



В. В. Меньшиков,
дипломант конкурса ИНФО-2016 в номинации
«Современные модели нетрадиционного урока информатики»,
средняя общеобразовательная школа № 5, г. Сеgezha, Республика Карелия

УРОК-ИГРА НА ТЕМУ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»*

Аннотация

Представленный в статье урок направлен на формирование у учащихся знаний и умений в выявлении информационной угрозы, определении степени ее опасности и противостоянии ей. В ходе урока в игровой форме учащиеся знакомятся с основными опасностями сети Интернет и с направлениями деятельности отдела информационной безопасности.

Ключевые слова: информационная безопасность, угрозы, спам, вирус, троян, хакер, мошенничество, контент-фильтры, защита авторских прав, защита личных данных, защита от утечки информации.

Контактная информация

Меньшиков Виталий Владимирович,
учитель информатики средней общеобразовательной школы № 5, г. Сеgezha, Республика Карелия; *адрес:* 186420, Республика Карелия, г. Сеgezha, пр-д Бумажников, д. 7; *телефон:* (814-31) 7-07-32; *e-mail:* vitalimen@mail.ru

V. V. Menshikov,
School 5, Segezha, Republic of Karelia

THE LESSON-GAME ON THE THEME "INFORMATION SECURITY"

Abstract

The lesson presented in the article aims at developing students' knowledge and skills in the identification of information threats, determining the degree of danger and opposition to it. During the lesson in a playful way students get acquainted with the main dangers of the Internet and with the activities of the Information Security Department.

Keywords: information security, threats, spam, virus, trojan, hacker, fraud, content filters, copyright protection, protection of personal data, information leakage protection.

Данный урок был проведен в рамках проходившей с 5 по 15 сентября 2016 года Всероссийской акции, посвященной безопасности школьников в сети Интернет.

Тема урока: Информационная безопасность.

Цель урока: формирование у учащихся активной позиции в получении знаний и умений в выявлении информационной угрозы, определении степени ее опасности, предвидении последствий информационной угрозы и противостоянии ей.

Задачи урока:

обучающие:

- повторение понятий «информация», «безопасность»;
- знакомство с понятием «информационная безопасность»;
- знакомство с различными угрозами информационной безопасности;

развивающие:

- совершенствование коммуникативных навыков через умение излагать мысли, вести диалог;
- продолжение работы над умением определять план действий;
- формирование навыков поведения в информационном обществе с целью обеспечения информационной безопасности;
- повышение уровня информационной культуры;
- развитие познавательного интереса учащихся;
- расширение кругозора учащихся;
- продолжение формирования общеучебных умений и навыков;
- развитие коммуникативности, креативного мышления, активности и самостоятельности;
- повышение уровня социальной адаптации учащихся;

воспитательные:

- воспитание стремления к получению новых знаний;
- воспитание ответственности за свои действия;
- воспитание ответственности, самостоятельности, умения работать в паре и в группе;
- воспитание культуры общения.

Класс: V—VII.

Оснащение урока:

- цветные человечки (красный, зеленый, желтый, синий — см. фото 7), символизирующие определенную службу в деловой игре урока;
- листы цветной бумаги (красный, зеленый, желтый, синий) — раскладываются на столах в соответствии с названием группы (службы);
- карточки с анаграммами — для задания 1;

* Материалы к статье можно скачать на сайте ИНФО:
http://infojournal.ru/journals/school/school_02-2017/

- карточки с фрагментами определения информационной безопасности — для задания 5;
- тексты из интернет-источников, отражающие направления защиты информационной безопасности — для задания 7 (файлы *Приложение_1.doc* — *Приложение_8.doc*);
- конверты с фигурками детей для раскрашивания — для задания 8;
- листки со строчками текста стихотворения про информационную безопасность — для задания 9.

Список интернет-источников, использованных при подготовке урока.

1. *Абрамян С.* Авторские права и их защита в Интернете // Юрисконсульт. <http://www.urisconsult.spb.ru/info/article/avtorskie-prava-i-ix-zashhita-v-internete/>
2. *Беляев Д.* Преимущества использования лицензионного программного обеспечения: Мемуары о будущем // <http://bda-expert.com/2010/07/preimushhestva-ispolzovaniya-licenzionnogo-programmnogo-obespecheniya/>
3. Как защитить свой компьютер от вирусов // НРС. BY. http://hpc.by/safety_on_the_internet
4. Как защитить себя от утечки персональных данных // THG.RU. http://www.thg.ru/education/zashchita_ot_utechki_dannykh/index.html
5. Методы защиты от мошенничества в Интернет // SD Company. Программирование и создание сайтов. <http://sd-company.su/article/security/main>
6. Мошенничество в интернете // Интертелеком. <http://www.intertelecom.ua/ru/info/zakhyst-vid-shakhraystva/shakhraystvo-v-interneti>
7. Практические советы по защите от мошенничества в интернете // Winlie. Мир операционных систем. http://www.winline.ru/articles/prakticheskiye_sovety_po_zashhite_ot_moshennichestva_v_internete.php?PAGEN_1=2
8. Спам — что это такое. Виды спама, борьба с ним // iPipe.ru. <http://www.ipipe.ru/info/spam.html>

Ход основного этапа урока

Учащиеся заранее разделены на группы и рассажены за четыре стола. Столы оформлены следующим образом (фото 1):

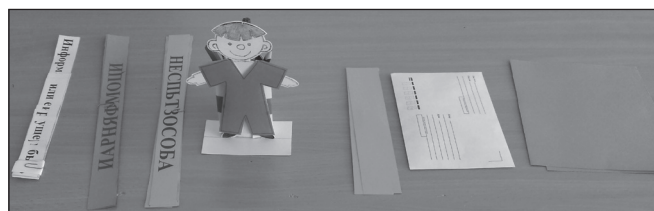


Фото 1

Учитель. Здравствуйте, ребята! Сегодня мы будем говорить об очень важных вещах. О чем именно, я пока вам не скажу, а предлагаю по ходу нашей работы узнать тему беседы.

Задание 1.

Учитель. У каждой группы на столе лежат полоски зеленого и розового цветов. Возьмите каждый одну полоску зеленого цвета и одну полоску розового цвета. На полосках записаны анаграммы. Разгадайте их.

Варианты анаграмм.

Группа 1. ЯФЦНИМОРАИ, ОЗЫТПСЕНСАБО.

Группа 2. ИАРНЯФМОЦИ, СЬСБОПОНАЗЕТ.

Группа 3. НЯРИЦАФИОМ, НЕСПЫТЗОСОБА.

Группа 4. ФМИНРАЦЯОИ, СЕЗЬПНАОСОТЬ.

Ответы. ИНФОРМАЦИЯ, БЕЗОПАСНОСТЬ.

После правильного ответа учащихся учитель вешает на доску таблички со словами «ИНФОРМАЦИЯ» и «БЕЗОПАСНОСТЬ» (фото 2).

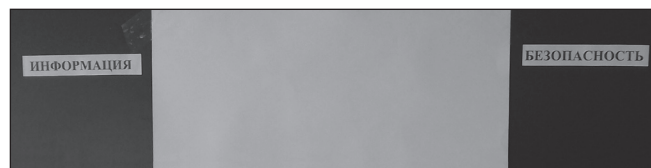


Фото 2

Задание 2.

Учитель. Обсудите в группах и дайте определения этих понятий.

После обсуждения каждая группа дает определения данных понятий. Учитель обобщает и, если необходимо, корректирует определения.

В результате учитель вешает на доску под табличкой со словом «ИНФОРМАЦИЯ» табличку с надписью «сведения об окружающем мире», а под табличкой со словом «БЕЗОПАСНОСТЬ» — табличку с надписью «защищенность от угроз» (фото 3).

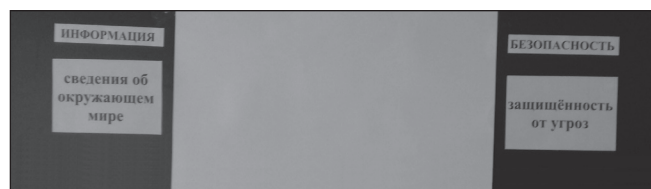


Фото 3

Задание 3.

Учитель. Составьте, пожалуйста, словосочетания из этих слов так, чтобы одно из них было существительным, а другое — прилагательным.

Ответ: безопасная информация, информационная безопасность.

Учитель вешает на доску таблички с надписями «БЕЗОПАСНАЯ ИНФОРМАЦИЯ» и «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» (фото 4).

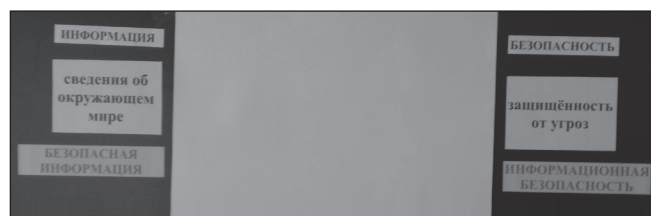


Фото 4

Задание 4.

Учитель. Сформулируйте, как вы понимаете словосочетание «безопасная информация».

Возможный ответ учащихся: безопасная информация — это сведения об окружающем мире, защищенные от угроз.

Учитель. Конечно, очень важно получать безопасную информацию и работать с ней, а также важно информацию защищать.

С 5 по 15 сентября 2016 года по инициативе Министерства образования и науки Российской Федерации в образовательных учреждениях проходит Всероссийская акция, посвященная безопасности школьников в сети Интернет. Поэтому я предлагаю создать сегодня в нашем классе отдел информационной безопасности.

Учитель наклеивает на лист ватмана табличку с надписью: «Отдел информационной безопасности» (фото 5).

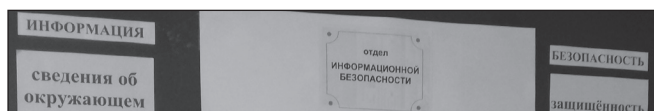


Фото 5

Задание 5.

Учитель. А что же такое информационная безопасность? Сформулируйте, пожалуйста, определение данного понятия. Для этого у каждой группы есть набор карточек со словами, из которых нужно собрать определение.

случайных	— это защищенность	инфор- мации	информа- ции
нанесение	от любых	может	которых
воздействий,	быть	самой	результата- том
ущерба	или злонамеренных	или ее владельцам	
Информационная безопасность			

Ответ. Информационная безопасность — это защищенность информации от любых случайных или злонамеренных воздействий, результатом которых может быть нанесение ущерба самой информации или ее владельцам.

Учитель наклеивает данное определение на лист ватмана под табличкой «Отдел информационной безопасности» (фото 6).

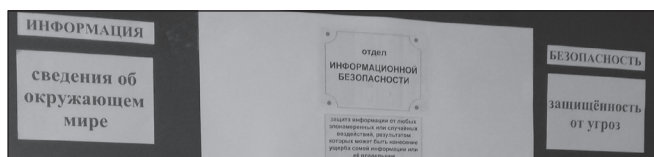


Фото 6

Учитель. Наш отдел информационной безопасности состоит из четырех служб, условно назовем их «Красная служба», «Зеленая служба», «Желтая служба» и «Синяя служба». На то, к какой именно службе относится каждая группа, указывают цветные человечки на столах (фото 7).



Фото 7

Задание 6.

Учитель. Уважаемые сотрудники отдела информационной безопасности! Предлагаю вам определить направления вашей работы, т. е. определить, защиту от каких воздействий на информацию будут осуществлять ваши службы (например, защиту личных данных).

Учитель наклеивает на лист ватмана надпись «защита личных данных» под надписью с определением понятия «информационная безопасность».

Учитель. Направления работы прошу записать на цветных листках, которые есть на ваших столах.

Работая в группах, учащиеся записывают на цветных листках направления работы. Через две-три минуты учитель по очереди спрашивает каждую службу, что они написали, и, если названное направление работы возможно, предлагает приклеить на лист ватмана соответствующий листок (фото 8).

По ходу обсуждения должен быть составлен список (если какие-то пункты не будут озвучены, то помогает учитель, если появляются дополнительные возможные пункты, то их тоже приклеивают).

- 1) установка контент-фильтров;
- 2) защита авторских прав;
- 3) защита личных данных, защита от утечки информации;
- 4) защита от вирусов, червей, троянов;
- 5) защита от мошенничества;
- 6) защита от спама;
- 7) защита от хакеров;
- 8) проверка лицензий программного обеспечения.

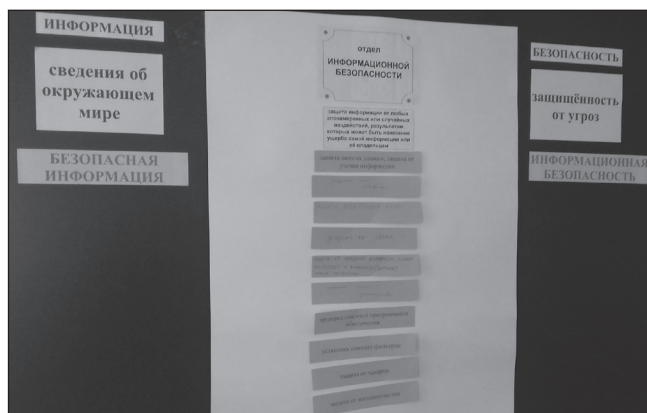


Фото 8

Задание 7.

Учитель. Молодцы! Мы обозначили направления работы отдела информационной безопасности. А теперь каждой службе предлагаю создать правила по каждому из этих направлений работы отдела.

Учитель предлагает каждой службе выбрать по два направления работы отдела информационной безопасности. Педагог выдает группам неадаптированные тексты (взяты из сети Интернет — см. выше список использованных источников) для работы службы. Каждая служба работает (в парах) с текстами и выписывает на лист своего цвета правила, позволяющие осуществить информационную безопасность.

Образец текста (файл *pril2.doc*).

Защита компьютера с помощью контент-фильтра.

Сегодня Интернет стал обязательной частью ежедневной жизни и образования.

Вместе с нужной информацией пользователи сталкиваются с ресурсами, имеющими неэтичное и враждебное содержание (контент). Терроризм, наркотики, националистический экстремизм, религиозные секты, неэтичная реклама — яркие образцы контента, с которым имеют все шансы соприкоснуться пользователи. Отказываться от Интернета и информационных технологий бессмысленно, но бесконтрольный доступ пользователей к Интернету может привести к:

- компьютерной зависимости;
- заражению вредоносными программами при скачивании файлов;
- нарушению нормального развития;
- знакомству с человеком с недобрыми намерениями.

Контент-фильтр, или программа ограничения веб-контента, — устройство или набор программ, которые обеспечивают отбор сайтов по их содержанию и не позволяют получить доступ к определенным сайтам или услугам сети Интернет.

Установка на компьютер контент-фильтра позволит ограничивать доступ не просто к отдельным веб-сайтам, а к целым категориям сайтов, объединенных по определенной теме.

Задачи контентной фильтрации:

- полное ограничение доступа к опасным, вредным, незаконным ресурсам, таким как насилие, терроризм и т. д.;
- запрет в рабочее время посещать социальные сети, развлекательные, новостные, игровые и другие не имеющие отношения к работе сайты;
- осуществление анализа доступа в разрезе категорий с определением, какие сайты наиболее популярны и на что стоит обратить внимание.

Во все российские школы поступила система контентной фильтрации — программа, позволяющая перекрыть выход на интернет-сайты, пропагандирующие экстремизм или наркотики. Важно, чтобы контент-фильтры были установлены во всех организациях, где компьютеры имеют выход в Интернет. Фильтр проводит проверку запросов пользователей. Когда набранное в браузере слово либо набор букв есть в черном перечне фильтра, запрос блокируется. В случае если, к примеру, происходит обращение к «нехорошему» ресурсу, неизвестному системе контентной фильтрации, то это обращение фиксируется, гиперссылка на него механически пересылается контентным фильтром на центральный узел системы. Там ресурс обрабатывается (определяется его содержание), и при следующем обращении к этому ресурсу доступ к нему будет заблокирован.

После работы с текстом представители каждой службы выступают по выбранным направлениям и при-

клеивают на лист ватмана результаты своей работы. «Сотрудники» других служб внимательно слушают и готовят вопросы по услышанному выступлению. После выступления задаются вопросы, на которые отвечают выступающие.

Возможные записи на цветных листах:

Защита компьютера с помощью контент-фильтра.

Задачи контентной фильтрации:

1. Полное ограничение доступа к опасным, вредным, незаконным ресурсам, таким как насилие, терроризм и т. д.
2. Запрет в рабочее время посещать социальные сети, развлекательные, новостные, игровые и другие не имеющие отношения к работе сайты.
3. Осуществление анализа доступа в разрезе категорий с определением, какие сайты наиболее популярны и на что стоит обратить внимание.

Защита авторских прав.

1. Правообладатель может использовать знак охраны авторского права.
2. Необходимо заключать авторский договор.
3. По возможности опубликовать в официальных средствах массовой информации свою статью с датой и указанием авторства.
4. Обратиться за консультациями к юристу или в юридическую фирму.
5. Защищать посредством записи информации на лазерный диск.
6. Установка водяных знаков в электронных копиях фотографий и изображений.
7. Защита при помощи специализированного программного обеспечения.
8. Включение в код веб-сайта команд, делающих невозможным копирование информации.
9. Ведение «черных списков» пользователей.
10. Получение сертификатов, удостоверяющих факт публикации.

Защита личных данных, защита от утечки информации.

1. Используйте временные адреса электронной почты.
2. Используйте одноразовые номера кредитных карт.
3. Используйте свой пароль для каждого аккаунта.
4. Не предоставляйте личную информацию.
5. Никогда не давайте номера документов.
6. Иногда придется выдать свой адрес.

Защита от вирусов, червей, троянов.

1. Работайте с ограниченными правами на своем компьютере.
2. Внимательно работайте с электронной почтой, особенно с вложениями.
3. Обновляйте операционную систему и самые распространенные программы.
4. Будьте осторожны при работе с внешними носителями информации.
5. Не переходите по ссылкам на сторонние сайты.
6. Не используйте креки, взломанные файлы и генераторы ключей.
7. Периодически сканируйте ваш компьютер на наличие вирусов с помощью дополнительных антивирусных утилит.

Защита от мошенничества.

1. Не оставляйте свои персональные данные на открытых ресурсах.
2. Не загружайте ничего со случайных сайтов.
3. Не проходите по ссылкам в спамовых письмах.
4. Не открывайте приложения в письмах, если есть хоть какие-то сомнения в надежности адресанта.
5. Не откликайтесь на заманчивые предложения, особенно если они связаны с получением быстрых денег.
6. Не сообщайте людям, которых вы не знаете, свои пароли от электронной почты, социальных сетей и форумов.
7. Не указывайте в паролях персональные данные (дату рождения, ФИО, номер телефона и т. д.).
8. Проверяйте адрес социальной сети.
9. Присмотритесь к названию сайта, почитайте отзывы про этот сайт в Интернете и старайтесь покупать товары там, где оплата будет уже после доставки.
10. Не отправляйте SMS на неизвестный номер.
11. Скачивайте новые версии браузера или антивирусной защиты исключительно с официального сайта.

Защита от спама.

1. Использование фильтров, предназначенных для защиты против нежелательной рекламы.
2. Установка капчи.
3. Использование антиспам-надстроек в блогах.

Защита от хакеров.

1. Не доверяйте спаму.
2. Скачивайте информацию с проверенных сайтов.
3. Обновляйте программное обеспечение.
4. Устанавливайте на компьютер антивирус с обновленными базами.
5. Не посещайте сомнительные сайты.
6. Будьте осторожны с тем, что попадает на ваш компьютер.

Преимущества использования лицензионного программного обеспечения.

1. Консультации специалистов.
2. Качество и полнота продукта.
3. Оперативная техническая поддержка фирмы-разработчика и компании-поставщика.
4. Получение обновлений.
5. Оформление подписки.
6. Надежность и защищенность.
7. Престиж и уважение.
8. Рациональное использование денежных средств.

Задание 8.

Учитель. Я благодарю всех за хорошую работу. Посмотрите, какой замечательный информационный плакат мы сделали. Осталось только его немного украсить и подписать авторов. Для этого в конвертах есть

фигурки людей. Выберите ту, которая больше всего похожа на вас:



Раскрасьте одежду человечка цветным карандашом цветом вашей службы и напишите на фигурке свое имя. Готовую фигурку приклейте на наш информационный плакат (фото 9).

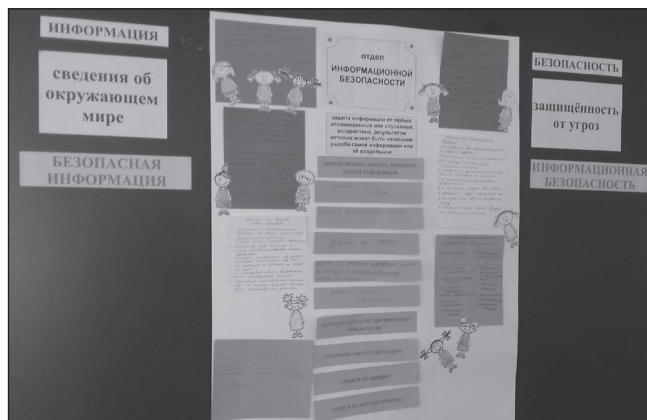


Фото 9

Учащиеся раскрашивают фигурки, подписывают на них свои имена и приклеивают на плакат.

В это время учитель раздает стихотворение, разрезанное на строчки.

Задание 9.

Учитель. В завершение нашей беседы предлагаю всем вместе прочитать стихотворение. Читаем по цепочке.

Информация — вещь очень хрупкая,
 Без защиты ей просто труба.
 А когда бережешь ее сутками,
 Подлых вирусов злитесь гурьба.
 Гигабайты своей информации
 Как зеницу очей сохраняй
 От любой сетевой махинации,
 За нее головой отвечай!
 В общем, будь начеку в наш суровый век,
 Файлы важные не растеряй,
 Будь предельно внимателен, человек,
 И пароль никому не вверяй.

Учитель. Мир информационной безопасности — огромный, сложный и очень интересный. В погоне за данными иногда разворачиваются целые войны. Мы сегодня поговорили о том, кто может охотиться за информацией и как ее защитить.