РЕГИОНАЛЬНЫЙ ЦЕНТР ВЫЯВЛЕНИЯ, ПОДДЕРЖКИ И РАЗВИТИЯ СПОСОБНОСТЕЙ И ТАЛАНТОВ ДЕТЕЙ И МОЛОДЁЖИ СТАВРОПОЛЬСКОГО КРАЯ «СИРИУС 26»

СОГЛАСОВАНО
Экспертным советом регионального центра выявления, поддержки и развития способностей и талантов детей и молодёжи Ставропольского края «Сириус 26», протокол № 1/2025 от 03.02.2025 г .

УТВЕРЖДЕНО
Директором Центра «Поиск» Томилиной О.А.

приказ № 13/1 от 04.02.2025 г.

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА

«ЦИФРОВАЯ БЕЗОПАСНОСТЬ: ПРОТИВОДЕЙСТВИЕ КИБЕРУГРОЗАМ»

Направленность:	техническая
Возраст обучающихся:	14-17 лет
Объем программы:	92 часа
Срок освоения:	2 месяца
Форма обучения:	очная с применением дистанционных образовательных технологий
Авторы программы:	Невзорова Валерия Алексеевна, педагог дополнительного образования Кувшин Ирина Анатольевна, педагог дополнительного образования

Ставрополь
2025

ОГЛАВЛЕНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

В эпоху цифровых технологий, когда информация быстро и беспрепятственно распространяется по всему миру, вопрос цифровой безопасности становится особенно актуальным. Стремительное развитие интернета, а также широкое использование мобильных устройств и облачных сервисов создают новые возможности для образования и обмена знаниями. Однако с этими возможностями приходят и серьезные риски, связанные с киберугрозами в сети Интернет.

Программа необходима для формирования у участников навыков безопасного поведения в цифровом пространстве. Поддержка культуры безопасности информации в образовательных учреждениях способствует не только защите данных, но и повышению общих знаний о цифровом мире. В конечном итоге, успешная реализация программы позволит не только защитить образовательные ресурсы, но и подготовить пользователей к более безопасному и осознанному взаимодействию с технологиями.

Большая часть времени отводится освоению методов решения задач повышенного и высокого уровня сложности, применению языка программирования Python в криптографии для решения практических задач.

1. Основные характеристики программы

1.1. Направленность программы

Программа направлена на обучение и повышение осведомленности учащихся о современных киберугрозах, методах защиты данных и основах цифровой безопасности. Она включает в себя как теоретические аспекты, так и практические навыки с применением популярного языка программирования Python для противодействия кибератакам. В рамках программы изучаются основные концепции цифровой безопасности, технологии защиты информации, а также методики выявления и предотвращения потенциальных угроз в цифровой среде.

В связи с этим рассматриваются три актуальных аспекта изучения:

1) теоретический: содержание программы рассматривается как средство овладения конкретными знаниями о цифровой безопасности и умениями, необходимыми для применения в практической деятельности;

2) прикладной: содержание программы рассматривается как средство познания виртуального мира и программирования, с помощью которого осуществляется научно- технический прогресс;

3) *общеобразовательный:* содержание программы рассматривается как средство развития основных познавательных процессов, умения анализировать, выявлять сущности и отношения, описывать планы действий и делать логические выводы, опираясь на такие дисциплины, как математика и др.

1.2. Адресат программы

Программа предназначена для обучающихся 8-10 классов образовательных организаций Ставропольского края:

- проявляющих повышенный интерес к цифровой безопасности и успешно прошедших конкурсный отбор по итогам вступительного задания,
- демонстрирующих высокую мотивацию к обучению и высокие академические способности,
- желающих изучить курс программирования языка Python,
- являющихся победителями и призёрами муниципального этапа, и участниками регионального этапа Всероссийской олимпиады школьников.

1.3. Актуальность программы

В условиях современного общества, в котором цифровые технологии занимают значительное место в нашей жизни, проблемы цифровой безопасности становятся все более актуальными. Киберугрозы, такие как вирусы, фишинг, атаки «отказ в обслуживании», становятся постоянной угрозой для личных данных, финансовой информации и критической инфраструктуры. По данным различных исследований, количество кибератак постоянно увеличивается, затрагивая как личные, так и корпоративные данные. Это ставит под угрозу как безопасность отдельных пользователей, так и целых организаций.

Образовательная программа «Цифровая безопасность: противодействие киберугрозам» направлена на повышение уровня осведомленности и укрепление навыков защиты от этих угроз.

Цифровая безопасность, как учебный предмет, является мощным инструментом развития умственных и интеллектуальных способностей обучающихся, формирует у обучающихся осознанное представление об виртуальном и инновационном мире.

Педагогическая целесообразность программы обусловлена тем, что в процессе её реализации, обучающиеся овладевают теоретическими знаниями формирования безопасной культуры, ведь в современном мире необходима культурная формация, где безопасное использование технологий и осознание потенциальных угроз является нормой, умениями решать практические задачи разного уровня сложности с помощью языка программирования Python, что, в свою очередь, способствует развитию основных познавательных процессов: памяти, внимания, мышления, воображения, профессиональному самоопределению.

Программа способствует выявлению, развитию и поддержке талантливых учащихся.

1.4. Отличительные особенности/новизна программы

Программа «Цифровая безопасность: противодействие киберугрозам» имеет ряд уникальных характеристик и новизну, которые отличают ее от других инициатив в области обучения цифровой безопасности. Рассмотрим подробно

каждую из этих особенностей:

1. Мультидисциплинарный подход.

Программа объединяет знания из различных областей, включая информационные технологии, право, этику и даже психологию. Такой подход позволяет глубже понять природу киберугроз и механизмы влияния на пользователей. Например, психологические аспекты киберугроз — такие как манипуляции и фишинг — рассматриваются в контексте человеческого поведения и восприятия информации. Это делает обучение более полным и основанным на реальных сценариях.

2. Интерактивные форматы обучения, такие как:

- *Кейс-стадии*: Программа включает разбор реальных случаев киберугроз, которые произошли в различных организациях. Это помогает участникам увидеть, как лучше всего реагировать на подобные инциденты, и понять практическую значимость теоретических знаний.
- *Групповые проекты:* Учащиеся работают в группах для разработки различных стратегий защиты данных и реагирования на инциденты. Это не только укрепляет командные навыки, но и способствует более глубокому взаимодействию и обмену опытом.

3.Изучение языка программирования: освоение основных концепций языка Python, таких как переменные, условия, циклы, функции, классы и модули.

Программа регулярно обновляется с учетом новых данных о киберугрозах и изменений в законодательстве в сфере цифровой безопасности. Лекционный материал, практические упражнения и рекомендованные ресурсы основаны на последних исследованиях и тенденциях, что делает обучение более значимым и актуальным для участников.

Особую роль в реализации программы играет подготовка обучающихся к участию в олимпиадах и конкурсах разного уровня, что способствует их самореализации и повышению мотивации к самостоятельному совершенствованию, выработке ключевых компетенций в области кибербезопасности, позволяет выявить наиболее способных и высокомотивированных обучающихся к дальнейшему изучению направления на углубленном уровне.

Уровень освоения программы — углубленный.

1.5. Объем и срок освоения программы

Объем программы – 92 часа.
Срок реализации программы – 2 месяца.

1.6. Цели и задачи программы

Цель программы:

Формирование у учащихся способности к разностороннему и комплексному анализу информации, размещенной на различных интернет-ресурсах, в интересах безопасного и рационального использования интернет-пространства, привлечение к проектно-исследовательской деятельности.

Задачи программы:

1. Образовательные:

– сформировать у учащихся представление о структуре и типах информации в интернет-пространстве, больших данных и больших пользовательских данных;

– ознакомить учащихся с методами и средствами поиска информации в интернет-пространстве;

– сформировать у учащихся способность распознавать опасный и вредоносный контент и идентифицировать явления манипулирования сознанием в интернет-пространстве, внушения деструктивных идей и вовлечения в социально опасные группы в социальных сетях;

– сформировать у учащихся способность определять социальные характеристики и индивидуальные особенности людей и обнаруживать признаки опасного поведения на основании их аккаунтов в социальных сетях;

– обучить учащихся приемам противодействия негативным воздействиям в интернет-пространстве.

– освоение основных концепций языка Python, таких как переменные, условия, циклы, функции, классы и модули.

– практическое применение изученных концепций через выполнение различных задач и участие в проектах.

– разработка собственных программ и скриптов на Python для решения конкретных задач.

– изучение алгоритмов и структур данных с использованием Python.

2. Развивающие:

– сформировать у учащихся способность выявлять и критически оценивать источники и каналы распространения информации в интернет-пространстве и определять ее качество;

– сформировать у учащихся способность успешной самопрезентации и создания позитивного имиджа в социальных сетях;

– развивать познавательные способности ребенка, память, внимание, пространственное мышление, аккуратность и изобретательность;

– способствовать развитию коммуникативных навыков, психологической совместимости и адаптации в учебной группе.

– сформировать у школьников системный подход к изучению программирования.

– развивать любознательность, наблюдательность, память, пространственные представления школьников.

– развивать умение сравнивать, выявлять сходство и различие, анализировать и делать выводы.

– совершенствовать стремление школьников к познанию, расширению кругозора, информированности в рамках предметной области.

3. Воспитательные:

– сформировать у учащихся культуру позитивного использования интернет-пространства;

– привить информационную культуру: ответственное отношение к информации с учетом правовых и этических аспектов её распространения, избирательного отношения к полученной информации;

– содействовать выработке целесообразных ценностных ориентаций, потребностей и мотивов поведения школьника в сфере компьютерного обеспечения;

– формировать понятие о ценности математического образования как источника эффективных алгоритмов необходимых для обеспечения Информационного общества.

2. Организационно-педагогические условия реализации программы

2.1. Язык реализации программы

Реализация дополнительной общеобразовательной общеразвивающей программы «Цифровая безопасность: противодействие киберугрозам» осуществляется на государственном языке Российской Федерации (на русском языке).

2.2. Форма обучения: очная с применением дистанционных образовательных технологий.

2.3. Особенности реализации программы

Программа реализуется по модульному принципу с использованием дистанционных образовательных технологий.

1 модуль – дистанционный учебно-отборочный курс в течение 2-х недель;

2 модуль – очная профильная смена в течение 2-х недель;

3 модуль – дистанционный учебно-тренинговый курс в течение 3-х недель.

Основная часть содержания программы реализуется в формате очной профильной смены в течение 2-х недель.

При реализации программы используется технология крупноблочной подачи информации и погружения в предмет с последующей самостоятельной проработкой основных вопросов, обозначенных темой программы (учебно-тренинговый курс).

Программой предусмотрена система взаимосвязанных занятий, выстроенных в логической последовательности и направленных на активизацию познавательной сферы обучающихся.

Образовательная программа включает в себя лекции, практикумы по решению физических задач (ПРЗ) повышенного и высокого уровня сложности, проведение экспериментальных работ и обработку полученных экспериментальных данных в форме отчётов, выполнение контрольных и тестовых заданий.

Большая часть времени отводится на овладение методами решения различных типов задач.

Программа оснащена системой электронного тестового контроля знаний учащихся по изучаемым темам.

Система оценки знаний учащихся осуществляется по международной шкале.

Участие школьников в программе осуществляется на бюджетной основе.

2.4. Условия набора и формирования групп

Для участия в образовательной программе школьникам необходимо:

– подать заявку на официальном сайте регионального центра «Сириус 26»,

– пройти дистанционный учебно-отборочный курс;

– выполнить задание отборочного теста;

– документально подтвердить высокие достижения в интеллектуальных конкурсах и соревнованиях регионального, всероссийского и международного уровней по направлению программы (если имеются).

На обучение зачисляются учащиеся 8-10 классов образовательных организаций Ставропольского края в соответствии с рейтингом и установленной квотой:

1) подавшие заявку и успешно прошедшие конкурсный отбор;

2) по результатам участия в олимпиадах и других интеллектуальных конкурсах по физике, астрономии, математике регионального и всероссийского уровней начисляются дополнительные баллы.

Условия конкурсного отбора гарантируют соблюдение прав учащихся в области дополнительного образования и обеспечивают зачисление наиболее способных и подготовленных обучающихся к освоению программы.

Условия формирования групп: разновозрастные.

Группы формируются из обучающихся 8-10 классов.

2.5. Формы организации и проведения занятий

Формы организации занятий – аудиторные, групповые (под непосредственным руководством преподавателя) и дистанционные (самостоятельная работа при прохождении учебно-отборочного и учебно-тренингового курсов, выполнении контрольных заданий).

Формы проведения занятий: комбинированные, теоретические, практические, лабораторные, самостоятельные, контрольные.

Формы организации деятельности обучающихся: фронтальная, групповая, индивидуальная.

Режим занятий:

Очная форма обучения: по 8 уроков в день в течение 10 учебных дней. Программа реализуется в г. Михайловске.

Дистанционная форма обучения: обучающиеся проходят учебно-отборочный курс в течение 3-х недель в удобное для обучающегося время, который завершается отборочным тестированием. Учащиеся, участвующие в очной профильной смене по её завершении проходят в течение 3-х недель учебно-тренинговый курс и получают сертификат об освоении программы установленного образца.

Продолжительность академического часа – 40 минут.

Учебное занятие состоит из двух уроков.

УЧЕБНЫЙ ПЛАН

№ темы	Наименование модуля, учебного курса	Количество часов			Формы контроля
		Теория	Практика	Всего	
1.	Учебно-отборочный курс «Введение в цифровую грамотность»	2	4	6	Тестирование
2.	Учебный курс «Цифровая безопасность: противодействия киберугрозам»	16	64	80	Тестирование
3.	Учебно-тренинговый курс «Реализация дешифратора шифра Цезаря на языке python»	2	4	6	Выполнение заданий с самопроверкой
Итого:		**20**	**72**	**92**	

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Наименование модуля, учебного курса	Дата начала обучения	Дата окончания обучения	Кол-во учебных недель	Кол-во учебных дней	Кол-во учебных часов	Режим занятий
Учебно-отборочный курс «Введение в цифровую грамотность»	05.05.2025	21.05.2025	2		6 час.	Дистанционное обучение
Учебный курс «Цифровая безопасность: противодействие киберугрозам»	16.06.2025	28.06.2025	2	10	80 час.	Очное обучение, 5 раз в неделю по 8 часов
Учебно-тренинговый курс «Реализация дешифратора шифра Цезаря на языке python»	28.06.2025	20.07.2025	3		6 час.	Дистанционное обучение

РАБОЧАЯ ПРОГРАММА
УЧЕБНО-ОТБОРОЧНОГО КУРСА
«Введение в цифровую грамотность»
8-10 классы

Курс «Введение в цифровую грамотность» знакомит учащихся с методическими основами и практикой анализа информации в интернет-пространстве и демонстрирует социальную значимость аналитической работы, а также знакомит обучающихся с областью программирования на языке Python.

Основное внимание в курсе уделено решению проблемных задач, связанных с противодействием различных киберугроз. Они рассматриваются в видеофрагментах с демонстрацией методов борьбы соответствующих явлений.

Курс реализуется в дистанционной форме.

В результате освоения учебного курса обучающийся должен:

знать:

- знание структуры интернет-пространства, типы источников информации и разновидностей контента;
- владение методологией исследования информации в интернет-пространстве;
- знание признаков рискованного и опасного поведения и различных угроз в интернет-пространстве (фишинг, мошенничество, вовлечение в опасные виды деятельности) и умение идентифицировать их в социальных сетях;
- знание правил безопасного поведения в интернет-пространстве, рационального использования персональных данных, защиты от вредоносных воздействий;
- навык написания простых программ и скриптов на Python для решения базовых задач.
- подготовка к дальнейшему изучению языка программирования Python

ТЕМАТИЧЕСКИЙ ПЛАН

№ темы	Наименование темы, учебного курса	Количество часов			Формы контроля
		Теория	Практика	Всего	
1.	Киберугрозы сети Интернет.	2	1	3	Ответы на вопросы самоконтроля
2.	Введение в Python и его применение в криптографии.	1	2	3	Ответы на вопросы самоконтроля Тестирование
Итого:		**3**	**3**	**6**	

СОДЕРЖАНИЕ УЧЕБНО-ОТБОРОЧНОГО КУРСА
«Введение в цифровую грамотность»

Тема. Киберугрозы сети Интернет.

Теория: Понятие киберугроз сети Интернет и кибервойны. Деятельность кибервойск. Анализ самых громких кибератак. Оценка рисков и уязвимостей в организациях. Методы защиты от кибератак. Шифрование данных в сети Интернет.

Практика: Решение задач на объяснение методов борьбы с киберугрозами

Тема. Введение в Python и его применение в криптографии.

Теория: Что такое Python и его применение в криптографии. Ввод/вывод данных. Переменные. Типы данных. Условия. Циклы.

Практика: Списки и строки.

Основные методы и формы реализации содержания программы:

- наглядные: презентация, видео-демонстрация
- словесные: видеолекции;
- практические: решение задач.

Средства обучения: персональный компьютер с выходом в интернет; образовательная платформа «Геткурс», демонстрационные материалы; дидактические материалы для самостоятельного решения задач.

Форма подведения итогов: выполнение заданий с самопроверкой, отборочного теста.

РАБОЧАЯ ПРОГРАММА
УЧЕБНОГО КУРСА «ЦИФРОВАЯ БЕЗОПАСНОСТЬ: ПРОТИВОДЕЙСТВИЕ КИБЕРУГРОЗАМ»
8-10 классы

В рамках программы «Цифровая безопасность: противодействие киберугрозам» на углубленном уровне рассматриваются основные вопросы четырех тем:

- Поисковые системы
- Работа с информацией в сети Интернет
- Шифрование данных в сети Интернет
- Криптография на Python.

Курс знакомит обучающихся с анализом информации в интернет-пространстве, в частности. Она акцентирует внимание на медиаграмотности и шифрованию данных в сети Интернет посредством языка программирования Python.

Курс реализуется в очно в формате профильной смены.

В результате освоения учебного курса обучающийся должен:

знать:

– знание структуры интернет-пространства, типы источников информации и разновидностей контента;

– владение методологией исследования информации в интернет-пространстве;

– знание признаков рискованного и опасного поведения и различных угроз в интернет-пространстве (фишинг, мошенничество, вовлечение в опасные виды деятельности) и умение идентифицировать их в социальных сетях;

– знание правил безопасного поведения в интернет-пространстве, рационального использования персональных данных, защиты от вредоносных воздействий;

– умение свободно ориентироваться в интернет-пространстве, использовать различные типы источников для решения собственных задач;

– умение грамотно представлять в интернет-пространстве свои личные и персональные данные, формировать и поддерживать собственный позитивный имидж в социальных сетях.

– понимание основных концепций программирования на языке Python, таких как переменные, условия, циклы и функции.

– навык написания простых программ и скриптов на Python для решения базовых задач.

– умение использовать элементарные структуры данных (например, списки) и их методы в Python.

ТЕМАТИЧЕСКИЙ ПЛАН УЧЕБНОГО КУРСА

«Цифровая безопасность: противодействие киберугрозам»

№	Наименование раздела, темы	Количество часов		
		Теория	Практика	Всего
Тема 1. «Поисковые системы»		**6**	**4**	**10**
	Лекция №1 «Поисковые системы»	6		
	ПРЗ-1 «Перевод IP-адресов в двоичную систему счисления»		4	4
Тема 2. «Работа с информацией в сети Интернет»		**2**	**12**	**14**
	Лекция № 2 «Фактечинг»	2		2
	Лекция №3 Фишинг и социальная инженерия: как злоумышленники манипулируют пользователями	4		4
	ПРЗ-2 «Проверка достоверности и точности информации в сети Интернет»		8	8
Тема 3. «Шифрование данных в сети Интернет»		**6**	**18**	**24**
	Лекция № 4 «История шифрования информации»	2		2
	Лекция № 5 «Шифровальные машины»	4		4
	Лекция №6 «Безопасное поведение в интернете: пароли, двухфакторная аутентификация, конфиденциальность»	4		4
	ПРЗ-3 «Шифр Виженера»		8	8
	ПРЗ-4 «Шифр Цезаря»		6	6
Тема 4. «Криптография на Python»				**32**
	ПРЗ-5 «Основы синтаксиса Python»	4	8	12
	ПРЗ-6 «Функции и модули»	2	2	4
	ПРЗ-7 «Реализация шифра Цезаря на		8	8

	Python»			
	ПРЗ-8 «Реализация шифра Виженера на Python»		8	8
	Итого:	**14**	**66**	**80**

СОДЕРЖАНИЕ УЧЕБНОГО КУРСА «ЦИФРОВАЯ БЕЗОПАСНОСТЬ: ПРОТИВОДЕЙСТВИЕ КИБЕРУГРОЗАМ»

Тема 1. Поисковые системы

Теория. Определение поисковые системы. Основные функции поисковых систем: поиск информации и индексация. Этапы развития поисковых систем: от простых текстовых рынков до современных алгоритмов. Появление первых поисковых систем: Archie, Yahoo и Google. Типы поисковых систем. Специализированные поисковые системы (поиск на конкретных платформах, академические поисковики). Процесс сборки информации с веб-страниц (роботы, пауки). Как поисковые системы находят и индексируют новые страницы. Что такое индекс и как он работает. Методы индексирования: текстовый, метаданные, ссылки. Как работают алгоритмы поиска информации. Как выбрать и использовать ключевые слова для оптимизации. Вопросы приватности: сбор и использование данных пользователей. Проблемы манипуляций с выдачей результатов. Инструменты и ресурсы для самостоятельной работы и изучения.

Практика. Эффективное использование разных поисковых операторов для нахождения информации, оценить качество и релевантность результатов поиска, ознакомиться с принципами работы IP-адресации и освоить процесс перевода IP-адресов из десятичной системы счисления в двоичную.

Работа 1. Перевод IP-адресов в двоичную систему счисления

1. Разделение IP-адреса на четыре октета (для IPv4);
2. Основы двоичной системы: каждая цифра (бит) может быть 0 или 1;
3. Значение двоичного числа по его разрядам;
4. Перевод десятичного числа в двоичный формат.

Тема 2. Работа с информацией в сети Интернет

Теория. Что такое интернет: структура, компоненты и технологии. Статическая и динамическая информация. История развития интернета и его влияние на общество. Объектная информация: текст, изображения, видео, аудио. Источники информации: сайты, блоги, социальные сети, базы данных. Оптимизация контента для публикации в интернете и социальных сетях. Фактчекинг. Применение фактчекинга в профессиях и в жизни

пользователей сети Интернет. Фишинг и социальная инженерия: как злоумышленники манипулируют пользователями. Проблема фишинга в сети. Правила противодействия фишингу. Исследование фишинговых и коротких ссылок. Методы борьбы и противодействия фишингу в сети Интернет

Практика. Критическая оценка и проверка информации, доступной в Интернете. Навыки выявления недостоверных или манипулятивных источников информации. Освещение проблем достоверности и точности информации в интернете. Навык критического мышления. Научные статьи и исследования с помощью ресурса фактчекинг. Публикации на ресурсах по проверке фактов Snopes, FactCheck.org. Составление отчета проделанной работы с использованием рабочих инструментов наиболее полезных и современных.

Работа 2. Проверка достоверности и точности информации в сети Интернет

1. Выбор факта или утверждения для проверки;
2. Сбор информации с использованием разных поисковых систем;
3. Проведение фактчекинга;
4. Использование инструментов для фактчекинга;
5. Подготовка отчета, результаты проверки фактов, включая сведения о собранных источниках и их анализ.

Тема 3. Шифрование данных в сети Интернет

Теория. Ключевая тема в области информационной безопасности, особенно в условиях постоянных угроз кибератак и утечек данных. Тематика шифрования включает в себя понимание принципов, методов, применения и значимости шифрования для обеспечения конфиденциальности и целостности информации в сети Интернет. История шифрования информации. Различие между шифрованием, хэшированием и цифровыми подписями. Развитие методов шифрования от древности до современности. Шифровальные машины. Примеры исторических шифров (Цезарь, Виженер). Симметричное шифрование: принцип, алгоритмы (DES, AES, Blowfish). Ассиметричное шифрование: принцип, алгоритмы (RSA, ElGamal, ECC). Гибридные системы шифрования. Безопасное поведение в интернете: пароли, двухфакторная аутентификация, конфиденциальность

Практика. Методы шифрования данных с использованием симметричных шифров (например, AES или DES). Принципы работы и безопасность шифрования. Метод шифрования и расшифрования текста с использованием шифра Виженера и шифра Цезаря.

Работа 3. Шифр Виженера.

1. Подбор текста для шифрования.
2. Определить ключ.
3. Алгоритм шифрования текста, используя шифр Виженера.
4. Зашифрованный текст из части 1 и тот же ключ, написать алгоритм расшифрования.

Работа 4. Шифр Цезаря

1. Подбор текста для шифрования.
2. Определить величину сдвига букв в алфавите
3. Итоговый зашифрованный текст
4. Расшифровка текста
5. Повторение с разными сдвигами и текстами

Тема 4. Криптография на Python

Теория. Криптография — это фундаментальная область в информационной безопасности, занимающаяся методами шифрования и защиты данных. С развитием технологий и ростом угроз кибератак использование языка программирования Python стало популярным для реализации криптографических алгоритмов благодаря его простоте, гибкости и мощной библиотечной экосистеме. Обущающиеся познакомятся с основами синтаксиса языка Python: ввод и вывод данных, модули, переменные и типы данных, списки, строки и символы, ASCII и кодировка, условия и циклы.

Практика. Реализация шифров Цезаря и Виженера с использованием языка программирования Python.

Работа 5. Основы синтаксиса Python.

1. Ввод и вывод данных
2. Модули (Основы работы с модулями и импортом)
3. Переменные и типы данных
4. Списки
5. Строки и символы
6. ASCII и кодировка
7. Условия и циклы

Работа 6. Функции и модули.

1. Определение и использование собственных функций для организации кода

Работа 7. Реализация шифра Цезаря на Python.

1. Подбор текста для шифрования.
2. Выбор алфавита.
3. Задание величины сдвига.
4. Реализация алгоритма шифрования.
5. Вывод результата.
6. Протестировать программу с разными текстами и величинами сдвига

Работа 8. Реализация шифра Виженера на Python.

1. Подбор текста для шифрования.
2. Выбор алфавита.
3. Выбор ключа.
4. Подготовка ключа.
5. Реализация алгоритма шифрования
6. Вывод результата.
7. Протестировать программу с разными текстами и ключами

Основные методы реализации содержания программы:

Проблемный метод - при решении задач, выполнении экспериментальных работ.

Практический метод – при изучении теоретического материала, решении расчётных и математических задач.

Словесные и наглядные методы – при проведении лекционных занятий.

Эвристическая беседа – при проведении анализа тестов, контрольной работы, при подведении итогов выполнения экспериментальных работ.

Форма подведения итогов: контрольная работа- 1 «Проверка достоверности и точности информации в сети Интернет», контрольный тест-2 «Основы языка программирования Python», разработка программы шифра Цезаря с индивидуальными параметрами сдвига.

РАБОЧАЯ ПРОГРАММА
УЧЕБНО-ТРЕНИНГОВОГО КУРСА
«Реализация дешифратора шифра Цезаря на языке python»
8-10 классы

Курс «Реализация дешифратора шифра Цезаря на языке python» предназначен для обучающихся 8-10 классов, участников образовательной программы «Цифровая безопасность: противодействие киберугрозам».

В курсе «Реализация дешифратора шифра Цезаря на языке python» рассматривается применение языка программирования python для написания программы, способной расшифровать сообщение, закодированное с помощью шифра Цезаря.

Курс способствует закреплению алгоритмов и методов решения задач по цифровой безопасности, формированию навыков решения задач повышенного и высокого уровня сложности.

В результате освоения учебного курса обучающийся должен:

знать:
- основы языка программирования python;
- принцип шифрования методом Цезаря

уметь:
- применять алгоритмы и методы для решения задач повышенного и высокого уровня сложности.

ТЕМАТИЧЕСКИЙ ПЛАН

№ темы	Наименование модуля, учебного курса	Количество часов			Формы контроля
		Теория	Практика	Всего	
1.	Повторение основ языка программирование python		3	3	самостоятельная работа с самопроверкой
2.	Реализация программы-дешифратора шифра Цезаря на языке python		3	3	самостоятельная работа с самопроверкой
	Итого:		**6**	**6**	

СОДЕРЖАНИЕ
УЧЕБНО-ТРЕНИНГОВОГО КУРСА
«Реализация дешифратора шифра Цезаря на языке Python»
8-10 классы

Теория: Основы синтаксиса языка программирования python. Функции и модули.

Практика:

Реализация дешифратора шифра Цезаря на языке Python:

1. Разработка алгоритма для расшифровки текста, зашифрованного с использованием шифра Цезаря.

2. Написание и отладка программы на Python, которая принимает зашифрованный текст и возвращает расшифрованный вариант.

3. Решение проблем и особенностей при дешифровке текста с разными алфавитами.

Основные методы и формы реализации содержания программы: словесные (лекция), наглядные (презентация), практические.

По уровню деятельности обучающихся – объяснительно-иллюстративные (видео), репродуктивные (выполнение заданий по образцу).

Средства обучения: персональный компьютер с выходом в интернет; демонстрационные материалы; обучающие и демонстрационные файлы.

Форма подведения итогов: самостоятельная работа с самопроверкой.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Контроль и оценка результатов освоения образовательной программы «Цифровая безопасность: противодействие киберугрозам» осуществляется преподавателем в процессе проведения практических занятий: решение задач, итогового тестирования, итоговой контрольной работы.

Оценивание результативности деятельности обучающихся направлено на анализ освоения обучающимися содержания программы.

Оценка уровня усвоения содержания образовательной программы проводится по следующим показателям:

- степень усвоения содержания;
- степень применения знаний на практике;
- умение анализировать и делать выводы.

Обучающимся за время обучения в учебно-отборочном и учебно-тренинговом курсах предлагается выполнить определенный набор заданий: изучить теорию по теме, выполнить задания (тесты, вопросы самоконтроля) для проверки степени усвоения теоретического материала, рассмотреть примеры решения и оформления физических задач, решить самостоятельно несколько задач по образцу.

При самопроверке задач на всех этапах обращается внимание на следующие факторы:

1) понимание физической сущности задачи, области применимости решения;

2)рациональное использование математического аппарата, отыскание наилучшего из путей к решению;

3) получение как точного результата, так и в необходимом случае оценки;

4) умение довести решение до конца, до числа, грамотно и разумно использовать нужную систему единиц.

Использование автоматизированных средств контроля позволяет получать информацию о ходе и качестве усвоения учебного материала, а также стимулирует систематическую и целенаправленную работу обучающихся.

Освоение обучающимися содержания дополнительной общеобразовательной общеразвивающей программы «Цифровая безопасность: противодействие киберугрозам» проводится с помощью следующих форм контроля: входной, промежуточный, итоговый.

Входной контроль

Входной контроль предназначен для определения уровня подготовки обучающихся 8-10 классов по предмету информатика (стартовый контроль) в соответствии с требованиями Федерального компонента государственного стандарта среднего общего образования по информатике (базовый уровень) и основной образовательной программой среднего общего образования школы.

Цель входного контроля - выявление первоначального уровня знаний и умений, возможностей обучающихся.

Входной контроль проводится дистанционно в форме отборочного теста, который проводится после прохождения учебно-отборочного курса с

выполнением творческого задания по теме образовательной программы.

Для выполнения отборочного теста отводится 60 минут. На выполнение работы дается одна попытка. При вычислениях разрешается использовать непрограммируемый калькулятор. Дополнительные материалы и оборудование не используются. Все необходимые справочные данные приведены в тексте заданий.

Отборочный тест состоит из 30 заданий: 26 заданий с выбором одного верного ответа из предложенных, которые оцениваются в 1 балл; 4 задания с кратким ответом-оцениваются в 2 балла. В работе содержатся как задания базового уровня сложности, так и задания повышенного уровня сложности (до 30% заданий).

Работа позволяет оценить освоение обязательного минимума содержания основной образовательной программы по темам 8-10 классов.

По результатам входного контроля составляется рейтинговая таблица, которая используется для принятия решения о зачислении обучающегося на основную программу.

Оценка знаний осуществляется по 100-балльной шкале.

Наименование уровня/оценка	Результат диагностики, % (кол-во заданий)
Элементарный уровень/неудовлетворительно	0 – 49 % (0-14)
Низкий уровень/удовлетворительно	50 – 69 % (15-20)
Средний уровень/хорошо	70 – 84 % (21-25)
Высокий уровень/отлично	85 – 100 % (26-30)

Текущий контроль осуществляется на занятиях в течение всего обучения на очной профильной смене.

Формы:

- педагогическое наблюдение;
- устный фронтальный опрос.

Итоговый контроль проводится в рамках очной профильной смены с использованием компьютерных технологий.

Формы проведения: итоговое тестирование.

Итоговое тестирование проводится с использованием компьютера.

Тема «Методы борьбы с киберугрозами». Тест содержит 10 заданий с выбором ответа и с кратким ответом разного уровня сложности. Время выполнения одного теста – 40 мин.

На выполнение работы дается одна попытка. При выполнении работы можно использовать непрограммируемый калькулятор. Все необходимые справочные данные приведены в тексте заданий.

Формы фиксации результатов: составляется единая сводная рейтинговая таблица, в которую заносятся результаты по всем контрольным точкам: итоговой

тест.

Документальной формой подтверждения участия обучающегося в дополнительной общеобразовательной общеразвивающей программы и её освоения с прохождением учебно-тренингового курса является документ об обучении «Сертификат» (без оценки) установленного региональным центром «Сириус 26» образца.

Примеры контрольных заданий

Входной контроль:

Тест:

1. Выберите верные утверждение «Фишинговый (поддельный сайт) – это…»

1) Сайт, распространяющий поддельные пиратские ключи для платного программного обеспечения;

2) Сайт, созданный для распространения спама;

3) Сайт, замаскированный под внешний вид какого-либо другого сайта.

2. Какие из этих паролей являются надежными?

1) 12345678

2) L2jh3d61e%Fc

3) hellobeautifulandwonderfulworld

4) @dr9_2A#1@dc42B_4\gh

3. Какой из следующих операторов используется для сравнения значений в Python?

1) ==

2) =

3) +=

4) =!

4. Какое ключевое слово используется для определения функции в Python?

1) defination

2) def

3) func

4) lambda

Итоговый контроль:

Тест:

1. Какой метод строки используется, чтобы определить, является ли символ буквой?

1) isalpha()

2) isdigit()

3) isspace()

4) find()

2. Какое значение возвращает функция ord()?
1) Строку
2) Целочисленный код Unicode символа
3) Значение ASCII символа в виде строки
4) Длину строки

3. Каким способом вирус может попасть на Ваш компьютер?
1) По электронной почте
2) При скачивании зараженных файлов из интернета
3) Через флеш-накопители
4) При загрузке зараженного веб-сайта

4. Что относится к биометрической системе защиты?
1) Защита паролем;
2) Физическая защита данных
3) Антивирусная защита
4) Идентификация по радужной оболочке глаз

КАДРОВОЕ ОБЕСПЕЧЕНИЕ

Обеспечение реализации образовательной программы, нацеленной на предоставление высокого качества обучения, планируется за счет педагогических кадров, имеющих необходимую квалификацию для решения задач, определенных образовательной программой, способных к инновационной профессиональной деятельности. Приветствуется наличие удостоверения повышения квалификации в Образовательном центре «Сириус».

Требования к кадровым условиям включают:

- высшее педагогическое образование по предмету;
- знание предмета, владение методикой его преподавания, педагогическими технологиями;
- опыт работы по программам углубленного изучения физики;
- опыт подготовки выпускников к ОГЭ и ЕГЭ;
- опыт подготовке учащихся к олимпиадам и проектным конкурсам;
- высшая квалификационная категория, кандидат наук;
- непрерывность профессионального развития и самообразования;
- наличие навыков работы с компьютерной техникой;
- трудолюбие, открытость новшествам и освоению новых форм и методов работы;
- коммуникабельность;
- творческая активность;
- аккуратность, целеустремленность, ответственность, доброжелательность, забота о развитии индивидуальности ученика, заинтересованность в его результатах.

Для реализации дополнительной общеобразовательной общеразвивающей программы необходимы высококвалифицированные специалисты:

- педагог дополнительного образования по направлению «Кибергигиена и работа с большими данными», «Программирование на языке Python» для проведения лекционных и практических (ПРЗ) занятий – 2 чел.;
- руководитель программы – 1 чел.

ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ПРОГРАММЕ

Требования к зданию/помещению

Для реализации образовательной программы «Цифровая безопасность: противодействие киберугрозам» требуется наличие учебных кабинетов оснащенных компьютерной техникой, которые удовлетворяют строительным, санитарным и противопожарным нормам.

Учебные кабинеты укомплектованы удобными рабочими местами за ученическими столами в соответствии с возрастом обучающихся.

В целях организации антитеррористической защищённости охрана здания учреждения обеспечена системой наружного видеонаблюдения, пропускным режимом и штатными охранниками. Территория учреждения имеет периметральное ограждение и наружное освещение в тёмное время суток.

Материально-техническое обеспечение

Кабинеты:

- кабинет для теоретических занятий с необходимой ученической мебелью на 12 ученических мест, компьютеры, пластиковой доской, маркеры и

1 учительское место;

- коворкинг-зона.

Технические средства и оборудование:

- проекционное оборудование;
- белая бумага для стандартной печати формата А4;
- маркеры для пластиковой доски;
- сплитсистема.

МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

Раздел, тема	Форма занятия	Приёмы и методы организации образовательного процесса	Дидактический материал. Электронные источники	Техническое оснащение	Форма подведения итогов
Раздел Цифровая безопасность: противодействие киберугрозам.	Комбинированная	1) Информационно-рецептивный. Репродуктивный. 3) Проблемное изложение. Частично-поисковый. Дистанционный.	1) Учебно-методическое пособие «Прекрасный, опасный, кибербезопасный мир» Раздаточные материалы и презентации Сайт mathus.ru https://www.company.rt.ru/social/cyberknowledge/book_cybersecurity/files/_SMakarov_fullBook_light.pdf	1) Персональный компьютер. 2) Проекционное оборудование. 3) Доступ к сети Интернет. 4) Наличие электронной почты.	Контрольный тест

СПИСОК ЛИТЕРАТУРЫ

Список литературы, использованной при написании программы

1. Основы кибербезопасности: учебно-методическое пособие. 5—11 классы / С. Н. Вангородский. — М.: Дрофа, 2019. — 238, [1] с. — (Российский учебник).

2. Цветкова, М.С. Информационная безопасность. Кибербезопасность . 7–9 классы: учебное пособие /М.С. Цветкова, И.Ю. Хлобыстова. — 2-е изд., пересмотр. — М.: БИНОМ. Лаборатория знаний, 2020 — 64 с.: ил.

3. Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы: учеб.пособие для общеобразоват. организаций / М.С. Наместникова. – М.: Просвещение, 2019. – 79 с.: ил. – (Внеурочная деятельность).

4. Макаров С. Прекрасный, опасный, кибербезопасный мир. Все, что важно знать детям и взрослым о безопасности в интернете –М.: 2022. – 568 с.: ил.-.

5. Гэддис Т. Начинаем программировать на Python. – 4-е изд.: Пер. с англ. – СПб.: БХВ-Петербург, 2019. – 768 с.

Перечень литературы, рекомендованной обучающимся:

1.Баранова Е.К., Бабаш А.В. Основы информационной безопасности: учебник / Е.К. Баранова, А.В. Бабаш. — М.: РИОР: ИНФРА-М, 2019. — 202 с. — (Среднее про - фессиональное образование)

2. Бирюков А.А. Информационная безопасность защита и нападение.: Издательство: ДМК-Пресс., 2018, 474 с.

3. Макаров С. Прекрасный, опасный, кибербезопасный мир. Все, что важно знать детям и взрослым о безопасности в интернете –М.: 2022. – 568 с.: ил.-.

4. Гэддис Т. Начинаем программировать на Python. – 4-е изд.: Пер. с