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

«КРИПТОГРАФИЯ»

Направленность:	техническая
Возраст обучающихся:	15-16 лет
Объем программы:	90 часов
Срок освоения:	2 недели
Форма обучения:	очная с использованием дистанционных образовательных технологий
Автор программы:	Пономаренко Елена Александровна, руководитель структурного подразделения методического объединения информационных технологий ГАОУ ДО «Центр для одаренных детей «Поиск»; Лапина Мария Анатольевна, доцент кафедры вычислительной математики и кибернетики Северо-Кавказского федерального университета

Ставрополь
2025

ОГЛАВЛЕНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1. Основные характеристики программы

Программа «Криптография» характеризуется практическим подходом, балансом теоретических знаний и прикладных задач, использованием современных криптографических алгоритмов и технологий. Она направлена на формирование у слушателей не только понимания теоретических основ, но и практических навыков работы с криптографическими системами. Обучение включает в себя решение задач, работу с программным обеспечением и анализ реальных кейсов.

1.1. Направленность программы

Программа направлена на формирование у слушателей критического мышления в отношении безопасности информационных систем, способности оценивать уязвимости и разрабатывать эффективные меры защиты. Слушатели получат знания, необходимые для понимания угроз информационной безопасности и применения современных криптографических методов для противодействия им. Программа готовит специалистов, способных анализировать и решать задачи в области защиты данных.

1.2. Адресат программы

Программа адресована обучающимся от 15 до 16 лет.

Программа предназначена для одаренных школьников, проявляющих повышенный интерес к информатике, с повышенным уровнем мотивации к обучению, желающих развить навыки XXI века, получить углубленные теоретические и практические знания и навыки по актуальным в настоящее время направлениям в сфере цифровой экономики.

1.3. Актуальность программы

Актуальность программы обусловлена постоянно растущей ролью информационных технологий во всех сферах жизни и, как следствие, возрастающей необходимостью защиты информации от несанкционированного доступа, модификации и уничтожения. В условиях цифровой экономики компетенции в области криптографии становятся все более востребованными для специалистов различного профиля. Программа отвечает на современные вызовы и обеспечивает слушателей актуальными знаниями и навыками.

1.4. Отличительные особенности/новизна программы

Новизна программы заключается в интеграции новейших достижений в области постквантовой криптографии и использовании интерактивных методов обучения, позволяющих слушателям самостоятельно проверять свои знания и навыки на практических заданиях. Программа использует современное

программное обеспечение и актуальные примеры из практики, что делает обучение более эффективным и интересным. Особое внимание уделяется практическому применению знаний, а не только теоретическому освоению материала.

Уровень освоения программы – углубленное изучение основ криптографической защиты информации.

1.5. Объем и срок освоения программы

Объем программы – 90 часов.

Срок реализации программы – 2 недели.

1.6. Цели и задачи программы

Цель программы – развитие и поддержка одаренных детей Ставропольского края в сфере криптографии, их интеграция в программы государственной поддержки. Программа обеспечит школьников базовыми знаниями и навыками в области современной криптографии, фундаментальными концепциями и технологиями, необходимыми для понимания и применения криптографических методов защиты информации.

Задачи программы

1) Обучающие:

- Изучение основ современной криптографии, включая симметричные и асимметричные алгоритмы шифрования.
- Ознакомление с криптографическими протоколами и их применением в различных системах.
- Изучение методов защиты информации от различных типов угроз, таких как перехват, подмена и модификация данных.
- Обучение основам криптографического анализа и выявления уязвимостей в криптографических системах.
- Изучение современных тенденций в криптографии, включая квантовую криптографию.

2) Развивающие:

- Развитие логического и абстрактного мышления, необходимых для понимания сложных криптографических алгоритмов.
- Развитие навыков самостоятельного поиска и анализа информации в области криптографии.
- Развитие умения формулировать и решать криптографические задачи.
- Формирование способности к критическому мышлению и оценке рисков в области информационной безопасности.

- Развитие навыков работы с криптографическим программным обеспечением.

3) Воспитательные:

- Формирование ответственного отношения к защите информации и понимания важности криптографии в современном мире.
- Развитие навыков командной работы при решении криптографических задач.
- Ранняя профориентация школьников, знакомство с профессиями в области информационной безопасности и криптографии.
- Понимание роли криптографии в защите национальных интересов и культурного наследия.

1.7. Планируемые результаты освоения программы

1. Предметные результаты:

- Знание основных принципов современной криптографии, включая симметричные и асимметричные алгоритмы шифрования.
- Понимание работы криптографических протоколов и их применения в различных системах.
- Умение применять основные методы защиты информации от распространенных угроз.
- Способность к анализу простых криптографических систем и выявлению уязвимостей.
- Базовое понимание современных тенденций и направлений развития криптографии.

2. Метапредметные результаты:

- способность соотносить и оценивать результаты своей деятельности с поставленной целью;
- использование цифровых технологий в качестве инструмента достижения цели;
- понимание связи цифровых технологий с другими научными направлениями;
- осуществление саморефлексии и рефлексии деятельности группы, результатом которой будет опробование новых стратегий поведения внутри своих же ролей.

3. Личностные результаты:

- понимание и правильное оценивание своих возможностей;
- развитие навыков группового общения, умения работать в команде;
- обучение рациональному распределению времени работы;
- формирование способностей эффективно распределять роли в ходе выполнения командной работы.

2. Организационно-педагогические условия реализации программы

2.1. Язык реализации программы

Реализация дополнительной общеобразовательной общеразвивающей программы «Криптография» осуществляется на государственном языке Российской Федерации (на русском языке).

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

2.3. Особенности реализации программы

Программа реализуется по модульному принципу с использованием дистанционных образовательных технологий.

2.4. Условия набора и формирования групп

На обучение зачисляются обучающиеся 9 классов общеобразовательных школ Ставропольского края:

1) по результатам конкурсного отбора успешного прохождения учебно – отборочного курса «Криптография»;

2) по результатам участия в олимпиадах и других интеллектуальных конкурсах регионального и всероссийского уровней.

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

Состав групп: одновозрастные.

2.5. Формы организации и проведение занятий

Формы организации занятий - дистанционные, аудиторные (под непосредственным руководством преподавателя), внеаудиторные (самостоятельная подготовка обучающихся к олимпиаде за рамками учебного плана).

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

Формы организации деятельности обучающихся:

- фронтальная: работа педагога со всеми учащимися одновременно;
- групповая: организация работы в малых группах, в т.ч. в парах, для выполнения определенных задач; задание выполняется таким образом, чтобы был виден вклад каждого учащегося;
- коллективная: организация проблемно-поискового взаимодействия между всеми детьми одновременно;
- индивидуальная: организуется для коррекции пробелов в знаниях и отработки отдельных навыков.

Режим занятий. Программа реализуется в г. Ставрополе в очной форме пять раз в неделю по восемь учебных часов.

Основные методы и формы реализации содержания программы

Метод двумерной дидактики

В качестве основного метода обучения используется метод двумерной дидактики. Необходимость использования этого метода возникает в том случае, когда знаний, умений и навыков обучающихся, полученных на уроках в школе, не достаточно для освоения дополнительной программы. Метод предполагает подбор таких форм обучения, чтобы ребенок не просто решил задачу, а освоил терминологию и технологию, понял суть и смысл, оценил достоинства и недостатки предлагаемого или полученного решения, предложил другие варианты решения, и всё это осуществляется в весьма сжатые сроки. Таким образом, суть метода двумерной дидактики заключается в том, чтобы в зависимости от уровня подготовки детей, организовать результативный учебный процесс. Системное использование метода двумерной дидактики способствует усвоению сложного материала с опережением на несколько лет. Это происходит в результате спирального дублирования данных и информации, расширения поля понятий и знаний, применения в разных ситуациях и рассмотрения с разных точек зрения.

Проблемный метод

Проблемный метод включает спектр приемов, которые используются для выполнения заданий с неоднозначными вариантами разрешения противоречий в условиях недостатка или избытка информации. Основная образовательная цель проблемного метода заключается в овладении обучающимися аналитическими операциями такими, как сравнение, сообщение, выводы, за счет активной мыслительной деятельности в процессе решения разнообразных задач повышенного уровня сложности. Все задания базируются на имеющихся знаниях и умениях, однако предусматривают самостоятельный поиск новых знаний, сведений и фактов, которые потребуются для. В результате осознание недостаточности собственных знаний мотивирует ребенка на поиск новых знаний, а это одно из важнейших условий творческого госта и развития.

Следует обратить внимание на самое важное достоинство проблемного метода обучения - это овладение технологией принятия решений в условиях ситуации неопределенности и/или неоднозначности, влекущих за собой разработку различных вариантов решения проблемы, предусматривающих дефицит информации и данных, финансовые ограничения, недостатки ресурсов.

Словесные методы

Лекция с обратной связью - один из словесных методов при изложении теоретических сведений, характеризующийся тем, что при изложении материала учитель периодически задает вопросы с целью выяснения усвоения содержания. Вопросы планируются и формулируются заранее для определенных контрольных точек.

Эвристическая беседа - вопросно-ответная форма. Свое название эвристическая беседа получила от греческого «эвристика» - отыскиваю, открываю. Суть метода заключается в том, что учитель выстраивает определенный ряд вопросов, которые направляют мысли и ответы детей в нужное русло. Он базируется на интуитивных и неявных знаниях детей, полученных на основе самостоятельного опыта. Эвристическая беседа может использоваться в качестве мотивационной беседы, особенно при введении в новую тему.

Метод дизайн-мышления

Это метод создания продуктов/услуг, ориентированных на интересы пользователя. Любая идея здесь – это решение потребности человека.

Принципы дизайн-мышления:

1) Ошибайся раньше, ошибайся чаще.
2) Создай прототип вместо того, чтобы рассказать о продукте.
3) В первую очередь зафиксируй пожелания пользователя.
4) Делай продукт вместе с пользователем.

Три кита дизайн-мышления:

1) Процесс: есть алгоритм, интерактивность, смешанные команды;
2) Подход: человекоцентричность, эмпатия, культ быстрых ошибок;

Среда: осязаемый мыслительный процесс, возможность «думать руками».

УЧЕБНЫЙ ПЛАН

№ темы	Наименование модуля, учебного курса	Контактная работа обучающихся с преподавателем, часов			Формы контроля / аттестации
		Теория	Практика	Всего	
1.	Учебно-отборочный курс «Элементарная криптография»	2	2	4	Тест с самопроверкой. Разработка веб-страницы.
2.	Учебный курс «Основы современной криптографии»	20	60	80	Разработка и дизайн веб-сайта.
3.	Учебно-тренинговый курс «Инструменты криптографии»	3	3	6	Тест с самопроверкой.
Итого:		**25**	**65**	**90**	

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Наименование модуля, учебного курса	Дата начала обучения	Дата окончания обучения	Количество учебных недель	Количество учебных дней	Количество учебных часов	Режим занятий
Учебно-отборочный курс «Элементарная криптография»	06.01.2025	22.01.2025	2	14	4	Дистанционное обучение
Учебный курс «Основы современной криптографии»	10.02.2025	22.02.2025	2	10	80	Очное обучение, 5 раз в неделю по 8 часов
Учебно-тренинговый курс «Инструменты криптографии»	22.02.2025	16.03.2025	3	21	6	Дистанционное обучение

РАБОЧАЯ ПРОГРАММА УЧЕБНО-ОТБОРОЧНОГО КУРСА «ЭЛЕМЕНТАРНАЯ КРИПТОГРАФИЯ»

Курс «Элементарная криптография» предназначен для обучающихся 9 классов. Изучение основ криптографии является важным шагом для понимания принципов защиты информации в цифровом мире. Этот курс даёт базовые знания о шифровании и дешифровании информации, знакомя с историей криптографии и простыми, но эффективными методами защиты данных.

В курсе «Элементарная криптография» рассматриваются следующие вопросы: история криптографии, простые шифры подстановки и перестановки, основы теории чисел, необходимые для понимания некоторых криптографических алгоритмов (простые числа, НОД, НОК), принципы работы симметричных и асимметричных шифров (на примере простых алгоритмов), понятие хеш-функций, краткое знакомство со стеганографией.

В результате освоения учебного курса обучающийся должен:

знать:

- Основные понятия криптографии: шифрование, дешифрование, ключ.
- Примеры исторических шифров и их уязвимости.
- Принципы работы простых шифров подстановки и перестановки.
- Основные понятия теории чисел, необходимые для понимания простых криптографических алгоритмов.

уметь:

- Шифровать и дешифровать сообщения с помощью простых шифров подстановки и перестановки.
- Применять базовые знания криптографии для решения простых задач по защите информации.

Тематический план курса

№	Наименование раздела, темы	Контактная работа обучающихся с преподавателем, час.		
		Теория	Практика	Всего
1	Введение в Азбуку Морзе.	1		1
2	Решетка Кардано.		1	1
3	Шифр Цезаря.		1	1
4	Тестирование.		1	1
Итого:		**1**	**3**	**4**

СОДЕРЖАНИЕ КУРСА «ЭЛЕМЕНТАРНАЯ КРИПТОГРАФИЯ»

Тема 1. Введение в Азбуку Морзе.

Теория. Принцип кодирования: соответствие букв, цифр и знаков препинания коротким и длинным сигналам (точками и тире).

Практика. Отработка навыков перевода текста в код Морзе и обратно, сначала с помощью таблицы.

Тема 2. Решетка Кардано.

Теория. Принцип работы решетки Кардано: заполнение ячеек решетки по определенному алгоритму.

Практика. Ручное шифрование и дешифрование коротких текстов с использованием самодельной решетки Кардано (небольшого размера).

Тема 3. Шифр Цезаря.

Теория. Принцип работы шифра: сдвиг букв алфавита на определенное число позиций.

Практика. Ручное шифрование и дешифрование коротких текстов с помощью шифра Цезаря при различных значениях сдвига.

Форма подведения итогов: тестирование с самопроверкой.

РАБОЧАЯ ПРОГРАММА КУРСА «ОСНОВЫ СОВРЕМЕННОЙ КРИПТОГРАФИИ»

Курс «Основы современной криптографии» предназначен для обучающихся 9 классов.

В рамках курса школьники изучат основы современной криптографии, включая симметричные и асимметричные методы шифрования, познакомятся с различными криптографическими алгоритмами и протоколами. Они получат навыки анализа простых криптосистем и выявления уязвимостей, а также изучат основы криптографической защиты информации, включая принципы обеспечения конфиденциальности, целостности и аутентичности данных. Курс «Основы современной криптографии» включает рассмотрение следующих тем: основы теории чисел и алгебры, необходимые для понимания криптографических алгоритмов; изучение основных симметричных и асимметричных шифров; анализ хеш-функций и цифровых подписей; изучение принципов работы криптографических протоколов. В результате, школьники смогут создавать и анализировать простые криптографические системы.

В результате освоения учебного курса обучающийся должен:

знать:

- Основные принципы симметричного и асимметричного шифрования.
- Классификацию криптографических алгоритмов (например, блочные и потоковые шифры, хеш-функции, цифровые подписи).
- Основные понятия криптографической защиты информации (конфиденциальность, целостность, аутентификация, неотказуемость).
- Принципы работы криптографических протоколов (например, TLS/SSL, SSH).
- Основные типы криптографических атак и методы защиты от них.

уметь:

- Применять на практике базовые криптографические алгоритмы (например, шифрование Цезаря, шифр Вернама).
- Анализировать простые криптографические системы и выявлять их уязвимости.
- Выбирать подходящие криптографические методы для решения конкретных задач защиты информации.
- Использовать криптографические инструменты и библиотеки.
- Оценивать риски, связанные с применением криптографических методов.

ТЕМАТИЧЕСКИЙ ПЛАН

№ темы	Наименование раздела, темы	Контактная работа обучающихся с преподавателем, часов		
		Теория	Практика	Всего
1	Введение в криптографию: криптография в древнем мире.	2		2
2	История криптографии в России.	2		2
3	Простые шифры подстановки, шифр Цезаря.		4	4
4	Простые шифры перестановки, решетка Кардано.	2	4	6
5	Механические устройства для шифрования, принцип работы шифровальная машина Энигма.	2	2	4
6	Теория чисел и математические основы криптографии.	2	2	4
7	Основы теории чисел, простые числа, делимость, НОД и НОК на Python.	2		2
8	Модулярная арифметика.	2	2	4
9	Поточные шифры, генераторы псевдослучайных чисел.	2	2	4
10	Принцип работы симметричных шифров: стандарты шифрования DES и AES.	2	4	6
11	Профориентационная игра "Старт в IT"		4	4
12	Принцип работы асимметричных шифров: RSA-шифрование, электронная подпись	2	4	6
13	Хеш-функции и их применение	2	4	8
14	Стеганография: методы сокрытия информации в изображениях и текстовых файлах	2	2	4
15	Экскурсия СКФУ		4	4
16	Квантовая криптография, блокчейн	2	2	4
17	Шифровальный квест		4	4
18	Проектная работа		8	8
	Итого	**26**	**54**	**80**

СОДЕРЖАНИЕ КУРСА «ОСНОВЫ СОВРЕМЕННОЙ КРИПТОГРАФИИ»

Тема 1. Введение в криптографию: криптография в древнем мире.

Теория. Обзор исторических методов шифрования (например, шифр Цезаря в древнем Риме, скитала в Спарте). Знакомство с понятием криптографии и ее ролью в истории.

Тема 2. История криптографии в России.

Теория. Обзор исторических методов шифрования (например, шифр Цезаря в древнем Риме, скитала в Спарте). Знакомство с понятием криптографии и ее ролью в истории.

Тема 3. Простые шифры подстановки, шифр Цезаря.

Практика. Обзор исторических методов шифрования (например, шифр Цезаря в древнем Риме, скитала в Спарте). Знакомство с понятием криптографии и ее ролью в истории.

Тема 4. Простые шифры перестановки, решетка Кардано.

Теория. Принцип работы шифра перестановки, использование решетки Кардано. Анализ уязвимостей.

Практика. Шифрование и дешифрование текстов с использованием решетки Кардано.

Тема 5. Механические устройства для шифрования, принцип работы шифровальная машина Энигма.

Теория. Принцип работы машины Энигма, ее механизм и криптографическая стойкость. История использования во время Второй мировой войны.

Практика. Изучение симуляторов машины Энигма (онлайн-ресурсы) для понимания ее работы.

Тема 6. Теория чисел и математические основы криптографии.

Теория. Основные понятия теории чисел: делимость, простые числа, наибольший общий делитель (НОД), наименьшее общее кратное (НОК). Связь с криптографией.

Практика. Решение задач на НОД и НОК, ручное и с помощью программ.

Тема 7. Основы теории чисел, простые числа, делимость, НОД и НОК на Python.

Теория. Повторение основных понятий теории чисел.

Тема 8. Модулярная арифметика.

Теория. Определение модулярной арифметики, основные операции (сложение, вычитание, умножение). Связь с криптографией.

Практика. Выполнение арифметических операций в заданном модуле.

Тема 9. Поточные шифры, генераторы псевдослучайных чисел.

Теория. Принцип работы поточных шифров, генераторы псевдослучайных чисел (ГПСЧ). Критерии качества ГПСЧ.

Практика. Изучение работы простых ГПСЧ (например, линейного конгруэнтного метода).

Тема 10. Принцип работы симметричных шифров: стандарты шифрования DES и AES.

Теория. Принцип работы блочных шифров, описание DES и AES (на высоком уровне, без углубления в детали). Сравнение.

Практика. Использование готовых криптографических библиотек для шифрования/дешифрования данных с помощью DES/AES.

Тема 11. Профориентационная игра "Старт в IT".

Практика. Проведение игры.

Тема 12. Принцип работы асимметричных шифров: RSA-шифрование, электронная подпись.

Теория. Принцип работы RSA, понятие открытого и закрытого ключей. Электронная цифровая подпись.

Практика. Использование готовых библиотек для генерации ключей RSA и выполнения шифрования/дешифрования.

Тема 13. Хеш-функции и их применение.

Теория. Определение хеш-функций, их свойства (коллезия, односторонность). Примеры хеш-функций (MD5, SHA).

Практика. Вычисление хешей для различных данных с использованием готовых библиотек.

Тема 14. Стеганография: методы сокрытия информации в изображениях и текстовых файлах.

Теория. Основные методы стеганографии (в изображениях, звуке, тексте).

Практика. Использование онлайн-инструментов для сокрытия информации в изображениях (на простом уровне).

Тема 15. Экскурсия СКФУ.

Практика. Экскурсия.

Тема 16. Квантовая криптография, блокчейн.

Теория. Обзор квантовой криптографии и блокчейна, их возможности и перспективы.

Практика. Изучение видеоматериалов и статей по данной теме.

Тема 17. Шифровальный квест.

Практика. Выполнение квеста.

Тема 18. Проектная работа.

Практика. Выполнение индивидуального или группового проекта.

РАБОЧАЯ ПРОГРАММА УЧЕБНО-ТРЕНИНГОВОГО КУРСА «ИНСТРУМЕНТЫ КРИПТОГРАФИИ»

Курс «**ИНСТРУМЕНТЫ КРИПТОГРАФИИ**» предназначен для обучающихся 9 классов.

В курсе «**ИНСТРУМЕНТЫ КРИПТОГРАФИИ**» рассматриваются основные принципы работы с современными инструментами **криптографии**.

В результате освоения учебного курса обучающийся должен:

знать:

- Основные принципы симметричного и асимметричного шифрования.
- Классификацию криптографических алгоритмов (например, блочные и потоковые шифры, хеш-функции, цифровые подписи).
- Основные понятия криптографической защиты информации (конфиденциальность, целостность, аутентификация, неотказуемость).
- Принципы работы криптографических протоколов (например, TLS/SSL, SSH).
- Основные типы криптографических атак и методы защиты от них.

уметь:

- Применять на практике базовые криптографические алгоритмы (например, шифрование Цезаря, шифр Вернама).
- Анализировать простые криптографические системы и выявлять их уязвимости.
- Выбирать подходящие криптографические методы для решения конкретных задач защиты информации.
- Использовать криптографические инструменты и библиотеки.
- Оценивать риски, связанные с применением криптографических методов.

Тематический план

№ темы	Наименование раздела, темы	Контактная работа обучающихся с преподавателем, часов		
		Теория	Практика	Всего
1	Технологии распределенного реестра.	1	1	2
2	Квантовая криптография.	1	1	2
3	Цифровая подпись.	1	1	2
	Итого	3	3	6

СОДЕРЖАНИЕ КУРСА «ИНСТРУМЕНТЫ КРИПТОГРАФИИ»

Тема 1. Технологии распределенного реестра

Теория. Познакомиться с основными принципами работы технологии распределенного реестра (блокчейн технологии), изучить принципы организации криптовалюты.

Практика. Поиск хэша.

Форма подведения итогов: тестирование с самопроверкой

Тема 2. Квантовая криптография.

Теория. ознакомиться с основными принципами квантовой криптографии, изучить сформировать понимание ключевых понятий и получить представление о работе механизмов квантовой криптографии.

Практика. Решение простейших задач квантовой криптографии.
Форма подведения итогов: тестирование с самопроверкой.

Тема 3. Цифровая подпись.

Теория. познакомиться с основными принципами электронной подпись, сформировать понимание ключевых понятий и получить представление о работе механизмов цифровой подписи.

Практика. Работа в программе Kleopatra.
Форма подведения итогов: тестирование с самопроверкой.

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

№ п/п	Название раздела, темы	Формы учебного занятия	Формы, методы, приемы обучения. Педагогические технологии	Материально-техническое оснащение, дидактико-методический материал	Форма подведения итогов
1	Тема 1. Введение в криптографию.	Комбинированная	Объяснительно-иллюстративный. Частично-поисковый. Исследовательский.	Проекционное оборудование, ПК. Доступ к сети Интернет.	Тестирование
2	Тема 2. Симметричное шифрование.	Комбинированная	Объяснительно-иллюстративный. Частично-поисковый. Исследовательский.	Проекционное оборудование, ПК. Доступ к сети Интернет.	Тестирование
3	Тема 3. Ассиметричное шифрование.	Комбинированная	Объяснительно-иллюстративный. Частично-поисковый. Исследовательский.	Проекционное оборудование, ПК. Доступ к сети Интернет.	Тестирование
4	Тема 4. Криптографические протоколы.	Комбинированная	Объяснительно-иллюстративный. Частично-поисковый. Исследовательский.	Проекционное оборудование, ПК. Доступ к сети Интернет.	Тестирование

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

В процессе обучения проводятся разные виды контроля результативности усвоения программного материала.

1) Входной контроль

Входной контроль проводится целью выявления первоначального уровня знаний и умений, возможностей обучающихся. Входной контроль проводится с каждым обучающимся индивидуально по следующим параметрам – теоретическим и практическим.

Формы: тестирование и проектная деятельность.

Отборочный тест проводится в рамках дистанционного учебно-отборочного курса с целью отбора участников очной профильной смены.

1. Отборочный тест состоит из 25 заданий разного уровня сложности, направлен на проверку основных понятий, рассматриваемых тем.
2. Разработка творческого проекта с целью определения уровня умений и навыков самостоятельной работы, критического мышления и творческого подхода обучающихся на основе имеющихся знаний.

Во время проведения входной диагностики педагог заполняет информационную карточки «Результаты входной диагностики», пользуясь шкалой «Оценка параметров входного контроля».

Оценка параметров входного контроля

Наименование уровня	Результат диагностики, %
Элементарный уровень	0 - 54%
Низкий уровень	55 - 69%
Средний уровень	70 - 84%
Высокий уровень	85 - 100%

Примерные задания:

Вопрос 1. Дайте определение цифровой подписи

1. Способ шифрования данных для защиты от несанкционированного доступа.
2. Уникальный идентификатор, подтверждающий авторство электронного документа.
3. Метод сжатия данных для уменьшения их объема.
4. Технология для создания резервных копий данных.

Вопрос 2. Какой алгоритм чаще всего используется для создания цифровой подписи?

1. AES

2. RSA
3. SHA-1
4. MD5

Вопрос 3. Что обеспечивает цифровая подпись с точки зрения безопасности? (Выберите несколько вариантов)
1. Конфиденциальность данных
2. Целостность данных
3. Аутентификацию отправителя
4. Сжатие данных

Вопрос 4. Дайте определение хэш-функция в контексте цифровой подписи?
1. Алгоритм для шифрования данных
2. Функция, которая преобразует данные в уникальную строку фиксированной длины
3. Метод для создания ключей шифрования
4. Способ сжатия данных

Вопрос 5. Укажите, какой из перечисленных стандартов относится к цифровой подписи.
1. ГОСТ Р 34.10-2012
2. ISO 9001
3. IEEE 802.11
4. TCP/IP

Вопрос 6. Установите соответствие между терминами и их определениями:
Термин
1. Закрытый ключ
2. Открытый ключ
3. Сертификат
4. Хэш-функция. Определения:
A. Ключ, используемый для проверки подписи
B. Ключ, используемый для создания подписи
C. Документ, подтверждающий принадлежность ключа
D. Функция для создания уникального хэша данных

Вопрос 7. Какая организация выдает сертификаты для цифровой подписи?
1. Удостоверяющий центр (УЦ)
2. Банк
3. Интернет-провайдер
4. Государственная налоговая служба

2) *Текущий контроль* проводится в рамках очной профильной смены на занятиях в виде наблюдения за успехами каждого обучающегося, процессом формирования компетенций. Текущий контроль успеваемости служит для определения педагогических приемов и методов для индивидуального подхода к каждому обучающемуся, корректировки плана работы с группой.

Формы:

- устные и письменные работы;
- индивидуальный опрос.

Практические задания, домашние работы, учащиеся выполняют в форме устной или письменной речи. Оценка основывается на ясности выражения мыслей и использовании предметных знаний.

Текущий контроль успеваемости служит для определения педагогических приемов и методов для индивидуального подхода к каждому обучающемуся, корректировки плана работы с группой. Осуществляется в форме наблюдения, тестирования, контрольного опроса (устного или письменного), собеседования, психологического мониторинга.

Варианты примерных заданий.

Вопрос 1. Установите последовательность шагов для создания цифровой подписи:

1. Проверка подписи
2. Создание хэша документа
3. Подписание хэша закрытым ключом
4. Передача документа и подписи

Вопрос 2. Определите понятие блокчейн.

1. Централизованная база данных для хранения информации.
2. Децентрализованная распределенная база данных, состоящая из цепочки блоков.
3. Технология для шифрования данных.
4. Метод сжатия данных для уменьшения их объема.

Вопрос 3. Укажите, какой принцип лежит в основе работы блокчейна.

1. Централизованное управление данными.
2. Децентрализация и распределенное хранение данных.
3. Использование одного сервера для хранения данных.
4. Шифрование данных с помощью симметричных ключей.

Вопрос 4. Дайте определение понятия "блок" в блокчейне.

1. Единица измерения объема данных.
2. Структура, содержащая набор транзакций и ссылку на предыдущий блок.
3. Метод шифрования данных.

4. Устройство для хранения криптовалюты.

Вопрос 5. Дайте определение "майнинг" в контексте блокчейна.
1. Процесс создания новых блоков и добавления их в цепочку.
2. Метод шифрования данных.
3. Способ сжатия данных.
4. Процесс передачи данных между узлами сети.

Вопрос 6. Что является основой безопасности в квантовой криптографии?
1. Классические алгоритмы шифрования
2. Квантовая суперпозиция и запутанность
3. Вычислительная сложность
4. Использование симметричных ключей

Вопрос 7. Какой из перечисленных методов НЕ используется в квантовой криптографии?
1. Генерация случайных чисел с помощью квантовых состояний
2. Использование квантовой запутанности
3. Применение классических алгоритмов шифрования
4. Передача ключей через квантовый канал

Вопрос 8. Какая проблема решается с помощью квантовой криптографии?
1. Ускорение передачи данных
2. Защита от квантовых компьютеров
3. Обеспечение абсолютной безопасности передачи ключей
4. Увеличение пропускной способности сети

1) Промежуточная аттестация. Проводится в форме теста с самопроверкой.

2) Итоговая аттестация. Завершает второй модуль, проводится в виде создания творческого проекта.

Формы отслеживания результатов: наблюдение, тестирование, контрольный опрос (устный или письменный), психологический мониторинг.

Формы фиксации результатов: аналитическая справка, оценочные материалы, результаты психологического мониторинга, отчёт.

Документальной формой подтверждения итогов реализации отдельного курса программы является документ об обучении «Сертификат» (без оценки) установленного Центром «Поиск» образца.

КАДРОВОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

Обеспечение реализации программы, нацеленной на предоставление высокого качества обучения, планируется за счет штата, состоящего из высококвалифицированных специалистов, обладающих определенными компетенциями и выполняющими определенный функционал. Из них:

- учитель информатики высшей квалификационной категории - 2 чел.;
- педагог-психолог высшей квалификационной категории - 1 чел.;
- педагог-организатор высшей квалификационной категории - 1 чел.

МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ПРОГРАММЕ

Требования к зданию/помещению

Для реализации программы помещение должно удовлетворять строительным, санитарным и противопожарным нормам.

Учебные кабинеты укомплектованы удобными рабочими местами за ученическими столами в соответствии с ростом обучающихся, состоянием их зрения и слуха.

Кабинеты информатики оборудованы в соответствии с гигиеническими требованиями, предъявляемыми к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы с ними. Используемые цифровые образовательные ресурсы, инструменты учебной деятельности (программные средства) лицензированы для использования во всём учреждении или на необходимом количестве рабочих мест. В работе используются комплекты лицензионного или свободно распространяемого программного обеспечения.

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

Учебно-методическое и информационное обеспечение программы

Аудитории:

- аудитория для теоретических занятий с необходимой ученической мебелью, пластиковой доской;
- компьютерный класс на 12 ученических и 1 учительское место;
- коворкинг-зона.

Технические средства и оборудование:

- проекционное оборудование;
- персональные компьютеры с выходом в сеть интернет и необходимым для стандартного функционирования программным обеспечением;

- обучающие и демонстрационные файлы;
- черно-белый лазерный принтер;
- белая бумага для стандартной печати формата А4;
- маркеры для пластиковой доски;
- сплитсистема.

Лицензионное программное обеспечение:

- Операционная система Linux;
- Среда разработки Visual Studio Code;
- Офисный пакет LibreOffice.

Средства защиты:

- антибактериальные салфетки;
- антибактериальный спрей;
- огнетушитель;
- рециркулятор.

УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ

1. Перечень литературы, необходимой для освоения программы

1.1. Перечень литературы, использованной при написании программы

1) Васильева И. Н. Криптографические методы защиты информации. М.: Юрайт. 2024. 350 с.

2) Глухов М. М., Круглов И. А., Пичкур А. Б. Введение в теоретико-числовые методы криптографии. М.: Лань. 2024. 396 с.

3) Лось А. Б., Нестеренко А. Ю., Рожков М. И. Криптографические методы защиты информации для изучающих компьютерную безопасность. М.: Юрайт. 2024. 474 с.

4) Мартынов Л. М. Алгебра и теория чисел для криптографии. М.: Лань. 2024. 456 с.

5) Омассон Жан-Филипп. О криптографии всерьез. Практическое введение в современное шифрование. М.: ДМК Пресс. 2021. 328 с.

1.2. Перечень литературы, рекомендованной обучающимся

6) Романьков В. А. Введение в криптографию. Курс лекций. М.: Форум. 2023. 240 с.

7) Рубин Фрэнк. Криптография с секретным ключом. Шифры. М.: ДМК Пресс. 2022. 386 с.

1.3. Перечень литературы, рекомендованной родителям

8) Кови С. «7 навыков высокоэффективных людей. Мощные инструменты развития личности» - Альпина Паблишер, 2019

9) Ицхак Пинтусевич «Действуй! 10 заповедей успеха» изд. Эксмо 2018 г.

10) Стивен Кови «Восьмой навык. От эффективности к величию» «Альпина Паблишер», 2020 г.

2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения программы:

1. Сайт дистанционной подготовки https://olymp.itmo.ru/.

2. Сборники тренировочных тестов по информатике https://ctege.info/ege-po-informatike.

Список литературы

1. Адаменко М. В. Основы классической криптологии. Секреты шифров и кодов. М.: ДМК Пресс. 2016. 296 с.

2. Бабаш А. В., Баранова Е. К., Ларин Д. А. Информационная безопасность. История защиты информации в России. М.: КДУ. 2017. 736 с.

3. Болотов А. А., Гашков С. Б., Фролов А. Б. Элементарное введение в эллиптическую криптографию. Книга 1: Алгебраические и алгоритмические основы. М.: Ленанд. 2019. 376 с.

4. Болотов А. А., Гашков С. Б., Фролов А. Б. Элементарное введение в эллиптическую криптографию. Книга 2: Протоколы криптографии на эллиптических кривых. М.: Ленанд. 2019. 376 с.

5. Глухов М. М., Круглов И. А. Элементы теории обыкновенных представлений и характеров конечных групп с приложениями в криптографии. М.: Лань. 2015. 176 с.

6. Логачев О. А., Сальников А. А., Смышляев С. В. Булевы функции в теории кодирования и криптологии. М.: Ленанд. 2021. 576 с.

7. Музыкантский А. И., Фурин В. В. Лекции по криптографии. М.: МЦНМО. 2019. 94 с.

8. Новые правила ввоза и вывоза электроники и подобных товаров, имеющих функции шифрования (криптографии) // СПС КонсультантПлюс. 2010.

9. Панкратова И. А. Булевы функции в криптографии. М.: Лань. 2019. 92 с.