

Методические рекомендации по организации урока информационной безопасности в старшей школе

Анализ УМК по информатике и ИКТ для старшей школы на предмет изучения информационной безопасности позволяет сделать вывод о том, что на уровне среднего (полного) общего образования в рамках предмета «Информатика» акцент в соответствии с требованиями ФГОС делается на формировании знания норм информационной этики и права, принципов обеспечения информационной безопасности, способов и средств обеспечения надёжного функционирования средств ИКТ.

УМК «Информатика» 10-11 класс, базовый уровень, автор Угринович Н. Д.

11 класс. Тема «Компьютер как средство автоматизации информационных процессов» (5 ч) Содержание темы: Защита от несанкционированного доступа к информации. Защита с использованием паролей. Биометрические системы защиты. Физическая защита данных на дисках. Защита от вредоносных программ. Вредоносные и антивирусные программы. Компьютерные вирусы и защита от них. Сетевые черви и защита от них. Троянские программы и защита от них. Хакерские утилиты и защита от них. Тема «Информационное общество» (3 ч) Содержание темы: Право в Интернете. Этика в Интернете. Перспективы развития информационных и коммуникационных технологий.

УМК «Информатика» 10-11 класс, профильный уровень, автор Угринович Н. Д.

10 класс. Тема «Архитектура компьютера и защита информации» (7 ч) Содержание темы: Защита информации от вредоносных программ. Вредоносные программы и антивирусные программы. Компьютерные вирусы и защита от них. Сетевые черви и защита от них. Троянские программы и защита от них. Рекламные и шпионские программы и защита от них. Спам и защита от него. Хакерские утилиты и защита от них. Тема «Информационное общество» (10 ч) Содержание темы: Право в Интернете. Этика в Интернете. Перспективы развития информационных и коммуникационных технологий.

УМК «Информатика» 10-11 класс, базовый уровень, авторы Семакин И.Г. и др.

10 класс Тема «Защита информации» (2 ч) Содержание темы: Защита информации. Методы защиты.

11 класс Тема «Основы социальной информатики» (3 ч) Содержание темы: Информационная цивилизация. Информационные ресурсы общества. Информационная культура. Этические и правовые нормы информационной деятельности человека. Информационная безопасность.

УМК «Информатика» 10-11 класс, углубленный уровень (ФГОС), автор Семакин И.Г. и др.

11 класс Тема «Основы социальной информатики» (2 ч) Содержание темы: Информационная деятельность человека в историческом аспекте. Информационное общество. Информационные ресурсы общества. Информационное право и информационная безопасность

УМК «Информатика» 10-11 класс, углубленный уровень (ФГОС), авторы Поляков К.Ю., Еремин Е.А.

10 класс. Тема «Информационная безопасность» (6 ч) Содержание темы: Вредоносные программы. Защита от вредоносных программ. Шифрование. Хэширование и пароли. Современные алгоритмы шифрования. Стеганография. Безопасность в Интернете. Тема «Программное обеспечение» (1 ч). Содержание темы: Правовая охрана программ и данных. Тема «Компьютерные сети». Содержание темы: Право и этика в Интернете.

УМК «Информатика» 10-11 класс, углубленный уровень (ФГОС), авторы Калинин И. А., Самылкина Н. Н.

11 класс Тема «Сети и сетевые технологии» (12 ч) Содержание темы: Защита данных в сетях. Анализ передаваемых по сети данных. Настройка персонального брандмауэра. Контроль работы приложений с сетью. Обнаружение внешних атак. Сертификаты и доверие. Демонстрация применения шифрования при передаче Web-страниц. Установка доверенного сертификата. Тема «Социальная информатика» (12 ч) Содержание темы: Роль информации в современном обществе. Законодательное регулирование в информационной области. Персональная информационная безопасность с законодательной точки зрения. Электронная подпись.

УМК «Информатика» 10-11 класс, базовый и профильный уровни, авторы Гейн А.Г, Юнерман Н.А. и др.

11 класс Тема «Правовые вопросы Интернета. Безопасность и этика Интернета. Защита информации».

Таким образом, все авторы УМК по информатике, изучаемой на базовом уровне, уделяют достаточное время для изучения правовых аспектов защиты информации. На углубленном уровне изучаются также современные методы защиты информации. Следует отметить, что некоторые школьники уже в старших классах начинают вести экономическую и профессиональную деятельность в сети Интернет, делая он-лайн покупки, оказывая информационные услуги. Они хранят «в облаке» свои файлы и данные, регистрируются на сайтах госуслуг, записываются на прием к врачу через Интернет, создают свои группы в сетевых сообществах. При этом информационные технологии развиваются очень быстро, а вместе с развитием технологий растет и количество угроз. И, конечно, ни один учебник информатики не успевает обновляться с такой же скоростью, что и информационная сфера. Поэтому совершенно необходимо дополнительное

проведение занятий по информационной безопасности для старшеклассников. Это могут быть классные часы, внеурочные занятия, уроки проектной деятельности в рамках недели информационной безопасности.

Какое содержание выбрать для проведения занятий со старшеклассниками? К 10 классу обучающиеся часто информационно более подкованы, чем некоторые учителя. В рамках уроков информатики они изучают уже не только нормы сетевой этики, но и методы защиты информации, законодательное регулирование в информационной области. Т.е. обучающиеся обладают необходимыми знаниями. Вопрос в том, насколько школьники используют данные знания в повседневной жизни. Поэтому в первую очередь уроки информационной безопасности в данном возрасте должны носить не информирующий, а деятельностный характер. Например, это может быть проект «Проблемы информационной безопасности. Касаются ли они лично меня?» или «Мифы информационной безопасности».

Введение в проблему проекта можно реализовать с помощью он-лайн анкеты. Обучающимся предлагается ответить на вопросы анкеты Гугл, предложенной учителем <http://bit.ly/U5wDxE>.

Вопрос 1. Вам пришло письмо (далее идет текст письма, в ответ на которое убедительно требуют написать логин и пароль электронной почты) Каковы Ваши действия в ответ на это письмо?

Вопрос 2. Для чего, на Ваш взгляд, нужны зоны свободного доступа к Интернету (Free Wi-Fi)?

Вопрос 3. Установлена ли на Вашем смартфоне (планшете) антивирусная программа?

Вопрос 4. Являетесь ли Вы участником одной из соцсетей?

Вопрос 5. Какую информацию о Вас можно найти на Вашей странице в соцсети?

Необходимо отметить, что при заполнении анкеты ребятам нужно лишь выбрать подходящий ответ из предложенных. После того, как все обучающиеся отправят свои ответы, автоматически сформируется отчет в виде диаграмм, доступный для просмотра. Эти диаграммы педагог предлагает обучающимся для обсуждения. Цель обсуждения – определить нашу готовность к современным киберугрозам. К сожалению, на сегодняшний день мы уделяем слишком мало внимания информационной безопасности, поэтому скорее всего результатом беседы станет выявление соответствующей проблемы. После обсуждения вариантов ее решения целесообразно распределиться на группы для разработки рекомендаций (памятки) по безопасному поведению в сети на основе мифов информационной безопасности.

Обучающимся предлагается подтвердить или развенчать мифы информационной безопасности:

- Миф 1. В сети я абсолютно анонимен...
 - Вопросы: Возможна ли анонимность в сети? Что можно узнать обо мне, имея лишь ip-адрес? Какую информацию обо мне можно получить из Интернета?
 - Материалы для изучения: «Система технических средств для обеспечения функций оперативно-розыскных мероприятий» <http://ru.wikipedia.org/COPM>, «Whois-сервисы» <http://ru.wikipedia.org/wiki/WHOIS>, <http://ipgeobase.ru/>, «Методы анонимности в сети», <http://habrahabr.ru/post/190396/>
- Миф 2. Я не нарушаю закон.
 - Вопросы: Что мне будет за нарушение авторских прав? Что нелегального есть на «моём» компьютере? Каковы могут быть причины проверки моего компьютера специальными органами?
 - Материалы для изучения: «Новости по тегу «пиратство» от SecurityLab» <http://link.ac/37a6>, «Авторские права. Ответственность за нарушение авторских прав», <http://bit.ly/U5fPk7>, «Законодательство о пиратстве», <http://bit.ly/1iDiXzB>, «Антипиратский закон» http://ru.wikipedia.org/wiki/Федеральный_закон_от_2_июля_2013_года_№_187-ФЗ.
- Миф 3. Социальные сети - место общения.
 - Вопросы: Что нельзя делать в социальных сетях и почему? Что нужно делать, если мою учётную запись «взломали»? Чем опасны социальные сети?
 - Материалы для изучения: «Сайт «Одноклассники.ру» несет угрозу безопасности России» <http://bit.ly/1pDUxO8>, «Социальную сеть «ВКонтакте» признали пиратским сайтом», <http://bit.ly/UHrIU6>, «Социальные сети, психология, криминал и шпионаж. Что связывает?», <http://bit.ly/1vynivz>.
- Миф 4. Я защищён антивирусом.
 - Вопросы: Как выбрать антивирус? Как часто нужно обновлять антивирус? Можно ли отключать антивирус, если программа установки просит это сделать и почему? Достаточно ли просто удалить вирус? Кто еще, кроме меня может пострадать от моего «зараженного» компьютера?
 - Материалы для изучения: «Securelist. Угрозы», <http://www.securelist.com/ru/threats>, «Качество антивирусной защиты и проблемы антивирусных программ», <http://bit.ly/1n8tOD8>, «Для чего используют ботнеты?», <http://bit.ly/1vyDfCf>, «Финансовые киберугрозы», <http://bit.ly/1uzY7Xb>.
- Миф 5. Реклама - двигатель торговли.
 - Вопросы: Нужно ли запретить рекламу? Нужно ли намеренно защищаться от рекламы и почему? Как защититься от скрытой

рекламы и НЛП? Можно ли утверждать, что информация, размещенная на надежном сайте, является истинной?

- Материалы для изучения: «НЛП в действии», <http://bit.ly/1lw6r4V>, «Скрытая реклама - способ управления сознанием», <http://report.ru/articles/36369/>, «Информационная война», <http://ru.wikipedia.org/Информационная война>, «Информационные войны: правила и примеры», <http://www.echo.msk.ru/blog/apopova/1273448-echo/>
- Вопросы для всех: Достаточно ли только технического обеспечения информационной безопасности? Зачем меня кому-то взламывать?

Результатом проекта может стать презентация или видеоролик, содержащий ответы на вопросы, а также правила безопасного поведения в информационной среде.

Предложенные материалы также допустимо использовать для организации дискуссий на основе предложенных педагогом материалов.

Полезные ссылки для подготовки урока информационной безопасности:

- Интернет-игра по информационной безопасности <http://игра-internet.ru/game>. Много разных игр для всех возрастов. Требуется бесплатная регистрация.
- «Основы безопасности детей и молодежи в Интернете» — интерактивный курс по Интернет-безопасности. <http://laste.arvutikaitse.ee/rus/html/etusivu.htm>
- «Лаборатория Касперского» для образования <http://academy.kaspersky.ru/>
- Securelist (современные угрозы, аналитика, статистика, глоссарий, описания и блог от «Лаборатории Касперского») <http://www.securelist.com/ru/>
- VirusTotal (<https://www.virustotal.com/>) - бесплатный сервис, анализирует подозрительные файлы и веб-сайты и облегчает быстрое обнаружение вирусов, червей, троянов и всех видов вредоносных программ.
- Всероссийский конкурс социальной рекламы в форме видеороликов и плакатов "Безопасный Интернет - детям". Работы победителей. <http://www.fid.su/projects/saferinternet/year/photovideo/>
- Все о безопасном Интернете (очень много ссылок на полезные ресурсы) на Информационном портале школьных библиотек России <http://www.rusla.ru/rsba/technology/safety/>

Сайт фонда развития Интернет. Дети России Онлайн

<http://www.detionline.com/>