

ИНДИВИДУАЛЬНЫЙ ПРЕДПРИНИМАТЕЛЬ
АЛИБАЕВА МАРИЯ НИКОЛАЕВНА

ИНН: 027303678489, ОГРНИП: 324028000172392

Юридический адрес: 450105, республика Башкортостан, г. Уфа, ул. Юрия Гагарина, д. 35, кв. 25

«УТВЕРЖДАЮ»

Индивидуальный предприниматель
Алибаева М.Н.

Приказ № 01-П от 28.09.2026 г.

ДОПОЛНИТЕЛЬНАЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

ДОПОЛНИТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА

«ЦИФРОВАЯ ГРАМОТНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ»

Адресат программы: от 18 лет

Срок реализации: 2 недели

Объем программы (трудоемкость): 24,00 академических часа

Форма обучения: заочная (с применением исключительно электронного обучения и дистанционных образовательных технологий)

Направленность: техническая направленность

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дополнительная общеобразовательная программа – дополнительная общеразвивающая программа «Цифровая грамотность и защита информации» (далее – Программа) составлена в соответствии с:

- Федеральным законом Российской Федерации от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Приказом Минпросвещения РФ от 27.07.2022 № 629 "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам";
- Постановлением Правительства РФ от 11.10.2023 № 1678 "Об утверждении Правил применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ" (далее – Постановление № 1678);
- Методические рекомендации Минобрнауки России по проектированию дополнительных общеразвивающих программ (включая разноуровневые программы) от 18.11.2015 г. № 09-3242.

Направленность Программы: техническая направленность.

Уровень освоения – стартовый (ознакомительный).

Актуальность Программы

В условиях цифровой трансформации общества и активного внедрения информационно-коммуникационных технологий во все сферы жизнедеятельности возрастает необходимость формирования у граждан устойчивых компетенций в области безопасного использования цифровых ресурсов. Расширение спектра электронных услуг, дистанционных форм взаимодействия и цифровых сервисов обуславливает потребность в повышении уровня цифровой грамотности населения и развитии навыков безопасной работы с информацией.

Одновременно с развитием цифровой среды увеличивается количество и сложность угроз информационной безопасности, включая интернет-мошенничество, фишинговые атаки, распространение вредоносного программного обеспечения и утечки персональных данных. Значительная часть инцидентов связана с недостаточным уровнем подготовки пользователей и несоблюдением ими базовых требований информационной безопасности. В соответствии с положениями Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации» обеспечение защиты информации и формирование безопасного информационного пространства являются важнейшими задачами государственной политики.

Реализация программы «Основы информационной безопасности и цифровой грамотности» направлена на формирование у слушателей комплекса знаний, умений и навыков, обеспечивающих безопасное и ответственное использование цифровых технологий. Программа соответствует приоритетным направлениям государственной политики в области цифрового развития, способствует повышению уровня защищённости граждан в информационной среде и имеет значимую социальную направленность.

Адресат Программы – программа предназначена для людей с возрастной категории от 18 лет без предъявления требований к уровню образования.

Объем Программы: 24,00 академических часов.

Срок реализации Программы: 2 недели.

Режим занятий: продолжительность занятия составляет 1 академический час¹. Режим занятий – 4 дня в неделю, 3 акад. часа в день.

Форма реализации Программы: заочная (с применением исключительно дистанционных образовательных технологий и электронного обучения).

¹Для всех видов занятий академический час устанавливается продолжительностью 45 минут.

Особенности реализации Программы заключаются в открытом характере набора слушателей: обучение доступно для взрослого населения без предъявления требований к уровню предварительной подготовки.

Программа ориентирована на начальный (ознакомительный) уровень и рассчитана на широкий круг лиц, заинтересованных в освоении основ информационной безопасности и повышении цифровой грамотности.

Ключевая специфика Программы состоит в её практико-ориентированной направленности и адаптивности содержания. Учебный материал разработан с учётом потребностей слушателей, не имеющих профильного образования в области информационных технологий, что обеспечивает доступность и понятность изложения. Программа позволяет не только получить базовые теоретические знания, но и сформировать навыки их применения в профессиональной деятельности и повседневной жизни.

В отличие от специализированных курсов, ориентированных на IT-специалистов, данная Программа направлена на формирование у слушателей базовых компетенций в области защиты информации в бытовой и социальной среде. Содержание обучения отражает современные вызовы цифровой среды, включая распространённые виды угроз: интернет-мошенничество, фишинговые атаки, утечки персональных данных, вредоносное программное обеспечение и несанкционированный доступ к цифровым ресурсам.

Программа носит комплексный характер и объединяет технические, правовые и поведенческие аспекты информационной безопасности. Это способствует формированию у обучающихся целостного представления о защите информации. Обучение осуществляется с применением дистанционных образовательных технологий, что обеспечивает гибкость организации учебного процесса и возможность освоения материала в индивидуальном темпе.

Структура программы реализована по модульному принципу. Каждый учебный модуль завершается промежуточной аттестацией, направленной на закрепление изученного материала и оценку уровня его освоения. Такой подход способствует повышению учебной мотивации и позволяет эффективно контролировать образовательные результаты.

Особое внимание в программе уделяется формированию цифровой культуры и развитию личной ответственности за обеспечение информационной безопасности. Акцент делается не только на освоении технических инструментов, но и на формировании устойчивых моделей безопасного поведения. Это придаёт программе социальную значимость и обеспечивает её соответствие современным приоритетам государственной политики Российской Федерации в сфере цифрового развития и кибербезопасности.

2. ЦЕЛЬ И ЗАДАЧИ ПРОГРАММЫ

Цель программы – формирование у слушателей базовых знаний, практических навыков и культуры безопасного поведения в цифровой среде, развитие компетенций в области защиты информации, персональных данных и устойчивого использования современных информационно-коммуникационных технологий в повседневной и профессиональной деятельности.

Задачи программы:

Обучающие

- сформировать у слушателей системное представление о сущности и целях информационной безопасности, её правовых и технических основах;
- обучить принципам защиты персональных данных и правилам безопасного обращения с информацией в сети Интернет;
- познакомить с видами угроз и рисков, типичными для цифрового пространства, и способами их предупреждения;
- освоить практические приёмы работы с программными и техническими средствами защиты информации (антивирус, резервное копирование, настройка конфиденциальности и др.);
- сформировать понимание значения организационных и правовых мер обеспечения ИБ в Российской Федерации;
- развить умение применять полученные знания при работе с электронными устройствами, онлайн-сервисами, социальными сетями и электронными платежными системами.

Развивающие

- развить у обучающихся критическое и аналитическое мышление при взаимодействии с информацией в сети;
- сформировать навыки самостоятельного анализа и оценки достоверности источников информации;
- повысить уровень цифровой грамотности, уверенности и самостоятельности при работе в информационной среде;
- способствовать развитию навыков рационального, безопасного и ответственного использования цифровых технологий в личной и профессиональной сфере;
- развить умение распознавать признаки фишинга, мошенничества, утечек данных и иных киберугроз.

Воспитательные

- формировать ответственное и этичное отношение к информации как к личной и общественной ценности;
- воспитывать культуру информационной безопасности, дисциплину и осознанность при обращении с цифровыми ресурсами;
- содействовать развитию уважения к правам других лиц в цифровой среде, соблюдению конфиденциальности и норм сетевого этикета;
- укреплять чувство личной ответственности за сохранность данных, правомерность действий и соблюдение законодательства Российской Федерации в сфере информационной безопасности;
- способствовать формированию гражданской позиции в вопросах защиты информации и цифрового суверенитета России.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

В результате освоения Программы слушатели приобретают знания, умения и компетенции, необходимые для безопасного, осознанного и ответственного использования информационных технологий в личной, социальной и профессиональной деятельности.

Предметные результаты:

- знают основные понятия и принципы информационной безопасности: информация, угрозы, риски, конфиденциальность, целостность, доступность;
- понимают роль информационной безопасности в современном обществе, знают её правовые, технические и организационные основы;
- различают виды угроз и уязвимостей, осознают последствия несанкционированного доступа, утечки и искажения информации;
- владеют базовыми методами и средствами защиты данных: создание надёжных паролей, резервное копирование, антивирусная защита, настройка конфиденциальности;
- знают основы законодательства Российской Федерации в сфере защиты информации и персональных данных (ФЗ № 149, № 152, № 187 и др.);
- умеют применять полученные знания при работе с компьютером, мобильными устройствами, интернет-сервисами и социальными сетями;
- осваивают алгоритмы безопасного поведения в сети Интернет и при осуществлении онлайн-покупок, финансовых операций и коммуникаций;
- способны выявлять признаки мошеннических схем, фишинга и иных угроз цифровой среды и принимать меры по их предотвращению.

Метапредметные результаты:

- формируют навыки критического анализа информации и оценки достоверности источников;

- развивают умение применять универсальные способы защиты данных в различных цифровых ситуациях (работа, учёба, личная жизнь);
- осваивают практические методы организации собственной информационной безопасности (контроль доступа, настройка устройств, управление обновлениями);
- приобретают опыт самостоятельного принятия решений в нестандартных ситуациях, связанных с нарушением безопасности данных;
- умеют использовать полученные знания для консультирования коллег, членов семьи или обучающихся по вопросам безопасного поведения в сети;
- развивают способность работать с информацией законным, этичным и рациональным образом;
- демонстрируют осознанность в действиях и гибкость при выборе способов защиты информации в зависимости от ситуации и уровня угрозы.

Личностные результаты:

- осознают личную ответственность за сохранность и правомерное использование информации;
- формируют устойчивые установки безопасного и этичного поведения в цифровом пространстве;
- проявляют внимательность, критичность и дисциплину при работе с электронными устройствами и данными;
- развивают внутреннюю культуру цифрового взаимодействия, соблюдают сетевой этикет и уважение к конфиденциальности других лиц;
- демонстрируют уважительное отношение к интеллектуальной собственности и правам пользователей информационных систем;
- стремятся к постоянному повышению уровня цифровой грамотности и осведомлённости о новых технологиях защиты информации;
- воспринимают информационную безопасность как неотъемлемую часть гражданской ответственности и личной культуры современного человека.

4. УЧЕБНЫЙ ПЛАН

№ п/п	Наименование модулей	Количество часов				Форма контроля
		Всего	в том числе:			
			Теория	Практика	Самост. работа (СРС)	
1	Модуль 1. Основы информационной безопасности	8	4	-	4	Промежуточная аттестация
2	Модуль 2. Персональные данные и их защита	8	4	-	4	Промежуточная аттестация
3	Модуль 3. Безопасная работа в интернете	8	5	-	3	Промежуточная аттестация
Итого по программе:		24	13	-	11	

5. СОДЕРЖАНИЕ УЧЕБНОГО ПЛАНА

Наименование модулей	Количество часов				Форма контроля
	Всего	в том числе:			
		Теория	Практика	СРС	
Модуль 1. Основы информационной безопасности	8	4	-	4	
Тема 1.1. Введение в информационную безопасность	1	1	-	-	Устный опрос
Тема 1.2. Угрозы и риски в информационной безопасности	2	1	-	1	Практич. работа
Тема 1.3. Угрозы информационной безопасности в повседневной жизни	2	1	-	1	Практич. работа
Тема 1.4. Культура цифровой безопасности: личная ответственность	2	1	-	1	Практич. работа
Промежуточная аттестация	1	-	-	1	Тест
Модуль 2. Персональные данные и их защита	8	4	-	4	
Тема 2.1. Защита персональных данных	2	1	-	1	Практич. работа
Тема 2.2. Персональные данные в цифровую эпоху	2	1	-	1	Практич. работа
Тема 2.3. Защита персональных данных: почему это важно	2	1	-	1	Практич. работа
Тема 2.4. Правовые основы информационной безопасности в России	1	1	-	-	Устный опрос
Промежуточная аттестация	1	-	-	1	Тест
Модуль 3. Безопасная работа в интернете	8	5	-	3	
Тема 3.1. Введение в цифровую гигиену	1	1	-	-	Устный опрос
Тема 3.2. Безопасное использование сайтов и сервисов	2	1	-	1	Практич. работа
Тема 3.3. Организационные меры защиты информации	2	1	-	1	Практич. работа
Тема 3.4. Технические средства информационной безопасности	1	1	-	-	Устный опрос
Тема 3.5. Информационная безопасность в повседневной жизни	1	1	-	-	Устный опрос
Промежуточная аттестация	1	-	-	1	Тест
Итого:	24	13	-	11	

6. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Обучение организуется согласно утвержденному календарному учебному графику, который формируется по мере набора учебной группы на соответствующий период обучения. Курс обучения не привязан к началу или окончанию учебного и календарного года. Прием заявок на курс происходит в течение всего календарного года. Календарный учебный график является примерными утверждается отдельно для каждой учебной группы.

Срок освоения программы – 2 недели, 24,00 академических часа. Начало обучения – по мере набора группы. Режим занятий – 12,00 академических часов в неделю.

Форма обучения – заочная (с применением исключительно электронного обучения и дистанционных образовательных технологий).

Дата начала занятий	Дата окончания занятий	Кол-во учебных недель	Кол-во учебных часов	Режим занятий
По мере набора группы	-	2	24	12 академических часов в неделю

7. РАБОЧАЯ ПРОГРАММА

Вид занятий	Кол-во часов	Наименование модулей и их содержание
Модуль 1. Основы и ключевые понятия информационной безопасности		
Тема 1.1. Введение в информационную безопасность		
Теория	1	Слушатели знакомятся с понятием информации, её свойствами — конфиденциальностью, целостностью и доступностью. Рассматривается, почему защита информации необходима каждому человеку и организации. Объясняется значение триады ЦИА и её роль в сохранении устойчивости цифровой среды. Отдельное внимание уделяется влиянию информационной безопасности на повседневную жизнь, социальные отношения и государственную стабильность.
Тема 1.2. Угрозы и риски в информационной безопасности		
Теория	1	В теме раскрываются понятия «угроза», «риск» и «уязвимость». Объясняется, какие бывают угрозы — естественные, искусственные, внешние и внутренние — и как они соотносятся с элементами триады ЦИА. Приводятся примеры типичных инцидентов: фишинг, вирусы, инсайдерские действия, сбои оборудования. Слушатели учатся понимать, что риск — это не только вероятность угрозы, но и оценка возможного ущерба.
Практика	1	Прочитать описанный кейс: Сотрудник случайно отправил таблицу с личными телефонами клиентов на общий корпоративный чат». Определить: 1) какая угроза реализовалась; 2) была ли уязвимость; 3) каков риск и возможные последствия. Записать свои выводы в таблицу (Угроза – Уязвимость – Риск – Последствие – Меры предотвращения)
Тема 1.3. Угрозы информационной безопасности в повседневной жизни		
Теория	1	В рамках темы рассматриваются основные угрозы в сфере информационной безопасности, возникающие при использовании сети Интернет и цифровых технологий. Изучаются виды вредоносного программного обеспечения, способы распространения компьютерных вирусов, признаки фишинговых атак и методы интернет-мошенничества, а также причины и

		последствия утечек персональных данных и конфиденциальной информации. В ходе занятия обучающиеся знакомятся с основными мерами защиты информации, правилами безопасного поведения в цифровой среде и принципами цифровой гигиены. Формируются навыки распознавания подозрительных сайтов, писем и сообщений, безопасного использования интернет-ресурсов и защиты персональных данных и учетных записей.
Практика	1	Подготовить аналитический текстовый отчет (эссе) на тему: «Основные угрозы информационной безопасности и способы защиты информации в цифровой среде». В работе необходимо: а) охарактеризовать основные виды угроз информационной безопасности (вирусы, фишинг, утечки данных); б) привести примеры возможных ситуаций, связанных с данными угрозами; в) описать возможные последствия для пользователя или организации; г) предложить меры по предотвращению и снижению рисков информационной безопасности.
Тема 1.4. Культура цифровой безопасности: личная ответственность		
Теория	1	Изучаются принципы цифровой гигиены и осознанного поведения в сети Интернет. Рассматривается понятие социальной инженерии, типичные сценарии обмана, правила защиты аккаунтов и персональных данных. Подчеркивается значение личной ответственности, сетевого этикета и уважения к чужой информации. Лекция формирует у слушателей представление о культуре безопасного цифрового взаимодействия как о гражданской обязанности.
Практика	1	Написать мини-эссе (от 1 страницы) на тему: «Какие правила я установлю для себя, чтобы безопасно пользоваться интернетом, соцсетями и банковскими сервисами». Включить не менее пяти конкретных пунктов и пояснить, почему они важны.
Промежуточная аттестация	1	Тестирование
Модуль 2. Персональные данные и их защита		
Тема 2.1. Защита персональных данных		
Теория	1	Изучаются понятие и структура персональных данных, их категории и правовые основы защиты. Объясняется, что такое оператор и субъект персональных данных, как даётся согласие на обработку, какие права имеет гражданин. Разбираются типичные ошибки организаций и пользователей, приводящие к утечкам. Рассматривается ответственность за нарушения и пути предотвращения инцидентов.
Практика	1	Разберите кейс: «Менеджер компании сохранил копии паспортов клиентов на личной флешке и потерял её.» Ответьте письменно: 1. какое нарушение произошло; 2. какие последствия могут наступить; какие меры защиты следовало применить.
Тема 2.2. Персональные данные в цифровую эпоху		
Теория	1	В рамках темы рассматриваются основные риски утечки персональных данных, причины возникновения утечек информации и возможные последствия для граждан и организаций. Изучаются основные права субъектов персональных данных, порядок их реализации и меры по защите персональной информации в цифровой среде.

Практика	1	Подготовить краткий текстовый отчет на тему: «Основные риски утечки персональных данных и способы защиты прав субъектов персональных данных» В работе необходимо привести примеры возможных утечек персональных данных, описать их последствия и указать основные права субъекта персональных данных и меры защиты информации.
Тема 2.3. Защита персональных данных: почему это важно		
Теория	1	В рамках темы рассматриваются основные правила безопасного обращения с личной информацией и принципы обработки персональных данных. Изучаются требования к законной обработке персональных данных, меры защиты информации и правила безопасного поведения в цифровой среде.
Практика	1	Подготовить краткий текстовый отчет на тему: «Основные правила безопасного обращения с личной информацией». В работе необходимо привести примеры персональных данных, описать основные принципы их обработки и указать меры по защите личной информации при использовании цифровых сервисов и сети Интернет.
Тема 2.4. Правовые основы информационной безопасности в России		
Теория	1	Рассматриваются ключевые федеральные законы, регулирующие сферу защиты информации: № 149-ФЗ, № 152-ФЗ, № 187-ФЗ, № 98-ФЗ. Объясняется роль ФСТЭК, ФСБ и Роскомнадзора, их полномочия и функции. Разбираются права и обязанности граждан и операторов информации, принципы законности и ответственности за нарушения. Дается понимание, почему правовая грамотность является основой личной и корпоративной безопасности.
Промежуточная аттестация	1	Тестирование
Модуль 3. Безопасная работа в интернете		
Тема 3.1. Введение в цифровую гигиену		
Теория	1	В рамках темы рассматриваются основные правила цифровой гигиены и безопасного поведения в сети Интернет. Изучаются принципы создания надежных паролей, защиты персональных данных, безопасного использования сайтов, электронной почты и цифровых сервисов, а также меры по предотвращению интернет-угроз и мошенничества.
Тема 3.2. Безопасное использование сайтов и сервисов		
Теория	1	В рамках темы рассматриваются основные правила безопасного использования сайтов и цифровых сервисов. Изучаются признаки надежных и подозрительных интернет-ресурсов, правила безопасной регистрации и авторизации, защита персональных данных, безопасное использование онлайн-платежей и меры предосторожности при работе в сети Интернет.
Практика	1	Обучающемуся необходимо разработать памятку: «Правила безопасной работы с сайтами и интернет-сервисами». Памятка должна содержать рекомендации по безопасному использованию сайтов, защите учетных записей и персональных данных, а также признаки подозрительных интернет-ресурсов и мошеннических схем.
Тема 3.3. Организационные меры защиты информации		
Теория	1	Рассматриваются основные организационные механизмы обеспечения безопасности: политика ИБ, приказы, инструкции, распределение ответственности. Поясняется, что

		организационные меры формируют систему управления ИБ и предотвращают ошибки персонала. Затрагивается роль руководителя, ответственного за ИБ и пользователей, а также значение обучения и контроля. Лекция подчёркивает, что организационная безопасность начинается с документирования процессов.
Практика	1	Составить краткий перечень организационных мер для небольшой компании (5–7 пунктов), обеспечивающих защиту персональных данных сотрудников. Пример: назначение ответственного за ИБ, ведение журнала инцидентов и т.д. Сформулировать каждую меру в виде конкретного действия или регламента.
Тема 3.4. Технические средства информационной безопасности		
Теория	1	Описываются технические способы защиты информации: антивирусы, межсетевые экраны, резервное копирование, криптографические средства. Дается понимание, как эти инструменты работают в комплексе. Рассматриваются типичные ошибки пользователей при настройке защиты и принципы регулярного обновления. Делается акцент на практическом применении технологий в быту и на работе.
Тема 3.5. Информационная безопасность в повседневной жизни		
Теория	1	Лекция посвящена защите информации в быту: безопасное использование социальных сетей, онлайн-банкинга, электронной почты, мобильных устройств. Раскрываются принципы управления паролями, предотвращения мошенничества, защиты цифровой репутации. Формируется понимание, что ИБ — это ежедневный навык, а не технический процесс. Слушатели получают рекомендации по построению личной стратегии безопасности.
Практика	1	Составить «10 правил цифровой безопасности для себя и своей семьи». Включите пункты, касающиеся паролей, социальных сетей, онлайн-платежей, мобильных устройств и поведения в сети. Оформите в виде памятки, которую можно разместить дома или передать другим.
Промежуточная аттестация	1	Тестирование
Итого:	24 академических часа	

8. ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ

В процессе реализации Программы используется текущий контроль (по итогам отдельных тем) и промежуточный контроль. Текущий контроль включает в себя устный опрос и выполнение практических работ (заданий). Промежуточный контроль включает в себя прохождение тестирования. Оценка качества освоения Программы осуществляется преподавателем на основе текущего контроля.

Для получения допуска к новой учебной теме, обучающемуся необходимо ознакомиться с текстовой лекцией, видео лекцией и презентацией на платформе, загрузить практические задания, выполненные по итогам предыдущей темы. Задания размещены в системе электронной образовательной среды (платформы), они доступны авторизованному пользователю платформы, зачисленному в качестве обучающегося.

В процессе контроля педагог оценивает результат практического задания и выставляет общую оценку. При положительной оценке обучающийся может перейти к следующей теме.

При оценке знаний по результатам тестирования учитывается:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.
5. Умение делать обобщения, выводы.

При оценке практического задания учитывается:

1. Умение определить и четко сформулировать цель работы;
2. Оригинальность идеи, исследовательский подход, подобранным и проанализированным материалом;
3. Содержание работы изложено логично;
4. Творческий подход к решению проблемы, имеются собственные предложения;
5. Сделанные выводы свидетельствуют о самостоятельности ее выполнения.

Критериями оценки уровня освоения Программы являются:

1. соответствие уровня теоретических знаний, слушателей программным требованиям;
2. свобода восприятия теоретической информации;
3. самостоятельность работы;
4. осмысленность действий;
5. разнообразие освоенных технологий;
6. соответствие практической деятельности программным требованиям;
7. уровень творческой активности слушателя:
 - количество реализованных проектов, выполненных самостоятельно на основе изученного материала;
 - качество выполненных работ, как по заданию педагога, так и по собственной инициативе.

Для аттестации слушателей на соответствие их персональных достижений требованиям образовательной программы созданы фонды оценочных средств, включающие типовые задания, позволяющие оценить знания и умения.

9. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

9.1. Особенности организации образовательного процесса

Обучение по программе осуществляется в форме теоретических и практических занятий.

Методы обучения. Методическое обеспечение программы предусматривает наличие следующих видов методического материала: электронные учебники, текстовые лекции.

В процессе обучения по данной Программе используются следующие методы:

- исследовательский, применяемый при самостоятельной работе слушателя;
- репродуктивный, используемый в процессе применения, полученных в процессе обучения знаний;
- наглядный, в процессе которого осуществляется демонстрация мультимедийных иллюстраций и рисунков, видеороликов;
- практический, при помощи которого слушатель выполняют творческие работы (задания), отвечают на вопросы по изученному материалу;
- объяснительно-иллюстративный материал (изображений, видеороликов) для формирования знаний и образа действий;
- стимулирующий (развитие познавательного интереса у слушателя, эмоциональное стимулирование и т.д.).

Педагогические технологии и методики. В обучении применяются особые технологии, выбор которых будет зависеть от выбранной модели обучения индивидуально каждым слушателем. Личностно – ориентированные технологии ставят в центр всей образовательной системы личность

обучаемого. Обеспечение комфортных, бесконфликтных условий ее развития, реализацию ее природных потенциалов. Именно на такие технологии опирается программа с индивидуальным форматом обучения.

Учебно-методический комплекс программы состоит из трех компонентов:

- учебные и методические материалы для педагогов и обучающихся;
- система средств обучения;
- система средств контроля результативности обучения.

Реализация программы осуществляется исключительно с применением электронного обучения и дистанционных образовательных технологий.

Реализация программы производится в соответствии с Постановлением № 1678.

Электронная образовательная среда - система дистанционного обучения, которая создает условия для функционирования электронной информационно-образовательной среды, обеспечивающей освоение учащимися образовательной программы в полном объеме независимо от места нахождения учащихся.

Для самостоятельной работы слушатели должны иметь компьютер и выход в Интернет. Местом обучения при обучении в системе дистанционного обучения является образовательная организация независимо от места нахождения учащихся.

Обучение по Программе организуется в индивидуальном формате или в формате мини-групп, представляет собой занятие, транслируемое в режиме реального времени через программы для видеоконференцсвязи (Яндекс Телемост). В случае проведения занятий в группе, количество участников не превышает 8 человек. Также учащиеся проходят обучение на онлайн-платформе ИП Алибаевой М.Н. по электронному адресу (URL): <https://antitreningi.ru/panel/400317/lessons>. На платформе имеется текстовые и видео лекции по всем темам, практические задания к темам, а также тест к каждому модулю для прохождения промежуточной аттестации.

Формы учебно-методической помощи:

- Индивидуальные консультации (онлайн): проводятся по запросу обучающегося. Формат – видеоконференцсвязь (Яндекс Телемост), а также текстовый и голосовой чат на образовательной платформе <https://antitreningi.ru/>.

- Групповые консультации: проводятся в формате вебинаров или онлайн-обсуждений, включающих разбор типичных ошибок, выполнение практических заданий, мини тесты.

Методическая связь и консультации с педагогом обеспечиваются также через образовательную платформу, мессенджеры.

Информационно-библиотечный фонд укомплектован электронными изданиями учебной литературы по теме преподаваемого предмета.

Обучающимся предоставляется доступ (удаленный доступ) к современным профессиональным базам данных и информационным справочным системам, электронной библиотеке, состав которых определяется настоящей программой.

При осуществлении дистанционного обучения слушателям выдаются логин и пароль для входа на образовательную платформу, с помощью которой необходимо будет реализовывать требования программы.

После освоения обучающимся программы и успешной сдачи зачетных заданий ему выдается документ (сертификат), удостоверяющий прохождение обучения, образец которого устанавливается образовательной организацией самостоятельно.

Продолжительность академического часа устанавливается в размере **до 45 минут**. Один академический час включает аудиторную часть (текстовые лекции, видео лекции и вебинары) и внеаудиторную часть (самостоятельная работа с материалами, выполнение заданий, тестирование).

9.2. Педагогические условия

Программу реализует педагог(и) дополнительного образования.

Реализация программы обеспечивается педагогическими кадрами, имеющими среднее профессиональное или высшее образование (по направлению, соответствующему направлению программы, реализуемой организацией, осуществляющей образовательную деятельность) и отвечающими квалификационным требованиям, указанным в квалификационных справочниках, и

(или) профессиональным стандартам, а также с опытом практической работы не менее двух лет в должности педагога дополнительного образования, иной должности педагогического работника - для старшего педагога дополнительного образования.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

10.1. Материально-техническая база организации, осуществляющей обучение, оснащена необходимым оборудованием для доступа в интернет по выделенному каналу.

10.2. Организация, осуществляющая обучение, имеет необходимое программное обеспечение, серверное оборудование, обеспечивающее функционирование электронной информационно-образовательной среды, и высокоскоростной канал доступа к электронной информационно-образовательной среде.

10.3. Обучение проводится посредством электронной образовательной среды (платформы) Антитренинги <https://antitreningi.ru/>.

Платформа позволяет:

- размещать обучающие материалы и задания;
- загружать слушателю выполненные письменные, фото, видео задания, а также вопросы в адрес преподавателя;
- проводить вебинары преподавателями, а также в процессе их проведения задавать вопросы в форме текстовых сообщений;
- осуществлять контроль прогресса изучения учебных материалов, количество выполненных слушателями заданий, а также проверять выполненные ими задания.

10.4. Для освоения образовательной программы слушатель должен иметь доступ в сеть интернет, а также персональный компьютер или смартфон.

Рекомендации к материально-техническим условиям со стороны учащегося (потребителя образовательной услуги):

1. Компьютер с колонками, микрофоном и клавиатурой (либо ноутбук с соответствующим оборудованием).

Рекомендуемая конфигурация компьютера:

- Разрешение экрана от 1280x1024
- Pentium 4 или более новый процессор с поддержкой SSE2
- 512 Мб оперативной памяти
- 200 Мб свободного дискового пространства
- Современный веб-браузер актуальной версии (Firefox 22, Google Chrome 27, Opera 15, Safari 5, Internet Explorer 8 или более новый).

Со совокупность информационных технологий, телекоммуникационных технологий, соответствующих технологических средств организации, осуществляющей обучение, обеспечивает освоение слушателями программы в полном объеме независимо от места нахождения слушателями.

11. ИНФОРМАЦИОННЫЕ И УЧЕБНО-МЕТОДИЧЕСКИЕ УСЛОВИЯ

Информационное обеспечение

Для реализации программы применяются: аудио-, видео-, фотоматериалы, интернет-источники, специальная и учебная литература.

Основные компоненты информационного обеспечения:

- Программа для организации веб-конференций: Яндекс Телемост.
- Онлайн-платформа Антитренинги: с авторизацией учащегося, представляющий собой набор взаимосвязанных веб-сервисов и модулей, составляющих единое пространство для организации обучения. Онлайн-платформа доступна по адресу: <https://antitreningi.ru/panel/400317/lessons>.

Онлайн-платформа включает в себя следующие модули, обеспечивающие учебный процесс по программе:

- ✓ теоретические материалы;
- ✓ практические задания;
- ✓ промежуточные тесты для оценки результативности обучения.

Основная литература:

Добродеев, А. Ю. Показатели информационной безопасности как характеристика (мера) соответствия сетей и организаций связи требованиям информационной безопасности / А. Ю. Добродеев // Труды ЦНИИС. Санкт-Петербургский филиал. – 2020. – Т. 2, № 10. – С. 50-78. – EDN NRYSL. Ссылка: <https://elibrary.ru/item.asp?id=44547904>

Дополнительная литература:

Полыхань, К. О. Проблемы и особенности состояния информационной безопасности в соответствии с доктриной информационной безопасности Российской Федерации / К. О. Полыхань // Устойчивое развитие науки и образования. – 2019. – № 5. – С. 154-160. – EDN XNBSUW. Ссылка: <https://elibrary.ru/item.asp?id=38596126>

Интернет-ресурсы:

1. Интернет-сайт организации - <http://eduufa.ru/>.
2. Система дистанционного обучения ИП Алибаевой М.Н. - <https://antitreningi.ru/panel/400317/lessons>. Доступ для работы на образовательной платформе открыт в режиме 24 часа 7 дней в неделю.
3. Научная электронная библиотека Elibrary - <https://elibrary.ru/>.

12. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Типовые контрольные задания, необходимые для оценки знаний, умений, навыков, характеризующих этапы формирования компетенций в процессе освоения программы.

Типовые вопросы тестирования (промежуточный контроль)

Тестирование Модуля 1. «Основы и ключевые понятия информационной безопасности»

1. Что означает термин «информационная безопасность»?

- а) Защиту только государственных данных
- б) Состояние защищённости информации, при котором обеспечены её конфиденциальность, целостность и доступность
- в) Комплекс технических средств для шифрования данных
- г) Мету ответственности оператора информации

2. Какое из свойств не относится к триаде информационной безопасности?

- а) Конфиденциальность
- б) Целостность
- в) Масштабируемость
- г) Доступность

3. Что понимается под конфиденциальностью информации?

- а) Возможность просмотра информации любым пользователем
- б) Гарантия, что информация не будет доступна посторонним
- в) Обеспечение сохранности данных на сервере
- г) Контроль скорости обработки информации

4. Какова основная цель системы обеспечения ИБ в обществе?

- а) Ограничить свободный доступ к информации
- б) Создать равные условия доступа к госуслугам
- в) Снизить вероятность утечек и неправомерных действий с информацией
- г) Контролировать публикации в сети Интернет

5. Что является угрозой информационной безопасности?

- а) Мера защиты данных
- б) Потенциальная возможность нарушения конфиденциальности, целостности или доступности информации
- в) Отчёт о проверке безопасности
- г) Инструкция по резервному копированию

6. Как правильно соотнести понятия «угроза» и «риск»?

- а) Риск — это любое действие, а угроза — его последствие
- б) Угроза — событие, риск — вероятность и величина ущерба
- в) Риск — разновидность угрозы
- г) Эти понятия тождественны

7. К какому типу угроз относится фишинг?

- а) Естественная
- б) Искусственная, преднамеренная
- в) Искусственная, непреднамеренная
- г) Природная

8. Что такое уязвимость в контексте ИБ?

- а) Любой компьютер
- б) Слабое место системы, которое может быть использовано угрозой
- в) Метод резервного копирования
- г) Уровень сложности пароля

9. Что является примером угрозы доступности информации?

- а) Публикация персональных данных
- б) Подделка документов
- в) DDoS-атака
- г) Утечка коммерческой тайны

10. Какой закон является основным в регулировании вопросов защиты информации в России?

- а) № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- б) № 98-ФЗ «О коммерческой тайне»
- в) № 44-ФЗ «О контрактной системе»
- г) № 210-ФЗ «Об организации предоставления государственных услуг»

11. Что регулирует Федеральный закон № 152-ФЗ?

- а) Защиту коммерческой тайны
- б) Правила использования государственных символов
- в) Обработку персональных данных граждан
- г) Лицензирование операторов связи

12. Какая государственная структура отвечает за контроль в сфере персональных данных?

- а) Минцифры России
- б) ФСБ России
- в) Роскомнадзор
- г) ФСТЭК России

13. Что регулирует закон № 187-ФЗ «О безопасности критической информационной инфраструктуры»?

- а) Защиту интернет-магазинов
- б) Безопасность ИТ-систем, имеющих значение для функционирования государства
- в) Сферу авторских прав
- г) Безопасность образовательных организаций

14. Что является основой культуры информационной безопасности?

- а) Владение антивирусами
- б) Знание паролей коллег
- в) Осознанное и ответственное отношение к информации и действиям в цифровой среде
- г) Умение работать в социальных сетях

15. Какая мера относится к цифровой гигиене?

- а) Хранение паролей в записках телефона
- б) Переход по ссылкам из неизвестных писем
- в) Регулярное обновление программного обеспечения
- г) Передача данных третьим лицам

Тестирование Модуля 2. Практические аспекты и меры обеспечения информационной безопасности.

1. Что понимается под организационными мерами информационной безопасности?

- а) Программные средства защиты информации
- б) Управленческие и регламентные меры, направленные на обеспечение защиты данных
- в) Только действия системного администратора

2. Какой принцип организационной защиты предполагает предоставление пользователю минимально необходимого доступа к информации?

- а) Принцип ротации полномочий
- б) Принцип минимально необходимого доступа
- в) Принцип разделения ответственности

3. Что должно быть оформлено для документального закрепления мер ИБ в организации?

- а) Локальные нормативные акты
- б) Личные заявления сотрудников
- в) Акты технических испытаний

4. Кто несёт общую ответственность за обеспечение информационной безопасности в организации?

- а) Руководитель организации
- б) Ответственный за ИБ
- в) Системный администратор

5. Что относится к техническим средствам защиты информации?

- а) Локальные нормативные документы
- б) Программные и аппаратные решения
- в) Только кадровые проверки

6. Какое назначение имеет межсетевой экран (firewall)?

- а) Контролировать сетевой трафик и блокировать несанкционированные соединения
- б) Сохранять копии данных на сервере
- в) Устанавливать антивирусные обновления

7. Что представляет собой система резервного копирования (backup)?

- а) Программа для удаления временных файлов
- б) Средство для шифрования информации
- в) Создание копий данных для восстановления после сбоев

8. Для чего используется двухфакторная аутентификация?

- а) Для сокращения числа паролей
- б) Для проверки личности пользователя с помощью двух независимых факторов
- в) Для ускорения входа в систему

9. Что относится к персональным данным согласно закону № 152-ФЗ?

- а) Только паспортные данные
- б) Любая информация, относящаяся к конкретному человеку
- в) Только сведения, размещённые в сети Интернет

10. Кто является субъектом персональных данных?

- а) Организация, которая собирает данные
- б) Гражданин, к которому относятся эти данные
- в) Государственный оператор информации

11. Какое условие обязательно для обработки персональных данных гражданина?

- а) Согласие субъекта на обработку

- б) Согласие только работодателя
- в) Поручение от внешней компании

12. Что обязан сделать оператор при обработке персональных данных?

- а) Сообщить гражданину о сборе данных и обеспечить их защиту
- б) Хранить данные бессрочно
- в) Передавать данные третьим лицам без согласия

13. Какое правило относится к базовой цифровой гигиене?

- а) Использование одного пароля для всех сервисов
- б) Регулярное обновление программ и антивирусов
- в) Хранение паролей на рабочем столе

14. Что считается проявлением осознанного поведения в сети?

- а) Переход по любым ссылкам
- б) Проверка достоверности источников информации перед действием
- в) Использование общего аккаунта несколькими людьми

15. Как следует поступить при звонке “из банка” с просьбой назвать код из SMS?

- а) Сообщить код для подтверждения операции
- б) Перезвонить в официальный контакт-центр банка
- в) Продиктовать код только после уточнения фамилии сотрудника

Тестирование Модуля 3. Безопасная работа в интернете.

1. Что является основной целью информационной безопасности?

- Увеличение скорости обработки данных
- Обеспечение конфиденциальности, целостности и доступности информации
- Ограничение доступа граждан к информации
- Создание резервных копий документов

2. Что понимается под угрозой информационной безопасности?

- Средство защиты информации
- Правило хранения документов
- Потенциальная возможность нарушения безопасности информации
- Процесс резервного копирования

3. Какая из перечисленных угроз относится к социальной инженерии?

- DDoS-атака
- Фишинг
- Ошибка жесткого диска
- Повреждение кабеля связи

4. Что является характерным признаком фишингового сайта?

- Использование защищенного соединения HTTPS
- Наличие официального логотипа компании
- Требование срочно ввести персональные данные или пароль
- Размещение контактной информации организации

5. Какое действие наиболее повышает риск утечки персональных данных?

- Использование двухфакторной аутентификации
- Регулярное обновление программ
- Передача кодов подтверждения третьим лицам
- Проверка адреса сайта перед вводом данных

6. Что относится к персональным данным согласно законодательству РФ?

- Только паспортные данные
- Только сведения о доходах
- Любая информация, относящаяся к определенному физическому лицу
- Только биометрические данные

7. Кто является субъектом персональных данных?

Организация, обрабатывающая данные
Государственный орган
Физическое лицо, к которому относятся персональные данные
Оператор связи

8. Кто является оператором персональных данных?

Любое лицо, осуществляющее обработку персональных данных
Только государственный орган
Только работодатель
Исключительно интернет-провайдер

9. Какой принцип обработки персональных данных предполагает обработку только тех данных, которые необходимы для достижения конкретной цели?

Принцип конфиденциальности
Принцип минимизации данных
Принцип открытости
Принцип резервирования

10. Какое право имеет субъект персональных данных?

Требовать удаления незаконно обрабатываемых данных
Самостоятельно изменять государственные базы данных
Получать доступ к данным других граждан
Передавать чужие персональные данные третьим лицам

11. Какое действие относится к правилам цифровой гигиены?

Использование одного пароля для всех сервисов
Регулярное обновление программного обеспечения
Передача учетных данных коллегам
Хранение паролей в открытом текстовом файле

12. Что рекомендуется делать при использовании общественной сети Wi-Fi?

Совершать банковские операции без ограничений
Передавать конфиденциальные данные без защиты
Использовать защищенные соединения и избегать передачи чувствительной информации
Отключать антивирус

13. Какой пароль считается наиболее надежным?

12345678
qwerty
Дата рождения пользователя
Сложная комбинация букв, цифр и специальных символов

14. Для чего используется двухфакторная аутентификация?

Для ускорения входа в систему
Для дополнительной проверки личности пользователя
Для хранения резервных копий
Для удаления вредоносных файлов

15. Что относится к организационным мерам защиты информации?

Антивирусное программное обеспечение
Межсетевой экран
Разработка локальных нормативных актов и инструктаж сотрудников
Шифрование данных