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»

«23» 10 2025 г.

_____ **А.Б. Молотков**

М.П.

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»

Москва
2025 г.

Автор-составитель/разработчик:
Милованов Николай Юрьевич, менеджер образовательных программ, Акционерное общество «Лаборатория Касперского», к.п.н.

Рецензенты:
Пономарева Юлия Сергеевна, заведующий кафедрой информатики и методики преподавания информатики ФГБОУ ВО «Волгоградский государственный социально-педагогический университет», к.п.н., доцент.

Безвершенко Леонид Олегович, старший исследователь угроз информационной безопасности, Акционерное общество «Лаборатория Касперского».

Программа рассмотрена и согласована на заседании Совета Учреждения, протокол № __ от «__» октября 2025 г.

Раздел 1. Общая характеристика программы

1.1. Цель реализации программы

Цель реализации программы дополнительного профессионального образования 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 – ДПП ПК, Учреждение) формирование у слушателей знаний об основных понятиях курса информационной безопасности и умений защищать свое личное информационное пространство, для дальнейшего применения полученных знаний на уроках информатики в образовательных организациях.

1.2. Планируемые результаты обучения

Виды деятельности	**Общепрофессиональные, профессиональные, универсальные компетенции (ОПК, ПК, УК) или специализированные, профессионально-специализированные компетенции (СК, ПСК)**	**Практический опыт**	**Умения**	**Знания**
1	**2**	**3**	**4**	**5**
ВД 1. Получение теоретических и практических знаний, умений и навыков в области информационной безопасности.	ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.	Организация защиты личного информационного пространства. Классификация различных видов вредоносного ПО.	Различать атаки, угрозы, исходящие из программного обеспечения, сети Интернет, социальных сетей в современных условиях с применением инструментов Лаборатории Касперского.	Понятие информационной безопасности и необходимость в организации защиты своего личного информационного пространства. Типы атак, угроз в сети Интернет, социальных сетей. Вредоносное программное обеспечение и ее виды.
	ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного	Установка приложений Лаборатории Касперского. Защита личных аккаунтов надежным	Различать атаки, угрозы, исходящие из программного обеспечения, сети Интернет,	Стратегию различения атак и угроз, исходящих из сети Интернет, социальных сетей в

Виды деятельности	Общепрофессиональные, профессиональные, универсальные компетенции (ОПК, ПК, УК) или специализированные, профессионально-специализированные компетенции (СК, ПСК)	Практический опыт	Умения	Знания
1	2	3	4	5
	производства, для решения задач профессиональной деятельности.	паролем и подключением нескольких факторов аутентификаций.	социальных сетей в современных условиях с применением инструментов Лаборатории Касперского. 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	современных условиях с применением инструментов Лаборатории Касперского.

Виды деятельности	Общепрофессиональные, профессиональные, универсальные компетенции (ОПК, ПК, УК) или специализированные, профессионально-специализированные компетенции (СК, ПСК)	Практический опыт	Умения	Знания
1	2	3	4	5
			мероприятия профилактической направленности по этичному поведению в сети Интернет и защите личного информационного пространства.	
	ОПК-9. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	Классификация различных видов вредоносного ПО. Установка ПО, позволяющее защитить личное информационное пространство.	Различать атаки, угрозы, исходящие из программного обеспечения, сети Интернет, социальных сетей в современных условиях с применением инструментов Лаборатории Касперского.	Понятие информационной безопасности и необходимость в организации защиты своего личного информационного пространства. Типы атак, угроз в сети Интернет, социальных сетей. Вредоносное программное обеспечение и ее виды. Стратегию различения атак и угроз, исходящих из сети Интернет, социальных сетей в современных условиях с применением инструментов Лаборатории Касперского.

Виды деятельности	Общепрофессиональные, профессиональные, универсальные компетенции (ОПК, ПК, УК) или специализированные, профессионально-специализированные компетенции (СК, ПСК)	Практический опыт	Умения	Знания
1	2	3	4	5
ВД 2. Получение теоретических и практических знаний, умений и навыков в области теории и методики обучения основам информационной безопасности в школьном курсе информатики.	ОПК-4. 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.	Построение траектории защиты личного информационного пространства от конкретного метода социальной инженерии.	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	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.

Виды деятельности	Общепрофессиональные, профессиональные, универсальные компетенции (ОПК, ПК, УК) или специализированные, профессионально-специализированные компетенции (СК, ПСК)	Практический опыт	Умения	Знания
1	2	3	4	5
			и защите личного информационного пространства.	
	ОПК-6. Способен использовать психолого-педагогические технологии в профессиональной деятельности, необходимые для индивидуализации обучения, развития, воспитания, в том числе обучающихся с особыми образовательными потребностями.	Конструирование и анализ уроков по информационной безопасности.	Использовать психолого-педагогические технологии в профессиональной деятельности, необходимые для индивидуализации обучения, развития, воспитания, в том числе, обучающихся с особыми образовательными потребностями.	Методические основы преподавания информационной безопасности в школьном курсе информатики.
	ОПК-8. Способен осуществлять педагогическую деятельность на основе специальных научных знаний.	Шифрование и дешифрование данных различными алгоритмами. Сокрытие и обнаружение информации в графических файлах. Решение конкретных математических задач.	Конструировать системы задач для обеспечение практической составляющей школьного курса информатики.	Математические основы в курсе информационной безопасности.

1.3. Категория слушателей

К освоению ДПП ПК допускаются без предъявления требований к стажу работы:

- лица, имеющие среднее профессиональное и (или) высшее образование;
- лица, получающие среднее профессиональное и (или) высшее образование.

Требования к квалификации – учителя информатики, учителя технологии, учителя математики и педагоги дополнительного образования, чей предмет взаимосвязан с информационной безопасностью.

1.4. Форма обучения и сроки освоения

Форма обучения – 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 40 академических часов.

1.5. Период обучения и режим занятий

Период обучения для каждого запуска программы определяется в индивидуальном режиме с учетом количества слушателей и составляет 4 недели, включая итоговую аттестацию.

1.6. Документ о квалификации

Лицам, успешно освоившим соответствующую ДПП ПК 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 ДПП ПК и (или) отчисленным из Учреждения, выдается справка об обучении или о периоде обучения по образцу, самостоятельно устанавливаемому Учреждением.

Раздел 2. Содержание программы

2.1. Учебный план

№ п/п	Наименование дисциплины (модуля)	Трудоемкость, ак.ч	Дистанционные занятия			СР, ак.ч	Промежуточная аттестация
			Всего, ак. ч.	в том числе			
				лекции	прак. занятия, семинары		
1	2	3	4	5	6	7	8
1	Представление об информационной безопасности	18	18	5	1	10	2
2	Основы криптологии	20	20	8	1	10	1
	Итоговая аттестация	2	2				
	Итого	40	40	13	2	20	3

2.2. Учебно-тематический план

№ п/п	Наименование дисциплины (модуля)	Всего, ак.ч	В том числе, ак.ч		
			Лекции	Самостоятельная работа	Практические занятия
1	2	3	4	5	6
Представление об информационной безопасности		**18**	**5**	**12**	**1**
1.1	Вводная лекция. Необходимость в информационной безопасности. Аутентификации и пароли	4	1	3	
1.2	Безопасность в мессенджерах	2	1	1	
1.3	Безопасность в браузерах	1		1	
Промежуточная аттестация по модулям 1.1-1.3		1		1	
1.4	Вредоносное программное обеспечение и различные уязвимости	3	1	2	
1.5	Антивирусные решения	2		2	
1.6	Социальная инженерия	4	2	2	
Промежуточная аттестация (практическая работа по модулю 1.6)		1			1
Основы криптологии		**20**	**8**	**11**	**1**
2.1	Криптология	2	1	1	
2.2	Стеганография	3	2	1	
Промежуточная аттестация (практическая		1			1

№ п/п	Наименование дисциплины (модуля)	Всего, ак.ч	В том числе, ак.ч		
			Лекции	Самостоятельная работа	Практические занятия
1	2	3	4	5	6
работа по модулю 2.2)					
2.3	Математические основы криптологии	3	1	2	
2.4	Симметричные методы шифрования	5	2	3	
2.5	Асимметричные методы шифрования	3	1	2	
2.6	Протокол Диффи-Хеллмана	1		1	
2.7	Машинное обучение, нейросети и информационная безопасность	2	1	1	
Итоговая аттестация		2			
Итого		40	13	23	2

2.3. Календарный учебный график

Период обучения (дни, недели*)	Наименование дисциплины (модуля)
**Даты обучения будут определены в расписании занятий при наборе группы на обучение*	

2.4. Рабочие программы дисциплин (модулей)

№ п/п	Содержание лекций (количество ак.ч.)	Наименование практических занятий или семинаров (количество ак.ч.)	Виды СР (количество ак.ч.)
1	2	3	4
1. Представление об информационной безопасности			
1	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.	Рассмотрение конкретных ситуаций социальной инженерии с проведением дискуссии. Практическая работа по построению траектории защиты личного информационного пространства от конкретного метода социальной инженерии. (1 ак.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. (10 ак.ч.)

№ п/п	Содержание лекций (количество ак.ч.)	Наименование практических занятий или семинаров (количество ак.ч.)	Виды СР (количество ак.ч.)
1	2	3	4
	Вредоносное программное обеспечение и ее типы. Уязвимость нулевого дня. Базы данных, SQL-инъекция. Антивирусные решения. Фишинг, вишинг, доксинг. Социальная инженерия и ее методы. (5 ак.ч.)		
2. Основы криптологии			
1	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. Машинное обучение и нейросети. (8 ак.ч.)	Практическая работа по стеганографии (извлечение скрытой информации из изображения с последующим поиском информации). (1 ак.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. (10 ак.ч.)

Раздел 3. Формы аттестации и оценочные материалы

ДПП ПК предусмотрены промежуточная и итоговая аттестации. Формой промежуточной аттестации является выполнение практических работ и тестирования. Формой итоговой аттестации является тестирование.

3.1. Промежуточная аттестация

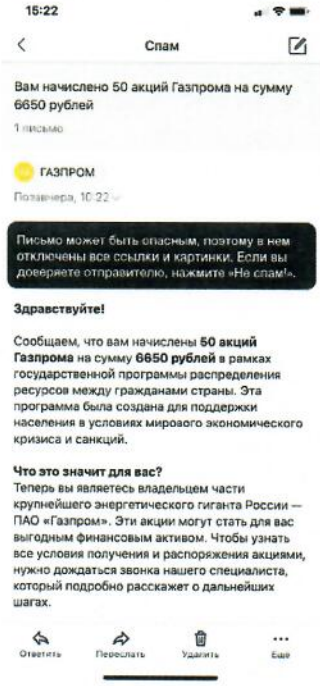
Промежуточная аттестация слушателей обеспечивает оценивание промежуточных результатов обучения по разделам (модулям) ДПП ПК. Содержание

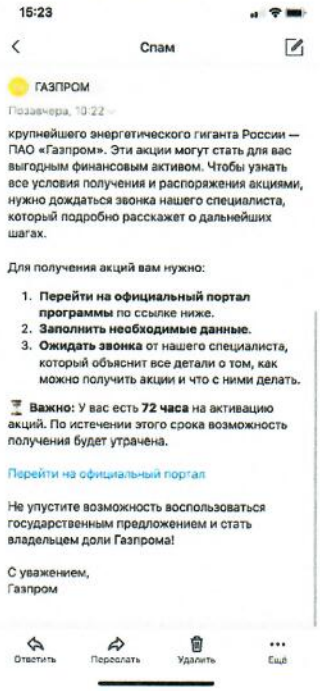
вопросов/заданий соответствует содержанию разделов (модулей). Промежуточная аттестация слушателей осуществляется в форме практических работ и тестирования. Успешное прохождение промежуточной аттестации является допуском к итоговой аттестации.

Типовые задания

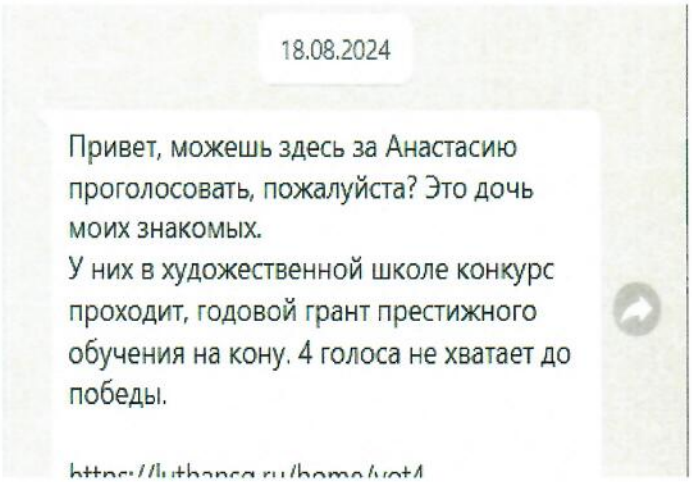
Примеры вопросов, ответы на которые необходимо рассмотреть в формате практической работы по теме «Социальная инженерия»:

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?

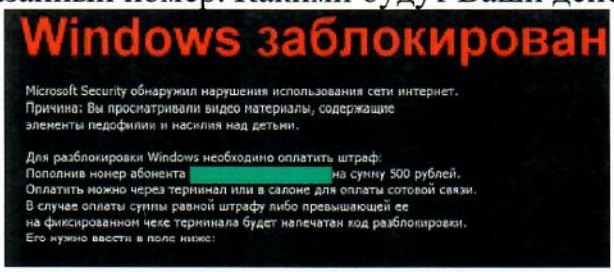




2. Вы получаете в мессенджере сообщение с просьбой проголосовать в конкурсе. Какими будут Ваши действия?



3. 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 практической работы 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 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 ДПП ПК, заявленным целям и планируемым результатам обучения, определяет уровень усвоения слушателями 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»).

Оценка «зачтено» выставляется если слушатель правильно определил истинность 8 и более высказываний предложенного теста. В противном случае выставляется оценка «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 литературы

Основная литература

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: 29.09.2025).

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, 2024. – 209 с. – (Высшее образование). – ISBN 978-5-9916-7088-3. – Текст: электронный //

Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/536733 (дата обращения: 30.09.2025).

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, 2024. – 245 с. – (Высшее образование). – ISBN 978-5-9916-7090-6. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/537383 (дата обращения: 02.10.2025).

Дополнительная литература

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, 2024. – 107 с. – (Высшее образование). – ISBN 978-5-534-16388-9. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/544290 (дата обращения: 30.09.2025).

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, 2024. – 473 с. – (Высшее образование). – ISBN 978-5-534-12474-3. – Текст: электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/536132 (дата обращения: 30.09.2025).

Электронные и интернет-ресурсы

1. Блог Касперского [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/blog/ (дата обращения: 01.10.2025).

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: 01.10.2025).

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: 25.09.2025).

4. Курс «Математика в кибербезопасности» на платформе Stepik [Электронный ресурс]. – Режим доступа: https://stepik.org/62247 (дата обращения: 01.10.2025).

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) Учреждения.

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

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, МойОфис;

– браузер, совместимый с Яндекс.Телемост и электронной информационно-образовательной средой Учреждения;

– 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 и (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, кандидат педагогических наук	Менеджер образовательных программ Лаборатории Касперского, кандидат педагогических наук	–	14	4	1. Представление об информационной безопасности. 2. Основы криптологии.
Савушкин Алан Сергеевич	Высшее образование, математика и компьютерные науки, магистр «Интеллектуальные системы. Теория и приложения»	Руководитель направления исследования данных Лаборатории Касперского	–	5	5	2. Основы криптологии. (Тема 2.7. Машинное обучение, нейросети и информационная безопасность).

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**
Сидорин Леонид Олегович	Высшее образование, инженер промышленного и гражданского строительства	Методист-преподаватель Хаба Знаний, МойОфис	Курсовая подготовка Ispring «Руководитель отдела обучения»	8	8	1. Представление об информационной безопасности. (Тема 1.2. Безопасность в мессенджерах).