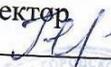


Утверждаю
Директор

Герасимова В.А.

Согласовано
Зам. директора

Родионова А.Ю.



АННОТАЦИЯ

**Программа элективного курса
«Информационная безопасность»
Учитель: Салихов С.М.**

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 пользователей, 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 «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 34 часа и изучается в течении одного учебного года по 1 часу в неделю в 11 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.

Цель курса: · 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.

Задачи курса: 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.

Контроль:

1. Текущий контроль: практическая работа, самостоятельная работа.
2. Тематический контроль: тест.
3. Промежуточная аттестация: контрольная работа

Требования к уровню подготовки 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.