МИНИСТЕРСТВО ОБРАЗОВАНИЯ КУЗБАССА

ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
«СИРИУС. КУЗБАСС»

Принято на заседании
Педагогического совета
Протокол № 9 от 09.09.2024 г.

УТВЕРЖДАЮ
Директор ГАУДО
«Сириус. Кузбасс»
Г.Т. Васильчук

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА ТЕХНИЧЕСКОЙ НАПРАВЛЕННОСТИ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Уровень программы: базовый
Возраст обучающихся: 14-17 лет
Срок реализации: 2 недели

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00E685F7B8A09B51B064411E21A1633A02
Владелец: Васильчук Галина Талгатовна
Действителен: с 24.07.2024 до 17.10.2025

Разработчик программы:
Корнева А.В., к.т.н., доцент,
доцент кафедры прикладной
математики и информатики
ФГБОУВО «Сибирский
государственный
индустриальный университет»,
заместитель директора по УВР
ГАУДО «Сириус. Кузбасс»

Кемеровский муниципальный округ
2024 г.

Кураторы программы:
Борздун В.Н., кандидат химических наук, доцент, заместитель директора по науке ГАУДО «Сириус. Кузбасс»;
Корнева А.В., к.т.н., доцент, доцент кафедры прикладной математики и информатики ФГБОУ ВО «Сибирский государственный индустриальный университет», заместитель директора по УВР ГАУДО «Сириус. Кузбасс»;

Разработчик программы:
Корнева А.В., к.т.н., доцент, доцент кафедры прикладной математики и информатики ФГБОУ ВО «Сибирский государственный индустриальный университет», заместитель директора по УВР ГАУДО «Сириус. Кузбасс»;

Организатор:
ГАУДО «Сириус. Кузбасс»;

Эксперты: Павлова Л.Д., д.т.н., профессор, директор института «Информационных технологий и автоматизированных систем» ФГБОУ ВО «Сибирский государственный индустриальный университет».
Рыбенко И.А., д.т.н., зав. кафедрой «Прикладных информационных технологий и программирования» ФГБОУ ВО «Сибирский государственный индустриальный университет».
Соловьева Ю.А., к.т.н., доцент кафедры «Прикладных информационных технологий и программирования» ФГБОУ ВО «Сибирский государственный индустриальный университет».

Партнеры:
Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный индустриальный университет».

Перспективы применения навыков и компетенций, полученных в ходе освоения программы:
Принять участие в муниципальном и региональном этапах Всероссийской олимпиады школьников по информатике (региональный январь-февраль 2024 г), а также в олимпиадах школьников, входящих в перечень, утвержденный Министерством науки и высшего образования Российской Федерации.

Поступить в образовательные учреждения Кемеровской области на специальности, связанные с программированием и с капитализацией полученных компетенций:
Федеральное государственное бюджетное образовательное учреждение высшего образования «Кемеровский государственный университет»;
Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный индустриальный университет»;
Федеральное государственное бюджетное образовательное учреждение высшего образования «Кузбасский государственный технический университет имени Т.Ф. Горбачева».

Содержание

Раздел 1 Комплекс основных характеристик программы

1.1 Пояснительная записка

Дополнительная общеобразовательная общеразвивающая программа «Информационная безопасность» **технической направленности**. Нормативно-правовые документы для основания разработки программы:

– Федеральный закон от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации» с изм. и доп.);

– Приказ Министерства Просвещения Российской Федерации от 27 июля 2022 года № 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;

– Распоряжение правительства РФ № 678-р от 31 марта 2022 года «Об утверждении Концепции развития дополнительного образования детей до 2030 года»;

– Постановление Главного государственного санитарного врача РФ от 28 сентября 2020 года №28 «Об утверждении СанПиН 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи»;

– Приказ Министерства просвещения Российской Федерации от 03 сентября 2019 года № 467 «Об утверждении Целевой модели развития региональных систем дополнительного образования детей» (с изм. и доп.);

– Приказ Министерства труда и социальной защиты Российской Федерации 22 сентября 2021 года № 652н «Об утверждении профессионального стандарта «Педагог дополнительного образования детей и взрослых»;

– Письмо Министерства образования и науки Российской Федерации от 18 ноября 2015 года № 09-3242 «Методические рекомендации по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы)»

– Письмо Министерства просвещения Российской Федерации от 29 сентября 2023 года N АБ-3935/06 «О методических рекомендациях» (вместе с «Методическими рекомендациями по формированию механизмов обновления содержания, методов и технологий обучения в системе дополнительного образования детей, направленных на повышение качества дополнительного образования детей, в том числе включение компонентов, обеспечивающих формирование функциональной грамотности и компетентностей, связанных с эмоциональным, физическим, интеллектуальным, духовным развитием человека, значимых для вхождения

Российской Федерации в число десяти ведущих стран мира по качеству общего образования, для реализации приоритетных направлений научно-технологического и культурного развития страны»);

– Приказ Министерства образования и науки Российской Федерации от 23 августа 2017 года № 816 «Об утверждении порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;

– Распоряжение Правительства Кемеровской области-Кузбасса от 20 сентября 2022 года № 531-р «О концепции выявления, развития и поддержки способностей и талантов у детей и молодежи в Кемеровской области – Кузбассе на 2022-2025 годы и комплекса мер по ее реализации.

– Локальные акты учреждения.

Уровень освоения программы: базовый.

Актуальность программы. Роль информации в современном обществе неуклонно растет. Она становится одной из главных общественных ценностей. Информационная сфера сегодня – это совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также систему регулирования возникающих при этом отношений. Развитие информационной сферы, обеспечение ее безопасности становится одним из приоритетов национальной политики нашего государства. В «Доктрине информационной безопасности Российской Федерации» в качестве одной из основных задач указывается необходимость защиты интересов личности, общества, государства в информационной сфере. Особую актуальность этой проблеме придает реализация национального проекта «Цифровая экономика», а также федерального закона № 152-ФЗ «О персональных данных», существенно повышающим требования к организациям, которые хранят, собирают, передают или обрабатывают персональные данные с применением информационных технологий.

Решение указанных выше проблем делает актуальным изучение Информационной безопасности, что способствует повышению уровня грамотности школьника в сфере информационных технологий и присущих данной сфере деятельности угроз. Обучение базовым принципам противодействия данным угрозам способствует повышению уровня личной ответственности, организованности школьника и его заинтересованности в изучении новейших информационных технологий.

Отличительные особенности программы. Программа раскрывает общую стратегию обучения, воспитания и развития учащихся средствами учебного предмета в соответствии с целями изучения информационной безопасности, которые определены стандартом для профильного уровня. Данный курс структурируется на основе различных аспектов информационной безопасности: криптографические средства информационной безопасности, техническая защита информации, разработка защищенного программного обеспечения, обнаружение компьютерных атак.

Новизна изучаемого материала состоит в том, что обучающимся даётся представление о возможностях, которые предоставляют современные средства и методы обеспечения информационной безопасности.

Педагогическая целесообразность Педагогическая целесообразность программы состоит в том, чтобы сформировать у подрастающего поколения новые компетенции, необходимые в обществе, использующем современные информационные технологии; позволит обеспечивать динамическое развитие личности ребенка, его нравственное становление; формировать целостное восприятие мира, людей и самого себя, развивать интеллектуальные и творческие способности ребенка в оптимальном возрасте. Умение выделить систему понятий, представить их в виде совокупности атрибутов и действий, описать алгоритмы действий и схемы логического вывода (то есть то, что и происходит при информационно-логическом моделировании), улучшает ориентацию ребенка в любой предметной области и свидетельствует о его развитом логическом мышлении.

Адресат программы:

- обучающиеся 8-11 классов (14-17 лет) общеобразовательных организаций Кемеровской области с хорошими и отличными знаниями по математике/информатике, мотивированные к занятиям программированием и инженерному образованию;
- победители олимпиад математика/информатика (физика, если проявляют уклон к цифровым технологиям);
- дети из классов с углубленным изучением информатики, системы дополнительного образования (кванториумы, инженерные школы, кружки/клубы).

Практическая значимость для целевой группы: изучение аспектов информационной безопасности способствует повышению уровня грамотности школьника в сфере информационных технологий и присущих данной сфере деятельности угроз. Обучение базовым принципам противодействия данным угрозам способствует повышению уровня личной

ответственности, организованности школьника и его заинтересованности в изучении новейших информационных технологий.

Объем и срок освоения программы: общее количество учебных часов – 72, программа реализуется в течении 14 дней.

Форма обучения по программе: очная, с использованием дистанционных образовательных технологий.

Особенности организации образовательного процесса:

В ходе занятий предусмотрено использование электронно-образовательных ресурсов и Интернет-ресурсов, расширяющих возможности реализации новых способов и форм самообучения и саморазвития, а также компьютеризации контроля знаний, способствующих реализации принципа индивидуализации обучения, столь необходимого для учащихся, в том числе при подготовке к олимпиадам.

Обучающиеся формируются в группы по 12 человек. Активно используется метод интенсивного погружения.

Режим занятий, периодичность и продолжительность занятий. Занятия проводятся ежедневно в период проведения смены согласно расписанию, продолжительность одного занятия 2 часа, максимальное количество часов в день не более 8 часов.

1.2 Цели и задачи программы

Цель программы: подготовить обучающихся в области информационной безопасности, способных решать основные комплексные задачи, связанные с защитой, надежным хранением, передачей и обработкой информации, опираясь при этом на передовые достижения в области математики и информационных технологий и используя современные аппаратно-программные средства.

Задачи:

Предметные:

– сформировать у учеников общее представление о видах и областях применения методов и средств защиты информации;
– сформировать у слушателей общее представление о видах и областях применения методик информационной безопасности;
– выработать навыки использования основных категорий инструментов в области защиты информации.
– сформировать представления о разнообразии угроз информационной безопасности;

– сформировать у учеников общее представление о методах анализа простейших шифров;
– сформировать умение подбирать пути устранения угроз информационной безопасности в сети Интернет;
– обучить критической оценке сетевого контента, анализу достоверности информации, навыкам эффективной интернет-коммуникации;
– сформировать у учеников базовые навыки криптоанализа простейших шифров.

***Личностные**:*

– способствовать развитию инженерного мышления;
– формировать навыки психологической адаптации школьников к интеллектуальным соревнованиям;
– формировать чувство уверенности в своих силах;
– развивать коммуникационных компетенций, формирование стремления к получению качественного законченного результата;
– развивать навыки командной работы при сохранении понимания личной ответственности за конечный результат;
– совершенствовать умения публичной презентации проекта.

***Метапредметные**:*

– укреплять интерес к дисциплинам: черчение, математика, физика, информатика, технология и формирование понимания взаимосвязи между ними;
– обучать использованию умений и навыков различных видов познавательной деятельности, применению основных методов познания (системно-информационный анализ, моделирование и т.д.) для изучения различных сторон окружающей действительности;
– формировать умение использовать основные интеллектуальные операции: формулирование гипотез, анализ и синтез, сравнение, обобщение, систематизация, выявление причинно-следственных связей, поиск аналогов;
– продолжить развивать интерес школьников к техническому творчеству;
– формировать навыки проектной и исследовательской работы;
– обучать определению цели и задач деятельности, выбору средства реализации целей и применению их на практике.

Коммуникативные универсальные учебные действия:

– способствовать повышению уровня информированности подростков и старшеклассников об опасностях и угрозах в информационно-телекоммуникационных сетях;

– умение организовывать учебное сотрудничество и совместную деятельность с преподавателем и сверстниками;
– умение работать индивидуально и в группе: находить общее решение на основе согласования позиций;
– умение формулировать, аргументировать и отстаивать свое мнение;
– умение осознанно использовать речевые средства в соответствии с задачей коммуникации для выражения своих мыслей, планирования и регуляции своей деятельности.

1.3 Содержание программы

Учебно-тематический план

№ п/п	Название раздела, темы	Количество часов			Форма контроля
		Теория	Практика	Всего	
1	**Основные понятия информационной безопасности**	**4**	**4**	**8**	
1.1.	Значение информационной безопасности и ее место в системе национальной безопасности. Классификация информации, подлежащей защите.	2	2	4	Тестирование
1.2	Базовое законодательство в области информационных технологий и защиты информации. Стандарты в области информационной безопасности.	2	2	4	Деловая игра
2	**Угрозы информационной безопасности**	**8**	**10**	**18**	
2.1	Угрозы информационной безопасности.	2	2	4	Тестирование
2.2	Виды атак на информационную систему	2	2	4	Практическое задание
2.3	Способы и методы защиты информации	2	2	4	Квест
2.4	Модели информационной безопасности	2	4	6	Деловая игра
3	**Криптографические методы защиты информации**	**6**	**24**	**30**	
3.1	История криптографии. Основные понятия.	2	6	8	Презентация
3.2	Симметричная криптография.	2	10	12	Практическое задание
3.3	Основы криптографии с открытым ключом.	2	8	10	Деловая игра
4	**Основы проектной деятельности**	**2**	**10**	**12**	
4.1	Этапы проектной деятельности	2	4	6	Деловая игра
4.2	Разработка проекта	0	6	6	Презентация
4.3	**Итоговое занятие**	**0**	**4**	**4**	Галерея проектов
	Всего	**20**	**52**	**72**	

Содержание учебного плана

Раздел 1. Основные понятия информационной безопасности.

Тема 1.1 Значение информационной безопасности и ее место в системе национальной безопасности. Классификация информации, подлежащей защите.

Теория. Понятие и современная концепция национальной безопасности. Принципы обеспечения информационной безопасности. Общие методы обеспечения информационной безопасности. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации. Свойства информации как предмета защиты. Источник конфиденциальной информации. Сведения, которые могут быть отнесены к государственной тайне. Основные виды конфиденциальной информации, нуждающейся в защите. Коммерческая тайна. Банковская тайна. Основные объекты профессиональной тайны.

Практика. Изучение методов обеспечения информационной безопасности.

Форма контроля – оценка результатов тестирования.

Тема 1.2 Базовое законодательство в области информационных технологий и защиты информации. Стандарты в области информационной безопасности.

Теория. Обзор законодательства России как основы для обеспечения интересов личности, общества и государства в информационной сфере. Характеристика стандартов в области информационной безопасности.

Практика. Изучение стандарта COBIT.

Форма контроля – деловая игра.

Раздел 2. Угрозы информационной безопасности.

Тема 2.1 Угрозы информационной безопасности.

Теория. Современные подходы к понятию угрозы защищаемой информации. Связь угрозы защищаемой информации с уязвимостью информации. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой информации. Структура явлений как сущностного выражения угрозы защищаемой информации. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.

Практика. Решение задач и выполнение практических заданий по изученной теории.

Форма контроля – оценка результатов практического задания.

Тема 2.2 Виды атак на информационную систему.

Теория. Основные способы несанкционированного доступа к конфиденциальной информации. Методы, используемые злоумышленниками для получения доступа к конфиденциальной информации либо вывода из строя информационной системы.

Практика. Решение задач и выполнение практических заданий по изученной теории.

Форма контроля – оценка результатов практического задания.

Тема 2.3 Способы и методы защиты информации.

Теория. Способы предупреждения возможных угроз. Способы обнаружения угроз. Способы пресечения или локализации угроз. Основные способы ликвидации последствий. Основные защитные действия при реализации способов защиты информации. Защита от разглашения. Защитные действия от утечки и от несанкционированных действий (НСД) к конфиденциальной информации. Мероприятия по технической защите информации.

Практика. Получение навыков работы с типовыми средствами защиты информации.

Форма контроля – Квест по группам.

Тема 2.4 Модели информационной безопасности.

Теория. Основные структурные элементы информационной безопасности компьютерных систем. Конфиденциальность, целостность и доступность. Понятие, классификация. Риски информационной безопасности. Классификация и оценка рисков. Методы сокращения рисков.

Практика. Изучение примеров реализации моделей информационной безопасности на предприятиях. Проведение совместных обсуждений с практикующими специалистами.

Форма контроля – деловая игра.

Раздел 3. Криптографические методы защиты информации.

Тема 3.1 История криптографии. Основные понятия.

Теория. Рассматриваются основные исторические этапы криптографии. Даются основные понятия и определения, относящиеся к криптографическим системам. Дается определение стойкости алгоритма. Рассматриваются основы теории Шеннона в области информационных систем.

Практика. Подготовка проекта по истории эволюции криптографических практик.

Форма контроля – защита проект.

Тема 3.2 Симметричная криптография.

Теория. Приводится схема симметричных криптосистем, ее основные особенности. Рассматриваются типы операций, используемые в алгоритмах симметричного шифрования. Рассматривается сеть Фейштеля, которая лежит в основе многих современных алгоритмов блочного симметричного шифрования. Изучаются международные стандарты блочного шифрования.

Практика. Практическая реализация шифров замены и перестановки.

Форма контроля – оценка результатов практического задания.

Тема 3.3 Основы криптографии с открытым ключом.

Теория. Рассматриваются основные понятия, относящиеся к криптографии с открытым ключом, а также способы их использования: шифрование, обмен ключа. Рассмотрены алгоритмы RSA и Диффи-Хеллмана.

Практика. Выполнение индивидуальных и групповых заданий.

Форма контроля – деловая игра.

Раздел 4. Основы проектной деятельности.

Тема 4.1 Этапы проектной деятельности.

Понятие проекта, проектной деятельности. Проблема. Выбор темы. Цель, задачи проекта. Результаты. Выводы. Виды проектов: практико-ориентированные (прикладные) проекты, исследовательские проекты. Требования к защите проекта, критерии оценки проекта; правила успешного выступления; Методика поиска литературных и интернет-источников. Ресурсы. Календарный план. Правила оформления электронной презентации проекта.

***Практика*:** Поиск и анализ, систематизация информации по теме проекта. Составление календарного плана проекта. Определение ресурсной базы проекта.

***Форма контроля*:** Деловая игра.

Тема 4.2 Разработка проекта.

***Практика*:** Поиск и анализ информации по теме итогового проекта. Составление календарного плана проекта. Определение ресурсной базы проекта.

***Форма контроля*:** Презентация проекта.

Тема 4.3 Итоговое занятие: Подготовка проекта к итоговому мероприятию. Подготовка доклада.

***Практика*:** мини конференция по защите проектов, презентация проектов обучающихся.

***Форма контроля*:** галерея проектов.

1.4 Планируемые результаты

В результате освоения программы обучающийся должен **знать**:

– базовый понятийный аппарат в области информационной безопасности;

– виды и состав угроз информационной безопасности;

– принципы и общие методы обеспечения информационной безопасности;

– основные положения обеспечения государственной политики обеспечения информационной безопасности;

– критерии, условия и принципы отнесения информации к защищаемой; – виды носителей защищаемой информации;

– виды тайн конфиденциальной информации;

– виды уязвимостей защищаемой информации;

– источники, виды и способы дестабилизирующего воздействия на защищаемую информацию;

– каналы и методы несанкционированного доступа к конфиденциальной информации;

– классификацию видов, методов и средств защиты информации.

В результате освоения программы обучающийся должен **уметь**:

– выявлять угрозы информационной безопасности применительно к объектам защиты;

– определять состав конфиденциальной информации применительно к видам тайн;

– выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия;

– выявлять применительно к объекту защиты каналы и методы несанкционированного доступа к конфиденциальной информации;

– определять направления и виды защиты информации с учетом характера информации и задач по её защите.

В результате освоения программы обучающийся должен **владеть**:

– основными системными подходами к определению целей, задач информационно-аналитической работы и источников специальной информации.

В результате освоения программы обучающийся должен **освоить компетенции**:

- готовность осуществлять собственную профессиональную деятельность в полном соответствии с требованиями информационной безопасности;

- готовность к выбору решений из различных категорий методов и средств защиты информаций, соответствующих требованиям защиты информации в конкретных информационных системах;
- способность осуществлять оценку соответствия существующих решений требованиям защиты информации;
- готовность к разработке предложений по совершенствованию системы обеспечения информационной безопасности организации.

Личностные:

– осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;

– готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;

– освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;

– сформировать ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Метапредметные результаты. По итогам обучения обучающиеся будут знать:

– правила поведения в компьютерном классе и технику безопасности при работе с персональным компьютером;
– основы информационной безопасности в сети Интернет;
– как применять полученные навыки на практике;

По итогам обучения обучающиеся будут уметь:

– собирать, обрабатывать, анализировать и структурировать информацию;
– применять полученные знания на практике;
– самостоятельно проводить анализ, составлять план действий, моделировать варианты решения задач и решать поставленные задачи в соотношении с целями.

Раздел 2 Комплекс организационно-педагогических условий

2.1 Календарный учебный график

Количество учебных недель по программе – 2 недели.

Количество учебных дней – 14 учебных дней.

№ п/п	Форма занятия	Кол-во часов	Тема занятия	Место проведения	Форма контроля
1	Комбини-рованная	2	Значение информационной безопасности и ее место в системе национальной безопасности. Классификация информации, подлежащей защите.	Лекционная аудитория	Тестирование
		2	Базовое законодательство в области информационных технологий и защиты информации.	Лекционная аудитория	Деловая игра
Итого за день: 4 часа					
2	Комбини-рованная	2	Базовое законодательство в области информационных технологий и защиты информации.	Лекционная аудитория	Деловая игра
		2	Значение информационной безопасности и ее место в системе национальной безопасности. Классификация информации, подлежащей защите.	Лекционная аудитория	Тестирование
		2	Угрозы информационной безопасности.	Лекционная аудитория	Тестирование
Итого за день: 6 часов					
3	Комбини-рованная	2	Угрозы информационной безопасности.	Лекционная аудитория	Тестирование
		4	Виды атак на информационную систему	Лекционная аудитория	Фронтальный опрос
Итого за день: 6 часов					
4	Комбини-рованная	4	Способы и методы защиты информации	Лекционная аудитория	Квест
		2	Модели информационной безопасности	Лекционная аудитория	Фронтальный опрос
Итого за день: 6 часов					

№ п/п	Форма занятия	Кол-во часов	Тема занятия	Место проведения	Форма контроля
5	Комбини-рованная	2	Модели информационной безопасности	Лекционная аудитория	Фронтальный опрос
		2	История криптографии. Основные понятия.	Лекционная аудитория	Фронтальный опрос
Итого за день: 4 часа					
6	Комбини-рованная	2	Модели информационной безопасности	Лекционная аудитория	Фронтальный опрос
		2	История криптографии. Основные понятия.	Лекционная аудитория	Фронтальный опрос
Итого за день: 4 часа					
7	Комбини-рованная	2	История криптографии. Основные понятия.	Лекционная аудитория	Фронтальный опрос
		2	Основы криптографии с открытым ключом.	Лекционная аудитория	Фронтальный опрос
Итого за день: 2 часа					
8	Комбини-рованная	4	Симметричная криптография.	Лекционная аудитория	Фронтальный опрос
		2	История криптографии. Основные понятия.		
Итого за день: 6 часов					
9	Комбини-рованная	4	Основы криптографии с открытым ключом.	Лекционная аудитория	Фронтальный опрос
Итого за день: 4 часа					
10	Комбини-рованная	2	Основы криптографии с открытым ключом.	Лекционная аудитория	Фронтальный опрос
		4	Симметричная криптография.	Лекционная аудитория	Фронтальный опрос
Итого за день: 6 часов					
11	Комбини-рованная	4	Симметричная криптография.	Лекционная аудитория	Фронтальный опрос
		2	Основы криптографии с открытым ключом.	Лекционная аудитория	Фронтальный опрос
Итого за день: 6 часов					
12	Группо-вое задание	6	Этапы проектной деятельности	Компьютер-ный класс	Презентация
Итого за день: 6 часов					
13	Группо-вое задание	6	Разработка проекта	Компьютер-ный класс	Презентация
Итого за день: 6 часов					
14	Группо-вое задание	4	Итоговое занятие	Лекционная аудитория	Галерея проектов
Итого за день: 4 часа					

2.2 Условия реализации программы

Материально-техническое обеспечение

Для успешной реализации программы потребуется следующее оборудование, материалы, программное обеспечение и условия.

N п/п	Наименование оборудования, спортивного инвентаря	Единица измерения	Кол-во изделий
1.	Автоматизированное рабочее место ученика с доступом к сети Интернет	шт	16
2.	Демонстрационное оборудование (экран, проектор)	шт	1
3.	Смарт карты, флэшки	шт	16

Информационное обеспечение

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения.

1. Microsoft Windows/Linux.
2. Microsoft Office, Open Officce или LibreOffice.
3. Антивирус.
4. Архиватор.
5. Браузер Google Chrome.
6. Среда программирования по выбору.

Кадровое обеспечение

Программу может реализовывать педагог с высшим педагогическим образованием или техническим образованием; опытом работы по направлению не менее трех лет в области информационной безопасности и защиты информации.

2.3 Формы контроля

Форма фиксации образовательных результатов:

– приказ об утверждении состава участников программы;

– видео материалы лекционной части программы, групповой работы анализа работы, проектной защиты работ;

– перечень готовых работ;

– размещение информации на официальном сайте и паблике ГАУДО Сириус. Кузбасс»;

Формы демонстрации образовательных результатов - защита итоговой проектной работы в формате конкурса проектов.

2.4 Оценочные материалы

Промежуточный контроль осуществляется после изучения каждого раздела курса с использованием дистанционных образовательных технологий. Обучающийся в соответствии со своими образовательными потребностями и уровнем подготовленности может выбрать пороговый уровень промежуточной аттестации по каждой теме (тестирование) или повышенный уровень (решение практической задачи на материале организации).

Тест оценивается по шкале «зачтено – не зачтено» и считается успешно выполненным, если слушатель верно ответит на 60 и более процентов поставленных тестовых заданий. Для прохождения тестирования предоставляется две попытки, период прохождения тестирования – весь срок реализации программы. Взаимозависимости между прохождением промежуточной аттестации по предыдущей теме и допуском к прохождению следующей темы не устанавливается.

Практическое задание повышенной сложности оценивается преподавателем по 4-балльной шкале. Отметки 5, 4 и 3 – положительные. Отметка 2 – неудовлетворительная и означает, что практическое задание считается невыполненным. Слушатель может изменить решение о прохождении того или иного уровня промежуточной аттестации. Например, получив неудовлетворительную отметку по результатам выполнения практического задания, можно перейти к выполнению теста. Итоговая аттестация осуществляется по накопительной системе. Для прохождения итоговой аттестации слушатель должен выполнить с положительной отметкой одно задание по каждой теме и защитить итоговый проект.

2.5 Методические материалы

Особенности организации образовательного процесса: очно,_ методом интенсивного погружения.

Методы обучения:

- словесный;
- наглядный практический;
- частично-поисковый;
- исследовательский проблемный;
- проектный.

Методы воспитания: упражнение, стимулирование, мотивация.

Формы организации образовательного процесса — индивидуальная, групповая.

Формы организации учебного занятия:

- учебно-практические занятия;
- лекционные занятия;
- экспертные лекции;
- деловая игра;
- кейсовые технологии.

Педагогические технологии:

- технология группового обучения;
- технология коллективного взаимообучения;
- технология проблемного обучения;
- технология исследовательской деятельности;
- технология проектной деятельности;
- технология решения изобретательских задач.

Календарный план воспитательной работы

Разработан в соответствии с программой воспитания ГАУДО «Сириус. Кузбасс» с целью конкретизации форм, видов воспитательной деятельности и организации единого пространства воспитательной работы ГАУДО «Сириус. Кузбасс». В плане отражены основные направления воспитательной работы ГАУДО «Сириус. Кузбасс» в соответствии с Программой воспитания с учетом актуальных событий:

№ п/п	Наименование мероприятия	Срок проведения	Формат мероприятия
1.	Торжественная церемония открытия смены, поднятие флага, гимн	1 день	Торжественный концерт
2.	Инструктаж по правилам поведения, обеспечивающих безопасность жизни и здоровья детей	1 день	Беседа
3.	Профилактическая беседа с детьми в рамках Инструктажа по правилам поведения, обеспечивающих безопасность жизни и здоровья детей	1 день	Беседа
4.	Мероприятия на знакомства, сплочение и командообразование	2 день	Игровой квест «В кругу друзей»
5.	Интеллектуальная игра	Один раз в смену	КВИЗ на тему «История и символы России и Кузбасса»
6.	Встречи с представителями отраслевых направлений	2-3 раза за смену	Диалог
7.	Клубы по интересам	Каждую	Клубное занятие

		смену	
8.	Обеспечение строгого соблюдения режима дня, контроля за нахождением воспитанников на воспитательных, спортивных, культурно – массовых мероприятиях	Ежедневно	Беседа
9.	Контроль за соблюдением порядка, поведением детей в спальных помещениях в период «тихого часа», ночное время.	Ежедневно	Беседа
10.	Утренняя зарядка	Ежедневно	Физическая разминка и поддержание двигательной активности
11.	Торжественная церемония закрытия смены, награждение	Последний день	Торжественный концерт

2.6 Список литературы

Нормативно-правовые документы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г.) (с учетом поправок, внесенных Законами Российской Федерацию поправках к Конституции Российской Федерации от 30.12.2008 г. № 6- ФКЗ, от 30.12.2008 г. № 7-ФКЗ,от 05.02.2014 г. № 2-ФКЗ, от 21.07.2014 г. № 11- ФКЗ).

2. Федеральный закон «О безопасности» от 28.12.2010 г. № 390-ФЗ.

3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ (в ред. от 21.07.2011 г. № 252-ФЗ).

4. Федеральный закон «О государственной тайне» от 21.07.1993 г. № 5485-I (в ред. от 08.11.2011 г. № 309-ФЗ).

5. Федеральный закон «О коммерческой тайне» от 18.12.2006 г. №231-ФЗ.

6. Федеральный закон «О лицензировании отдельных видов деятельности» от 04.05.2011 г. № 99-ФЗ (в ред. от 28.07.2012г. №133-ФЗ). 7. Федеральный закон «О персональных данных» от 27.07.2006 г. № 149- ФЗ. 8. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации № 646от 05.12.2016 г.).

Основная литература

1. Глинская Е.В. Информационная безопасность конструкций ЭВМ и систем: учеб. пособие / Е.В. Глинская, Н.В. Чичварин. М.: ИНФРА-М, 2018. 118 с. URL: http://znanium.com/catalog.php?bookinfo=925825 (дата обращения: 27.11.2019).

2. Баранова Е.К. Информационная безопасность и защита информации: учеб. пособие / Е.К.Баранова, А.В. Бабаш. 3-е изд., перераб. и доп. М.: РИОР: ИНФРА-М, 2017. 322 с. URL:http://znanium.com/catalog.php?bookinfo=763644 (дата обращения: 25.04.2023).

3. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учеб.пособие. М.; Берлин: Директ-Медиа, 2015. 253 с. URL: http://biblioclub.ru/index.php?page=book&id=276557(дата обращения: 25.04.2023).

4. Нестеров С.А. Основы информационной безопасности: учеб. пособие. СПб.: Издательство Политехнического университета, 2014.322 с.URL: http://biblioclub.ru/index.php?page=book&id=363040 (дата обращения: 25.04.2023).

5. Информационная безопасность и защита информации: учеб. пособие для вузов / Ю.Ю. Громов и др. Старый Оскол: ТНТ, 2010. 384 с. 6. Бабаш А.В.Информационная безопасность: лабораторный практикум: учеб. пособие. 2-изд., стер. М.: КноРус, 2013. 136 с.

Дополнительная литература

1. Гришина Н.В. Информационная безопасность предприятия: учеб. пособие. 2-е изд., доп. М.: ФОРУМ: ИНФРА-М, 2017. 239 с. URL:http://znanium.com/catalog.php?bookinfo=612572 (дата обращения 25.04.2023).

2. Вдовенко Л.А. Информационная система предприятия: учеб. пособие. 2- е изд., пераб. и доп. М.: Вузовский учебник, НИЦ ИНФРА-М, 2015. 304 с. URL: http://znanium.com/catalog.php?bookinfo=501089 (дата обращения 25.04.2023).

3. Артемов А.В. Информационная безопасность: курс лекций. Open: МАБИВ, 2014. 257с. URL: http://biblioclub.ru/index.php?page=book&id=428605 (дата обращения 25.04.2023).

4. Золотарев В.В. Управление информационной безопасностью. Ч. 1. Анализ информационных рисков: учеб. пособие / В.В. Золотарев, Е.А. Данилова. Красноярск: Сиб. гос. аэрокосмич. ун-т, 2010. 144 с. URL: http://znanium.com/catalog.php?bookinfo=463037 (дата обращения 25.04.2023).

5. Жукова М.Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности: учеб. пособие / М.Н. Жукова, В.Г. Жуков, В.В. Золотарев. Красноярск: Сиб. гос. аэрокосмич. ун-т, 2012. 100 с. URL: http://znanium.com/catalog.php?bookinfo=463061 (дата обращения 25.04.2023).

6. Бабаш А.В. Информационная безопасность: лабораторный практикум: учеб. пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. М.: КНОРУС, 2019. 131 с.

7. Филин С.А. Информационная безопасность: учеб. пособие. М.: АльфаПресс, 2016. 412 с.

ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ПРОГРАММЫ

Для учебно-практических задач используются открытые данные Правительства РФ и подведомственных организаций.

1. Единая межведомственная информационно-аналитическая система (ЕМИСС) [Электронный ресурс] — URL: https://fedstat.ru/opendata

2. 3. Наборы открытых данных Росреестра[Электронный ресурс] URL: https://rosreestr.ru/wps/portal/cc ib opendata

3. Открытые данные Министерства цифрового развития, связи и массовых коммуникаций РФ [Электронный ресурс] — UR: https://digital.gov.ru/opendata/.

4. Открытые данные Сбербанка РФ [Электронный ресурс] URL: https://www.sberbank.com/ru/analy!ics/opendata

5. Открытые данные Федерального архивного агентства [Электронный ресурс] _URL: http://archives.ru/opendata

6. Портал открытых данных Министерства просвещения РФ[Электронный ресурс] — URL: https://opendata.edu.gov.ru/opendata/

7. Портал открытых данных Роспатент —Федеральная служба по интеллектуальной собственности [Электронный ресурс] — URL: https://rupto.ru/opendata

8. Портал открытых данных РФ[Электронный ресурс] URL: https://data.gov.ru

9. Правительство России [Электронный ресурс]

10. URL:http://government.ru/ministries/

11. Реестр открытых данных Кемеровской области [Электронный ресурс] — URL https://ako.ru/opendata/T

12. Федеральная служба государственной статистики: [Электронный ресурс] _URL: https://www.gks.ru

Список литературы для педагогов

1. Бирюков А.А. Информационная безопасность: защита и нападение. [Электронный ресурс]/ А.А. Бирюков. – Москва: ДМК Пресс, 2019. – 434с. - URL: https://e.lanbook.com/book/93278 (дата обращения 25.04.2023).

2. Зайцев А.П. Технические средства и методы защиты информации. [Электронный ресурс]/ А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, И.В. Голубятников. – М.: Горячая линия-Телеком, 2021. – 616с. - URL: https://e.lanbook.com/book/5154 (дата обращения 25.04.2023).

3. Новиков В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс]: учебное пособие / В.К. Новиков. - М.: Горячая линия-Телеком, 2019. – 176с. - URL: https://e.lanbook.com/book/111084 (дата обращения 25.04.2023).

4. Петров А.А. Компьютерная безопасность. Криптографические методы защиты, - Москва: ДМК, 2020. – 384 с.

5. Рацеев С.М. Математические методы защиты информации. [Электронный ресурс]: учебное пособие. Ульяновск: УлГУ, 2018. – 217с.

6. Рацеев С.М. Элементы криптографии. Ульяновск: УлГУ, 2018. – 315с.