Муниципальное образовательное учреждение
Школа с. Белоярск

Рассмотрена и одобрена научно-методическим советом МОУ Школа с. Белоярск Протокол № 1 от 30 августа 2022	УТВЕРЖДАЮ Директор МОУ Школа с. Белоярск Коростелева О.В. Приказ № 278 от «31» августа 2022 г.

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА

ТЕХНИЧЕСКОЙ НАПРАВЛЕННОСТИ

«*Кибербезопасность*»

Уровень программы: *базовый*

Срок реализации программы: *1 год (72 часа)*

Возрастная категория: от 9 до 14 лет

Форма обучения: очно

Разработчик:

Шабанов Владимир Федорович,
педагог дополнительного образования

с. Белоярск, 2022

Содержание

Раздел I. Комплекс основных характеристик программы

Пояснительная записка

1.1. Программа «Кибербезопасность» ***технической*** направленности. Программа является модифицированной версией курса «Введение в кибербезопасность». Модификация заключается в сокращении часов на изучение тем ив объединении тем.

1.2. Новизна, актуальность и педагогическая целесообразность

Новизна: программа составлена на основе курса электронного обучения компании Cisco.

Актуальность: сегодня у молодежи есть потребность удовлетворить познавательные интересы в сфере IT и определиться с выбором профессии.

Педагогическая целесообразность: учебный процесс индивидуально ориентирован и использует возможности электронного обучения. Электронное практическое обучение — это процесс обучения, построенный на принципе практического применения знаний

1.3. Отличительные особенности

При реализации программы используется электронное обучение и дистанционные технологии.

1.4. Адресат программы

Принимаются дети в возрасте 9-14 лет.
Наполняемость группы– 12-21 человек.
Предварительная подготовка не требуется.

1.5. Форма обучения и режим занятий

Форма обучения – очно-дистанционная
Общее количество часов – 72 часа.
Очные занятия проводятся 2 раза в неделю по 1учебному часу или 1 раз в неделю по 2 часа (1 час - 40 минут), перерыв между занятиями не менее 5 минут. Материалы дистанционных занятий публикуются в день проведения по расписанию или заранее.

1.6. Формы проведения контроля учащихся: зачет

Виды контроля и сроки проведения:

- **Входной контроль**: проводится при наборе, на начальном этапе формирования коллектива (в сентябре) или для учащихся, которые желают обучаться по данной программе не сначала учебного года и года обучения. Данный контроль нацелен на изучение: интересов ребенка, его знаний и умений, творческих способностей.
- **Текущий контроль**: проводится в течение учебного года, возможен на каждом занятии, по окончании изучения темы, раздела программы.
- **Промежуточный контроль**: проводится в конце I полугодия (в декабре-январе) и II полугодия (апрель-май) учебного года. Данный контроль нацелен на изучение динамики освоения предметного содержания учащимися, метапредметных результатов, личностного развития и взаимоотношений в коллективе.

Итоговый контроль: проводится в конце обучения по дополнительной общеобразовательной программе, как правило, в апреле-мае. Данный контроль нацелен на проверку освоения программы, учет изменений качеств личности каждого учащегося.

1.7. Особенности организации образовательного процесса

Состав группы постоянный.

Программа курса включает встроенные интерактивные электронные задания, стимулирующие обучение, позволяющие лучше усваивать знания и сделать весь процесс

обучения намного насыщеннее, благодаря чему учащимся будет намного легче понять содержание курса.

Среда обучения netacad.com — это важная часть общего взаимодействия между учениками и инструкторами во время обучения в Сетевой академии. Эти онлайн- материалы курса включают текст курса и относящиеся к нему интерактивные ресурсы, лабораторные работы (в бумажном виде) и разного рода тесты. Все эти материалы позволят ребенку оценить прогресс в ходе курса.

Группы формируются по возрастному принципу. Допускается зачисление детей в течение учебного года.

1.8. Уровни содержания программы, объем и сроки ее реализации

Уровень программы – ознакомительный. Она позволяет учащемуся познакомиться со средой netacad.com и изучить ступени дисциплины «Кибербезопасность», что позволяет увидеть перспективу дальнейшего обучения.

Объем программы – 72 часа.

Срок реализации программы – 1 год (36 учебных недель)

1.8. Цели и задачи дополнительной общеобразовательной общеразвивающей программы

Цель: содействие формированию представлений о кибербезопасности у подростков через реализацию электронного обучения в среде netacad.com в дистанционном режиме под руководством инструктора.

Основные задачи:

предметные

- познакомить с особенностями безопасного поведения в Интернете
- научить определять разные типы вредоносного ПО и атак
- научить составлять описание стратегий защиты, используемых организациями для борьбы с атаками

личностные

- сформировать потребность в личной безопасности при работе в интернете
- сформировать готовность использовать новые знания для своей будущей профессиональной деятельности.

метапредметные

- сформировать самостоятельность и ответственность за результат деятельности;
- сформировать умение вести самонаблюдение, самооценку, самоконтроль, навыки самообразования.

1.9. Планируемые результаты

Предметные результаты:

Учащийся научится:

- приемам безопасного поведения в интернете;
- определять разные типы вредоносного ПО и атак;
- описывать стратегии защиты, используемые организациями для борьбы с атаками

Личностные результаты:

–умение ставить цели и строить жизненные планы;

- ответственное отношение к занятиям, умение выдвигать гипотезы и находить несколько вариантов решения проблемы;
- готовность к саморазвитию и самообразованию, умение найти нужную информацию и материалы;
- умение сосредоточиться на решении поставленной задачи

Метапредметные результаты:

- потребность в личной безопасности при работе в интернете;
- - умение вести самонаблюдение, самооценку, самоконтроль, навыки самообразования

- готовность использовать новые знания для своей будущей профессиональной деятельности;
- самостоятельность, ответственность за результат деятельности.
- Формы предъявления и демонстрации образовательных результатов:
- выполненные лабораторные и практические работы.

2.0 Оценочные материалы: Оценочные материалы. Оценочные материалы, формирующие систему оценивания.

- Определение уровня освоения программы.
- 1. Высокий уровень:
- - свободное оперирование знаниями, умениями и навыками, полученными на занятиях;
- - высокая активность, быстрота включения в творческую деятельность, в коллективную работу (инициативность);
- - большая степень самостоятельности и качество выполнения творческих заданий; творческое отношение к выполнению практического задания.
-
- 2. Средний уровень:
- - хорошее оперирование знаниями, умениями и навыками, полученными на занятиях;
- - невысокая степень активности, невысокая инициативность;
- - небольшая степень самостоятельности при выполнении творческих заданий, когда ребёнок нуждается в дополнительной помощи педагога;
- - не очень высокое качество выполнения творческих заданий.
-
- 3. Достаточный уровень:
- - слабое оперирование знаниями, умениями, полученными на занятиях;
- - слабая активность включения в творческую деятельность, выполняет работу только по конкретным заданиям;
- - слабая степень самостоятельности при выполнении творческих заданий (выполнять творческие задания только с помощью педагога);
- - обучающийся проявляет интерес к деятельности, но его активность наблюдается только на определенных этапах работы.
-
-
- При устной проверке знаний оценка «5» ставится, если ученик:
- а) овладел программным материалом, ясно представляет форму предметов кибербезопасности.
- б) даёт чёткий и правильный ответ, выявляющий понимание учебного материала и характеризующий прочные знания; излагает материал в логической последовательности с использованием принятой в курсе терминологии;
- в) ошибок не делает, но допускает оговорки по невнимательности при чтении материала, которые легко исправляет по требованию учителя.
- Оценка «4» ставится, если ученик:
- а) овладел программным материалом, но материал читает с небольшими затруднениями вследствие ещё недостаточно развитого пространственного представления; знает правила и условные обозначения;
- б) даёт правильный ответ в определённой логической последовательности;
- в) при чтении материала допускает некоторую неполноту ответа и незначительные ошибки, которые исправляет с помощью учителя.
- Оценка «3» ставится, если ученик:
- а) основной программный материал знает нетвёрдо, но большинство изученных правил и обозначений усвоил;
- б) ответ даёт неполный, построенный несвязно, но выявивший общее понимание вопросов;
- в) материалы читает неуверенно, требует постоянной помощи учителя (наводящих вопросов)

и частичного применения средств наглядности.
- Оценка «2» ставится, если ученик:
- а) обнаруживает незнание или непонимание большей или наиболее важной части учебного материала;
- б) ответ строит несвязно, допускает существенные ошибки, которые не может исправить даже с помощью учителя.
- Оценка «1» ставится, если ученик обнаруживает полное незнание и непонимание учебного материала.
- При выполнении практических работ оценка «5» ставится, если ученик:
- а) самостоятельно, тщательно и своевременно выполняет практические работы и аккуратно ведёт тетрадь; материал читает свободно;
- б) при необходимости умело пользуется справочным материалом;
- в) ошибок в работе не делает, но допускает незначительные неточности и описки.
- Оценка «4» ставится, если ученик:
- а) самостоятельно, но с небольшими затруднениями выполняет работу и сравнительно аккуратно ведёт тетрадь;
- б) справочным материалом пользуется, но ориентируется в нём с трудом;
- в) при выполнении практической работы допускает незначительные ошибки, которые исправляет после замечаний учителя и устраняет самостоятельно без дополнительных объяснений.
- Оценка «3» ставится, если ученик:
- а) Работы выполняет и читает неуверенно, но основные правила оформления соблюдает; обязательные работы, предусмотренные программой, выполняет несвоевременно; тетрадь ведёт небрежно;
- б) в процессе графической деятельности допускает существенные ошибки, которые исправляет с помощью учителя.
- Оценка «2» ставится, если ученик:
- а) не выполняет обязательные практические работы, не ведёт тетрадь;
- б) читает материалы и выполняет только с помощью учителя и систематически допускает существенные ошибки.
- Оценка «1» ставится, если ученик не подготовлен к работе, совершенно не владеет умениями и навыками, предусмотренными программой.

1.10.Учебный план и его содержание

№	№ тем	№ занятия	Разделы и темы	Количество часов			Формы контроля
				Всего	Теория	Практика	
Раздел 1. Введение				**2**	**1**	**1**	тест
1	1	1-2	Введение	2	1	1	
Раздел 2. Потребность в кибербезопасности				**24**	**12**	**12**	Лабораторные работы
2	1	3-4	Потребность в кибербезопасности	2	1	1	
	2	5-6	Персональные данные	2	1	1	
	3	7-8	Идентификация онлайн и офлайн	2	1	1	
	4	9-10	Где хранятся ваши данные?	2	1	1	
	5	11-12	Вычислительные устройства	2	1	1	
	6	13-14	Они хотят ваши деньги	2	1	1	

	7	15-16	Они хотят ваши идентификационные данные	2	1	1	
	8	17-18	Корпоративные данные	2	1	1	
	9	19-20	Конфиденциальность,целостность и доступность данных	2	1	1	
	10	21-22	Последствия нарушения безопасности	2	1	1	
	11	23-24	Примеры нарушения безопасности	2	1	1	
	12	25-26	Лабораторная работа. Что пропало?	2	1	1	
Раздел 3. Атаки, понятия и техники				**16**	**8**	**8**	Лабораторные работы
3	1	27-28	Типы злоумышленников	2	1	1	
	2	29-30	Внутренние и внешние угрозы	2	1	1	
	3	31-32	Злоумышленники и эксперты по кибербезопасности	2	1	1	
	4	33-34	Юридические проблемы кибербезопасности	2	1	1	
	5	35-36	Этические проблемы кибербезопасности	2	1	1	
	6	37-38	Практическая работа: "Какого цвета хакер?"	2	1	1	
	7	39-40	Что такое кибервойна?	2	1	1	
	8	41-42	Понятие кибервойны.	2	1	1	

			Цель кибервойны				
Раздел 4. Защита данных и конфиденциальности				**20**	**10**	**10**	Лабораторные Практические работы
4	1	43-44	Поиск уязвимостей в системе безопасности	2	1	1	
	2	45-46	Категоризация уязвимостей в системе безопасности	2	1	1	
	3	47-48	Практическая работа: Определение термина уязвимость.	2	1	1	
	4	49-50	Типы вредоносного ПО	2	1	1	
	5	51-52	Симптомы заражения вредоносным ПО	2	1	1	
	6	53-54	Практическое занятие: Определение типов вредоносного ПО	2	1	1	
	7	55-56	Социальная инженерия	2	1	1	
	8	57-58	Взлом пароля Фишинг	2	1	1	
	9	59-60	Использование уязвимостей	2	1	1	
	10	61-62	DoS атака DDoS Отравление SEO	2	1	1	
Раздел 5. Защита организации				**8**	**4**	**4**	Практические работы
5	1	63-64	Защита вычислительных устройств	2	1	1	
	2	65-66	Шифрование данных	2	1	1	
	3	67-68	Типы межсетевых экранов	2	1	1	
	4	69-70	Устройства безопасности Обнаружение атак в реальном времени	2	1	1	
Раздел 6. Свяжете ли вы свое будущее с кибербезопасностью?				**2**	**1**	**1**	Итоговый тест
6	1	71-72	Свяжете ли вы свое будущее с кибербезопасностью?	2	1	1	
			ИТОГО:	**72**	**36**	**36**	

Содержание учебного плана

Раздел 1.Введение - 2 часа

Теория: знакомство с интерфейсом электронного модуля и особенностями работы в нем.

Практика: упражнения на поиск информации в системе

Раздел 2.Потребность в кибербезопасности - 24 часа

Теория: понятие «кибербезопасность», «учетная запись», признаки киберпреступников, этические нормы для специалистов по кибербезопасности, кибервойны

Практика: лабораторные работы на сравнение данных и поиск пропавшей информации.

Раздел 3.Атаки, понятия и техники - 16 часов

Теория: способы анализа последствий кибератаки. Категории уязвимости в системе безопасности. Типы вредоносного ПО и его симптомы. Смешанные атаки и их последствия.
Практика: определение типов вредоносного ПО.
Раздел 4.Защита данных и конфиденциальности - 20 часов
Теория: персональные устройства и персональные данные, защита устройств, создание надежных паролей и безопасное пользование беспроводными сетями. Техники аутентификации.
Практика: лабораторные и практические занятия по созданию надежных паролей и копированию резервных данных.
Раздел 5. Защита организации - 8 часов
Теория: технологии и процессы, используемые экспертами по кибербезопасности для защиты сети, оборудования и данных организации. Типы межсетевых экранов, устройствобеспечения безопасности и программного обеспечения. Ботнеты, убийственная цепочка (kill chain), использование NetFlow для мониторинга сети. Подход Cisco к кибербезопасности. Инструменты для обнаружения и предотвращения сетевых атак.
Практика: Лабораторные и практические занятия по определению типа межсетевых экранов, сканированию порта.
Раздел 6.Свяжете ли вы свое будущее с кибербезопасностью? - 2часа
Теория: обзор учебных курсов, которые можно пройти в Сетевой академии Cisco (NetAcad)
Практика: Итоговое тестирование

Раздел 2. Комплекс организационно-педагогических условий, включающих формы аттестации

2.1. Календарный учебный график программы

Раздел 2. Комплекс организационно-педагогических условий, включающих формы аттестации

2.1. Календарный учебный график программы

Название группы_____, дни недели_____, время _____, место проведения_____.

№ занятия	Разделы и темы	Количество часов	Форма занятия	Формы контроля	Дата проведения	
					План	Факт
	Раздел 1. Введение					
1-2	Введение	2				
	Раздел 2. Потребность в кибербезопасности					
3-4	Потребность в кибербезопасности	2				
5-6	Персональные данные	2				
7-8	Идентификация онлайн и офлайн	2				
9-10	Где хранятся ваши данные?	2				

11-12	Вычислительные устройства	2				
13-14	Они хотят ваши деньги	2				
15-16	Они хотят ваши идентификационные данные	2				
17-18	Корпоративные данные	2				
19-20	Конфиденциальность, целостность и доступность данных	2				
21-22	Последствия нарушения безопасности	2				
23-24	Примеры нарушения безопасности	2				
25-26	Лабораторная работа. Что пропало?	2				

	Раздел 3. Атаки, понятия и техники					
27-28	Типы злоумышленников	2				
29-30	Внутренние и внешние угрозы	2				
31-32	Злоумышленники и эксперты по кибербезопасности	2				
33-34	Юридические проблемы кибербезопасности	2				
35-36	Этические проблемы кибербезопасности	2				
37-38	Практическая работа: "Какого цвета хакер?"	2				
39-40	Что такое кибервойна?	2				
41-42	Понятие кибервойны. Цель кибервойны	2				
	Раздел 4. Защита данных и конфиденциальности					

43-44	Поиск уязвимостей в системе безопасности	2				
45-46	Категоризация уязвимостей в системе безопасности	2				
47-48	Практическая работа: Определение термина уязвимость.	2				
49-50	Типы вредоносного ПО	2				
51-52	Симптомы заражения вредоносным ПО	2				
53-54	Практическое занятие: Определение типов вредоносного ПО	2				
55-56	Социальная инженерия	2				
57-58	Взлом пароля Фишинг	2				
59-60	Использование уязвимостей	2				

61-62	DoS атака DDoS Отравление SEO	2				
	Раздел 5. Защита организации					
63-64	Защита вычислительных устройств	2				
65-66	Шифрование данных	2				
67-68	Типы межсетевых экранов	2				
69-70	Устройства безопасности Обнаружение атак в реальном времени	2				
	Раздел 6. Свяжете ли вы свое будущее с кибербезопасностью?					
71-72	Свяжете ли вы свое будущее с кибербезопасностью?	2				

Название группы_____, дни недели , время _____, место проведения_____.

№ занятия	Разделы и темы	Количество часов	Форма занятия	Формы контроля	Дата проведения	
					План	Факт
	Раздел 1. Введение					
1-2	Введение	2				
	Раздел 2. Потребность в кибербезопасности					
3-4	Потребность в кибербезопасности	2				
5-6	Персональные данные	2				
7-8	Идентификация онлайн и офлайн	2				
9-10	Где хранятся ваши данные?	2				
11-12	Вычислительные устройства	2				
13-14	Они хотят ваши деньги	2				
15-16	Они хотят ваши идентификационные данные	2				
17-18	Корпоративные данные	2				
19-20	Конфиденциальность, целостность и доступность	2				

	данных					
21-22	Последствия нарушения безопасности	2				
23-24	Примеры нарушения безопасности	2				
25-26	Лабораторная работа. Что пропало?	2				
	Раздел 3. Атаки, понятия и техники					
27-28	Типы злоумышленников	2				
29-30	Внутренние и внешние угрозы	2				
31-32	Злоумышленники и эксперты по кибербезопасности	2				
33-34	Юридические проблемы кибербезопасности	2				
35-36	Этические проблемы кибербезопасности	2				
37-38	Практическая работа: "Какого цвета хакер?"	2				
39-40	Что такое кибервойна?	2				
41-42	Понятие кибервойны. Цель кибервойны	2				
	Раздел 4. Защита данных и конфиденциальности					
43-44	Поиск уязвимостей в системе безопасности	2				
45-46	Категоризация уязвимостей в системе безопасности	2				
47-48	Практическая работа: Определение термина уязвимость.	2				

49-50	Типы вредоносного ПО	2				
51-52	Симптомы заражения вредоносным ПО	2				
53-54	Практическое занятие: Определение типов вредоносного ПО	2				
55-56	Социальная инжененрия	2				
57-58	Взлом пароля Фишинг	2				
59-60	Использование уязвимостей	2				
61-62	DoS атака DDoS Отравление SEO	2				
	Раздел 5. Защита организации					
63-64	Защита вычислительных устройств	2				
65-66	Шифрование данных	2				
67-68	Типы межсетевых экранов	2				
69-70	Устройства безопасности Обнаружение атак в реальном времени	2				
	Раздел 6. Свяжете ли вы свое будущее с кибербезопасностью?					
71-72	Свяжете ли вы свое будущее с кибербезопасностью?	2				

Название группы_____, дни недели _____время _____, место проведения_____.

№ занятия	Разделы и темы	Количество часов	Форма занятия	Формы контроля	Дата проведения	
					План	Факт
	Раздел 1. Введение					
1-2	Введение	2				
	Раздел 2. Потребность в кибербезопасности					
3-4	Потребность в кибербезопасности	2				
5-6	Персональные данные	2				
7-8	Идентификация онлайн и офлайн	2				
9-10	Где хранятся ваши данные?	2				
11-12	Вычислительные устройства	2				
13-14	Они хотят ваши деньги	2				
15-16	Они хотят ваши идентификационные данные	2				
17-18	Корпоративные данные	2				

19-20	Конфиденциальность, целостность и доступность данных	2				
21-22	Последствия нарушения безопасности	2				
23-24	Примеры нарушения безопасности	2				
25-26	Лабораторная работа. Что пропало?	2				
	Раздел 3. Атаки, понятия и техники					
27-28	Типы злоумышленников	2				
29-30	Внутренние и внешние угрозы	2				
31-32	Злоумышленники и эксперты по кибербезопасности	2				
33-34	Юридические проблемы кибербезопасности	2				
35-36	Этические проблемы кибербезопасности	2				
37-38	Практическая работа: "Какого цвета хакер?"	2				
39-40	Что такое кибервойна?	2				
41-42	Понятие кибервойны. Цель кибервойны	2				
	Раздел 4. Защита данных и конфиденциальности					
43-44	Поиск уязвимостей в системе безопасности	2				
45-46	Категоризация уязвимостей в системе безопасности	2				

47-48	Практическая работа: Определение термина уязвимость.	2				
49-50	Типы вредоносного ПО	2				
51-52	Симптомы заражения вредоносным ПО	2				
53-54	Практическое занятие: Определение типов вредоносного ПО	2				
55-56	Социальная инженеерия	2				
57-58	Взлом пароля Фишинг	2				
59-60	Использование уязвимостей	2				
61-62	DoS атака DDoS Отравление SEO	2				
	Раздел 5. Защита организации					
63-64	Защита вычислительных устройств	2				
65-66	Шифрование данных	2				
67-68	Типы межсетевых экранов	2				
69-70	Устройства безопасности Обнаружение атак в реальном времени	2				
	Раздел 6. Свяжете ли вы свое будущее с кибербезопасностью?					
71-72	Свяжете ли вы свое будущее с кибербезопасностью?	2				

2. 2. Условия реализации программы

Материально-техническое обеспечение:

Оборудование:

- Компьютер или ноутбук
- Программное обеспечение:

1. Операционная система Windows, MacOS

2.3. Формы аттестации

Вид аттестации	Форма аттестации	Фиксация результатов	Механизм оценивания	Сроки
Вводный контроль	Тест	кан результата тестирования	не менее 20%	1-2 занятия
Текущий контроль	Лабораторные и практические работы Ответы на контрольные вопросы	Скан материалов	Наличие (зачет)	Ежеурочно
межуточный контроль	Тест	Материал тестирования	Не менее 40%	35-36 занятия
Итоговый контроль	Тест	Аналитическая справка Скан материалов	Не менее 60%	71-72 занятия

2.4. Формы предьявления и демонстрации образовательных результатов:
выполненные лабораторные и практические работы.

2.6. Методические материалы

Методы обучения: текстовые, мультимедийные, симуляции

Технологии:

При организации занятий используется обучение при помощи информационных и электронных технологий.

Формы организации учебного занятия:

Дистанционное занятие

Дидактические материалы:

Формы	*Методическая продукция и материалы*
ЦОР	Тренажеры, мультимедийные ролики

Список литературы

1. Белова, С.Н., Ильина, И.В., Шамова, Т.И. Современные средства оценивания результатов обучения в школе / С.Н. Белова, И.В. Ильина, Т.И. Шамова. – М.: Педагогическое общество России, 2007. – 192 с.
2. Воспитательный процесс: изучение эффективности / Под ред. Е.Н. Степанова. – М.: ТЦ «Сфера», 2000. – 128 с.
3. Журкина, А.Я. Мониторинг качества образовательной деятельности в учреждении дополнительного образования детей // Приложение к журналу «Внешкольник», Выпуск №11. – М.: ГОУДОД ФЦРСДОД, 2005. – 72 с.
4. Золотарёва, А.В. Мониторинг результатов деятельности учреждения дополнительного образования детей: монография / А.В. Золотарёва. – Ярославль: ЯГПУ им. К.Д. Ушинского, 2005. – 200 с.
5. Попова, Г.П., Размерова, Г.А., Ремчукова, И.Б. Мониторинг качества учебного процесса: Принципы, Анализ Планирование / Г.П. Попова, Г.А. Размерова, И.Б. Ремчукова. – Ростов н/Д.: Учитель, 2007. – 124 с.
6. Талых, А. Предмет мониторинга – качество образования // Директор школы. – 1999. – №3. – С. 13 – 17.

Нормативно-правовые источники

1. Федеральный закон Российской Федерации от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (далее – ФЗ № 273).
2. Концепция развития дополнительного образования детей, утвержденная распоряжением Правительства Российской Федерации от 4 сентября 2014 г. № 1726-р (далее – Концепция).
3. Стратегия развития воспитания в Российской Федерации до 2025 года, утвержденная распоряжением Правительства РФ от 29.05.2015 г. № 996-р.
4 Приоритетный проект «Доступное дополнительное образование для детей», утвержденный 30 ноября 2016 г. протоколом заседания президиума при Президенте РФ.
5 Федеральный проект «Успех каждого ребенка», утвержденный 07 декабря 2018 г.
6 Приказ Министерства просвещения РФ от 09 ноября 2018 г. № «Об утверждении Порядка организации образовательной деятельности по дополнительным общеобразовательным программам».
7 Приказ Министерства просвещения РФ от 15 апреля 2019 г. № 170 «Об утверждении методики расчета показателя национального проекта«Образование» «Доля детей в возрасте от 5 до 18 лет, охваченных дополнительным образованием».
образовательных программ» (далее – Приказ № 2)
8. Постановление Главного государственного санитарного врача Российской Федерации от 4 июля 2014 г. № 41 «Об утверждении СанПиН 2.4.4.3172-14 «Санитарно-эпидемиологические требования к устройству, содержанию и организации режима работы образовательных организаций дополнительного образования детей».
9. Приказ Минтруда России от 05 мая 2018 г. № 298н «Об утверждении профессионального стандарта «Педагог дополнительного образования детей и взрослых» (зарегистрирован Минюстом России 28 августа 2018 г., регистрационный № 25016).
10. Письмо Минобрнауки РФ «О направлении методических рекомендаций по организации независимой оценки качества дополнительного образования детей» № ВК-1232/09 от 28 апреля 2017 г.
11. Методические рекомендации по проектированию дополнительных общеобразовательных общеразвивающих программ от 18.11.2015 г. Министерство образования и науки РФ.
12. Краевые методические рекомендации по проектированию дополнительных общеобразовательных общеразвивающих программ 2020 г.