МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ФОРМИРОВАНИЮ ОСНОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЧАЩИХСЯ ПРИ ОБУЧЕНИИ ИНФОРМАТИКЕ И ИКТ

В связи с переходом к информационному обществу и внедрением инновационных компьютерных технологий в образовательный процесс, с изменением целей обучения, его направленностью на развитие творческой активности школьников возрастает роль самостоятельной деятельности учащихся с использованием ресурсов сети Интернет. Доступ несовершеннолетних к сайтам дает им возможность изучать образовательный контент, общаться с ровесниками, узнавать о проводимых конкурсах, олимпиадах и, принимая в них участие, использовать интернет в качестве источника для собственного развития. Однако использование интернета вместе с возможностями несет и риски, такие как:

– прочтение несовершеннолетними информации, вредящей их мировоззрению и психотическому состоянию и др.;

– воровство их аккаунтов и личных данных;

– втягивание несовершеннолетних в асоциальную деятельность (группы с рекламой наркотиков, группы смерти и т.д.);

– издевательство ровесников и незнакомцев в сети над несовершеннолетним.

Поэтому есть основания утверждать, что проблемы информационной безопасности должны находиться в поле зрения не только специалистов в области национальной безопасности, правоведов, но и педагогов.

Базовым концептуальным документом, определяющим политику государства в этой области, является Доктрина информационной безопасности Приднестровской Молдавской Республики на 2020–2026 годы, в которой обозначены интересы личности и общества в целом. В области образования вопросы информационной безопасности детей и подростков нашли свое отражение в плане мероприятий, направленных на реализацию Доктрины информационной безопасности Приднестровской Молдавской Республики на 2020–2026 годы (Приказ МП ПМР от 10.11.2020 года № 1058).

Методические рекомендации подготовлены с целью оказания методической поддержки учителей информатики и ИКТ по проблеме формирования основ информационной безопасности учащихся.

Понятие информационной безопасности личности школьников толкуют как «состояние защищенности основных интересов учащихся от угроз, вызванных информационным воздействием на психику и социокультурное развитие различными социальными субъектами и информационной средой общества, в том числе образовательной средой» [2].

Рекомендации по организации обучения информационной безопасности в рамках школьного курса «Информатика и ИКТ»

Одним из путей обеспечения информационной безопасности школьников является организация учителем безопасного личностного информационного образовательного пространства. В организации безопасного личностного информационного пространства определены следующие группы мероприятий информационной безопасности школьников: правовые; технические и программные; организационные; моральные и этические. Рассмотрим их подробнее [1].

Правовое обеспечение – это специальные законы и другие нормативные акты, правила, процедуры и меры по обеспечению личной информационной среды учеников на законодательной и правовой основе для реализации единой государственной политики в сфере защиты детей от информационных материалов, наносящих вред их здоровью и психике.

Техническое и программное обеспечение – использование различных аппаратных и программных средств для препятствования нанесению материального и морального вреда человеку, в частности ребенку, разрушению программ информационного контроля, сетевых фильтров, технических средств защиты данных.

Организационная защита – это регламентация информационной деятельности подростков, контроль использования сетевых сервисов и сообществ, исключающие или ослабляющие нанесение вреда личному информационному образовательному пространству школьника. Для организации защиты сознания пользователя, в том числе сознания школьников, от вредного информационного

воздействия из сети Интернет на уровне программного обеспечения целесообразно осуществлять комплексное применение программ для защиты компьютерной системы от вирусов и вредоносного программного обеспечения, фильтрации контента сети Интернет, учительского контроля с применением постоянно возобновляемых «черных» и «белых» списков сайтов.

Моральный и этический аспект – соблюдение школьниками во время осуществления информационной деятельности норм и правил поведения в образовательном обществе, а также сетевой культуры и этики.

Также учителям информатики и ИКТ при составлении Рабочей программы учебного предмета необходимо учитывать информационные аспекты формирования информационной безопасности. С этой целью рекомендуется включить рассмотрение следующих вопросов обеспечения информационной безопасности при изучении целого ряда тем:

– тема «Информация и информационные процессы»: владелец информации; информация общедоступная, конфиденциальная, государственная, коммерческая и личная; особый вид информации – реклама (добросовестная и достоверная); информационная безопасность, виды угроз конфиденциальности информации (разглашение, утечка, несанкционированный доступ);

– тема «Компьютер – универсальное устройство обработки данных»: способы и средства обеспечения надежного функционирования средств ИКТ; применение специализированных программ для обеспечения стабильной работы средств ИКТ; технологические требования при эксплуатации компьютерного рабочего места;

– тема «Коммуникационные технологии»: инструменты коммуникации (электронная почта; социальные сети и мессенджеры); поиск информации; назначение файлов cookie; понятие «информационный след»; онлайн-игры; спам; пользовательское соглашение; защита интеллектуальной собственности в сети; информационные этика и право;

– тема «Компьютер как средство автоматизации информационных процессов»: организация информации в среде коллективного использования информационных ресурсов; защита информации шифрованием; электронная цифровая подпись;

– тема «Основы социальной информатики»: социальные сети – организация коллективного взаимодействия и обмена данными; проблема подлинности полученной информации; информационная культура; сертифицированные сайты и документы; технологии информационно-психологического воздействия (манипулирование информацией, эмоциональное комментирование, манипуляции с опросами общественного мнения; «эффект CNN»; пр.). При изучении этой темы необходимо рассмотреть и потребительские аспекты информационной безопасности – получение и приобретение различных товаров и услуг в сети Интернет: электронные деньги и банковские карты; покупки в сети; сетевое и мобильное мошенничество.

Рекомендации по организации обучения информационной безопасности в рамках внеклассных мероприятий по информатике и ИКТ

Для повышения эффективности внеклассных мероприятий по обеспечению информационной безопасности обучающихся при работе в сети Интернет рекомендуется учитывать различные цели обучения в зависимости от ступени обучения [3]. Так, по мнению практиков, для обучающихся начальной школы рекомендуется рассматривать основные аспекты осуществления деятельности в сети Интернет и мерах собственной защиты, в частности с учетом отсутствия у многих детей в данном возрасте собственной электронной почты. Для обучающихся средней школы вопросы информационной безопасности рекомендуется расширить за счет изучения технических аспектов информационной безопасности, вопросов законодательства и ответственности, правил и условий получения, изготовления и распространения информации и других аспектов, позволяющих обучающимся не только знать меры защиты, но и источники и принципы работы сетевых рисков. В старшей школе вопросы информационной безопасности рекомендуется изучать в той мере, которая позволит самому обучающемуся стать источником достоверной информации по вопросам информационной безопасности для своих ровесников и младших обучающихся.

При организации внеклассных мероприятий в аспекте обучения информационной безопасности рекомендуется придерживаться следующей примерной тематики:

1. Тема «Личное цифровое пространство и его безопасность». Тема предполагает следующее содержание: определения понятий «цифровое пространство», «личное цифровое пространство», «цифровой след», «цифровая репутация». Основные компоненты личного цифрового пространства в сети Интернет. Понятие «безопасность личного цифрового пространства». Актуальные угрозы личного цифрового пространства в сети Интернет.

2. Тема «Электронная почта как основа личного цифрового пространства. Безопасность персональной переписки» предполагает следующее содержание:

Электронная почта. Создание электронной почты. Настройка личного электронного ящика (настройка безопасности, оформления, настройка электронной подписи). Электронное письмо. Правила подготовки электронного письма. Работа с входящими письмами (сортировка писем, работа с помеченными письмами, удаление спама, очистка корзины). Актуальные угрозы информационной безопасности при работе с электронной почтой (утечка переписки, взлом личного почтового ящика, спам-рассылка, вирусы и фишинговые ссылки в письме). Методы защиты электронной почты.

3. Тема «Облачное хранилище и безопасность личного цифрового пространства в сети Интернет» предполагает следующее содержание:

Понятие «облачное хранилище». Облачное хранилище как часть личного цифрового пространства. Виды облачных хранилищ. Основные параметры и характеристики. Возможности облачных хранилищ. Создание папок в облачном хранилище. Загрузка и выгрузка файлов. Создание документа в облачном хранилище. Понятие «совместный доступ». Доступ по адресу. Доступ по ссылке. Совместная работа с документом в облачном хранилище. Создание таблиц. Работа с таблицами в совместном доступе. Создание презентаций. Работа с презентациями в совместном доступе. Выгрузка файлов, созданных в облачном хранилище. Актуальные угрозы информационной безопасности при работе с облачным хранилищем. Организация безопасной работы с облачным пространством в сети Интернет.

4. Тема «Блог и безопасность личного цифрового пространства в сети Интернет» предполагает следующее содержание:

Определение понятия «блог». Блог как компонент личного цифрового пространства в сети Интернет. Правила создания и ведения блога. Сервисы для создания блога. Разработка структуры личного блога. Дизайн блога. Создание личного блога. Блог и цифровая репутация. Правила проектирования цифровой репутации. Публикация материалов в личном блоге и защита авторского права. Этические нормы при разработке блога.

5. Тема «Безопасность личного цифрового пространства в социальной сети» предполагает следующее содержание:

Социальная сеть. Виды социальных сетей. Создание групп в социальной сети. Публикация материалов в группе в социальной сети. Сообщества. Создание сообщества. Публикация материалов в сообществе. Группы и форумы. Комментирование в форумах, группах, сообществах. Этические нормы при работе в социальной сети. Социальная сеть и цифровая репутация. Правила проектирования цифровой репутации в социальной сети. Актуальные угрозы безопасности личного цифрового пространства в социальной сети. Искажение информации. Кибербуллинг. Способы организации безопасной работы в социальной сети.

6. Тема «Информационная безопасность и личный видеоканал в сети Интернет» предполагает следующее содержание:

Видеоканал. Правила ведения видеоканала. Правила создания видеоматериалов для личного канала. Личный видеоканал и формирование цифрового имиджа. Создание видеоканала в YouTube. Личный видеоканал и информационная безопасность. Личный видеоканал и цифровая репутация. Этические нормы и правила при ведении личного видеоканала.

7. Тема «Информационная безопасность и управление личным цифровым пространством с использованием мобильного устройства» предполагает следующее содержание:

Работа с электронной почтой с использованием мобильного устройства. Настройка работы с облачным хранилищем на мобильном устройстве. Управление мобильными приложениями (электронные календари, планеры, мессенджеры, загрузки торрентов и файлов и др.). Управление документами на мобильном устройстве. Управление сообществом в социальной сети с использованием

мобильного устройства. Мобильный телефон и угрозы безопасности личного цифрового пространства в сети Интернет. Методы защиты от вредоносных программ. Меры обеспечения безопасности при работе в общедоступных сетях Wi-Fi. Меры по обеспечению безопасности мобильного телефона.

8. Тема «Презентация личного цифрового пространства в сети Интернет» предполагает следующее содержание:

Подготовка к презентации личного цифрового пространства в сети Интернет. Презентация личного цифрового пространства в сети Интернет.

Внеклассные мероприятия по формированию информационной безопасности учащихся можно приурочить к следующим профессиональным праздникам:

– Всемирный день информации (World Information Day) – 26 ноября. Праздник проводится ежегодно с 1994 года по инициативе Международной академии информатизации (МАИ), имеющей генеральный консультативный статус в Экономическом и Социальном советах ООН, и Всемирного информациологического парламента (ВИП);

– Международный день защиты информации – 30 ноября. Праздник существует с 1988 года, когда была зафиксирована первая массовая эпидемия компьютерного червя. Цель – напомнить всем о необходимости защиты компьютерной информации, а также обратить внимание производителей и пользователей аппаратных и программных средств на проблемы безопасности;

– Международный день безопасного интернета – второй вторник февраля (введен в 2004 году). Сайт Международного дня безопасности интернета www.saferinternetday.org

– Международный день интернета – ежегодно отмечается 4 апреля – в день смерти святого Исидора Севильского, покровителя учащихся и студентов, который создал первую в истории энциклопедию «Этимология» в 20 томах. Дата 4.04 очень похожа на ошибку HTTP 404;

– Всемирный день электросвязи и информационного общества (ВДЭИО) – празднуется ежегодно 17 мая с 1969 года.

При разработке содержания программы внеурочной деятельности по одной из предлагаемых выше тем следует учесть, что оно должно быть направлено

не только на ознакомление обучающихся с актуальными угрозами личного цифрового пространства в сети Интернет, мерами обеспечения безопасности этого пространства, но и на развитие компетенций обучающихся в направлении проектирования безопасного личного цифрового пространства в сети Интернет и его дальнейшего развития.

Основным методом обучения может стать метод проектов. В этом случае по завершении освоения программы внеурочной деятельности каждый обучающийся сможет представить проект личного безопасного цифрового пространства в сети Интернет или его элемента (блога, сообщества, видеоканала в сети Интернет и т.п.). При реализации метода проектов может быть организована групповая работа, например, по проектированию безопасного цифрового пространства в сети Интернет. В этом случае по завершении освоения программы внеурочной деятельности группа обучающихся презентует интернет-проект элемента цифрового пространства (например, сообщество класса, блог класса, облачное пространство класса и т.п.).

Пример подготовки группой учащихся ментальной карты по теме «Безопасность детей в интернете» размещен по адресу http://www.mindmeister.com/ru/12485180/

Итогом реализации проектной деятельности может стать и WEB-квест. Для примера можно рассмотреть WEB-квест «Безопасный интернет» http://www.web-kvest.pldetstva.edusite.ru/p1aa1.html Особенностью образовательных веб-квестов является то, что часть или вся информация для самостоятельной или групповой работы учащихся с ним находится на различных веб-сайтах, ссылки на которые может предложить педагог, предварительно выбрав самые интересные и информативные по изучаемому вопросу. Кроме того, результатом работы с веб-квестом может стать публикация работ учащихся в виде веб-страниц и веб-сайтов (локально или в сети Интернет).

При продумывании методов организации внеурочной деятельности важно помнить об особенностях мышления современных учащихся – «клиповом» мышлении, которое не отличается глубиной проникновения в информацию, но зато

отличается большими скоростями пропускания через себя информации. Решением данной проблемы могут стать задания по преобразованию одного вида информации в другой вид. Например, можно предложить информацию из видео или текст перевести в графику – плакат, комикс, инфографику или, наоборот, по картинке, плакату, комиксу, инфографике составить рассказ, объясняющий вопросы безопасности информации. Результаты деятельности важно предоставить общественности – опубликовать в интернете, выпустить газету для школы с результатами деятельности, выступить перед младшими школьниками.

При проектировании содержания программы внеурочной деятельности следует учесть, что она может быть реализована модульно, в рамках нескольких лет обучения. В этом случае желательно использовать концентрический подход.

Полезные ресурсы:

– *http://ppt4web.ru/informatika/bezopasnyjj-internet.html* – презентации о безопасном интернете;

– *http://i-deti.org/* – портал «Безопасный инет для детей»: рекомендации, комиксы, подборка обучающих и развивающих видеоматериалов, которые помогут детям получить представление о приемлемых моделях поведения в интернете;

– *http://www.igra-internet.ru/* – интернет-игра «Изучи интернет – управляй им» поможет юным пользователям Сети научиться ориентироваться в интернет-пространстве. Участники игры узнают о техническом устройстве Сети, ее разнообразных сервисах и возможностях. В игре также рассказывается об основных угрозах, которые подстерегают пользователей интернета, и о том, как избежать этих рисков;

– *http://www.ifap.ru/library/book099.pdf* – по этому адресу можно скачать брошюру «Безопасность детей в интернете».

Рекомендации по организации методической работы и повышению профессиональной компетентности педагогов в аспекте формирования основ информационной безопасности несовершеннолетних

Очевидно, что решение проблемы информационной безопасности школьников должно проходить под руководством грамотного педагога, который может учитывать все составляющие информационной безопасности обучающихся, осознает большое значение информационной безопасности в становлении личности школьника и обладает знаниями об условиях обеспечения защиты несовершеннолетних от информационных угроз.

Реализация Доктрины информационной безопасности Приднестровской Молдавской Республики на 2020–2026 годы требует активизации методической работы в различных направлениях и на различных уровнях. Рекомендуется организовать работу по рассмотрению на уровне институциональных и муниципальных методических объединений учителей информатики и ИКТ актуальных вопросов теории и практики формирования основ информационной безопасности учащихся с учетом эффективного педагогического опыта работы педагогов района (города):

– проектирование учащимся личного безопасного цифрового пространства в сети Интернет;

– формирование устойчивых поведенческих навыков учащихся в сфере информационной безопасности;

– развитие у учащихся способности распознавать и противостоять негативной информации в интернет-пространстве.

Вместе с тем вопросы информационной безопасности в интернете могут обсуждаться не только на уроках информатики, но и во время уроков ОБЖ, гражданского права, социологии и др. И в этом случае одним из главных условий повышения информационной безопасности является позиция взрослого (учителя, классного руководителя, психолога), сущность которой составляет желание укрепить позицию школьника в социуме, оказать своевременную поддержку в саморазвитии, оградить учащегося от совершения неприемлемых действий, открыть путь к социализации и адаптации в глобальном информационном обществе.

Как отмечают практики, для этой ситуации одной из эффективных форм организации методической работы с педагогическими работниками является решение ситуационных задач с использованием метода моделирования.

В решении ситуационной задачи выделяют несколько этапов: анализ ситуации, групповую дискуссию, моделирование конкретных действий на базе выработанного решения, подведение итогов.

Ниже предлагаются примеры ситуационных задач, позволяющих педагогическим работникам совместно выработать подходы к решению разного рода педагогических проблем, связанных с особенностями взаимодействия школьников в открытом информационном пространстве.

Ситуационная задача № 1. Ученица 5 класса рассказала своему классному руководителю, что группа ее одноклассников снимает на фото и видео все, что происходит на перемене. Чтобы было, что снимать, они берут чей-нибудь рюкзак, оставленный в коридоре, выбрасывают его в урну для мусора и ждут, когда владелец рюкзака начнет его искать. Фото и видео ученики выкладывают в разные социальные сети.

Ситуационная задача № 2. К психологу школы за советом обратился ученик 8 класса. Ученик рассказал, что около двух недель назад по электронной почте он получил приглашение от своего друга поиграть в интернет-игру, доступ к которой открывается по прикрепленной ссылке. Перейдя по указанной в письме ссылке, ученик в появившемся окне подтвердил свое участие, нажав какую-то кнопку. Игра оказалась очень увлекательной, но спустя день на электронную почту пришло письмо с незнакомого адреса с требованием оплаты участия. Ученик его проигнорировал, однако письма стали появляться каждый день и содержать угрозы благополучию его семьи. Со слов ученика он должен уже около 100 000 рублей. Родителям рассказать боится. Что предпринять, не знает.

Ситуационная задача № 3. Во время ужина ребенок сообщает своим родителям, что его одноклассники в социальных сетях создали группу, в которой публикуют видеозаписи фрагментов уроков, перемен, обсуждают деятельность педагогов и администрации школы, не стесняясь в выражениях. Ребенок не поддержал

идею своих одноклассников и открыто им об этом заявил, после чего стал получать сообщения, содержащие угрозы на свой телефон и страничку в социальной сети.

Ситуационная задача № 4. Во время перемены трое обучающихся 6 класса решили развлечься и снять фильм о своем классе. Один из компании учеников взял на себя роль оператора, а остальные принялись создавать разного рода ситуации, достойные, по их мнению, съемки. Дети громко назвали имена и фамилии одноклассников, которых снимали, выхватывали у них из рук вещи, пытались пинать, отбирали мобильные устройства, обзывали с использованием ненормативной лексики. В конце учебного дня видео с «приключениями» класса появилось в сети Интернет, которое смогли увидеть родители класса.

Очевидно, что участие в решении таких ситуационных задач психолога школы, классных руководителей, заместителя руководителя по воспитательной работе образовательной организации позволит не только выработать единые подходы к решению разного рода педагогических и организационных проблем формирования информационной безопасности учащихся, но и обозначить актуальные проблемы данного направления.

Таким образом, вопрос об обеспечении информационной безопасности несовершеннолетних особенно актуален. Ни для кого не секрет, что информация сегодня имеет куда больший вес, чем в прежние времена, и от того, какую информацию мы выбираем для себя истинной, напрямую зависит уровень информационной безопасности. Дети и подростки менее защищены в данном плане, именно поэтому тема обеспечения информационной безопасности несовершеннолетних востребована реальностью. Только грамотная и слаженная работа всех социальных институтов способна воспитать личность безопасного типа, и, что очень важно, работать нужно не вдогонку, а на опережение.

Список литературы

1. Бояров Е.Н. Безопасная информационная образовательная среда вуза: понятие и компоненты // Молодой ученый. 2014. № 18.1. – С. 20–23.

2. Бояров Е.Н. Теоретические основы построения безопасной информационной образовательной среды подготовки педагогов в области безопасности жизнедеятельности // Социосфера. 2012. № 4. – С. 101–106.

3. Дорофеева Т.В., Туманов И.А. Методические рекомендации по обеспечению информационной безопасности обучающихся при работе в сети Интернет. – СПб: ГБУ ДПО «СПбЦОКОиИТ», 2018.

***Н.Г. Пасевина**, вед. методист кафедры общеобразовательных дисциплин и дополнительного образования ГОУ ДПО «ИРОиПК»*