МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Министерство образования и науки Алтайского края
Комитет по образованию города Барнаула
МБОУ "Лицей №129" им. Сибирского батальона 27-й стрелковой дивизии

СОГЛАСОВАНО	УТВЕРЖДЕНА
Педагогическим советом	приказом директора
МБОУ "Лицей № 129"	МБОУ "Лицей №129"
(протокол от 24.08.2022 №1)	от 25.08.2022 №187-осн
	_____ С.Н. Кутлан

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 5D28E3B21EE3442A31DCE4D63CB401E
Владелец: Кутлан Сергей Николаевич
Действителен: с 15.03.2022 до 08.06.2023

СОГЛАСОВАНО
Кафедрой ЕМД
МБОУ "Лицей № 129"
(протокол от 23.08.2022 №1)

Рабочая программа

элективного курса "Основы информационной безопасности в телекоммуникационных сетях"

для 11 класса

уровень образования:	среднее общее образование
класс:	11 (А, Б, В)
учебный год:	2022-2023

Составитель:
Рыжова Ирина Михайловна, учитель информатики и ИКТ

Барнаул, 2022

Содержание

Пояснительная записка

Нормативные документы, на основе которых разработана рабочая программа

Рабочая программа элективного курса "Основы информационной безопасности в телекоммуникационных сетях" составлена на основе следующих нормативных документов:

- приказа Министерства образования и науки РФ от 17 мая 2012 г. N 413 "Об утверждении федерального государственного образовательного стандарта среднего общего образования" (с изменениями и дополнениями);
- 2012 г. № 39, 31 января 2012 г. № 66, 23 июня 2015 г. № 609, 7 июня 2017 г. № 506);
- основной образовательной программы МБОУ "Лицей № 129" среднего общего образования;
- положения о рабочих программах учебных предметов и курсов МБОУ "Лицей № 129";
- учебного плана МБОУ "Лицей № 129";
- годового календарного учебного графика МБОУ "Лицей № 129";

Цель курса: освоение основных знаний и формирование умений по обеспечению информационной безопасности при работе в сети.

Задачи курса: Для реализации поставленной задачи необходимо решение следующих задач:

- освоение учащимися основных понятий информационной безопасности, а также формирование умений по устранению и уменьшению последствий ее нарушения;
- формирование умений работать с основными классами программных для обеспечения информационной безопасности при работе в сети и практических навыков их установки, настройки и использования на конкретных примерах;
- ознакомление с методами шифрования информации и системами сертификации;
- ознакомление учащихся с методами контроля источников информации;
- формирование навыков построения персонального защитного комплекса для одиночного компьютера;
- воспитание уважительного отношения к другим пользователям сети, соблюдения правил сетевого этикета.

Общая характеристика элективного курса

Программа предлагаемого элективного курса ориентирована на развитие знаний и умений по обеспечению информационной безопасности при работе на персональном компьютере в сети, полученных в основной школе в ходе изучения определенных тем учебного предмета "Информатика и ИКТ". Данный курс предназначен для тех, кто определил информатику как сферу своих будущих профессиональных интересов в качестве основного направления.

Курс "Основы информационной безопасности в телекоммуникационных сетях", опираясь на ранее изученный материал, призван развить наиболее актуальные вопросы технологии и средств защиты информации в сети, а также сформировать целостную, пригодную к практическому использованию систему понятий данной области деятельности.

Курс позволит учащимся освоить необходимые программные средства и сформировать у них необходимые практические навыки. При изучении данного курса предполагается использование современных демонстрационных или свободно распространяемых средств и доступ к системам обновления для обеспечения максимальной актуальности материала.

Место курса "Основы информационной безопасности в телекоммуникационных сетях" в базисном учебном плане

Курс "Основы информационной безопасности в телекоммуникационных сетях" является элективным. В соответствии с учебным планом рабочая программа курса рассчитана на **34 часа** по **1 часу** в неделю и реализуется в течение одного года.

Для организации исследовательской и проектной деятельности учащихся можно использовать часы, отведенные на внеурочную деятельность.

1. Требования к результатам изучения элективного курса "Основы информационной безопасности телекоммуникационных сетях"

Учащиеся должны

знать:

- назначение и области использования основных технических средств ИКТ и информационных ресурсов;
- различные системы шифрования и области их применения;
- базовые принципы организации и функционирования компьютерных сетей;
- основные понятия информационной безопасности;
- средства обеспечения информационной безопасности;
- основные опасности и ошибки при работе в сетях, методы борьбы с ними;
- понятие вируса, "троянской" программы; средства удаленного управления, средства борьбы с ними;
- способы удостоверения и контроля аутентичности входящей и исходящей информации, методы проверки ее источников;
- правовые основы в области защиты информации, персональных данных и использования электронной цифровой подписи;

уметь:

- оперировать информационными объектами, используя имеющиеся знания о возможностях информационных и коммуникационных технологий, в том числе создавать структуры хранения данных;
- пользоваться справочными системами и другими источниками справочной информации;
- соблюдать права интеллектуальной собственности на информацию;
- устанавливать и настраивать программные средства защиты;
- разграничивать доступ к ресурсам локальной машины;
- своевременно обновлять программное обеспечение;
- контролировать источники информации по их заголовкам и сертификатам;
- использовать полученные знания и навыки для организации собственной безопасной работы в сети.

2. Формы и методы организации учебного процесса

Элективный курс реализуется через классно-урочную систему. Теоретическая и прикладная часть элективного курса осваиваются параллельно, чтобы сразу закреплять теоретические вопросы на практике, формировать соответствующие умения.

Элективный процесс организуется в двух взаимосвязанных и взаимодополняющих формах:

- урочной форме, когда с помощью учителя осваивается новый материал, учитель консультирует учащихся в процессе решения задач, учащиеся выполняют практикумы, защищают выполненные задания, проектные работы (практика);
- внеурочной форме, когда учащиеся после занятий самостоятельно выполняют задания компьютерного практикума, проектные работы.

Единицей учебного процесса является урок. В первой части урока проводится актуализация знаний и изучение нового материала, а во второй - планируется компьютерный практикум (практические работы) для получения основных навыков работы, в каждом задании формулируется цель и предлагается способ ее достижения, предлагаются задания для самостоятельного выполнения. Каждое занятие начинается с мотивационного этапа, ориентирующего учащегося на выполнение практического задания по теме. Учащийся имеет доступ к компьютеру и выполняет практические работы по описанию самостоятельно или, при необходимости, с консультацией и помощью учителя. Каждое занятие начинается с мотивационного этапа, ориентирующего учащегося на выполнение практического задания по теме.

Наряду с индивидуальной применяется и групповая работа, преимущественно в проектной форме. В задачи учителя входит создание условий, проблемных ситуаций, разрешение которых подводит учащихся к конструированию авторских разработок. Выполнение проекта завершается защитой результата с последующим рефлексированием.

Основной тип занятий – практикум. Большинство заданий курса выполняется с помощью персонального компьютера и необходимых программных средств. Формирование пользовательских навыков подкрепляется *самостоятельной творческой работой*, личностно-значимой для обучающегося.

3. Методы и технологии обучения

Для развития познавательной, информационно-коммуникативной, рефлексивной деятельности используются:

- технология проблемного обучения, которая предполагает организацию самостоятельной поисковой деятельности обучающихся по решению проблем: учитель не сообщает знания в готовом виде, а ставит перед учеником проблему, заинтересовывает его, пробуждает желание найти способ ее решения. В ходе проблемного обучения у обучающихся формируются новые знания и умения, развиваются познавательная активность, творческое мышление и другие личностные качества;
- технология проектного обучения, которая предполагает решение практических задач, проживание конкретных ситуаций, конструирование новых процессов. Целью проектного обучения является не столько усвоение суммы знаний, а развитие и обогащение собственного опыта обучающихся и их представлений о мире;

- дифференцированное обучение – создание групп разного уровня по качеству знаний, темпам усвоения материала, учебной мотивацией, способу мышления.

При организации занятий школьников по информатике необходимо использовать различные методы и средства обучения с тем, чтобы с одной стороны, свести работу за компьютером к регламентированной норме; с другой стороны, достичь наибольшего педагогического эффекта.

На уроках параллельно применяются общие и специфические методы, связанные с применением средств ИКТ:

- словесные методы обучения (рассказ, объяснение, эмпирическая беседа, работа с учебником);
- наглядные методы (наблюдение, иллюстрация, использование компьютерных презентаций и других цифровых образовательных ресурсов);
- практические методы (устные и письменные упражнения, практические работы за ПК);
- проблемное обучение;
- метод проектов.

Основные типы уроков:

- урок изучения нового материала;
- урок контроля знаний;
- обобщающий урок;
- комбинированный урок.

Для активизации познавательной деятельности обучающихся на уроках информатики учебный материал представляется в мультимедийном и интерактивном виде.

Основными методами обучения предмету являются: объяснительно-иллюстративный, частично-поисковый и репродуктивный.

На уроках используются элементы следующих технологий: личностно-ориентированное обучение, обучение с применением опорных схем, ИКТ, элементы системно-деятельностного подхода.

Для учащихся, ***испытывающих трудности в освоении*** предмета предусмотрены

- возможность индивидуальной уровневой дифференциации практических заданий,
- послеурочные предметные консультации,
- дистанционные консультации (e-mail, Skype),
- предварительная проверка правильности выполнения практических заданий с обсуждением ошибок и помощи в их исправлении,
- система "работы над ошибками",
- размещение в открытом доступе материалов для проведения тестов, практических, контрольных и самостоятельных работ.

4. Критерии выставления отметок успеваемости

При освоении элективного курса принята и используется зачетная система.

Для отслеживания результатов освоения элективного курса предусматриваются следующие **виды контроля**:

Самооценка, самоконтроль или взаимный контроль выполняется самостоятельно учащимися с соответствии критериями, предложенными учителем или разработанными вместе с ним.

Текущий контроль уровня усвоения материала осуществляется по результатам устных опросов, выполнения учащимися практических заданий на каждом уроке или в форме наблюдения:

- прогностический, то есть проигрывание всех операций учебного действия до начала его реального выполнения;
- пооперационный, то есть контроль за правильностью, полнотой и последовательностью выполнения операций, входящих в состав действия;
- рефлексивный, контроль, обращенный на ориентировочную основу, "план" действия и опирающийся на понимание принципов его построения;
- контроль по результату, который проводится после осуществления учебного действия методом сравнения фактических результатов или выполненных операций с образцом.

Тематический контроль осуществляется по завершении темы. Он позволяет оценить знания и умения обучающихся, полученные в ходе достаточно продолжительного периода работы и реализуется в форме проверочных работ, рекомендованных авторами УМК, тематического тестирования.

Итоговый контроль проводится в конце каждого учебного периода и в конце учебного года

В конце каждого учебного периода учащийся предоставляет портфолио выполненных работ (практических и проверочных).

Критерии оценивания проверочных работ

Проверочная работа (контрольная работа, тест) считается выполненной (зачет), если учащийся набрал не менее 50% баллов от максимально возможного количества баллов, иначе - незачет.

Критерии оценок при выполнении практических заданий:

Практическая работа считается не выполненной, если ученик самостоятельно не справился с работой, технологическая последовательность нарушена, при выполнении операций допущены большие отклонения, работа оформлена небрежно и имеет незавершенный вид, изображение не соответствует образцу.

Критерии оценок для творческого проекта:

- эстетичность оформления,
- содержание, соответствующее теме работы,
- отражение всех знаний и умений учащихся в данной работе,
- успешная защита проекта.

Система оценивания

Из выполненных практических работ и написанных проверочных работ учащийся формирует портфолио, которое представляет учителю в конце учебного периода.

Система оценивания - **зачетная** ("зачет", "незачет"). В конце учебного периода учащемуся выставляется отметка "зачет", если он регулярно посещал занятия (не менее 2/3 от количества занятий в отчетном периоде) и выполнил не менее 50% учебных заданий (определяется по представленному портфолио), а в конце учебного года успешно защитил итоговый проект.

Перечень ошибок

Грубые ошибки

- Незнание определений, основных понятий, правил, основных положений теории, приемов составления алгоритмов.
- Неумение выделять в ответе главное.
- Неумение применять знания для решения задач, неправильно сформулированные вопросы задачи или неверное объяснение хода ее решения, незнание приемов решения задач, аналогичных ранее решенным в классе; ошибки, показывающие неправильное понимание условия задачи, неправильный выбор инструментов для выполнения работы
- Неумение пояснить этапы решения, обосновать выбор необходимых средств для ее решения.
- Неумение подготовить к работе компьютер, запустить программу, получить результаты и объяснить их.
- Небрежное отношение к компьютеру.
- Нарушение требований правил безопасного труда при работе на компьютере.

Негрубые ошибки

Погрешность (негрубая ошибка) свидетельствует о нечетком представлении рассматриваемого объекта:

- Неточность формулировок, определений, понятий, вызванные неполнотой охвата основных признаков определяемого понятия; ошибки синтаксического характера.
- Нерациональный выбор инструментов для выполнения задания.

Недочеты

- Неточности в устной и письменной речи, не искажающие смысла ответа или решения, случайные описки и т.п.
- Отдельные неточности в формулировке вопроса или ответа.
- Небрежное выполнение записей.
- Орфографические и пунктуационные ошибки

5. Содержание элективного курса "Основы информационной безопасности в телекоммуникационных сетях"

Правовое обеспечение информационной безопасности (9 ч.)

Классификация информации. Информационная безопасность: основные понятия. Аспекты безопасности. Принципы информационной безопасности. Разновидности угроз информационной безопасности. Классификация уязвимостей систем безопасности. Обеспечение информационной безопасности в России. Кибервойны

Информация как объект правового регулирования. Информация ограниченного доступа. Понятие компьютерного преступления. Уголовное законодательство и компьютерная преступность. Правовое регулирование отношений в сфере информатизации общества и деятельности органов внутренних дел

Современные методы защиты информации (13 ч.)

Типы аппаратуры в сетях Интернет. Мероприятия от утечки информации по техническим каналам

Перехват информации. Методы и средства защиты информационных систем

Типы атак

Классы безопасности информационных систем

Защита передаваемых электронных данных

Персональные данные. Защита персональных данных

Использование персональных брандмауэров для оптимизации работы в сети Интернет.

Системы шифрования с открытым ключом. Симметричное шифрование. Сертификаты, обмен сертификатами, доверие. Шифрование информации на прикладном уровне. Электронная цифровая подпись

Стеганография

Безопасность программного обеспечения и данных (9 ч.)

Безопасность операционных систем. Правила создания и замены паролей, разграничение доступа на основе пользовательских записей.

Безопасность баз данных

Обеспечение безопасности доставки, печати, сканирования и передачи экзаменационных материалов ЕГЭ

Вредоносные программы. Типы вирусов. Признаки заражения компьютера. Защита от вредоносных программ. Антивирусные программы, программы детектирования и удаления нежелательных внедрений

Проведение обновления программного обеспечения

Организация контроля за поступающей и исходящей информацией.

6. Контрольно-тематическое планирование элективного курса "Основы информационной безопасности в телекоммуникационных сетях"

Содержание раздела	Количество часов		Вид контроля	Дата проведения контроля (номер недели)
	общее	КР и ПР		
Правовое обеспечение информационной безопасности	8			
Современные методы защиты информации	13			
Безопасность программного обеспечения	9			
Контроль знаний и умений: тестирование, выполнение итоговой практической работы	3	3	Тестирование, ПР	27.04 – 02.05 (31) 04.05 – 09.05 (32) 11.05 – 16.05 (33)
Итоговое повторение, резерв	1			
Итого 11 класс	**34**	**3**		

7. Поурочно-тематическое планирование

№ урока	Тема урока	Содержание (основные понятия)		Возможные виды контроля	ИКТ	Дата (номер недели)
	Правовое обеспечение информационной безопасности (9 ч.)					
1	Классификация информации	Виды классификаций. Классификация информации по форме представления, по области возникновения, по способу передачи и восприятия, по общественному назначению, по способам кодирования		ФКО	+	1
2	Информационная безопасность: основные понятия. Аспекты безопасности	Основные понятия ИБ. Аспекты безопасности (целостность, доступность, конфиденциальность		ФКО	+	2
3	Принципы информационной безопасности. Разновидности угроз информационной безопасности	Основные принципы ИБ: простота использования, достаточная стойкость, разграничение доступа, минимальные привилегии и т.д. Основные типы угроз: конфиденциальности, целостности, доступности. Источники угроз; внутренние и внешние.		ФКО	+	3
4	Классификация уязвимостей систем безопасности	Классификация уязвимостей: уязвимости проектирования (проектирование); уязвимости реализации (реализация); уязвимости конфигурации (эксплуатация). ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем		ФКО	+	4
5	Обеспечение информационной безопасности в России и мире. Кибервойны	Роль ИБ в мире и России. Структурные элементы информационной безопасности на международном и внутригосударственном уровне. Информационная безопасность в России. Проблемы и угрозы ИБ на международном уровне		ФКО, сообщение	+	5
6	Информация как объект правового регулирования. Информация ограниченного доступа	Информация как объект правового регулирования. Свойства информации. Документированная информация и документ. Правовое обеспечение информационной безопасности РФ. Понятие, признаки и структура информации сограниченным доступом. Виды информации ограниченного доступа		ФКО	+	6
7	Понятие компьютерного преступления. Уголовное законодательство и компьютерная преступность	Понятие компьютерного преступления и его особенности. Виды компьютерных преступлений. .Методы обнаружения и предупреждения преступлений в информационной среде. Общая характеристика преступлений		ФКО, ПР	+	7

№ урока	Тема урока	Содержание (основные понятия)		Возможные виды контроля	ИКТ	Дата (номер недели)
		в компьютерной сфере по современному Российскому уголовному законодательству. УК РФ: преступления в сфере компьютерной информации				
8	Правовое регулирование отношений в сфере информатизации общества и деятельности органов внутренних дел	Основные задачи правовой информатизации. Система информационного законодательства. Правовые информационные системы. Органы внутренних дел в механизме правового регулирования в сфере обеспечения информационной безопасности		ФКО	+	8
	Современные методы защиты информации (13 ч.)					
9	Типы аппаратуры в сетях Интернет. Мероприятия от утечки информации по техническим каналам	Сетевое оборудование. Виды. Основные понятия. Типы кабелей. Средства и способы защиты. Защита информации от утечки по каналам: акустическим; электромагнитным; за счет взаимного влияния проводов и линий связи; за счет высокочастотного навязывании; в волоконно-оптических линиях и системах связи.		ФКО	+	9
10	Перехват информации. Методы защиты.	Способы перехвата информации. Противодействие перехвату информации. Защита личных данных		ФКО, ПР	+	10
11	Средства защиты информационных систем	Методы защиты информации в информационных системах (препятствие на пути предполагаемого похитителя, управление, маскировка, регламентация; принуждение; побуждение). Средства защиты информации в информационных системах (организационные и технические). Аутентификация и идентификация		ФКО	+	11
12	Типы атак	Виды и классификация атак на информационные системы (по характеру воздействия на сеть; по цели воздействия; по наличию обратной связи с атакуемой сетью; по условию начала осуществления атаки; по расположению субъекта атаки относительно объекта; по уровню эталонной модели ISO.). Методы защиты. DDoS-атаки: типы, защита, устранение атак		ФКО, сообщение	+	12
13	Классы безопасности информационных систем	Требования к уровням и классам ИБ (произвольное управление; безопасность повторного использования; метки безопасности; принудительное управление; метка объекта). Уровни и классы ИБ (A, B, C,D)		ФКО	+	13
14	Защита передаваемых электронных данных	Защита электронных документов: обеспечение целостности и конфиденциальности		ФКО	+	14
15	Персональные данные. Защита персональных	Понятие персональных: данных. Категории и состав персональных дан-		ФКО	+	15

№ урока	Тема урока	Содержание (основные понятия)		Возможные виды контроля	ИКТ	Дата (номер недели)
	данных	ных. Этапы работ по защите персональных данных. Защита персональных данных, ответственность за нарушение. ФЗ о персональных данных.				
16	Использование персональных брандмауэров для оптимизации работы в сети Интернет.	Что такое брандмауэр. Выбор брандмауэра. Конфигурация сетевого экрана. Методы использования брандмауэра, хакерские атаки на брандмауэр		ФКО, ПК	+	16
17	Системы шифрования с открытым ключом. Симметричное шифрование.	Идея криптосистемы с открытым ключом (общие принципы, реализация через одностороннюю функцию). Схема шифрования с открытым ключом. Симметричное шифрование.		ФКО, ПР	+	17
18	Сертификаты, обмен сертификатами, доверие.	Сертификат: понятие. Запрос, установка сертификата. Добавление сертификата в хранилище		ФКО	+	18
19	Шифрование информации на прикладном уровне.	Шифрование информации на прикладном уровне. Инфраструктура защиты на прикладном уровне		ФКО	+	19
20	Электронная цифровая подпись	ЭП: основные принципы. История возникновения. Алгоритмы. Подделка подписей. Управление ключами. Использование ЭП		ФКО	+	20
21	Стеганография	Стеганография: понятие. Цели, актуальность, практическоеприменение. Классическая и компьютерная стеганография. Стеганография в современных кибератаках		ФКО, ПР	+	21
	Безопасность программного обеспечения и данных (9 ч.)					
22	Безопасность операционных систем	Проблема безопасности. Требования к безопасным систем: конфиденциальность, доступность, целостность, аутентичность. Механизмы защиты ОС.		ФКО	+	22
23	Правила создания и замены паролей, разграничение доступа на основе пользовательских записей.	Надежный пароль. Правила создания надежны паролей. Правила хранения и использования паролей. Восстановление паролей. Методы разграничения доступа. Методы управления доступом. Типичные ошибки при разработке прав доступа		ФКО, ПР	+	23
24	Безопасность баз данных	Режимы работы с БД. Особенности защиты БД. Основные требования к защите БД. Требования по управлению доступом в базах данных. Требования по управлению целостностью в базах данных. Механизмы защиты БД		ФКО	+	24
25	Обеспечение безопасности доставки, печати, сканирования и передачи экзаменационных материалов ЕГЭ	Обеспечение безопасности доставки, печати, сканирования и передачи экзаменационных материалов ЕГЭ		ФКО	+	25

№ урока	Тема урока	Содержание (основные понятия)		Возможные виды контроля	ИКТ	Дата (номер недели)
26	Вредоносные программы. Типы вирусов	Вредоносная программа: определение, классификация. Компьютерный вирус: определение, жизненный цикл, классификация		ФКО	+	26
27	Признаки заражения компьютера	Признаки заражения компьютера. Последствия заражения		ФКО, сообщение	+	27
28	Защита от вредоносных программ. Антивирусные программы, программы детектирования и удаления нежелательных внедрений	Способы защиты от компьютерных вирусов		ФКО, ПР	+	28
29	Проведение обновления программного обеспечения	Способы обновления ПО, создание расписания обновления, необходимость регулярного обновления ПО		ФКО, ПР	+	29
30	Организация контроля за поступающей и исходящей информацией.	Организация контроля за поступающей и исходящей информацией, проверка источников информации, анализ заголовков писем, борьба со спамом и ее последствия		ФКО, ПР	+	30
	Контроль знаний и умений (3 ч.)					
31 32 33	**Итоговый контроль знаний и умений учащихся тестирование, защита итогового проекта**			**Тестирование, защита проекта**		**31 32 33**
	Итоговое повторение, резерв (1 ч)					
34	Резерв					**34**
	Итого	**34 ч.**				

Нумерация учебных недель 2022-2023 уч. год

№ недели	Период	№ недели	Период
1	01.09 – 03.09	17	09.01 – 14.01
2	05.09 – 10.09	18	16.01 – 21.01
3	12.09 –17.09	19	23.01 –28.01
4	19.09 –24.09	20	30.01 – 04.02
5	26.09 – 01.10	21	06.02 – 11.02
6	03.10 – 08.10	22	13.02 – 18.02
7	10.10 - 15.10	23	20.02 – 25.02
8	17.10 – 22.10	24	27.02 – 04.03
9	24.10 –28.10	25	06.03 - 11.03
каникулы	29.10 – 06.11	26	13.03 – 18.03
10	07.11 –12.11	27	20.03 – 23.03
11	14.11 – 19.11	каникулы	26.03 –.03.04
12	21.11 – 26.11	28	03.04 - 08.04
13	28.11 – 03.12	29	10.04 – 15.04
14	05.12 – 10.12	30	17.04 – 22.04

№ недели	Период	№ недели	Период
15	12.12 –17.12	31	24.04 – 29.04
16	19.12 – 24.12	32	02.05 – 06.05
	26.12 – 28.12	33	08.05 – 13.05
каникулы	29.12 – 08.01	34	15.05 – 20.05
		35	22.05 – 27.05
			29.05 – 31.05

8. Материально-техническое и учебно-методическое обеспечение элективного курса "Основы информационной безопасности в телекоммуникационных сетях"

8.1. Список технических средств обучения в кабинете

Для реализации элективного курса "Основы информационной безопасности в телекоммуникационных сетях" необходимо наличие компьютерного класса в соответствующей комплектации. Наиболее рациональным с точки зрения организации деятельности детей в школе является установка в компьютерном классе 13–15 компьютеров (рабочих мест) для школьников и одного компьютера (рабочего места) для педагога.

Предполагается объединение компьютеров в локальную сеть с возможностью выхода в Интернет, что позволяет использовать сетевые цифровые образовательные ресурсы.

Минимальные **требования к техническим характеристикам** каждого компьютера следующие:

- процессор – не ниже Celeron с тактовой частотой 2 ГГц;
- оперативная память – не менее 256 Мб;
- жидкокристаллический монитор с диагональю не менее 15 дюймов;
- жёсткий диск – не менее 80 Гб;
- клавиатура;
- мышь;
- устройство для чтения компакт-дисков (желательно).

Кроме того в кабинете информатики должны быть:

- принтер на рабочем месте учителя;
- проектор на рабочем месте учителя;
- сканер на рабочем месте учителя

На компьютерах, которые расположены в кабинете информатики, должна быть установлена операционная система *Windows* или *Linux*, а также необходимое программное обеспечение:

- текстовый процессор (*Word* или *OpenOfficeWriter*);
- табличный процессор (*Excel* или *OpenOffice.orgCalc*);

- браузер;
- архиватор;
- антивирусная программа с доступом к системе обновления;
- сканер уязвимостей;
- другие программные средства.

8.2. Учебно-методическое обеспечение элективного курса "Основы информационной безопасности в телекоммуникационных сетях"

1. StudFiles: файловый архив студентов. URL https://studfile.net/preview/4404078/page:3/
2. Анисимов В.В. Основы информационной безопасности и защиты информации, URL: https://www.sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema1
3. Классификация медодов защиты информации. URL: https://camafon.ru/informatsionnaya-bezopasnost/metodyi-zashhityi
4. https://pirit.biz/reshenija/informacionnaja-bezopasnost
5. Угрозы информационной безопасности. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/
6. Обеспечение безопасности персональных данных. URL: https://www.intuit.ru/studies/courses/697/553/lecture/12442
7. Цирлов В.Л. Основы информационной безопасности автоматизированных систем: краткий курс.- Ростов-на-Дону: Феникс, 2008. URL: https://www.e-reading.mobi/bookreader.php/134422/Cirlov_-_Osnovy_informacionnoii_bezopasnosti._Kratkiii_kurs.pdf
8. Информация и средства ее защиты. URL: https://itnan.ru/post.php?c=1&p=343498 (классификация информации)
9. Основы защиты информации: учебное пособие. Изд. 5-е, перераб. и
10. доп. – Томск: В-Спектр, 2011. URL: http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_ozi.pdf
11. http://pro-spo.ru/secure/270--l-r-ad-awarer-personal

Лист регистрации изменений, внесённых в рабочую программу

№ п./п.	Дата	№ стр. с изменениями	Характеристика изменений	Реквизиты документа, закрепляющего изменение	ФИО работника, внесшего изменение	Подпись работника