РАБОЧАЯ ПРОГРАММА ЭЛЕКТИВНОГО КУРСА «КОМПЬЮТЕРНАЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Епанчинцева М.В. учитель
информатики и ИКТ МБОУ «СОКШ №4»
г.Нефтеюганск ХМАО-Югра

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Одно из основных мест в системе предпрофильной подготовке занимают элективные курсы. Каждый элективный курс представляет собой завершенную дидактическую единицу, нацеленную на получение образовательных результатов.

Предложенный курс преследует такие **цели**, как: овладение учащимися навыков профилактики и защиты программного обеспечения и информации; приобретения опыта в предупреждении и нейтрализации угроз информации; научиться создавать и реализовывать информационные проекты. Перед курсом ставятся образовательная, развивающая и воспитательная **задачи.**

Данный элективный курс поможет получить актуальные, на сегодняшний день, знания, умения и навыки в современных информационных технологиях.

Информационная безопасность — защита конфиденциальности, целостности и доступности информации. Защита информации – комплекс мероприятий, направленных на обеспечение информационной безопасности.

Содержание элективного курса

Сегодня уже ни у кого не вызывает сомнения тот факт, что XXI век – век информации и научных знаний. Развитие глобального процесса информатизации общества, охватывающего все развитые и многие развивающиеся страны мира, приводит к формированию новой информационной среды, информационного уклада и профессиональной деятельности. Однако при этом пропорционально возрастает уязвимость личных, общественных и государственных информационных ресурсов со стороны негативного воздействия средств инфомационно-коммуникационных технологий. Таким образом, мировое сообщество стоит перед глобальной социотехнической проблемой – проблемой обеспечения информационной безопасности. Под информационной безопасностью понимается область науки и техники, охватывающая совокупность программных, аппаратных и организационно-правовых методов и средств обеспечения безопасности информации при обработке, хранении и передаче с использованием современных информационных технологий. А так же под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей

инфраструктуры. Под угрозой информационной безопасности понимают потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Решение проблемы безопасности вообще и информационной безопасности в частности невозможно без достаточного количества как высококвалифицированных профессионалов, так и квалифицированных пользователе, компетентных в сфере защиты информации. Задача подготовки таких специалистов является особенно актуальной ещё и потому, что одной из важнейших задач современности является борьба с компьютерной преступностью и кибертерроризмом. Спектр преступлений в сфере информационных технологий весьма широк, он варьируется от интернет-машенничества и до такой потенциально опасной деятельности, как электронный шпионаж и подготовка к террористическим актам.

В настоящее время достаточно свободно распространяются различные печатные издания, где описываются технологии совершения компьютерных преступлений; публикуются книги, освещающие приёмы атак на информационные системы. В Интернете представлено огромное количество сайтов, обучающих компьютерному взлому, проводятся форумы, виртуальные конференции и семинары по «повышению квалификации» и «обмену опытом» совершения компьютерных преступлений. Среди выявленных преступников, в отношении которых возбуждены дела за противоправные действия в сфере информационных технологий, свыше 75% составляет молодёжь. Всё это подчёркивает важность ещё одной задачи – активного противодействия вовлечению молодёжи в преступную среду и разработки активных методов проведения воспитательной работы среди молодёжи. Очевидно, что насущной задачей современного образования становится разработка таких методов учебно-воспитательной работы, которые гармонично сочетают обучение современным информационным технологиям и формирование информационной культуры, высоких нравственных качеств, способствует выработке иммунитета к совершению неэтичных, противоправных действий в сфере информационных технологий.

Таким образом, можно считать актуальным и значительным старших классов изучение элективного курса «Компьютерная и информационная безопасность» в образовательной области «Информатика». Курс ориентирован на подготовку подрастающего поколения к жизни и деятельности в совершенно новых условиях информационного общества, в котором вопросы обеспечения информационной безопасности личных, общественных и государственных информационных ресурсов особенно актуальны.

Курс служит средством внутри профильной специализации в области информатики и информационных технологий, что способствует созданию дополнительных условий для построения индивидуальных образовательных траекторий учащихся классов информационно-технологического профиля. Курс рассчитан на 35 часов и изучается в течение одного учебного года по 1 часу в неделю в 10 классе.

Данный курс может с успехом использоваться не только в информационно-технологическом, но и в других профилях старшей школы, поскольку проблема информационной безопасности сегодня актуальна во всех сферах современного общества – гуманитарной, социальной, экономической и др.

Для успешного изучения курса «Компьютерная и информационная безопасность» необходимы базовые знания, полученные учащимися при изучении информатики и информационных технологий.

Учащиеся должны **знать:**

- свойства алгоритмов и основные алгоритмические структуры;
- основные конструкции языка программирования;
- назначение и области использования основных технических средств информационных и коммуникационных технологий и информационных ресурсов;
- базовые принципы организации и функционирования компьютерных сетей.

Учащиеся должны **уметь:**

- составлять программы на языке программирования;
- проводить статистическую обработку данных с помощью компьютера;
- строить таблицы, графики, диаграммы;
- представлять информацию в виде мультимедийных объектов с системой ссылок;
- подготавливать доклады и проводить выступления;
- участвовать в коллективном обсуждении без использования современных программных и аппаратных средств коммуникаций и с их использованием.

Данный курс преследует следующие **цели**:

- Овладение учащимися умениями: профилактики, защиты программного обеспечения; обнаружения и удаления компьютерных вирусов; защиты информации в автоматизированных системах обработки данных, в глобальной сети Интернет.
- Приобретение учащимися опыта по предупреждению и нейтрализации негативного воздействия информационных угроз на людей и программно-технические комплексы; опыта информационной деятельности в сферах обеспечения защиты информации, актуальных на рынке труда.
- Приобретения учащимися опыта создания, редактирования, оформления, сохранения, передачи информационных объектов различного типа с помощью современных программных средств; коллективной реализации информационных проектов, преодоления трудностей в процессе проектирования, разработки и реализации учебных проектов.

Перед данным элективным курсом ставятся следующие **задачи**:

Образовательные:

- освоение учащимися знаний, относящихся к основам обеспечения информационной безопасности, и их систематизация;
- изучение учащимися мер законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в системах связи;

развивающие:

- повышение интереса учащихся к изучению информатики;
- приобретение учащимися навыков самостоятельной работы с учебной, научно-популярной литературой и материалами сети Интернет;
- развитие у учащихся способностей к исследовательской деятельности;

воспитательные:

- воспитание у учащихся культуры в области применения ИКТ в различных сферах современной жизни;
- воспитание у учащихся чувства ответственности за результаты своего труда, используемые другими людьми;
- воспитание у учащихся умения планировать, работать в коллективе;
- воспитание у учащихся нравственных качеств, негативного отношения к нарушителям информационной безопасности;
- воспитание у учащихся установки на позитивную социальную деятельность в информационном обществе, недопустимость действий, нарушающих правовые и этические нормы работы с информацией.

Педагогическое сопровождение элективного курса

Педагогическое сопровождение основывается на принципах системности, актуальности, прогностики, комплексности решения образовательных проблем, гуманизации образования, и должно быть направлено на решение совокупности научных, методических и практических задач. Педагогическое сопровождение проблем безопасности должно быть ориентировано по основным направлениям подготовки специалистов информационно-технического профиля.

С учетом специфики все виды безопасности должны быть детерминированы по соответствующим видам подготовки. В этом случае изучение вопросов обеспечения информационной безопасности должно, в основной своей части, решаться в рамках информационной подготовки и, с учетом ее дифференциации, соответствовать основным уровням, этапам и направленности.

Акцент на защиту информации при использовании информационно-коммуникационных технологий, сохранившихся «по инерции» со времён, когда собственником информации было только государство, и оно же решало все вопросы, связанные с защитой информации, а главенствующим был аспект конфиденциальности. Такой акцент, правомерен, например, при подготовке специалистов в области криптографии, защита информации в

органах управления и автоматизированных системах критических приложений. Система такой подготовки сформирована на базе Учебно-методического объединения вузов России по образованию в области информационной безопасности, региональных учебно-научных центров по проблемам информационной безопасности в системе высшей школы. Основополагающим является наличие ГОС и разработанных на их базе основных образовательных программ в области информационной безопасности.

Если подготовка специалистов в области информационной безопасности и защиты информации, имеющая давние исторические корни, имеет соответствующее педагогическое обеспечение, то для специалистов-пользователей информационно-коммуникационных технологий такого рода подготовка не имеет системного характера, необходимого научного педагогического сопровождения. Теперь абсолютность «полезности» информационно-коммуникационных технологий сопровождается невежеством в области информационной безопасности большинства пользователей, что не способствует трезвой оценке угроз информационной безопасности и адекватному применению средств защиты информации. Отрывочные знания о некоторых угрозах информационной безопасности (в основном о вирусах и вредоносных программах) не позволяют, с одной стороны, очертить спектр многочисленных угроз информационной безопасности, а с другой – утверждают пользователей в пессимистическом мнении о невозможности им противостоять. В рамках информационной подготовки специалистов не закладывается чувство личной ответственности за состояние безопасности информационной безопасности на корпоративном и индивидуальном уровнях, необходимый уровень умений и навыков по применению общедоступных мер и средств защиты информации.

Таким образом, педагогическое сопровождение проблемы информационной безопасности в подготовке специалистов информационно-технического профиля должно обеспечить построение логически-стройной, внутренне непротиворечивой системы подготовки в рамках профессионального образования по целому комплексу вопросов информационной безопасности и защиты информации, характеризующих эту важную предметную область.

Анализ функциональной деятельности выпускников вузов, тенденций и перспектив информационных систем, информационных и коммуникационных технологий свидетельствует, что основным направлением в подготовке к профессиональной деятельности должно являться привитие обучающимся достаточно глубоких знаний информатики, основ построения и функционирования современных информационных систем и информационно-коммуникационных технологий, практических умений и навыков их эксплуатации и применения. Такой подход должен постоянно реализовываться с учетом текущего состояния и современных достижений отраслевой науки и практики, осуществляться поэтапно и охватывать достаточно широкий спектр вопросов. Поэтому одним из

важнейших видов подготовки специалистов для различных информационных сфер является информационная подготовка, направленная на формирование у обучаемых знаний и навыков по применению информационных технологий в их дальнейшей профессиональной деятельности. Главной задачей информационной подготовки является обеспечение будущего специалиста глубокими теоретическими знаниями и прочными практическими навыками в области информатики, позволяющими ему не только эффективно решать повседневные производственные задачи с применением средств вычислительной техники, но и хорошо ориентироваться в основных тенденциях развития информационных технологий, их применения в избранной сфере профессиональной деятельности.

В связи с этим, помимо решения традиционных задач обучения информационно-коммуникационных технологий, информационная подготовка должна быть направлена на сознательное восприятие пользователем всей сложности и ответственности проблемы обеспечения информационной безопасности компьютерных систем, понимание трудностей по обеспечению информационной безопасности на корпоративном и личностном уровне и связанных с этим жестких ограничений и больших материальных затрат. В результате изучения такого курса пользователи информационных технологий должны знать: сущность проблемы обеспечения информационной безопасности компьютерных сетей и ее особенности применения, ее важность и актуальность, основные понятия в этой предметной области; особенности информации и информационных систем как объекта защиты, основные методы и средства обеспечения информационной безопасности компьютерных сетей (аутентификация и идентификация пользователей и технических средств, организация защиты информации в персональных компьютеров, криптографическое преобразование информации и электронная подпись; критерии защищенности компьютерных систем и принципы проектирования систем защиты информации; особенности защиты информации в сетях телекоммуникаций; основы компьютерной вирусологии, методы и средства защиты от компьютерных вирусов и вредоносных программ; требования к пользователям компьютерных систем и рекомендации по обеспечению информационной безопасности).

В практической части дисциплин как базовой информационной подготовки (в рамках изучения информатики), так и предметной информационной подготовки (при получении практических навыков по использованию различных автоматизированных систем в области профессиональной деятельности) необходимо акцентировать внимание обучаемых на применении тех или иных механизмов парирования угроз (ограничения и разграничения доступа, администрирования в сетевых структурах, использовании защиты в бизнес-приложениях и т.п.). Особое внимание при этом может быть уделено работе в сети с цифровой подписью, практическому ознакомлению с мерами безопасности в Internet, (при работе с электронной почтой, защите от спама), использованию современных средств

архивирования, идентификации и аутентификации, защиты от несанкционированного копирования, пакетов антивирусной защиты.

Концепция обучения основам информационной безопасности студентов должна основываться на понимании назначения, роли и целей этих знаний в современной системе образования, трактовке способов их отражения в качестве обязательной составляющей информационной подготовки. Построение такой концепции, в общем плане, включает следующие этапы: обоснование необходимости создания; формирование целей обучения с учётом прогностики; выявление межпредметных связей; определение принципов отбора содержания и его структуры; разработку структуры подготовки по основам информационной безопасности; разработку предложений по корректировке законодательной базы в части ГОС, требований к уровню и качеству подготовки обучаемых в области информационной безопасности; выбор основных подходов к организации учебного процесса; изложение требований к разработке учебных программ и планов, дидактических материалов, технологической поддержке обучения; планирование мероприятий по реализации концепции; выявление долгосрочных перспектив развития подготовки в области информационной безопасности как составной части информационной подготовки.

Программа курса

1. Общие проблемы информационной безопасности.

Информация и информационные технологии. Актуальность проблемы обеспечения безопасности информационных технологий. Основные термины и определения. Субъекты информационных отношений, их интересы и безопасность. Конфиденциальность, целостность, доступность. Пути нанесения ущерба. Цели и объекты защиты.

2. Угрозы информационной безопасности.

Понятие угрозы. Виды проникновения или «нарушителей». Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам. Каналы утечки информации и их характеристика.

3. Вредоносные программы. Методы профилактики и защиты.

Общие сведения о вредоносных программах. Классификация по среде обитания, поражаемой операционной системе, особенностям алгоритма работы. Принципы функционирования, жизненный цикл и среда обитания компьютерных вирусов. Симптомы заражения и вызываемые вирусами эффекты. Полиморфные и стелс-вирусы. Вирусы-макросы для Microsoft Word и Microsoft Excel. Вирусы-черви. Профилактика заражения. Программные антивирусные средства. Определения и общие принципы функционирования фагов, детекторов, ревизоров, вакцин, сторожей. Структура антивирусной программы. Виды антивирусных программ.

4. Правовые основы обеспечения информационной безопасности.

Законодательство в информационной сфере. Виды защищаемой информации. Государственная тайна как особый вид защищаемой

информации; система защиты государственной тайны; правовой режим защиты государственной тайны. Конфиденциальная информация. Лицензионная и сертификационная деятельность в области защиты информации. Основные законы и другие нормативно-правовые документы, регламентирующие деятельность организации в области защиты информации. Защита информации ограниченного доступа. Ответственность за нарушение законодательства в информационной сфере. Информация как объект преступных посягательств. Информация как средство совершения преступлений. Отечественные и зарубежные стандарты в области информационной безопасности.

5. Современные методы защиты информации в автоматизированных системах обработки данных.

Обзор современных методов защиты информации. Основные сервисы безопасности: идентификация и аутентификация, управление доступом, протоколирование и аудит. Криптографическое преобразование информации. История криптографии; простейшие шифры и их свойства. Принципы построения криптографических алгоритмов с симметричными и несимметричными ключами. Электронная цифровая подпись. Контроль целостности; экранирование; анализ защищённости; обеспечение отказоустойчивости; обеспечение безопасного восстановления.

6. Технические и организационные методы защиты информации.

Технические средства охраны объектов (физическая защита доступа, противопожарные меры). Защита от утечки информации (перехвата данных, электростатических и электромагнитных излучений и др.). Технические средства противодействия несанкционированному съёму информации по возможным каналам её утечки. Организационные меры защиты. Определение круга лиц, ответственных за информационную безопасность, обеспечение надёжной и экономичной защиты. Требования к обслуживающему персоналу.

7. Защита информации в компьютерных сетях.

Примеры взломов сетей и веб-сайтов. Причины уязвимости сети Интернет. Цели, функции и задачи защиты информации в компьютерных сетях. Безопасность в сети Интернет. Методы атак, используемые злоумышлиниками для получения или уничтожения интересующей информации через Интернет. Способы отделения интрасети от глобальных сетей. Фильтрующий маршрутизатор, программный фильтр и т.д.

8. Проблемы информационно–психологической безопасности личности.

Определение понятия информационно-психологической безопасности. Основные виды информационно-психологических воздействий. Виртуальная реальность и её воздействие на нравственное, духовное, эмоциональное и физическое здоровье школьников. Игромания, компьютерные манипуляции, фишинг, киберугрозы и пропаганда других опасных явлений в Интернете. Способы Защиты от нежелательной информации в Интернете. Нравственно-этические проблемы информационного общества.

К данной программе можно предложить следующий календарный план.

Календарно-тематическое планирование

Номер урока	Тема урока	Вид урока	дата
1. Общие проблемы информационной безопасности – 2 часа.			
1-2	Основные понятия информационной безопасности. Актуальность проблемы обеспечения безопасности ИТ.	лекция	
2. Угрозы информационной безопасности – 4 часа.			
3-4	Понятие угрозы информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам.	лекция	
5-6	Методы защиты компьютеров от вредоносных программ. Восстановление информации.	лекция + практическая работа	
4. Правовые основы обеспечения информационной безопасности – 6 часов			
7-8	Законодательство в области защиты информации.	лекция	
9-10	Преступление и наказание в сфере информационных технологий.	лекция + практическая работа	
11-12	Отечественные и зарубежные стандарты в области информационных технологий.	лекция	
5. Современные методы защиты информации в автоматизированных системах обработки данных – 8 часов.			
13-14	Основные сервисы безопасности. Идентификация и аутентификация.	лекция	
15-16	Управление доступом. Протоколирование и аудит. Криптографическая защита.	лекция + практическая работа	
17-18	Принципы построения криптографических алгоритмов с симметричными и несимметричными ключами.	лекция + практическая работа	
19-20	Контроль целостности; экранирование; анализ защищённости.	лекция	
6.Технические и организационные методы хранения информации – 3 часа.			
21-23	Технические средства защиты информации. Организационные меры защиты.	лекция	
7. Защита информации в компьютерных сетях – 2 часа.			
24	Защита информации в компьютерных сетях. Безопасность в сети Интернет.	лекция	
25	Фильтрующий маршрутизатор, программный фильтр, системы типа FireWall (брандмауэр, экранирующий фильтр) и т.д.	лекция + практическая работа	
8. Проблемы информационно–психологической безопасности личности –10 часов.			
26	Виртуальная реальность и её воздействие на нравственное, духовное, эмоциональное и	лекция	

	физическое здоровье школьников.		
27	Способы защиты от нежелательной информации в Интернете.	лекция + практическая работа	
28-33	Работа над проектом «Перспективные направления в области обеспечения информационной безопасности».	практическая работа	
34-35	Итоговое занятие. Защита проектов.	практическая работа	

После прохождения курса, должен быть достигнут следующий перечень знаний, умений и навыков учащихся.

Учащиеся должны **знать:**

- основные понятия и определения из области обеспечения информационной безопасности;
- методы и средства борьбы с угрозами информационной безопасности;
- классификацию вредоносных программ и их влияние на целостность информации; порядок заражения файлов;
- методы проведения профилактики, защиты и восстановления пораженных вредоносными программами объектов;
- нормативные руководящие документы, касающиеся защиты информации, существующие стандарты информационной безопасности;
- принципы выбора пароля, аппаратные и программные средства для аутентификации по паролю;
- основные понятия криптографических методов защиты информации, механизмы цифровой электронной подписи;
- существующие программные продукты, предназначенные для защиты электронного обмена данными в Интернете, способы отделения интрасети от глобальных сетей;
- нормы информационной этики и права.

Учащиеся должны **уметь:**

- объяснять необходимость изучения проблемы информационной безопасности;
- применять методы профилактики и защиты информационных ресурсов от вредоносного программного обеспечения;
- восстанавливать повреждённую информация;
- соблюдать права интеллектуальной собственности на информацию;
- применять методы ограничения, контроля, разграничения доступа, идентификации и аутентификации;
- использовать современные методы программирования для разработки сервисов безопасности;
- производить простейшие криптографические преобразования информации;

- планировать организационные мероприятия, проводимые при защите информации;
- применять методы защиты информации в компьютерных сетях;
- различать основные виды информационно-психологических воздействий в виртуальной реальности;
- соблюдать требования информационной безопасности, этики и права;
- искать и обрабатывать информацию из различных источников, приводить собственные примеры явлений и тенденций, связанных с безопасностью информационного общества;
- интерпретировать изучаемые явления и процессы, давать им сущностные характеристики, высказывать критическую точку зрения и свои суждения по проблемным вопросам;
- сравнивать, анализировать и систематизировать имеющийся учебный материал;
- участвовать в групповой работе и дискуссиях, решении задач в игровых ситуациях и проектной деятельности;
- представлять результаты учебных исследовательских проектов с использованием информационно-коммуникационных технологий.

Литература

1. Гостехкомиссия России. Руководящий документ: Защита от несанкционированного доступа к информации. Термины и определения. – М.: ГТК 1992.
2. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Издательство Агентства «Яхтсмен», 1996.
3. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности. – М.: Радио и связь, 2000.
4. Казарин О.В. Безопасность программного обеспечения компьютерных систем. Монография. – М.: МГУЛ, 2003. – 212 с.
5. Новиков А.А., Устинов Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий: Учебное пособие. – М. «Радио и связь» 2003.
6. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – МЦНМО, 2003.
7. Введение в криптографию. – Сб. под ред. В.В.Ященко. МЦНМО, 1999.
8. Спесивцев А.В., Вегнер В.А., Крутяков А.Ю. и др. Защита информации в персональных ЭВМ. – М. «Радио и связь», Веста, 1992.