Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

Институт цифровых компетенций

ОБСУЖДЕНО И ОДОБРЕНО
На Ученом совете институтов и
школ дополнительного
профессионального образования

Протокол от 19.04. 2022 г.
№ 12

УТВЕРЖДАЮ
Проректор по дополнительному
профессиональному образованию

_____ Е.А. Диденко
«19» 04 2022 г.

ПРОГРАММА
повышения квалификации

Аналитик кибербезопасности

Москва – 2022

Общая характеристика программы

Цель реализации программы: совершенствование (получение) компетенций и практических навыков, необходимых для профессиональной деятельности в области сетевых технологий, информационной и кибер-безопасности.

Планируемые результаты освоения программы: программа позволит слушателям повысить свой профессиональный уровень, сформировать (совершенствовать) профессиональные компетенции в области обеспечения безопасности информации компьютерных систем и сетей в условиях существования угроз их информационной безопасности.

В результате успешного освоения курса слушатель получает подготовку и базовые навыки работы и знания в области предотвращения, детектирования и расследования инцидентов безопасности в защищаемой корпоративной инфраструктуре в составе команды Центра обеспечения безопасности (Security operations center - SOC).

При разработке программы использованы:

1. Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 г. № 273-ФЗ.
2. Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам, утвержденного приказом Министерства образования и науки Российской Федерации от 01.07.2013 г. № 499.
3. Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 года № 598н (Зарегистрировано в Министерстве юстиции Российской Федерации 28 ноября 2016 года, регистрационный № 44464).

Трудовые функции выпускника по профессиональному стандарту «Специалист по безопасности компьютерных систем и сетей», код 06.032 (Защита информации в компьютерных системах и сетях)

Обобщенные трудовые функции			Трудовые функции		
код	наименование	уровень квалификации	наименование	код	уровень (подуровень) квалификации
A	Обслуживание средств защиты информации в компьютерных системах и сетях	5	Обслуживание программно-аппаратных средств защиты информации в операционных системах	A/01.5	5
			Обслуживание программно-аппаратных средств защиты	A/02.5	5

			информации в компьютерных сетях		
			Обслуживание средств защиты информации прикладного и системного программного обеспечения	A/03.5	5
B	Администрирование средств защиты информации в компьютерных системах и сетях	6	Администрирование подсистем защиты информации в операционных системах	B/01.6	6
			Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	B/02.6	6
			Администрирование средств защиты информации прикладного и системного программного обеспечения	B/03.6	6
C	Оценивание уровня безопасности компьютерных систем и сетей	7	Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	C/01.7	7
			Разработка требований по защите, формирование политик безопасности компьютерных систем и сетей	C/02.7	7
			Проведение анализа безопасности компьютерных систем	C/03.7	7
			Проведение сертификации программно-аппаратных средств защиты информации и анализ результатов	C/04.7	7
			Проведение инструментального мониторинга защищенности компьютерных систем и сетей	C/05.7	7

			Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	C/06.7	7
D	Разработка программно-аппаратных средств защиты информации компьютерных систем и сетей	8	Разработка требований к программно-аппаратным средствам защиты информации компьютерных систем и сетей	D/01.8	8
			Проектирование программно-аппаратных средств защиты информации компьютерных систем и сетей	D/02.8	8
			Разработка и тестирование средств защиты информации компьютерных систем и сетей	D/03.8	8
			Сопровождение разработки средств защиты информации компьютерных систем и сетей	D/04.8	8

Возможные наименования должностей, профессий лиц, окончивших программу:

- Техник по безопасности компьютерных систем и сетей
- Техник по защите информации I категории
- Техник по защите информации II категории
- Техник по защите информации
- Специалист по защите информации в компьютерных системах и сетях
- Эксперт по анализу защищенности компьютерных систем и сетей

Профессиональные компетенции, совершенствуемые и приобретаемые слушателями в процессе освоения программы:

- способность организовывать собственную деятельность, выбирая типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество;
- готовность принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность;

- готовность участвовать в мониторинге эффективности применяемых программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности в автоматизированных системах;
- способность применять нормативные правовые акты, нормативно-методические документы по обеспечению информационной безопасности инженерно-техническими средствами.

Планируемые результаты обучения по программе

В результате изучения программы слушатели должны:

знать:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- источники угроз информационной безопасности и меры по их предотвращению;
- жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;

уметь:

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- применять основные правила и документы системы сертификации Российской Федерации;
- классифицировать основные угрозы безопасности информации;

владеть:

- навыками проведения экспериментов по заданной методике, осуществлять обработку результатов, оценку погрешности и определять достоверность получаемых результатов; способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности
- навыками, позволяющими разрабатывать предложения по совершенствованию системы управления информационной безопасностью и формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью
- методом проведения анализа информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов и способностью проводить эксперименты по заданной методике, осуществлять обработку результатов, оценку погрешности и определять достоверность получаемых результатов.

Федеральное государственное образовательное бюджетное учреждение
высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

Институт цифровых компетенций

ОБСУЖДЕНО И ОДОБРЕНО
На Ученом совете институтов и
школ дополнительного
профессионального образования

Протокол от 19.04.22
№ 12

УТВЕРЖДАЮ
Проректор по дополнительному
профессиональному образованию

_____ Е.А. Диденко
«__» _____ 2022 г.

УЧЕБНЫЙ ПЛАН

программы повышения квалификации

АНАЛИТИК КИБЕРБЕЗОПАСНОСТИ

Требования к уровню образования слушателей	лица, имеющие высшее образование; лица, получающие высшее образование
Категории слушателей	ИТ-специалисты с базовыми знаниями основ кибербезопасности; лица, планирующие свою профессиональную деятельность области сетевых технологий, информационной и кибер-безопасности
Срок обучения	72 часа
Форма обучения	очно-заочная, с применением электронного обучения и дистанционных образовательных технологий
Режим занятий	не более 4 часов в день

№ № п/п	Наименование дисциплины, модуля	Трудоем-кость		В том числе				Форма контроля
				Аудиторные занятия*			Самостоятельная работа*	
		В зачетных единицах.	В часах	Всего часов	из них			
					Лек-ции	Практи-ческие занятия		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
1	**Модуль 1.** Основы и принципы кибербезопасности		39	21	11	10	18	Зачет методом тестирования
2	**Модуль 2.** Организация кибербезопасности		31	17	6	11	14	Зачет методом тестирования
3	**Всего:**		**68**	**38**	**17**	**21**	**32**	
4	**Итоговая аттестация**		**2**	**2**		**2**		Экзамен в форме защиты практической работы
5	**Общая трудоемкость программы:**	**2**	**72**	**40**	**17**	**23**	**32**	

Программа разработана Носковым Антоном Николаевичем эксперт-инструктором академии сетевых технологий, руководитель инновационного центра «Кибербезопасности и телекоммуникационных систем».

Занятия по программе повышения квалификации «Аналитик кибербезопасности» проводят ведущие профессора и доценты Финансового университета, а также приглашенные ведущие специалисты в сфере профессионального образования, имеющие сертификаты в области информационных технологий и кибербезопасности.

Директор
Института цифровых компетенций _____ М.А. Каткова
« 19 » 04 2022 г.

* с применением дистанционных образовательных технологий и электронного обучения

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

программы повышения квалификации

АНАЛИТИК КИБЕРБЕЗОПАСНОСТИ

№ п/п	Наименование раздела, темы	Всего часов трудоемкости	В том числе				Форма контроля
			Аудиторные занятия*			Самостоятельная работа*	
			Всего часов	из них			
				Лекции	Практические занятия		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1.	**Модуль 1. Основы и принципы кибербезопасности**	**39**	**21**	**11**	**10**	**18**	
2.	Тема 1.1. Кибербезопасность и центр мониторинга и управления безопасностью	3	2	2		1	Практическое задание
3.	Тема 1.2. Операционная система Windows	8	4	2	2	4	Практическое задание
4.	Тема 1.3. Операционная система Linux	6	4	2	2	2	Практическое задание
5.	Тема 1.4. Сетевые протоколы и службы	8	4	2	2	4	Практическое задание
6.	Тема 1.5. Сетевая инфраструктура	5	3	1	2	2	Тестирование
7.	Тема 1.6. Принципы обеспечения безопасности сети	8	4	2	2	4	Практическое задание
8.	Промежуточная аттестация	1				1	Зачет методом тестирования
9.	**Модуль 2. Организация кибербезопасности**	**31**	**17**	**6**	**11**	**14**	
10.	Тема 2.1. Сетевые атаки. Углубленный разбор	6	3	1	2	3	Тестирование
11.	Тема 2.2. Защита сети	8	4	2	2	4	Практическое задание
12.	Тема 2.3. Криптография и инфраструктура общих ключей	3	2	1	1	1	Тестирование
13.	Тема 2.4. Защита и анализ оконечных устройств	3	2		2	1	Практическое задание
14.	Тема 2.5. Мониторинг безопасности	4	2	1	1	2	Тестирование
15.	Тема 2.6. Анализ данных вторжений	4	3	1	2	1	Тестирование

* с применением дистанционных образовательных технологий и электронного обучения

№ п/п	Наименование раздела, темы	Всего часов трудоемкости	В том числе				Форма контроля
			Аудиторные занятия*			Самостоятельная работа*	
			Всего часов	из них			
				Лекции	Практические занятия		
16.	Тема 2.7. Реагирование на инциденты и их обработка	2	1		1	1	Практическое задание
17.	Промежуточная аттестация	1				1	Зачет методом тестирования
18.	**Итоговая аттестация**	**2**	**2**		**2**		Экзамен в форме защиты практической работы
19.	**Общая трудоемкость дисциплины:**	**72**	**40**	**17**	**23**	**32**	

Директор
Института цифровых компетенций _____ М.А. Каткова
« ____ » _____ 2022 г.

Календарный учебный график

Федеральное государственное образовательное бюджетное учреждение
высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)

Институт цифровых компетенций

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

программы повышения квалификации

АНАЛИТИК КИБЕРБЕЗОПАСНОСТИ

Объем программы 72 часа (2 з.е.). Продолжительность обучения 18 дней

Форма обучения – очно-заочная с применением ЭО и ДОТ

Образовательный процесс по программе может осуществляться в течение всего учебного года. Занятия проводятся по мере комплектования учебных групп.

№ п/п	Наименование дисциплины (модулей)	1 день	2 день	3 день	4 день	5 день	6 день	7 день	8 день	9 день	10 день	11 день	12 день	13 день	14 день	15 день	16 день	17 день	18 день	КР	СР	ИА	Всего
1	Тема 1.1. Кибербезопасность и центр мониторинга и управления безопасностью	3																		2	1		3
2	Тема 1.2. Операционная система Windows	1	4	3																4	4		8
3	Тема 1.3. Операционная система Linux			1	4	1														4	2		6
4	Тема 1.4. Сетевые протоколы и службы					3	4	1												4	4		8
5	Тема 1.5. Сетевая инфраструктура							3	2											3	2		5
6	Тема 1.6. Принципы обеспечения безопасности сети								2	4	2									4	4		8

№ п/п	Наименование дисциплины (модулей)	1 день	2 день	3 день	4 день	5 день	6 день	7 день	8 день	9 день	10 день	11 день	12 день	13 день	14 день	15 день	16 день	17 день	18 день	ПА	КР	СР	ИА	Всего
7	Промежуточная аттестация										1									1		1		1
8	Тема 2.1. Сетевые атаки. Углубленный разбор										1	4	1								3	3		6
9	Тема 2.2. Защита сети												3	4	1						4	4		8
10	Тема 2.3. Криптография и инфраструктура общих ключей														3						2	1		3
11	Тема 2.4. Защита и анализ оконечных устройств															3					2	1		3
12	Тема 2.5. Мониторинг безопасности															1	3				2	2		4
13	Тема 2.6. Анализ данных вторжений																1	3			3	1		4
14	Тема 2.7. Реагирование на инциденты и их обработка																	1	1		1	1		2
15	Промежуточная аттестация																		1	1		1		
16	**Итоговая аттестация**																		2		2		2	4
Всего		4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	2	40	32	2	72

Директор
Института цифровых компетенций
« 19 » 04 2022 г.

М.А. Каткова

Условные обозначения	
ПА	Промежуточная аттестация
П	Практика
С	Стажировка
ИА	Итоговая аттестация
КР	Контактная работа
СР	Самостоятельная работа