандидата педагогических наук / Иркутск: ГОУ ВПО «Иркутский государственный педагогический университет», 2008. 168 с.

[8] Англия вводит школьный курс безопасности в Интернете // http://soft.mail.ru/pressrl_page.php?id=36325
Internet safety for children targeted / By Jonathan Fildes. Technology reporter, BBC News.// http://news.bbc.co.uk/2/hi/technology/8398763.stm

Достаточно полную информацию о состоянии компьютерной преступности, проблемах организации борьбы с компьютерной преступностью и кибертерроризмом дает сайт Центра исследования компьютерной преступности (Computer Crime Research Center) являющийся международной, некоммерческой, негосударственной, научно-исследовательской организацией, функционирующей на принципах волонтерства. (http://www.crimeresearch.ru)[9]. Главное направление в деятельности Центра – широкое информирование общественности об основных проблемах, с которыми сталкивается общество в сфере противодействия компьютерной преступности, и о способах их решения.

В сети Интернет на многих сайтах даны рекомендации по обеспечению информационной безопасности детей[10]. Например, для того чтобы незнакомец не смог «заговорить» и обмануть ребёнка, на одном из сайтов предлагается так отрепетировать порядок разговора:

Шаг 1. Оцениваем ситуацию. Ребёнок должен осознать, что перед ним – незнакомый человек. Неважно, кто это – девочка, мальчик, дедушка, молодая женщина; если незнакомец, вести себя со всеми ними нужно практически одинаково.

Шаг 2. Держим дистанцию! Необходимо отмерить дома на полу расстояние 2 метра и попросить ребёнка запомнить его для выполнения важного правила – вести беседу с незнакомцем можно только на безопасной дистанции. Если человек приближается – надо уходить или убегать в безопасном направлении.

Шаг 3. Умело пресекаем разговор на 5-й секунде. Среди злоумышленников попадаются прекрасные психологи, которые могут «заболтать» и взрослого, не говоря уж о ребёнке. Поэтому беседа может длиться 5–10 секунд, после чего необходимо принимать решение.

Шаг 4. Уходим в безопасное место. Это значит, нужно подойти к находящимся во дворе знакомым мамам и папам других детей либо уйти домой (информировать родителей о произошедшем инциденте)[11].

Таким образом, предлагается простой алгоритм действия в определённой ситуации потенциальной угрозы ребёнку. Проанализировав и обобщив подобные конкретные ситуации информационных угроз, можно получить типовой алгоритм поведения ребенка в таких ситуациях.

Основными задачами обучения младшего школьника информационной безопасности являются:

- обучение анализу информации с точки зрения воздействия на физическое, психическое здоровье, нравственные ценности;

- создание мотивации для получения необходимых знаний в области ИБ;

- формирование понятия информационной угрозы, умения выявлять источники информационной угрозы;

- развитие способности размышлять о себе и мире вокруг себя;

- развитие логических форм мышления – суждения, умозаключения, действия по алгоритму.

Учебная деятельность, основанная на моделировании, предполагает усвоение алгоритма действий, способствующего формированию осознанной цели учения и рациональной организации учебных действий. Игровое моделирование, опираясь на важные методические правила (партнерский стиль игрового взаимодействия и пространственновременные ограничения сферы общения между участниками игрового обучения), имеет большие возможности, т. к. игра как модель объективной реальности делает более понятной ее структуру и вскрывает важные причинноследственные связи.

[9] Маклаков Г. Ю. Научно-методологические аспекты подготовки специалистов в области информационной безопасности Источник: Crime-Research.Ru, http://daily.sec.ru/dailypblshow.cfm?rid=45&pid=11837&pos=13&stp=50 (Публикация от 10-02-2005)

[10] Информационная программа безопасности граждан // http://ugrozenet.ru
Безопасность в Интернет // http://letopisi.ru/index.php/Безопасность_в_Интернет, http://www.webwisekids.com.
Безопасный интернет / Портал Российского Оргкомитета по проведению Года Безопасного Интернета // http://saferinternet.ru

[11] Ветка ивы. Насилие не сломает нас // http://www.vetkaivi.ru/main/kids

Рассматривая необходимость формирования практических умений и навыков в режиме игрового взаимодействия, требуется соблюдение комплекса общих принципов:

• обучающей направленности игрового моделирования (выражается в передаче и усвоении новых знаний, умений и навыков, причем учащиеся не получают «готовые знания», а сами приходят к ним в силу своей активности);

• упражнения (включение активности участников);

• подготовленности (касается индивидуальной мотивации участников игрового обучения и внутреннего желания сделать все возможное для принятия решения по предлагаемой проблеме);

• ассоциаций (предполагает, что усвоение новых сведений в условиях обучения с помощью игрового моделирования будет более эффективным, если обучение базируется на имеющейся информации);

• группового взаимодействия и общения (позволяет оттачивать коммуникативные умения, апробировать выбор стратегий взаимодействия и моделей общения, снять стереотипы, научить сотрудничеству)[12].

В человеческой деятельности сосуществуют и противоборствуют два компонента – нормативный и вариативный. Первый закрепляет уже накопленный людьми опыт, а без второго не может быть творчества, развития, движения вперед. Если социальные действия как процесс разбить на последовательность отдельных шагов (операций), то необходим учет соблюдения их последовательности, т.е. построения алгоритма. Огромное разнообразие задач, способов их решения определяется и порядком выполнения действий: разветвляющимся и циклическим. В отличие от линейных алгоритмов, рассматривающих получение результата по одной и той же последовательности, социальные алгоритмы изначально предполагают более сложную структуру с развилками (выбор социального действия), циклами с предусловием, с постусловием (действия, учитывающие определенные ограничения, например, по времени принятия решения, ресурсам и т.д.). Идея алгоритмизации положена в основу идеологии технологизации социальных процессов, поскольку социальные технологии определяются как способ осуществления деятельности, связанный с ее расчленением на отдельные операции (действия), соблюдением их определенной последовательности, выбором наиболее рациональных способов (методов) выполнения. Социальные алгоритмы составляют существо социальных технологий, собственно технологическую их часть, а творческая часть определяется спецификой социальной деятельности[13].

Для обучения ребёнка информационной безопасности необходимо рассмотреть типовые ситуации информационных угроз. Младший школьник только начинает постигать азы продуктивной умственной деятельности, требующей от него усидчивости, сдерживания эмоций, сосредоточения и поддерживания внимания, поэтому целесообразно занятия по информационной безопасности в начальных классах строить в форме игровых занятий с учётом возрастных особенностей, с проигрыванием социальнопсихологических ролей. В результате формируется определенный алгоритм поведения в конкретной ситуации информационной угрозы, общий вид которого представлен на рисунке 3.

Для примера рассмотрим алгоритм поведения ребенка в ситуации информационной угрозы «Звонок в дверь»: ребёнок дома один, в дверь звонит незнакомый человек, говорит, что в доме пожар и необходимо срочно эвакуироваться.

На первом этапе возникшей ситуации угрозы нужно, по возможности, не обнаруживая себя и не сообщая о себе (особенно о том, что ребёнок находится один) никакой информации, получить как можно больше сведений. В данном случае – посмотреть

[12] **Фоминых М.В.** Технология игрового моделирования как фактор активного развития личности обучающегося в процессе непрерывного профессионального образования // Проблемы непрерывного образования: проектирование, управление, функционирование: Материалы международной научно-практической конференции. В 3 ч. Липецк: ЛГПУ, 2009. Ч. 1. 275 с. С. 175-177.

[13] **Бурмыкина И.В.** К вопросу о соотношении понятий «социальный алгоритм» и «социальная технология» // Проблемы непрерывного образования: проектирование, управление, функционирование: Материалы международной научно-практической конференции. В 3 ч. Липецк: ЛГПУ, 2009. Ч. 2. 190 с. С. 128–129.

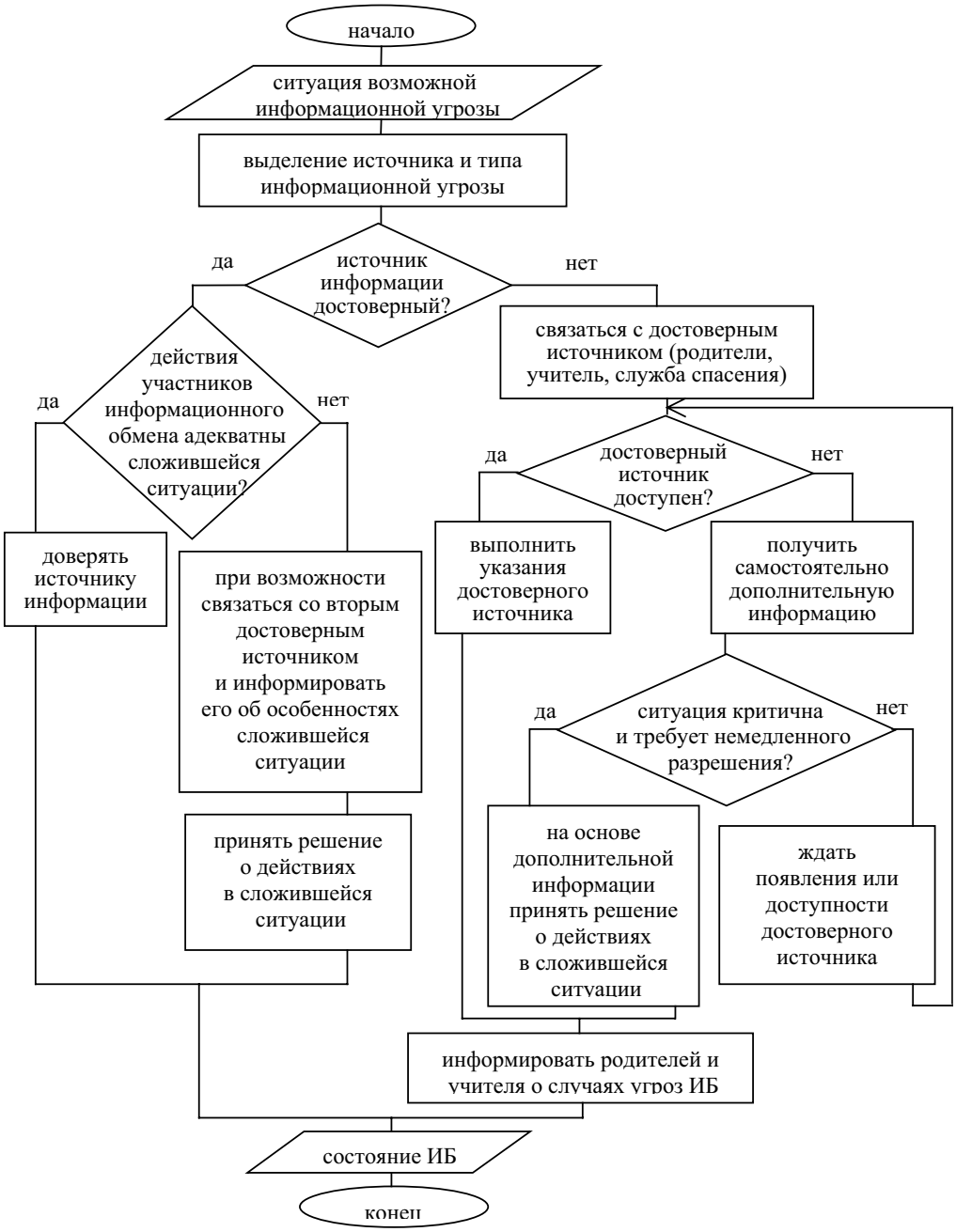

Рис. 3 Типовой алгоритм поведения ребенка в ситуации информационной угрозы.

в «глазок», прислушаться к раздающимся за дверью голосам, убедиться в том, что пахнет дымом.

Прежде всего, ребёнку необходимо уметь дать объективную оценку предлагаемой информации, удостовериться в её истинности и надёжности и в соответствии с полученным результатом принять единственно правильное решение, которое поможет сохранить жизнь и избежать риска быть обманутым недобросовестными людьми. Для анализа информации важно понять: от кого она поступила, и кто в этот момент находился рядом с источником информации (милиционеры, пожарные, соседи, другие люди); не проявляют ли незнакомые люди интерес только к вашей квартире, не раздаётся ли за дверью подозрительный шёпот (незнакомцы втайне

договариваются о своих последующих действиях).

Если человек незнакомый, то нужно попытаться:

• связаться с родителями и/или получить дополнительную информацию, посмотрев в окно (есть ли во дворе пожарная или милицейская машина, скорая помощь, пожарные, соседи, вышедшие из своих квартир с самыми необходимыми вещами, дым);

• связаться с соседями по телефону, выйти на балкон и позвать на помощь соседей, попросить их подойти к двери вашей квартиры и проверить людей, обращающихся к вам через дверь.

При успешном разрешении ситуации информационной угрозы, даже если ситуация показалась ребёнку незначительной, необходимо научить его информировать родителей о подобных случаях. Родители должны обсудить с ребёнком правильность его действий и порекомендовать, как себя вести в подобных ситуациях, а также принять меры, соответствующие повторным ситуациям информационных угроз.

При проигрывании этой и других ситуаций на уроках под руководством учителя можно рассмотреть типовые варианты развития ситуаций информационных угроз, а также обратить внимание на развитие критического мышления ребёнка.

В обучении информационной безопасности должны принимать участие родители, учителя, сотрудники правоохранительных органов и социальных служб, ответственные за воспитательную работу в образовательном учреждении. Не только младших школьников необходимо обучать ИБ, их родителям следует знать основы совместного (с учителями и с самим ребёнком) обеспечения ИБ.

Вследствие неразработанности проблемы обеспечения непрерывной информационной безопасности школьников и методики ее комплексной реализации на уровне семьи и школы происходит перекладывание ответственности педагогов на родителей, а родителей, в свою очередь, на педагогов и работников системы дополнительного образования. В связи с этим родители должны обеспечить ребенка средствами оперативной связи, чтобы при необходимости информировать их (либо учителя или службу спасения) о возможных угрозах. При невозможности немедленного личного вмешательства в ситуацию угрозы ребенку, родители должны оценить сложившуюся ситуацию, привлечь к её разрешению других людей или социальные службы, находящиеся в непосредственной близости от ребёнка, способные максимально быстро вмешаться в ситуацию. Родители также должны успокоить ребёнка и в нескольких словах объяснить, как ему действовать в данной ситуации.

Работа с родителями по поддержке обучению учащихся ИБ может проходить на родительских собраниях. Моделировать ситуации информационных угроз, в которых роли будут распределяться между учителями, родителями и самими учащимися, можно как на классных часах, так и на уроках информатики.

Методика изучения основ ИБ в учебных центрах системы дополнительного образования может базироваться на системе задач, моделирующих реальную ситуацию, в которой требуется на основе анализа данной ситуации выстроить систему информационной защиты[14].

Задача преподавателя заключается в распределении ролей и управлении ходом развития смоделированной ситуации. После того как ситуация проиграна, учащиеся совместно со взрослыми под руководством учителя (педагога дополнительного образования) обсуждают правильность действий ребенка, подвергшегося информационной угрозе, объясняют возможные варианты развития событий, дают советы по оптимальному разрешению ситуации. ❑

[14] Самоделова Л.А. Изучение основ информационной безопасности в системе дополнительного образования // Автореферат диссертации на соискание ученой степени кандидата педагогических наук / М.: Институт содержания и методов обучения РАО, 2005. 17 с.