Министерство просвещения Российской Федерации
Федеральное государственное автономное научное учреждение
«Федеральный институт цифровой трансформации в сфере образования»
(ФГАНУ «ФИЦТО»)

УТВЕРЖДАЮ

исполняющий обязанности
директора федерального
государственного автономного
научного учреждения
«Федеральный институт цифровой
трансформации в сфере
образования»

«04» марта 2025 г.

_____ /**А.Б. Молотков**/

М.П.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
повышения квалификации
«Основы информационной безопасности в школьном курсе информатики с применением инструментов Лаборатории Касперского» (36 ч.)
в федеральном государственном автономном научном учреждении
«Федеральный институт цифровой трансформации в сфере образования»

Автор-составитель:
Милованов Николай Юрьевич
к.п.н., менеджер образовательных
программ Лаборатории Касперского

Москва
2025 г.

СОДЕРЖАНИЕ

Раздел 1. Общая характеристика программы

1.1. Нормативно-правовые основания разработки программы

Нормативную правовую основу разработки программы составили:

– Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

– приказ Минобрнауки России от 01.07.2013 № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

– Методические рекомендации по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов, утвержденные Минобрнауки России 22.01.2015 № ДЛ-1/05вн;

– приказ Минобрнауки России от 22.02.2018 № 126 «Об утверждении федерального государственного образовательного стандарта высшего образования – магистратура по направлению подготовки 44.04.01 Педагогическое образование»;

– приказ Минобрнауки России от 22.02.2018 № 121 «Об утверждении федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 44.03.01 Педагогическое образование»;

– приказ Минобрнауки России от 22.02.2018 № 125 «Об утверждении федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки)»;

– приказ Минобрнауки России от 17.11.2020 № 1427 «Об утверждении федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность»;

– приказ ФГАНУ «ФИЦТО» от 02.07.2024 № 2024-0207-2-ОД «Об утверждении положений о дополнительных профессиональных программах»;

– Устав ФГАНУ «ФИЦТО».

Программа рассмотрена, обсуждена и рекомендована на заседании Совета ФГАНУ «ФИЦТО», протокол № 2/25 от 26.02.2025.

1.2. Цель реализации программы

Дополнительная профессиональная программа повышения квалификации «Основы информационной безопасности в школьном курсе информатики с применением инструментов Лаборатории Касперского» в федеральном государственном автономном научном учреждении «Федеральный институт цифровой трансформации в сфере образования» (далее – ФГАНУ «ФИЦТО»)

создана с целью формирования у слушателей знаний об основных понятиях курса информационной безопасности и умений защищать свое личное информационное пространство, а также для дальнейшего применения полученных знаний на уроках информатики в образовательных организациях.

Совершенствуемые компетенции

№ п/п	Компетенция	Код компетенции
1	2	3
1.	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.	ОПК-1
2.	Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности.	ОПК-2
3.	Способен осуществлять духовно-нравственное воспитание обучающихся на основе базовых национальных ценностей. Демонстрирует способность к формированию у обучающихся гражданской позиции, толерантности и навыков поведения в поликультурной среде, способности к труду и жизни в современном мире, общей культуры на основе базовых национальных ценностей.	ОПК-4
4.	Способен использовать психолого-педагогические технологии в профессиональной деятельности, необходимые для индивидуализации обучения, развития, воспитания, в том числе обучающихся с особыми образовательными потребностями.	ОПК-6
5.	Способен осуществлять педагогическую деятельность на основе специальных научных знаний.	ОПК-8
6.	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	ОПК-9

1.3. Планируемые результаты обучения

№ п/п	Знать	Код компетенции
1	2	3
1.	Понятие информационной безопасности и необходимость в организации защиты своего личного информационного пространства.	ОПК-1, ОПК-9
2.	Типы атак, угроз в сети Интернет, социальных сетей. Вредоносное программное обеспечение и ее виды.	ОПК-1, ОПК-9

№ п/п	Знать	Код компетенции
1	**2**	**3**
3.	Что такое социальная инженерия и ее основные методы как механизм создания основы для информационной угрозы. Знать правила поведения в поликультурной среде, организацию жизни в современном мире, общей культуры на основе базовых национальных ценностей.	ОПК-4
4.	Стратегию различения атак и угроз, исходящих из сети Интернет, социальных сетей в современных условиях с применением инструментов Лаборатории Касперского.	ОПК-2, ОПК-9
5.	Математические основы в курсе информационной безопасности.	ОПК-8
№ п/п	**Уметь**	**Код компетенции**
1	**2**	**3**
1.	Различать атаки, угрозы, исходящие из программного обеспечения, сети Интернет, социальных сетей в современных условиях с применением инструментов Лаборатории Касперского.	ОПК-1, ОПК-2, ОПК-9
2.	Разрабатывать стратегию обеспечения информационной безопасности в современных условиях реальной и виртуальной жизни, применяя теоретические знания информационной безопасности и прикладные программы (приложения) отечественного производства. Определять уровень сформированности у детей духовно-нравственного развития, планировать и осуществлять превентивные мероприятия профилактической направленности по этичному поведению в сети Интернет и защите личного информационного пространства.	ОПК-2, ОПК-4
3.	Конструировать системы задач для обеспечение практической составляющей школьного курса информатики.	ОПК-8
3.	Использовать психолого-педагогические технологии в профессиональной деятельности, необходимые для индивидуализации обучения, развития, воспитания, в том числе, обучающихся с особыми образовательными потребностями.	ОПК-6

1.4. Категория слушателей

Учителя информатики и педагоги дополнительного образования, чей предмет взаимосвязан с информационной безопасностью.

Требования к квалификации – среднее профессиональное образование, высшее образование без предъявления требований к стажу работы.

1.5. Формы обучения и сроки освоения

Форма обучения по программе повышения квалификации – заочная, исключительно с применением электронного обучения и дистанционных образовательных технологий. Электронная образовательная среда курса: https://lms.ficto.ru/local/crw/course.php?id=61. Объем образовательной программы составляет 36 часов.

1.6. Период обучения и режим занятий

Период обучения для каждого запуска программы определяется в индивидуальном режиме с учетом количества слушателей и составляет 6 недель, включая итоговую аттестацию.

1.7. Документ о квалификации

Лицам, успешно освоившим данную дополнительную профессиональную программу повышения квалификации и прошедшим итоговую аттестацию, выдается документ о квалификации: удостоверение о повышении квалификации с указанием срока освоения программы.

Лицам, не прошедшим итоговую аттестацию или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть дополнительной профессиональной программы и (или) отчисленным из ФГАНУ «ФИЦТО», выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому ФГАНУ «ФИЦТО».

Раздел 2. Содержание программы

2.1. Учебно-тематический план

№ п/п	Наименование модулей (разделов)	Всего часов	Виды учебных занятий, учебных работ		Самостоя-тельная работа	Формы контроля
			Лекции	Интерак-тивные занятия		
1	**2**	**3**	**4**	**5**	**6**	**7**
1.	Представление об информационной безопасности	16	7	3	6	Эссе, практическая работа
2.	Основы криптологии	18	10	4	4	Практическая работа
Итоговая аттестация		2				Тестирование

2.2. Распределение часов (трудоемкость) по темам и видам работ

№ п/п	Название модулей (разделов) и тем	Общая трудоемкость (часы)	Аудиторные занятия		Самостоя-тельные занятия (заочная форма) (часы)	Формы контроля
			Лекции (часы)	Семина-ры, практи-ческие занятия		
1	**2**	**3**	**4**	**5**	**6**	**7**
Представление об информационной безопасности		**16**	**7**	**3**	**6**	**Эссе, практическая работа**
1.1.	Необходимость в информационной безопасности	3	2	-	1	-
1.2.	Аутентификация. Надежность пароля	2	1	1	-	Практическая работа
1.3.	Безопасность в мессенджерах и браузерах	1	1	-	-	-
1.4.	Вредоносное программное обеспечение. Атака нулевого дня. SQL-инъекция	2	1	-	1	-
1.5.	Фишинг, вишинг, доксинг	3	1	1	1	
1.6.	Социальная инженерия	5	1	1	3	Эссе
Основы криптологии		**18**	**10**	**4**	**4**	**Практическая работа**
2.1.	Криптология. Шифрование данных. Хэш-функции	1	1	-	-	-
2.2.	Квантовые компьютеры	2	1	-	1	-

№ п/п	Название модулей (разделов) и тем	Общая трудоемкость (часы)	Аудиторные занятия		Самостоя-тельные занятия (заочная форма) (часы)	Формы контроля
			Лекции (часы)	Семина-ры, практи-ческие занятия		
1	**2**	**3**	**4**	**5**	**6**	**7**
	и постквантовое шифрование					
2.3.	Математические основы криптологии	6	2	2	2	-
2.4.	Шифры простой замены. Шифр Цезаря	2	1	-	1	-
2.5.	Частотный анализ	1	-	1	-	Практическая работа
2.6.	Шифр Вернама (XOR)	1	1	-	-	-
2.7.	Шифр Виженера	1	1	-	-	-
2.8.	Шифр RSA. Электронная цифровая подпись	2	2	-	-	-
2.9.	Стеганография	2	1	1	-	Практическая работа
Итоговая аттестация		**2**	**-**	**-**	**-**	**Тестирование**
Итого		**36**	**17**	**7**	**10**	

2.3. Календарный учебный график

Календарный учебный график представлен в форме расписания занятий при наборе группы на обучение.

Примерный вариант занятий

Неделя 1	***Пн***	***Вт***	***Ср***	***Чт***	***Пт***	***Сб***	***Вс***
Количество часов	*Выходной*	*2 ч.*	*Выходной*	*2 ч.*	*Выходной*	*1 ч. (Самостоятельное занятие (заочная форма))*	*Выходной*
Неделя 2	***Пн***	***Вт***	***Ср***	***Чт***	***Пт***	***Сб***	***Вс***
Количество часов	*Выходной*	*2 ч.*	*Выходной*	*2 ч.*	*Выходной*	*2 ч. (Самостоятельное занятие (заочная форма))*	*Выходной*
Неделя 3	***Пн***	***Вт***	***Ср***	***Чт***	***Пт***	***Сб***	***Вс***
Количество часов	*Выходной*	*2 ч.*	*Выходной*	*2 ч.*	*Выходной*	*4 ч. (Самостоятельное занятие (заочная форма))*	*Выходной*
Неделя 4	***Пн***	***Вт***	***Ср***	***Чт***	***Пт***	***Сб***	***Вс***
Количество часов	*Выходной*	*2 ч.*	*Выходной*	*2 ч.*	*Выходной*	*2 ч. (Самостоятельное занятие (заочная форма))*	*Выходной*
Неделя 5	***Пн***	***Вт***	***Ср***	***Чт***	***Пт***	***Сб***	***Вс***
Количество часов	*Выходной*	*2 ч.*	*Выходной*	*2 ч.*	*Выходной*	*1 ч. (Самостоятельное занятие (заочная форма))*	*Выходной*
Неделя 6	***Пн***	***Вт***	***Ср***	***Чт***	***Пт***	***Сб***	***Вс***
Количество часов	*Выходной*	*2 ч.*	*Выходной*	*2 ч.*	*Выходной*	*2 ч. (Итоговая аттестация)*	*Выходной*

2.4. Рабочие программы дисциплин (модулей)

1. Представление об информационной безопасности

Лекции (7 ч.)

Понятие информационной безопасности. Защита информации. Федеральные законы в сфере информационной безопасности. Конфиденциальность, целостность, доступность информации. История становления теории информационной безопасности. Карьера в сфере информационной безопасности. Аутентификация.

Надежность пароля. Мессенджеры, защита аккаунтов Telegram и WhatsApp. Браузеры и их расширения, режим инкогнито. Вредоносное программное обеспечение и ее типы. Уязвимость нулевого дня. Базы данных, SQL-инъекция. Антивирусные решения. Фишинг, вишинг, доксинг. Социальная инженерия и ее методы.

Семинары, практические занятия (3 ч.)

Разработка алгоритма по формированию надежного пароля на языке программирования Python. Рассмотрение конкретных ситуаций социальной инженерии с проведением дискуссии. Практическая работа по поиску информации в сети.

Самостоятельные занятия (6 ч.)

Ознакомление с информацией о необходимости информационной безопасности, основном вредоносном программном обеспечение и уязвимостях, а также о методах социальной инженерии на порталах: Блог Касперского и Securelist.

2. Основы криптологии

Лекции (10 ч.)

Криптология, криптография, криптоанализ. Шифрование данных. Шифр и его виды. Хэш-функции. Квантовые компьютеры и постквантовое шифрование. Понятия теории множеств, арифметики, теории вероятности, арифметики остатков, алгебры логики. Шифры простой замены и частотный анализ. Шифры Цезаря, Виженерна, Вернама, RSA. Цифровая подпись. Стеганография.

Семинары, практические занятия (4 ч.)

Решение математических задач, лежащих в математических основах криптологии. Практическая работа по применению частотного анализа для расшифровки текста, который был подвергнут шифрованию методом простой замены. Практическая работа по стеганографии в формате CTF.

Самостоятельные занятия (4 ч.)

Ознакомление с информацией об использовании квантовых компьютеров и элементов искусственного интеллекта в области информационной безопасности на порталах: Блог Касперского и Securelist. Решение конкретных математических задач, лежащих в математических основах криптологии. Ознакомление с видами шифров простой замены.

Раздел 3. Формы аттестации и оценочные материалы

Дополнительной профессиональной программой повышения квалификации предусмотрены промежуточная и итоговая аттестации.

Формой промежуточной аттестации является выполнение практических работ и эссе. Формой итоговой аттестации является тестирование.

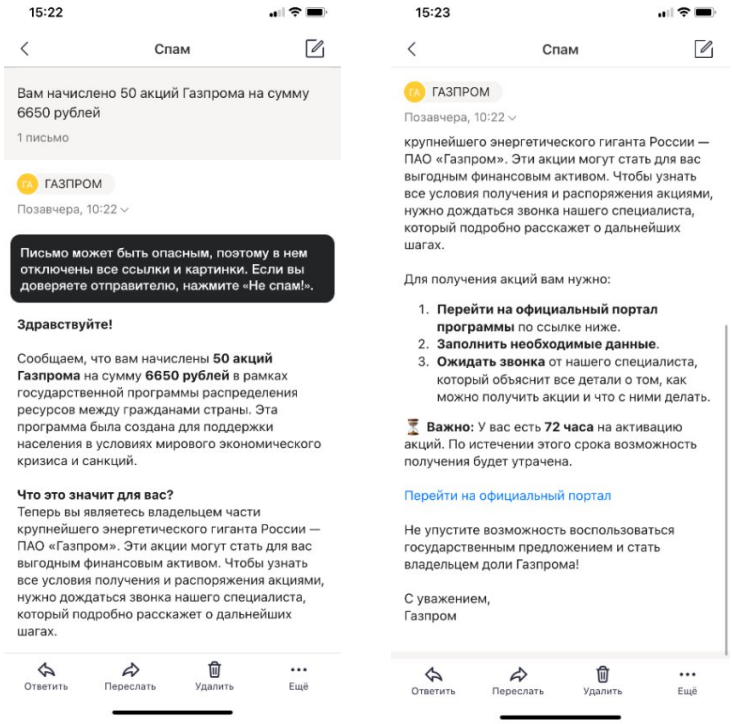
3.1. Промежуточная аттестация

Промежуточная аттестация слушателей обеспечивает оценивание промежуточных результатов обучения по разделам (модулям) дополнительной профессиональной программы. Содержание вопросов/заданий соответствует содержанию разделов (модулей). Промежуточная аттестация слушателей осуществляется в форме практических работ и эссе. Успешное прохождение промежуточной аттестации является допуском к итоговой аттестации.

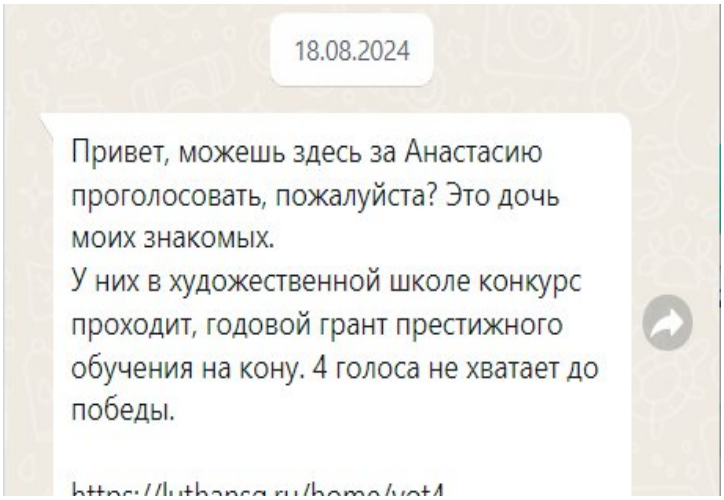
Типовые задания

Примеры вопросов, ответы на которые необходимо рассмотреть в формате эссе по теме «Социальная инженерия»:

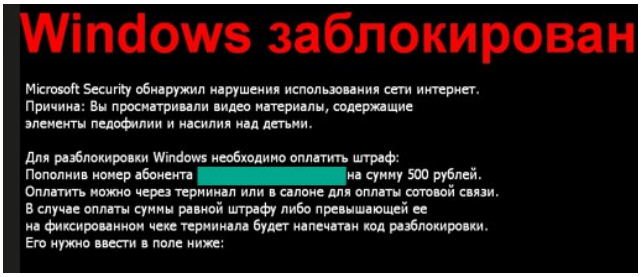
1. Вы получаете на электронную почту письмо, которое информирует Вас о зачислении денежных средств, предварительно требующее заполнения личных данных и банковских карт. Какими будут Ваши действия?



2. Вы получаете в мессенджере сообщение с просьбой проголосовать в конкурсе. Какими будут Ваши действия?



После установки приложения ПК перезагрузился и выдает сообщение на экране о недопустимом поведении в Интернете и требовании о переводе денежных средств на указанный номер. Какими будут Ваши действия?



Критерии оценивания

Оценивание задания в формате эссе происходит по двухбалльной системе («зачтено» или «не зачтено»).

Отметка «зачтено» выставляется если слушатель правильно определил метод социальной инженерии и пути ее предотвращения, прописав грамотный алгоритм действий в данной ситуации. В противном случае выставляется отметка «не зачтено». В последнем случае эссе можно выполнить повторно по другой тематике.

Пример практической работы по теме «Аутентификация. Надежность пароля»: Практическая работа заключается в разработке алгоритма генерации пароля на языке Python, с последующей проверкой на надежность. Если результат выполнения алгоритма не проходит проверку, то необходимо увеличить длину получаемого пароля.

Отметка «зачтено» выставляется если слушатель правильно написал алгоритм на языке программирования. В противном случае выставляется отметка

«не зачтено». В последнем случае практическую работу можно выполнить повторно.

Пример практической работы по теме «Частотный анализ»: Имеется файл, который подвергся атаке шифровальщика (использовался шифр простой замены). При помощи онлайн-калькулятора https://planetcalc.ru/733/ провести частотный анализ текста для расшифровки и получения ответа на поставленный вопрос. Необходимый файл предварительно выгружен на сервер.

Отметка «зачтено» выставляется если слушатель правильно ответил на поставленный вопрос. В противном случае выставляется отметка «не зачтено». В последнем случае практическую работу можно выполнить повторно.

Пример практической работы по теме «Стеганография»: Извлеките информацию из данных изображений при помощи онлайн-калькулятора https://planetcalc.ru/9345/. Все необходимые изображения предварительно выгружены на сервер.



Оценивание заданий в формате практической работы происходит по двухбалльной системе («зачтено» или «не зачтено»).

Отметка «зачтено» выставляется если слушатель правильно извлек информацию и нашел ответ на поставленный скрытый вопрос. В противном случае выставляется отметка «не зачтено». В последнем случае практическую работу можно выполнить повторно.

3.2. Итоговая аттестация

Итоговая аттестация слушателей обеспечивает проверку соответствия результатов освоения дополнительной профессиональной программы повышения квалификации, заявленным целям и планируемым результатам обучения, определяет уровень усвоения обучающимся учебного материала (изучение теоретических основ, приобретение профессиональных навыков). Допуском к итоговой аттестации является успешное прохождение промежуточной аттестации.

Формой итоговой аттестации является тестирование, состоящее из 10 предложений, истинность которых необходимо установить.

Критерии оценивания

Оценивание итоговой аттестации в формате тестирования происходит по двухбалльной системе («зачтено» или «не зачтено»).

Отметка «зачтено» выставляется если слушатель правильно определил истинность 8 и более высказываний предложенного теста. В противном случае выставляется отметка «не зачтено». В последнем случае тестирование можно выполнить повторно.

Оценка	**Кол-во баллов**
Зачтено	8-10
Не зачтено	0-7

Раздел 4. Организационно-педагогические условия реализации программы

4.1. Учебно-методическое и информационное обеспечение программы

Список основной литературы

1. Васильева И.Н. Криптографические методы защиты информации: учебник и практикум для вузов / И.Н. Васильева. – М.: Издательство Юрайт, 2025. – 310 с. – (Высшее образование). – ISBN 978-5-534-02883-6. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/560977 (дата обращения: 07.02.2025).
2. Фомичёв В.М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: учебник для вузов / В.М. Фомичёв, Д.А. Мельников; под редакцией В.М. Фомичёва. – М.: Издательство Юрайт, 2025. – 209 с. – (Высшее образование). – ISBN 978-5-9916-7088-3. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/536733 (дата обращения: 05.02.2025).
3. Фомичёв В.М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты: учебник для вузов / В.М. Фомичёв, Д.А. Мельников; под редакцией В.М. Фомичёва. – М.: Издательство Юрайт, 2025. – 245 с. – (Высшее образование). – ISBN 978-5-9916-7090-6. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/537383 (дата обращения: 05.02.2025).

Список дополнительной литературы

1. Зенков А.В. Информационная безопасность и защита информации: учебное пособие для вузов / А.В. Зенков. – 2-е изд., перераб. и доп. – М.: Издательство Юрайт, 2025. – 107 с. – (Высшее образование). – ISBN 978-5-534-16388-9. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/544290 (дата обращения: 11.02.2025).

2. Лось А.Б. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов / А.Б. Лось, А.Ю. Нестеренко, М.И. Рожков. – 2-е изд., испр. – М.: Издательство Юрайт, 2025. – 473 с. – (Высшее образование). – ISBN 978-5-534-12474-3. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/536132 (дата обращения: 14.02.2025).

Интернет-ресурсы

1. Блог Касперского [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/ (дата обращения: 03.02.2025).
2. Сайт со всей отчетностью Лаборатории Касперского об угрозах информационной безопасности, анализе угроз, реверс-инжиниринге вирусов и статистике «Securelist» [Электронный ресурс]. – Режим доступа: https://securelist.ru/ (дата обращения: 30.01.2025).
3. Сайт о защите детского информационного пространства, на котором расположены различные видео, тексты, интерактивы и методические разработки для проведения занятий по информационной безопасности «Kids safe media» [Электронный ресурс]. – Режим доступа: https://kids.kaspersky.ru/ (дата обращения: 14.02.2025).
4. Курс «Математика в кибербезопасности» на платформе Stepik [Электронный ресурс]. – Режим доступа: https://stepik.org/62247 (дата обращения: 07.02.2025).

4.2. Материально-техническое и программное обеспечение реализации программы

Программа реализуется полностью дистанционно с применением современных дистанционных образовательных технологий с использованием программного обеспечения «Среда электронного обучения 3KL». Одним из базовых условий обучения является наличие у слушателей технической возможности онлайн-обучения с нормальным качеством интернет-соединения.

Всем слушателям в начале курса предоставляется индивидуальный доступ к электронно-информационной образовательной среде (ЭИОС) ФГАНУ «ФИЦТО».

Накануне занятий предоставляются инструкции по использованию дистанционных образовательных технологий. Оперативная коммуникация со слушателями вне занятий (консультативного характера) осуществляется с помощью электронной переписки.

Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к образовательной платформе «Юрайт» (доступ к более чем 150 тысячам книг и учебно-методических материалов).

Для осуществления образовательного процесса необходимо следующее материально-техническое обеспечение:

- моноблок или ноутбук с выходом в Интернет;
- система для проведения видеоконференций (видеокамера, микрофон, блок управления);
- пакет офисных программ Р7-Офис;
- браузер, совместимый с Яндекс.Телемост и электронной информационно-образовательной средой ФГАНУ «ФИЦТО»;
- Яндекс.Телемост для компьютера;
- Программное обеспечение «Среда электронного обучения 3KL».

4.3. Кадровое обеспечение программы

Ф.И.О. педагогического (научно-педагогического) работника, участвующего в реализации образовательной программы	Уровень образования, наименование специальности, направления подготовки, наименование присвоенной квалификации	Должность, ученая степень, ученое звание	Сведения о повышении квалификации и (или) профессиональной переподготовки	Стаж научно-педагогической работы		Наименование читаемой дисциплины (модуля), практики/стажировки (при наличии) по данной программе
				Всего	В том числе по читаемой дисциплине (модулю)	
1	2	3	4	5	6	7
Милованов Николай Юрьевич	Высшее образование, математика и информатика, учитель математики и информатики	Менеджер образовательных программ Лаборатории Касперского, кандидат педагогических наук	-	10	3	1. Представление об информационной безопасности. 2. Основы криптологии.