

*Мащенко М.В.,  
к.п.н., доцент кафедры ИТ,  
Щелокова А.Д.,  
студентка факультета естествознания,  
математики и информатики,  
Филиал РГППУ в г. Нижний Тагил*

## **ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ИНТЕРАКТИВНЫХ ЛЕКЦИЙ ПРИ ОБУЧЕНИИ ШКОЛЬНИКОВ ОСНОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

### **Аннотация**

В данной статье показывается проблема незнания молодежью основ информационной безопасности предлагается ее решение за счет обучения школьников основам информационной безопасности в курсе информатики с использованием интерактивных лекций. Особое внимание уделяется необходимости создания условий взаимодействия подростков, погружения их в реалистичные и актуальные для них проблемные ситуации. В статье подробно раскрывается понятие, структура интерактивной лекции, показываются примеры различных видов интерактивных лекций для обучения информационной безопасности.

**Ключевые слова:** интерактивная лекция, сетевая технология, информационная технология, информационная безопасность, интерактивное обучение, подростки.

*Mashchenko M. V.,  
Ph. D., associate Professor of  
the Department of Information Technology  
Shchelokova A.D.,  
Student Faculty of Natural Sciences,  
Mathematics and computer science,  
Branch of Russian State Pedagogical University in Nizhny Tagil*

## **POSSIBILITIES OF USING INTERACTIVE LECTURES WHEN TEACHING PUPILS BASIS OF INFORMATION SECURITY**

### **Abstract**

This article shows the problem of young people's ignorance of the basics of information security, and offers its solution by teaching schoolchildren the basics of

information security in the informatics course using interactive lectures. Particular attention is paid to the need to create conditions for the interaction of adolescents, to immerse them in realistic and relevant problem situations for them. The article reveals in detail the concept, structure of an interactive lecture, shows examples of various types of interactive lectures for teaching information security.

**Keywords:** interactive lecture, network technology, information technology, information security, interactive learning, teenagers.

Интернет-технологии внесли и продолжают вносить существенные изменения в процесс социализации подрастающего поколения, став одними из ключевых участников этого процесса. Согласно статистике Института исследования Интернета, детская аудитория российского Интернета в 2018 насчитывала уже около 41 млн. пользователей до 14 лет. При этом около 40 % детей, регулярно посещающих сеть, просматривают Интернет-сайты с агрессивным и нелегальным контентом, подвергаются киберпреследованиям и виртуальным домогательствам. В этой связи согласно стратегии развития информационного общества на 2017–2030 года информационная безопасность детей и молодежи стала одним из основных направлений развития российских информационных и коммуникационных технологий. В основах государственной молодежной политики Российской Федерации на период до 2025 года подчеркивается, что проблемным фактором является деструктивное информационное воздействие на молодежь. Соответственно требуется обучать подростков основам информационной безопасности и это можно делать в рамках уроков информатики или внеурочной работы по предмету.

В настоящее время уже имеется определенный опыт обучения информационной безопасности. В России созданы региональные программы обеспечения безопасного интернета для детей, есть частные школы «Стоп Угроза!», компанией «Лаборатория Каперского» разработан электронный образовательный ресурс «Урок цифры». Однако принимаемых мер оказывается недостаточно, нет определенной системы обучения, охватывающей разные стороны безопасного поведения, актуальной для определенного возраста обучающихся.

В школьном курсе информатики изучение раздела «Информационная безопасность» начинается только в старшей школе (10-11 класс). В УМК К. Ю. Полякова изучаются вредоносные программы и защита от них, шифрование, хэширование и пароли, а также рассматриваются правовые основы информационной безопасности. Однако не уделяется внимания этике поведения в сети, опасности киберпреступлений и мер их предупреждения. В

УМК Л. Л. Босовой и И.Г. Семакина затрагиваются лишь правовые аспекты информационной безопасности. Н. Д. Угринович предлагает изучать способы защиты от несанкционированного доступа к информации с использованием паролей или биометрических систем уделяя особое внимание способам защиты от компьютерных вирусов. В УМК А.Г. Гейна изучение раздела информационная безопасность представляет собой теоретическую информацию об этике поведения в Интернете, правовых аспектах информационной безопасности и анализе способов защиты информации.

Соответственно имеющиеся материалы по обучению информационной безопасности должны быть дополнены такими вопросами как «Интернет и угрозы безопасности», «Кибербуллинг и травля: меры защиты», «Киберпреступления, связанные с мошенничеством и кражами и меры их предупреждения», «Киберпреступления, связанные с недозволёнными действиями и ответственность за них», «Интернет-зависимость: как не попасться в сети». При изучении данных вопросов необходимо обратить внимание на приобретение обучающимися опыта безопасного поведения в сети. В этой связи эффективными методами обучения могут стать интерактивные методы обучения, практические работы и проектная деятельность.

В подростковом возрасте обучение может происходить только в процессе взаимодействия, причем темы для обсуждения должны быть интересны молодежи. Покажем, как интерактивное обучение будет применяться на уроках информатики в системе (см. табл. 1).

Таблица 1

Планирование обучения информационной безопасности в школе

Тема	Используемые методы обучения
<b>7 класс</b>	
Интернет и угрозы безопасности	Интерактивная лекция с опросом обучающихся и интеллектуальной игрой.
Кибербуллинг и травля: меры защиты	Интерактивная лекция с разбором проблемной ситуации и использованием технологии кейс-стади.
Защита аккаунтов в социальных сетях	Практическая работа по настройке аккаунта в одной из социальных сетей.
<b>8 класс</b>	
Интернет-зависимость: как не попасться в сети	Интерактивная лекция с изготовлением информационного плаката правил безопасности.
Моя борьба с интернет-зависимостью	Исследовательский проект обучающихся внутри школы для сбора статистических данных.
Как не стать жертвой кибербуллинга	Метод проектов, групповая работа, направленная на составление мер защиты от кибербуллинга.

<b>9 класс</b>	
Киберпреступления, связанные с мошенничествами и кражами	Интерактивная лекция с использованием веб-квестов и разбором конкретных ситуаций.
Настройка браузера для безопасной работы в Интернете	Практическая работа по настройке браузера.
Платёжные системы и их надежность	Исследовательская практическая работа анализ наиболее безопасных платформ через которые можно совершать денежные операции.
<b>10 класс</b>	
Киберпреступления, связанные с недозволёнными действиями и ответственность за них	Интерактивная лекция с разбором проблемной ситуации и интеллектуальной игрой.
Ответственность за преступления, совершенные в Интернете	Интерактивная лекция с разбором конкретной ситуации и деловой игрой.
<b>11 класс</b>	
Киберпреступления, связанные с недозволёнными действиями и ответственность за них	Метод проектов, групповая работа результатом которой является буклет о видах ответственности за киберпреступления, связанные с недозволёнными действиями с конкретными примерами из судебной практики.
Основные угрозы безопасности в Интернете	Интерактивная лекция с использованием технологии кейс-стади и интеллектуальной игрой.

Таким образом, основой обучения информационной безопасности станут интерактивные лекции, рассмотрим их структуру, особенности организации более подробно.

Лекция предусматривает создание обучающей ситуации, при которой основной задачей обучающихся становится получение новой полезной информации и ее структурирование. Преимуществами данной формы обучения является возможность в короткие сроки дать обучающимся большой объем современной актуальной информации, отсутствующий в официальных печатных учебниках. Но данная форма обучения имеет и серьезные недостатки. К основным из них стоит отнести: усредненность уровня сложности содержания; требования к профессионализму и ораторским способностям лектора; отсутствие со стороны слушателей контроля за образовательным процессом и права выбора со стороны слушателей; трудности при удержании концентрации и внимания со стороны слушателей; отсутствие обратной связи, особенно при соблюдении строгого формата лекции; пассивная роль слушателя. Часть из выявленных недостатков можно исправить, если вместо обычной лекции проводить интерактивную.

Интерактивная лекция объединяет в себе аспекты традиционной лекции и тренинговых технологий [3]. Существуют различные виды интерактивных лекций [1]: проблемная лекция, лекция с заранее запланированными ошибками, лекция пресс-конференция, бинарная лекция, лекция-дискуссия, лекция-беседа, лекция-визуализация и др.

Если сравнивать обычную информационную лекцию с проблемной, то основное отличие заключается в том, что на информационной лекции материал предлагается в виде известного, подлежащего лишь запоминанию материала. А на проблемной лекции материал дается обучающимся с использованием учебной проблемной ситуации, вызывающей затруднение у слушателей. В этом случае информация, получаемая в процессе ответов на наводящие вопросы педагога, усваивается как личностное открытие еще неизвестного для себя знания. Во время такой лекции обучающиеся заинтересованы, потому что им интересно отгадать представленную в начале загадку и решить актуальную для себя учебную проблемную ситуацию. Вся лекция выстраивается как диалог. Разрешая противоречия, заложенные в проблемных ситуациях, слушатели могут прийти самостоятельно к тем выводам, которые преподаватель должен сообщить в качестве новых знаний. В отличие от традиционной информационной лекции проблемная позволяет сразу реализовывать обратную связь, особенно если она идёт в форме живого диалога.

При обучении информационной безопасности можно попросить обучающихся отгадать, чей портрет перед ними. Возможно показать портрет Энди Хопкинса – первого изобретателя антивирусных утилит или портрет Роберта Тэппэна Морриса, впервые создавшего вирус – сетевой червь. А далее с помощью наводящих вопросов, анализа дополнительных фактов, использования информации в сети ответить на вопрос какую роль данная личность сыграла в информационной безопасности.

Кроме того, на проблемной лекции перед обучающимися можно поставить вопрос «Какие киберпреступления в сети встречаются чаще и какие из них наиболее опасны для разных групп населения (молодежи, пенсионеров, предпринимателей и др.)?». Отвечая на этот вопрос в ходе диалога, разбирая личный опыт обучающихся можно проанализировать и систематизировать основные виды преступлений в сети.

При проведении такой лекции процесс обучения приближается к поисковой, исследовательской деятельности. Основной задачей лектора является не столько передача информации, сколько в приобщении слушателей

к объективным противоречиям развития научного знания и способам их преодоления, что порождает познавательную активность.

Лекция-провокация, или лекция с заранее запланированными ошибками. Лучше всего проводить в аудитории, где слушатели одинаково подготовлены по данной теме. Можно проводить, как обобщающую лекцию по теме или разделу. Преподаватель в начале занятия объявляет, что в лекции будут допущены ошибки, причем различного плана содержательные, методические, поведенческие и т. д. Задача слушателей в конце лекции назвать ошибки и дать правильные ответы, для этого преподаватель оставляет в конце лекции 10–15 минут. Исходная ситуация, как бы изначально побуждает слушателей к активности, личностный интерес еще более усиливается тем что интересно найти ошибки у преподавателя и узнать смогу ли я это сделать. Все это создаёт мотив, активизирующий психическую деятельность слушателя.

Например, при обучении информационной безопасности в качестве основных правил поведения при использовании сети выделить такие как: отвечать на оскорбления в социальных сетях в такой же грубой форме или нажимать на всплывающие окна с сообщениями о выигрыше.

Подобная лекция выполняет не только стимулирующие, но и контрольные функции, поскольку позволяет преподавателю оценить качество усвоения предыдущего материала, а слушателю свой уровень знания материала по данной теме.

Наиболее частые опасения преподавателей связаны с тем, что они считают, что слушатели запомнят ошибки, а не нужную информацию. Однако научить людей мыслить давая им всегда правильную информацию практически невозможно. Нужно противоречие, борьба мнений, спор, альтернатива, именно это и предлагает преподаватель на лекции с заранее запланированными ошибками. В конце лекции, после всех обсуждений, преподаватель по просьбе слушателей отдаёт листок, на котором написаны все ошибки, только в этом случае обеспечивается полное доверие преподавателя и аудитории.

Лекция вдвоём или бинарная лекция. Это работа двух преподавателей, читающих лекцию по данной теме и взаимодействующих между собой и аудиторией. Такая лекция содержит в себе конфликтность, которая может проявляться как в форме подачи материала, так и в столкновении разных точек зрения так и в сочетании теории и практики. Данная лекция создаёт положительную эмоциональную атмосферу и создаёт высокую степень мотивации вступления в диалог, слушателям наглядно представляют, способы ведения диалога, а также предоставляют возможность принять в нём участие. Такая лекция помогает передавать большой объём информации за счёт

переконструирования материала и поддержания высокого уровня внимания у слушателей.

Например, при обучении информационной безопасности один из преподавателей может придерживаться мнения о том, что Интернет не таит в себе угроз, а другой наоборот утверждать, что в сети опасности поджидают тебя повсюду.

Лекция-визуализация. Её применение связано с одной стороны с реализацией принципа проблемности, а с другой — с реализацией принципа наглядности. На такой лекции аудиоинформация сопровождается большим количеством рисунков, логических схем, диаграмм, опорных конспектов и д. р. Такая наглядность компенсирует недостаточную зрелищность учебного процесса. Основной акцент в такой лекции делается на визуальное мышление, что может существенно повысить эффективность восприятия, понимания и усвоения информации. а также в превращении её в знания. Подобная лекция создаёт своеобразную опору для мышления, развивает навыки наглядного моделирования, что помогает не только интеллектуальному развитию слушателей, но и повышает профессиональный потенциал слушателей. Выбор типов наглядности зависит от темы, но не стоит забывать о принципе посильной трудности и использовать сочетание изобразительной и символической наглядности. Применяя данную лекцию не стоит забывать о психофизиологических возможностях слушателей, чтобы предотвратить негативные последствия чрезмерной перегрузки зрительного канала восприятия [2].

Например, при обучении информационной безопасности можно показать обучающимся следующую схему (см. рис. 1) и предложить самим придумать классификацию угроз информационной безопасности.



Рис.1. Классификация угроз безопасности

Лекция пресс-конференция. В начале данной лекции преподаватель просит слушателей на листочках написать интересующие их вопросы по данной теме. Затем он сортирует эти вопросы по смысловому содержанию и в ходе лекции отвечает на них рассказывая материал. По ходу лекции слушатели могут так же задавать вопросы.

Лекция с разбором конкретных ситуаций. Преподаватель на обсуждение выносит не задачу, а конкретную ситуацию, которую необходимо решить. В обсуждении и анализе ситуации принимает участие вся аудитория. Преподаватель руководит и направляет процесс обсуждения, задавая провокационные вопросы, чтобы навести аудиторию к правильному решению или обобщению. Психологически и педагогически доказано, что наглядность способствует не только более успешному восприятию и запоминанию учебного материала, но и позволяет активизировать умственную деятельность.

Например, при обучении информационной безопасности можно взять ситуацию: одноклассники Влады создали в социальной сети «Вконтакте» группу и публиковали её фотографии с грубыми комментариями, такие же грубые комментарии они оставляли и под фотографиями девочки, которые она выставляла на личной странице. Что делать Владе?

Таким образом, при обучении информационной безопасности в качестве основного метода рационально использовать интерактивные лекции. С одной стороны, этот метод позволяет в ограниченные сроки выдать большой объем теоретического материала, а с другой – закрепить его в процессе обсуждения, решения проблемных ситуаций, кейсов, участия обучающихся в имитационных игровых ситуациях. Опыт работы показал, что в школе наиболее часто используются проблемные лекции и лекции, с разбором конкретных ситуаций.

## ЛИТЕРАТУРА

1. Еременко В. Т. Применение активных и интерактивных методов обучения при организации образовательного процесса. Орел.: ФГБОУ ВПО «Госуниверситет-УНПК», 2015. 50 с.

2. Реутова Е.А. Применение активных и интерактивных методов обучения в образовательном процессе вуза. Новосибирск.: НГАУ, 2012. 58 с.

3. Рюмина, Ю.Н. Интерактивная лекция как форма обучения в системе профессиональной подготовки бакалавров [Электронный ресурс]. URL: <http://shgpi.edu.ru/files/nauka/vestnik/2014/20.pdf> (дата обращения: 10.10.2019).