УЧЕБНЫЙ ПЛАН
программы профессиональной переподготовки
«КИБЕРБЕЗОПАСНОСТЬ»

№ п/п	Наименование модуля	Трудоемкость		В том числе				Форма контроля
				Внеаудиторные занятия			Самостоятельная работа*	
					из них			
		В зачетных единицах	В часах	Всего	Лекции*	Практические занятия		
1	Модуль 1. Основы информационной безопасности Модуль формирует понятийный аппарат дисциплины: свойства безопасности информации (конфиденциальность, целостность, доступность), модель угроз и модель нарушителя, классификацию актуальных атак. Слушатели знакомятся с историей отрасли, ключевыми векторами угроз современности и ролями участников рынка ИБ.	1	40	12	4	8	28	Зачет методом тестирования
2	Модуль 2. Нормативно-правовое регулирование в области защиты информации Рассматривается российская и международная правовая база: № 149-ФЗ, № 152-ФЗ, № 187-ФЗ, № 98-ФЗ, требования и методические документы ФСТЭК и ФСБ России. Отдельное внимание	1	40	12	4	8	28	Зачет методом тестирования

*С применением дистанционных образовательных технологий и электронного обучения

	уделяется обязанностям операторов персональных данных и субъектов критической информационной инфраструктуры.							
3	Модуль 3. Управление информационной безопасностью и оценка рисков Модуль посвящён построению системы менеджмента ИБ по ISO/IEC 27001: разработке политики безопасности, организации процессов СУИБ, проведению внутреннего аудита. Слушатели осваивают методики оценки рисков и учатся обосновывать выбор мер защиты.	1	40	12	4	8	28	Зачет методом тестирования
4	Модуль 4. Криптографические методы защиты информации Изучаются основы криптографии: симметричное и асимметричное шифрование, хэширование, электронная подпись, управление ключами и сертификатами. Практическая часть включает применение российских криптостандартов (ГОСТ) и сервисов ЭП в реальных задачах.	1	40	12	4	8	28	Зачет методом тестирования
5	Модуль 5. Безопасность сетевой инфраструктуры Разбирается архитектура защищённых сетей: сегментирование, межсетевые экраны, системы обнаружения и предотвращения вторжений (IDS/IPS), VPN-технологии. Слушатели получают навыки	1	40	12	4	8	28	Зачет методом тестирования

	администрирования средств сетевой защиты и анализа сетевого трафика.							
6	Модуль 6. Безопасность веб-приложений и защищённая разработка Модуль охватывает типовые уязвимости веб-приложений (SQL-инъекции, XSS, CSRF) и практики безопасной разработки (SDLC, OWASP Top 10). В ходе практикума слушатели выявляют уязвимости в учебных приложениях и устраняют их средствами защищённого программирования.	1	40	12	4	8	28	Зачет методом тестирования
7	Модуль 7. Защита данных: персональные данные, облака и резервирование Рассматриваются управление доступом, шифрование данных в покое и при передаче, построение систем резервного копирования и восстановления. Отдельные темы — обеспечение безопасности облачных сервисов (IaaS, PaaS, SaaS) и требования к обработке персональных данных.	1	40	12	4	8	28	Зачет методом тестирования
8	Модуль 8. Управление инцидентами информационной безопасности Модуль формирует навыки выявления, классификации и регистрации инцидентов ИБ, планирования реагирования и восстановления систем после атак. Включает основы цифровой криминалистики, противодействие социальной инженерии и организацию обучения персонала.	1	40	12	4	8	28	Зачет методом тестирования
9	Модуль 9. Современные технологии в обеспечении	1	40	12	4	8	28	Зачет методом тестирования

	информационной безопасности Модуль знакомит с перспективными направлениями отрасли: применением искусственного интеллекта и машинного обучения в защите, блокчейн-технологиями и квантовой криптографией. Слушатели оценивают новые технологии с точки зрения рисков и возможностей и осваивают средства автоматизации процессов ИБ.							
	Всего:	9	360	108	36	72	252	Зачет методом тестирования
	Итоговая аттестация		2					Экзамен методом тестирования
	Общая трудоемкость программы:	9	362	108	36	72	252	