Кочеткова О.С.
Подписано цифровой подписью: Кочеткова О.С.

Дополнительная общеобразовательная, общеразвивающая программа «Основы информационной безопасности»

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

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 информационно-коммуникационных технологий. Таким образом, мировое сообщество стоит перед глобальной социотехнической проблемой – проблемой обеспечения **информационной безопасности.**

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.

Деятельность программистов и других специалистов, работающих в сфере информатики, все чаще выступает в качестве объекта правового регулирования. Некоторые действия при этом могут быть квалифицированы как правонарушения (преступления).

Правовое сознание в целом, а в области информатики особенно, в нашем обществе находится на низком уровне. Все ли знают ответы на следующие вопросы:

- Можно ли, не копируя купленную программу, предоставить возможность пользоваться ею другому лицу?
- Кому принадлежит авторское право на программу, созданную студентом в ходе выполнения дипломной работы?
- Можно ли скопировать купленную программу для себя самого, чтобы иметь резервную копию?
- Можно ли декомпилировать программу, чтобы разобраться в ее деталях или исправить ошибки?
- В чем состоит разница между авторским и имущественным правом?

Вопросов, подобных этим, возникает множество. Есть, конечно, такие, ответы, на которые, очевидны: нельзя создавать вирусы, нельзя хулиганить в сетях, нельзя в некоммерческих телеконференциях запускать коммерческую информацию, нельзя вскрывать и искажать защищенную информацию в чужих базах данных и т.д., т.е. совершать поступки, которые могут быть объектом уголовного преследования. Но на многие вопросы ответы отнюдь не очевидны, а иногда запутаны. Необходимо отметить, что регулирование в сфере, связанной с защитой информации, программированием и т.д., является для законодательства принципиально новым.

Большая часть программного обеспечения, использующегося отдельными программистами и пользователями и целыми организациями, приобретена в результате незаконного копирования, т.е. хищения.

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 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 изучение элективного профориентационного курса «Основы информационной безопасности» в образовательной области «Информатика».

Данный курс можно 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 необходимы базовые знания, полученные учащимися при изучении информатики и информационных технологий.

ЦЕЛИ КУРСА

Образовательная и развивающая цель обучения – дать начальные знания основ информационной безопасности и ее связи с историей и обществознанием. На этой основе раскрыть значение информационных процессов в формировании современной научной карты мира, а также роль информационных технологий и вычислительной техники в развитии современного общества.

Практическая цель – внести вклад в трудовую и технологическую подготовку учащихся, то есть вооружить их теми знаниями, умениями и навыками, которые развивают ум и обогащают внутренний мир ребенка. А также обеспечат подготовку молодых людей к грамотному использованию компьютерной техники и других средств информационных и коммуникационных технологий в быту в повседневной жизни.

Воспитательная цель – обеспечивается, тем мощным мировоззренческим воздействием на ученика, которое оказывает осознание возможностей и роли вычислительной техники и средств информационных технологий в развитии общества и цивилизации в целом. При изучении курса на качественно новом уровне формируется культура умственного труда и такие важные общечеловеческие характеристики, как умение планировать свою работу, рационально ее выполнять, критически соотносить начальный план работы с реальным процессом ее выполнения. Изучение курса, требующие от учащихся умственных усилий, концентрации внимания, логичности и развитого воображения, должны способствовать развития таких ценных качеств личности, как настойчивость и целеустремленность, творческая активность и самостоятельность, ответственность и трудолюбие, дисциплина и критичность мышления, способность аргументировать свои взгляды и убеждения.

Ни одна из перечисленных выше основных целей не может быть достигнута изолированно друг от друга, они прочно взаимосвязаны.

ЗАДАЧИ КУРСА

Перед данным элективным курсом ставятся следующие задачи:

Образовательные:

- Межпредметную связь с историей и обществознанием;
- Учет интересов каждого ученика;
- Приобретение школьниками образовательных результатов для успешного продвижения на рынке труда;
- 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;
- Приобретение школьниками навыков работы с антивирусными программами, в среде Интернет;
- Формирование умений и способов деятельности для решения задач защиты и восстановления информации.

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.

МЕСТО КУРСА В УЧЕБНОМ ПЛАНЕ ШКОЛЫ

Курс «Основы информационной безопасности» выполняет основные функции:

⇒ Является «надстройкой» профильного курса, и становится в полной мере углубленным.

⇒ Развивает содержание базового курса, что позволяет поддерживать изучение смежных учебных предметов на профильном уровне или получить дополнительную подготовку для сдачи выпускного экзамена по предмету.

⇒ Способствует удовлетворению познавательных интересов в различных областях деятельности учащихся.

Курс рассчитан на 70 часов и изучается в течении одного учебного года по 2 часа в неделю в 11 классе.

РЕЗУЛЬТАТЫ ОСВОЕНИЯ КУРСА

Цели изучения курса «Основы информационной безопасности» направлены на достижение образовательных результатов, которые структурированы по ключевым задачам общего образования, отражающим индивидуальные, общественные и государственные потребности.

Личностные, метапредметные и предметные результаты освоения предмета:

Личностные результаты

- Сформированность мировоззрения, соответствующего современному уровню развития науки и техники;
- Готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности;
- Навыки сотрудничества со сверстниками, взрослыми в образовательной и других видах деятельности;
- Эстетическое отношение к миру, включая эстетику научного и технического творчества;
- Осознанный выбор будущей профессии и возможности реализации собственных жизненных планов; отношение к профессиональной деятельности как возможности участия в решении личных, общественных, государственных, общенациональных задач.

Метапредметные результаты

- Умение самостоятельно определять цели деятельности и составлять планы деятельности; самостоятельно осуществлять, контролировать и корректировать деятельность; использовать все возможные ресурсы для достижения поставленных целей и реализации планов деятельности; выбирать успешные стратегии в различных ситуациях;
- Умение продуктивно общаться и взаимодействовать в процессе совместной деятельности, учитывать позиции других участников деятельности, эффективно разрешать конфликты;
- Владение навыками познавательной и учебно-исследовательской деятельности, навыками разрешения проблем; способность и готовность к самостоятельному поиску методов решения практических задач, применению различных методов познания;
- Готовность и способность к самостоятельной информационно-познавательной деятельности, включая умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию, получаемую из различных источников;
- Умение использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности.

Предметные результаты

- Сформированность представлений о роли информации и связанных с ней процессов в окружающем мире;
- Умение создавать, редактировать, оформлять, сохранять, передавать информационные объекты различного типа с помощью современных программных средств;
- Решать задачи по обнаружения и удаления компьютерных вирусов.

Реализация программы предусматривает использование форм организации и методов обучения, направленных на повышение эффективности достижения предметных трехуровневых результатов (репродуктивного уровня; рефлексивного уровня; функционального уровня) и метапредметных результатов (самостоятельность; коммуникативность; общеинтеллектуальные навыки) с использованием ресурсов сетевого обучения:

- самостоятельное освоение содержания курса учащимися;
- аудиторные занятия учащихся;
- погружения – групповое углубление в содержание предмета с активным использованием метапредметных действий;
- критериальное оценивание предметных и метапредметных результатов;
- формирующее оценивание.

Учащиеся должны **знать:**

- назначение и области использования основных технических средств информационных и коммуникационных технологий и информационных ресурсов;
- базовые принципы организации и функционирования компьютерных сетей.

Учащиеся должны **уметь:**

- представлять информацию в виде мультимедийных объектов с системой ссылок;
- подготавливать проекты, доклады и проводить выступления;
- участвовать в коллективном обсуждении без использования современных программных и аппаратных средств коммуникаций и с их использованием.

2. СОДЕРЖАНИЕ КУРСА

I. Основные понятия и история информационной безопасности (6 часов)

Информация. Информационная среда. Информационная безопасность. Информационная война. Информационное оружие. Информационные противостояния от древности до Нового времени. Информационное противоборство. «Транспортная теорема». Хронология информационно-пропагандистских акций. Средства информационных коммуникаций.

Информационные войны XX век. США в организации информационных войн: Война во Вьетнаме. Войны в районе Персидского залива. Агрессия против Югославии. Борьба с терроризмом. Россия и информационные войны во второй половине XX века. Информационно-психологическая война США. Теория и практика военного искусства России.

II. Проблемы и угрозы информационной безопасности (6 часов)

Основные проблемы информационной безопасности. Гуманитарные проблемы. Научно-технические проблемы. Прикладные криптографические проблемы. Проблемы кадрового обеспечения информационной безопасности. Доктрина информационной безопасности Российской Федерации. Источники угроз информационной безопасности. Группы угроз в информационных системах. Средства обеспечения информационной безопасности. Программно-технические средства защиты информации. Информационная безопасность в системе национальной безопасности России. Основные составляющие национальных интересов России в информационной сфере. Конституционные права и свободы человека и гражданина в области получения и пользования информацией. Доведением до российской и международной общественности достоверной информации. Развитие современных информационных технологий. Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

III. Защита сведений, составляющих государственную и коммерческую тайну (8 часов)

Правовые основы защиты информации. Закон РФ «О безопасности». Закон РФ «О государственной тайне». Закон РФ «Об авторском праве и смежных правах». Федеральный закон «Об основах государственной службы». Уголовный кодекс РФ. Указ Президента РФ № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне». Классификация сведений, подлежащих защите. Государственная тайна. Коммерческая тайна. Сведения конфиденциального характера. Интеллектуальная собственность. Организация защиты информации. Меры защиты информации. Внешние мероприятия. Внутренние мероприятия. Технические средства защиты.

IV. Основные направления обеспечения информационной безопасности (8 часоа)

Защита информации в экономике, науке и технике. Доктрина информационной безопасности РФ. Нормативная правовая база. Причины экономического ущерба хозяйствующим субъектам. Внутренние и внешние угрозы внешней политики. Основными мероприятиями по обеспечению информационной безопасности.

Основные направления и мероприятия по защите электронной информации.

Атакующие средства информационного воздействия. Компьютерные вирусы. «Логические бомбы». Средства фальсификации. Средства внедрения компьютерных вирусов и «Логических бомб». Формы воздействия на киберпространство. Информационный терроризм. Защитные действия и меры противодействия информационному терроризму. Безопасность в сфере духовной жизни человека и общества. Психологическая агрессия. Основные объекты обеспечения информационной безопасности в сфере духовной жизни. Угрозы психологического характера. Основные направления обеспечения информационной безопасности в сфере духовной жизни.

V. Современные методы защиты информации в автоматизированных системах обработки данных (10 часов)

Организация защиты от интернет-угроз. Маршрутизаторы. Межсетевые экраны. Прокси-серверы. Системы обнаружения вторжений. Средства создания виртуальных сетей. Антивирусные средства. Экранирование подсети. Криптографические методы защиты информации. Требования к криптосистемам. Симметричные криптосистемы. Криптосистемы с открытым ключом. Электронная подпись. Управление ключами. Алгоритмы СОК. Электронная цифровая подпись (ЭЦП). Проблема аутентификации данных. Этапы технического шифрования/дешифрования с помощью хэш функций. Управление ключами. Ключевая информация. Элементы информационного процесса управления ключами. Генерация ключей. Накопление ключей. Распределение ключей. Подходы распределения ключей между пользователями. Задача управления ключами.

VI. Сущность и методы информационного воздействия на человека (12 часов)

Сущность и современное состояние манипуляции сознанием и поведением людей.

Значение термина манипуляция. Специфические признаки манипуляции. Этапы манипуляции. Цель программирования психики. Уровни манипуляции. История практик манипулирования. Защитные действия от манипуляции. Основные методы и средства информационного воздействия на человека. Поведенческие (бихевиористские) науки. Нейролингвистическое программирование. Цель НЛП. Дианетика как метод и технология манипулирования человеком. Сайентология. Внушение и гипноз. Средства манипуляции человеком. Защитные методы и приемы от манипулирования. Мифы как инструмент воздействия на людей. Традиционная мифология. Происхождение мифов. Современная мифология. Мифы о природе человека. Идеология как форма современной мифологии. Манипулятивные технологии в избирательных кампаниях. Исторические истоки пиара. Основные приемы манипулирования избирателями. Финансовые потери избирательных кампаний. Методы тоталитарных сект и способы защиты от них. Монастыри и «подвижничество». Методы инквизиции. Орден иезуитов. Современные тоталитарные секты. «Международная Церковь Христа». «Адвентисты седьмого дня». «Баптисты». «Свидетели Иеговы». «Церковь Единения Сан Муна». «Сатанисты». Секты восточной ориентации. Общие черты и традиции сектантства. Общие методы вербовки и зомбирования адептов. Методы противодействия, советы специалистов.

VII. Информационная безопасность в повседневной жизни (10 часов)

Рыночные отношения – социально-экономическая основа манипуляции людьми.

Рыночные отношения, конкуренция, соперничество, манипуляции. Взаимные манипуляции. Последствия рыночных манипуляций человеком. Влияние СМИ на мировоззрение людей. Исторические предпосылки возникновения СМИ. Рейтинг и эффективность воздействия. СМИ и «массовая культура». СМИ и молодежь. Защитные действия.

Роль рекламы в манипуляции сознанием людей. Инструмент формирования интересов и потребностей человека. Основные приемы рекламного воздействия. Личностные угрозы рекламы. Средства информационного воздействия и защита здоровья. Переход к

информационному обществу и проблемы здоровья. Характер информационного воздействия и здоровье. Психологическое здоровье. Физическое здоровье. Нравственное здоровье. Болезни зависимости. Игра. Защитные действия от игровой зависимости. Психотронные средства и здоровье.

VIII. «Глобальное общество» и проблемы информационной безопасности (10 часов)

Объективные и субъективные предпосылки создания глобального общества.

Идея установления общемирового порядка. Предпосылки глобализации информационного общества. Субъективные предпосылки глобализации. Роль Интернета в мировом информационном пространстве. Понятия Интернета. Индивидуальная и государственная защита от негативного воздействия сети. Признаки Интернет зависимости. Основные угрозы для пользователей глобальной информационной сети. Защитные мероприятия.

Глобальные ожидания и опасения человечества. Структура глобального мира. Дифференциация стран. Продукты обмена в глобальном общежитии. Духовная деградация – главная проблема безопасности.

3. ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

Планирование включает в себя:

- Раздел и тему урока;
- Основное содержание учебного материала **(ОСУМ)**;
- Учебные демонстрации;
- Профориентационные занятия **(ПОЗ);**
- Рекомендуемое учебное программное обеспечение **(ПО);**
- Формы контроля знаний.

I. Основные понятия и история информационной безопасности

Урок 1, 2. Основные понятия информационной безопасности

ОСУМ: Информация. Информационная среда. Информационная безопасность. Информационная война. Информационное оружие.

Демонстрация. Видеофильм «Информационная безопасность».

Презентация «Введение».

ПОЗ «Знакомство».

ПО: Microsoft PowerPoint. Мультимедийная система. Интернет.

Урок 3, 4. Информационные противостояния от древности до Нового времени.

ОСУМ: Информационное противоборство. «Транспортная теорема». Хронология информационно-пропагандистских акций. Средства информационных коммуникаций.

Демонстрация. Презентация «Книга Сунь Цзы».

ПОЗ Тест «Ваш темперамент».

ПО: Microsoft PowerPoint. Мультимедийная система.

Урок 5, 6. Информационные войны XX век.

ОСУМ: США в организации информационных войн: Война во Вьетнаме. Войны в районе Персидского залива. Агрессия против Югославии. Борьба с терроризмом. Россия и информационные войны во второй половине XX века. Информационно-психологическая война США. Теория и практика военного искусства России.

Демонстрация. Презентация «Информационные войны XX век».

ПО: Microsoft PowerPoint. Мультимедийная система.

II. Проблемы и угрозы информационной безопасности

Урок 7,8. Основные проблемы информационной безопасности.

ОСУМ: Основные проблемы компьютерной безопасности. Гуманитарные проблемы. Научно-технические проблемы. Прикладные криптографические проблемы. Проблемы

кадрового обеспечения информационной безопасности. Доктрина информационной безопасности Российской Федерации.

ПОЗ Классификация профессий по Е.К. Климову.

ПО: Microsoft PowerPoint. Мультимедийная система.

Урок 9,10. Источники угроз информационной безопасности.

ОСУМ: Группы угроз в информационных системах. Средства обеспечения информационной безопасности. Программно-технические средства защиты информации. **Демонстрация**. Презентация «Программно-технические средства защиты информации».

ПОЗ Игра «Полетаем».

ПО: Microsoft PowerPoint. Мультимедийная система.

Урок 11,12. Информационная безопасность в системе национальной безопасности России.

ОСУМ: Основные составляющие национальных интересов России в информационной сфере. Конституционные права и свободы человека и гражданина в области получения и пользования информацией. Доведением до российской и международной общественности достоверной информации. Развитие современных информационных технологий. Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем.

Демонстрация. Видеофильм «Профессия будущего. Специалист по информационной безопасности».

ПО: Мультимедийная система. Интернет.

III. Защита сведений, составляющих государственную и коммерческую тайну

Урок 13,14. Правовые основы защиты информации.

ОСУМ: Закон РФ «О безопасности». Закон РФ «О государственной тайне». Закон РФ «Об авторском праве и смежных правах». Федеральный закон «Об основах государственной службы». Уголовный кодекс РФ. Указ Президента РФ № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне».

Демонстрация. Презентация «Правовые основы защиты информации».

ПОЗ «Профессиональные склонности».

ПО: Microsoft PowerPoint. Мультимедийная система.

Урок 15,16. Классификация сведений, подлежащих защите.

ОСУМ: Государственная тайна. Коммерческая тайна. Сведения конфиденциального характера. Интеллектуальная собственность.

ПР/Р «Восстановление данных. Основные теоретические сведения».

ПО: TestDisk. PhotoRec. Компьютер.

Урок 17, 18. Организация защиты информации.

ОСУМ: Меры защиты информации. Внешние мероприятия. Внутренние мероприятия. Технические средства защиты.

Демонстрация. Видеофильм «Главная угроза информационной безопасности».

ПР/Р «Шифрование данных. Основные теоретические сведения».

ПО: PGP. TrueCrypt. LUKS. Компьютер. Мультимедийная система. Интернет.

Урок 19,20. Контрольные вопросы.

ОСУМ: Проверка знаний и умений учащихся.

Тест «Правовые основы защиты информации».

IV. Основные направления обеспечения информационной безопасности

Урок 21, 22. Защита информации в экономике, науке и технике.

ОСУМ: Доктрина информационной безопасности РФ. Нормативная правовая база. Причины экономического ущерба хозяйствующим субъектам. Внутренние и внешние угрозы

внешней политики. Основными мероприятиями по обеспечению информационной безопасности.

Демонстрация. Видеофильм «Обман».

ПО: Мультимедийная система. Интернет.

Урок 23, 24. Основные направления и мероприятия по защите электронной информации.

ОСУМ: Атакующие средства информационного воздействия. Компьютерные вирусы. «Логические бомбы». Средства фальсификации. Средства внедрения компьютерных вирусов и «Логических бомб». Формы воздействия на киберпространство. Информационный терроризм. Защитные действия и меры противодействия информационному терроризму.

Демонстрация. Видеофильм «Кибербезопасность - Истории из будущего».

ПО: Мультимедийная система. Интернет.

Урок 25, 26. Безопасность в сфере духовной жизни человека и общества.

ОСУМ: Психологическая агрессия. Основные объекты обеспечения информационной безопасности в сфере духовной жизни. Угрозы психологического характера. Основные направления обеспечения информационной безопасности в сфере духовной жизни.

Демонстрация. Видеофильм «Россия без террора. Завербованные смертью».

ПО: Мультимедийная система. Интернет.

Урок 27, 28. Контрольные вопросы.

ОСУМ: Проверка знаний и умений учащихся.

Круглый стол «Информационная война».

V. Современные методы защиты информации в автоматизированных системах обработки данных

Урок 29, 30. Организация защиты от интернет-угроз.

ОСУМ: Маршрутизаторы. Межсетевые экраны. Прокси-серверы. Системы обнаружения вторжений. Средства создания виртуальных сетей. Антивирусные средства. Экранирование подсети.

Демонстрация. Видеофильм «Зачем нужен прокси-сервер».

ПО: Мультимедийная система. Интернет.

Урок 31, 32. Криптографические методы защиты информации.

ОСУМ: Требования к криптосистемам. Симметричные криптосистемы. Криптосистемы с открытым ключом. Электронная подпись. Управление ключами. Алгоритмы СОК.

Демонстрация. Презентация «История криптографии».

ПО: Microsoft PowerPoint. Мультимедийная система.

Урок 33, 34. Электронная цифровая подпись (ЭЦП).

ОСУМ: Проблема аутентификации данных. Этапы технического шифрования/дешифрования с помощью хэш функций.

Демонстрация. Видеофильм «Электронная цифровая подпись (ЭЦП): регистрация и использование».

ПО: Мультимедийная система. Интернет.

Урок 35, 36. Управление ключами.

ОСУМ: Ключевая информация. Элементы информационного процесса управления ключами. Генерация ключей. Накопление ключей. Распределение ключей. Подходы распределения ключей между пользователями. Задача управления ключами.

ПОЗ «День профессионала».

Урок 37, 38. Контрольные вопросы.

ОСУМ: Проверка знаний и умений учащихся.

Тест «Криптографические методы защиты информации».

VI. Сущность и методы информационного воздействия на человека

Урок 39, 40. Сущность и современное состояние манипуляции сознанием и поведением людей.

ОСУМ: Значение термина манипуляция. Специфические признаки манипуляции. Этапы манипуляции. Цель программирования психики. Уровни манипуляции. История практик манипулирования. Защитные действия от манипуляции.

Демонстрация. Видеофильм «Куклы и кукловоды. Манипуляция сознанием».

ПО: Мультимедийная система. Интернет.

Урок 41, 42. Основные методы и средства информационного воздействия на человека.

ОСУМ: Поведенческие (бихевиористские) науки. Нейролингвистическое программирование. Цель НЛП. Дианетика как метод и технология манипулирования человеком. Сайентология. Внушение и гипноз. Средства манипуляции человеком. Защитные методы и приемы от манипулирования.

ПОЗ «Знакомьтесь: манипулятор обыкновенный».

Урок 43, 44. Мифы как инструмент воздействия на людей.

ОСУМ: Традиционная мифология. Происхождение мифов. Современная мифология. Мифы о природе человека. Идеология как форма современной мифологии.

ПОЗ «Законы психологической защищенности».

Урок 45, 46. Манипулятивные технологии в избирательных кампаниях.

ОСУМ: Исторические истоки пиара. Основные приемы манипулирования избирателями. Финансовые потери избирательных кампаний.

Демонстрация. Презентация «Информационно-технологическое оружие»

ПОЗ «Краткая антология манипулятивных уловок».

ПО: Microsoft PowerPoint. Мультимедийная система.

Урок 47, 48. Методы тоталитарных сект и способы защиты от них.

ОСУМ: Монастыри и «подвижничество». Методы инквизиции. Орден иезуитов. Современные тоталитарные секты. «Международная Церковь Христа». «Адвентисты седьмого дня». «Баптисты». «Свидетели Иеговы». «Церковь Единения Сан Муна». «Сатанисты». Секты восточной ориентации. Общие черты и традиции сектантства. Общие методы вербовки и зомбирования адептов. Методы противодействия, советы специалистов.

Демонстрация. Презентация «Секты».

ПОЗ «Черты и качества защищенной личности».

ПО: Microsoft PowerPoint. Мультимедийная система.

Урок 49, 50. Контрольные вопросы.

ОСУМ: Проверка знаний и умений учащихся.

Кроссворд «Методы информационного воздействия на человека».

VII. Информационная безопасность в повседневной жизни

Урок 51, 52. Рыночные отношения – социально-экономическая основа манипуляции людьми.

ОСУМ: Рыночные отношения, конкуренция, соперничество, манипуляции. Взаимные манипуляции. Последствия рыночных манипуляций человеком.

Демонстрация. Видеофильм «Манипуляции, НЛП, гипноз в продажах».

ПО: Мультимедийная система. Интернет.

Урок 53, 54. Влияние СМИ на мировоззрение людей.

ОСУМ: Исторические предпосылки возникновения СМИ. Рейтинг и эффективность воздействия. СМИ и «массовая культура». СМИ и молодежь. Защитные действия.

Демонстрация. Видеофильм «Как СМИ манипулируют нашим мнением».

ПО: Мультимедийная система. Интернет.

Урок 55, 56. Роль рекламы в манипуляции сознанием людей.

ОСУМ: Инструмент формирования интересов и потребностей человека. Основные приемы рекламного воздействия. Личностные угрозы рекламы.

Демонстрация. Видеофильм «Пси-технологии как от них защититься».

ПО: Мультимедийная система. Интернет.

Урок 57, 58. Средства информационного воздействия и защита здоровья.

ОСУМ: Переход к информационному обществу и проблемы здоровья. Характер информационного воздействия и здоровье. Психологическое здоровье. Физическое здоровье. Нравственное здоровье. Болезни зависимости. Игра. Защитные действия от игровой зависимости. Психотронные средства и здоровье.

ПОЗ Презентация «Секреты уверенности в себе».

ПО: Microsoft PowerPoint. Мультимедийная система.

Урок 59, 60. Контрольные вопросы.

ОСУМ: Проверка знаний и умений учащихся.

Круглый стол «Плюсы и Минусы информационной технологии».

VIII. «Глобальное общество» и проблемы информационной безопасности

Урок 61, 62. Объективные и субъективные предпосылки создания глобального общества.

ОСУМ: Идея установления общемирового порядка. Предпосылки глобализации информационного общества. Субъективные предпосылки глобализации.

ПОЗ «Матрица выбора профессии».

Урок 63, 64, 65. Роль Интернета в мировом информационном пространстве.

ОСУМ: Понятия Интернета. Индивидуальная и государственная защита от негативного воздействия сети. Признаки Интернет зависимости. Основные угрозы для пользователей глобальной информационной сети. Защитные мероприятия.

Кроссворд «Интернет».

Урок 66, 67, 68. Глобальные ожидания и опасения человечества.

ОСУМ: Структура глобального мира. Дифференциация стран. Продукты обмена в глобальном общежитии. Духовная деградация – главная проблема безопасности.

ПОЗ «Куда пойти учиться».

Урок 69, 70. Итоговое занятие.

ОСУМ: Проверка знаний и умений учащихся.

Тест «Основы информационной безопасности».

4. УЧЕБНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

№	Тема	Кол-во часов	теория	практика + сам. работа
I. Основы понятия и история информационной безопасности (6 часов)				
1.	Основные понятия информационной безопасности	2	1	1
2.	Информационные противостояния от древности до Нового времени	2	1	1
3.	Информационные войны XX век	2	1	1
II. Проблемы и угрозы информационной безопасности (6 часов)				
4.	Основные проблемы информационной безопасности	2	1	1
5.	Источники угроз информационной безопасности	2	1	1
6.	Информационная безопасность в системе национальной безопасности России	2	1	1
III. Защита сведений, составляющих государственную и коммерческую тайну (8 часов)				
7.	Правовые основы защиты информации	2	1	1
8.	Классификация сведений, подлежащих защите	2	1	1
9.	Организация защиты информации	2	1	1
10.	Контрольные вопросы	2	1	1
IV. Основные направления обеспечения информационной безопасности (8 часов)				
11.	Защита информации в экономике, науке и технике	2	1	1
12.	Основные направления и мероприятия по защите электронной информации	2	1	1
13.	Безопасность в сфере духовной жизни человека и общества	2	1	1
14.	Контрольные вопросы	2	1	1
V. Современные методы защиты информации в автоматизированных системах обработки данных (10 часов)				
15.	Организация защиты от интернет-угроз	2	1	1
16.	Криптографические методы защиты информации	2	1	1
17.	Электронная цифровая подпись (ЭЦП)	2	1	1
18.	Управление ключами	2	1	1
19.	Контрольные вопросы	2	1	1
VI. Сущность и методы информационного воздействия на человека (12 часов)				
20.	Сущность и современное состояние манипуляции сознанием и поведением людей	2	1	1
21.	Основные методы и средства информационного воздействия на человека	2	1	1
22.	Мифы как инструмент воздействия на людей	2	1	1
23.	Манипулятивные технологии в избирательных кампаниях	2	1	1
24.	Методы тоталитарных сект и способы защиты от них	2	1	1

25.	Контрольные вопросы	2	1	1
VII. Информационная безопасность в повседневной жизни (10 часов)				
26.	Рыночные отношения – социально-экономическая основа манипуляции людьми	2	1	1
27.	Влияние СМИ на мировоззрение людей	2	1	1
28.	Роль рекламы в манипуляции сознанием людей	2	1	1
29.	Средства информационного воздействия и защита здоровья	2	1	1
30.	Контрольные вопросы	2	1	1
VIII. «Глобальное общество» и проблемы информационной безопасности (10 часов)				
31.	Объективные и субъективные предпосылки создания глобального общества	2	1	1
32.	Роль Интернета в мировом информационном пространстве	3	2	1
33.	Глобальные ожидания и опасения человечества	3	2	1
34.	Итоговое занятие	2	1	1

5. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ

Планируемые результаты освоения учащимися программы курса «Основы информационной безопасности» уточняют и конкретизируют общее понимание личностных, метапредметных и предметных результатов как с позиции организации их достижения в образовательном процессе, так и с позиции оценки достижения этих результатов.

Личностные образовательные результаты:

1. способность учащихся к саморазвитию, личностному самоопределению;
2. развитость чувства личной ответственности за качество окружающей информационной среды;
3. формирование ответственного отношения к учебной деятельности;
4. формирование потребности к самообразованию, повышение своего образовательного уровня и подготовки к продолжению обучения с использованием обучающих, тестирующих программ или иных программных продуктов;
5. формирование целостного представления об окружающей действительности;
6. увеличение объема информационных знаний, соответствующих уровню развития науки и общественной практики
7. формирование уважительного и доброжелательного отношения к другому человеку, его мировоззрению;
8. готовность и способность вести диалог с другими людьми и достижение в нём взаимопонимания;
9. формирование нравственных чувств и нравственного поведения, ответственного отношения к собственным поступкам;
10. развитие морального сознания;
11. развитие умения критично относится к своим поступкам и поступкам окружающих;
12. формирование навыков общения и сотрудничества со сверстниками и взрослыми;
13. формирование осознанного выбора будущей профессии и возможности реализации собственных жизненных планов;
14. готовность к профессиональной деятельности как возможности участия в решении личных, общественных, государственных, общенациональных задач.

Метапредметные образовательные результаты:

1. формирование умение самостоятельно определять цели своего обучения;
2. развитие мотивов и интересов своей познавательной деятельности;
3. формирование понимания всех этапов решения задачи;
4. умение самостоятельно планировать пути достижения целей, выбирать оптимальные из них;
5. умение соотносить свои действия с планируемыми результатами;
6. умение контролировать свою деятельность в процессе достижения результата;
7. умение корректировать свои действия в соответствии с изменяющейся ситуацией;
8. умение оценивать правильность выполнения учебной задачи;
9. умение правильно оценивать собственные возможности решения задачи;
10. формирование навыков самоконтроля, самооценки своей деятельности;
11. формирование умения давать определения понятиям;
12. умение устанавливать причинно-следственные связи;
13. умение организовывать учебное сотрудничество и совместную деятельность с учителем и сверстниками;
14. умение работать индивидуально и в группе;
15. развитие навыков формулировать, аргументировать и отстаивать своё мнение;
16. формирование основных понятий в области использования ИКТ.

Предметные образовательные результаты:

1. умение применять полученные знания, результаты изучения, методы для решения задач из различных областей;
2. формирование информационной культуры;
3. формирование представления о компьютере как универсальном устройстве обработки информации;
4. развитие основных навыков и умений использования компьютерных устройств;
5. знание основных компонентов компьютера и их основные функции;
6. владение навыками работы с типовым интерфейсом основного программного обеспечения;
7. знание норм и правил, которым необходимо следовать при общении в Интернет;
8. представление об организации информационной безопасности;
9. умение выбирать способ представления данных в соответствии с поставленной задачей;
10. знание технических и гигиенических требований для безопасной работы с компьютером;
11. владение навыками использования основных средств телекоммуникаций.

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;
- ⇒ 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.
- ⇒ Использовать возможности ОС Windows XP для защиты информации;
- ⇒ Пользоваться архиватором и антивирусной программой.

Форма контроля

Текущий контроль осуществляется форме тестов, проектов, кроссвордов, «круглого стола».

Итоговый контроль осуществляется по завершении учебного материала в форме интерактивного тестирования, теста по опросному листу или компьютерного тестирования. Система оценивания – безотметочная. Используется только словесная оценка достижений учащихся.

СПИСОК ЛИТЕРАТУРЫ

1. Конституция Российской Федерации (основной закон).
2. Федеральный закон Российской Федерации от 27 июля 2006 года № 149 ФЗ «Об информации, информационных технологиях и о защите информации».
3. Закон Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации».
4. Доктрина информационной безопасности Российской Федерации (утверждена Президентом РФ 9 сентября 2001 года).
5. Безопасность жизнедеятельности: Государственные общеобразовательные стандарты. Библиографические источники. / Авт. – сост. С.В. Петров. – М.: Изд-во НЦ ЭНАС, 2005.
6. Буданцев Ю.П. Информационное оружие и информационная война в современных условиях. // Информационный сборник «Безопасность». 1999. № 3–4.
7. Ведеев Д. Защита данных в компьютерных сетях. // «Открытые системы». 1995. № 3.
8. Ганжин В.Т. Опасные «связи с общественностью». // Информационный сборник «Безопасность». 1999. № 1–2.
9. Грановская Р.М. Элементы практической психологии. – Л.: Изд-во Ленинградского университета, 1988.
10. Грачев Г.В., Мельник И.К. Манипулирование личностью. – М.: Изд-во «Эксмо», 2003.
11. Гриняев С. Информационное превосходство – основа военной стратегии XXI века. // «ОБЖ. Основы безопасности жизни». 2001. № 7.
12. Замятин А., Замятин В., Юсупов Р. Опасности информационно-психологической войны. // «ОБЖ. Основы безопасности жизни». 2002. № 6.
13. Извеков Н.Н. Исторические традиции как средство укрепления национального иммунитета в информационных войнах III тысячелетия. // Информационный сборник «Безопасность». 2001. № 7—12.
14. Кавеладзе И.Т. Практика защиты коммерческой тайны в США (руководство по защите вашей деловой информации). – М.: Изд-во «ЭКО-консалтинг», 1992.
15. Кара-Мурза С.Г. Манипуляция сознанием в России сегодня. – М.: Изд-во «Эксмо», 2001.
16. Колин К.К. Русский язык и национальная безопасность // Информационный сборник «Безопасность». 1997. № 1–2.
17. Матвеев В., Дружинин А., Маньков В. Информационные воздействия на человека и на общество. // «ОБЖ. Основы безопасности жизни». 2002. № 4.
18. Мифы народов мира. Энциклопедия. – М.: Изд-во «Советская Энциклопедия», 1991.
19. Мухин В., Лось А., Новиков В.О. некоторых подходах к определению сущности информационного оружия. // Информационный сборник «Безопасность». 1996. № 1–2.
20. Новопашин А.П. Информационная политика России. // Информационный сборник «Безопасность». 2002. № 11–12.
21. Носов Л. Оповещение населения о чрезвычайных ситуациях. // «ОБЖ. Основы безопасности жизни». 2004. № 1.
22. Петров С.В. Обеспечение безопасности образовательного учреждения. – М.: Изд-во ОАО «Московские учебники», 2005.
23. Прозоров А.Д. Как спасти себя и своего ребенка от тоталитарной секты. – СПб.: Издательский Дом «Литера», 2000.
24. Пугачев В.П. Управление свободой. – М.: Изд-во «КомКнига», 2005.
25. Смирнов Н.К. Здоровьесберегающие образовательные технологии и психология здоровья в школе. – М.: Изд-во «АРКТИ», 2006.
26. Сократов Н.В. Культура здоровья с основами безопасности жизнедеятельности. – Оренбург: Изд-во ОГПУ, 2006.
27. Уманский С.В. Психологическое воздействие: манипуляция или психотерапия. / В кн. «Психологическая теория и практика в изменяющейся России» (тезисы докладов Всероссийской научной конференции). – Челябинск: Изд-во ЮУрГУ, 2006.
28. Франкл В. Человек в поисках смысла: Сборник. – М.: Изд-во «Прогресс», 1990.

29. Фрейд З. Введение в психоанализ: Лекции. – М.: Изд-во «Наука», 1989.
30. Хаббард Л.Р. Дианетика. Современная наука душевного здоровья. – М.: Издательская группа Нью Эра, 1996.
31. Хвыля-Олинтер А. И., Лукьянов С. А.Опасные тоталитарные формы религиозных сект. – М.: Изд-во Свято-Владимирского Братства, 1996.
32. Шершнев Л.И. Четвертая мировая война и ее особенности. // «ОБЖ. Основы безопасности жизни». 2005. № 7, 9.
33. Шостром Э. Анти-Карнеги, или Человек-манипулятор. – Минск: Изд-во ТПЦ «Полифакт», 1992.
34. Ясперс К. Смысл и назначение истории. – М.: Изд-во «Республика», 1994.