

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уфимский государственный нефтяной технический университет»

УТВЕРЖДАЮ

Директор СЛФЛ

_____Н.Н. Лунева
(подпись)

29.06.2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

(6724)Информационная безопасность

Направление подготовки (специальность): **09.03.01 Информатика и вычислительная техника**

Направленность: **профиль«Технологии искусственного интеллекта в нефтегазовой отрасли»**

Уровень высшего образования: **бакалавриат**

Форма обучения: **очная;заочная;**

Кафедра, обеспечивающая преподавание дисциплины: **Информационных технологий (ИнТех);**

Трудоемкость дисциплины: **3 з.е. (108час)**

Салават 2023

Рабочую программу дисциплины разработал(и):

_____ ст. преподаватель, А.Г. Филиппова

_____ ст. преподаватель, Е.Ю Головина

Рецензент

_____ доцент, канд.тех.наук Т.М. Левина

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры Информационных технологий (ИнТех);, обеспечивающей преподавание дисциплины 29.05.2023, протокол №6.

Заведующий кафедрой

Информационных технологий (ИнТех)_____ Т.М. Левина

СОГЛАСОВАНО

Заведующий кафедрой ИнТех_____ Т.М. Левина

Год приема 2023 г.

Рабочая программа зарегистрирована 08.06.2023 № 6 в ОПЛА и внесена в электронную базу данных

1. Место дисциплины в структуре ОПОП ВО

Дисциплины, предшествующие изучению данной дисциплины (исходя из формирования этапов по компетенциям): Дискретная математика;Инженерная компьютерная графика;Информационные технологии;Информационные технологии (базовый уровень);Информационные технологии (продвинутый уровень) "Инструментарий математического моделирования и анализа данных";Информационные технологии (продвинутый уровень) "Инструментарий облачных вычислительных сервисов и систем искусственного интеллекта";Математическая логика и теория алгоритмов;Методика научно-исследовательской работы;Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы);Ознакомительная практика;Программирование;Системы искусственного интеллекта

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее (исходя из формирования этапов по компетенциям): Организация и управление научно-исследовательской деятельностью в сфере информационных технологий (проектная деятельность);Разработка информационно-управляющих систем;Сети и телекоммуникации

Блок: Блок 1. Дисциплины (модули);

Обязательная или часть, формируемая участниками образовательных отношений (в том числе элективные дисциплины): Обязательная часть;

Форма обучения: очная

Семестр, в котором преподается дисциплина	Трудоемкость дисциплины				Вид промежу- точной аттестации
	Зачет- ные едини- цы	Часы			
		Общая	В том числе		
			контакт- ная	СРО	
5	3	108	48	60	экзамен;
ИТОГО:	3	108	48	60	

Форма обучения: заочная

Семестр, в котором преподается дисциплина	Трудоемкость дисциплины				Вид промежу- точной аттестации
	Зачет- ные едини- цы	Часы			
		Общая	В том числе		
			контакт- ная	СРО	
5	3	108	16	92	экзамен;
ИТОГО:	3	108	16	92	

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

№ пп.	Формируемые компетенции	Шифр/индекс компетенции
1	Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	ОПК-2-22Г.-4
2	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3-22Г.-5
3	Способен разрабатывать алгоритмы и программы, пригодные для практического применения	ОПК-8-22Г.-3
4	Способен планировать и организовывать свою деятельность в цифровом пространстве с учётом правовых и этических норм взаимодействия человека и искусственного интеллекта и требований информационной безопасности	УК-и-11-2

В результате освоения дисциплины обучающийся должен:

Шифр компетенции	Индикаторы достижения компетенций	Шифр результата обучения	Результат обучения
ОПК-2-22Г.	ОПК 2.1 Знает современные информационные технологии и программные средства, в том числе отечественного производства, применяет их при решении задач профессиональной деятельности	З(ОПК-2-22Г.)	Знать: применимость современных информационных технологий и программных средств
		У(ОПК-2-22Г.)	Уметь: использовать современные информационные технологии

Шифр компетенции	Индикаторы достижения компетенций	Шифр результата обучения	Результат обучения
			при решении задач профессиональной деятельности
		В(ОПК-2-22Г.)	Владеть: навыками использования современных информационных технологий при решении задач профессиональной деятельности
ОПК-3-22Г.	ОПК 3.1 Знает основные принципы, методы и средства решения стандартных задач профессиональной деятельности	З(ОПК-3-22Г.)	Знать: основные требования, применяемые к информационной безопасности
		У(ОПК-3-22Г.)	Уметь: способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры
		В(ОПК-3-22Г.)	Владеть: навыками решения стандартных задач профессиональной деятельности с учетом требований информационной безопасности
ОПК-8-22Г.	ОПК 8.3 Интегрирует программные модули в инструментальные среды	З(ОПК-8-22Г.)	Знать: подходы интеграции программного модуля в инструментальные среды
		У(ОПК-8-22Г.)	Уметь: осуществлять интеграцию программного модуля в инстру-

Шифр компетенции	Индикаторы достижения компетенций	Шифр результата обучения	Результат обучения
			ментальные среды
		В(ОПК-8-22Г.)	Владеть: способностями интеграции программного модуля в инструментальные среды
УК-и-11	УК-11.2 Использует технологии сбора, обработки, интерпретации, анализа и обмена информацией с учётом требований информационной безопасности	З(УК-и-11)	Знать: подходы к организации деятельности в цифровом пространстве с учетом правовых и этических норм взаимодействия человека и искусственного интеллекта
		У(УК-и-11)	Уметь: осуществлять планирование и организацию своей деятельности в цифровом пространстве
		В(УК-и-11)	Владеть: способностями по организации своей деятельности в цифровом пространстве с учетом правовых и этических норм взаимодействия человека и искусственного интеллекта

3. Структура дисциплины

3.1. Виды учебной работы и трудоемкость (всего и по семестрам, в часах)

Форма обучения: очная

Вид учебной работы	Всего и по семестрам, часы	1	2	3	4	5	6	7	8	9	10	11	12

Контактная работа, всего в том числе:	48					48							
лекции (всего)	16					16							
-в т.ч. лекции on-line курс	0												
практические занятия (ПЗ)	8					8							
-в т.ч. практические занятия on-line курс	0												
лабораторные работы (ЛР)	18					18							
контролируемая самостоятельная работа (защита курсового проекта, курсовой работы и др. работ (при наличии))	0												
-в т.ч. лабораторные работы on-line курс	0												
иная контактная работа (сдача зачета, экзамена, консультации)	6					6							
проектная деятельность (ПД)	0												
Самостоятельная работа обучающихся (СРО), всего в том числе: (указать конкретный вид СРО)	60					60							
выполнение и подготовка к защите курсового проекта или курсовой работы	0												
выполнение и подготовка к защите РГР работы, реферата, патентных исследований, аналитических исследований и т.п	0												
изучение учебного материала, вынесенного на самостоятельную проработку	17					17							
подготовка к лабораторным и/или практическим занятиям	20					20							
подготовка к сдаче зачета, экзамена	23					23							
иные виды работ обучающегося (при наличии)	0												
освоение on-line курса	0												
самостоятельная проектная деятельность (СПД)	0												
ИТОГО ПО ДИСЦИПЛИНЕ	108					108							

Форма обучения: заочная

Вид учебной работы	Всего и по семестрам, часы	1	2	3	4	5	6	7	8	9	10	11	12
Контактная работа, всего в том числе:	16					16							

лекции (всего)	4					4							
-в т.ч. лекции on-line курс	0												
практические занятия (ПЗ)	2					2							
-в т.ч. практические занятия on-line курс	0												
лабораторные работы (ЛР)	4					4							
контролируемая самостоятельная работа (защита курсового проекта, курсовой работы и др. работ (при наличии))	0												
-в т.ч. лабораторные работы on-line курс	0												
иная контактная работа (сдача зачета, экзамена, консультации)	6					6							
проектная деятельность (ПД)	0												
Самостоятельная работа обучающихся (СРО), всего в том числе: (указать конкретный вид СРО)	92					92							
выполнение и подготовка к защите курсового проекта или курсовой работы	0												
выполнение и подготовка к защите РГР работы, реферата, патентных исследований, аналитических исследований и т.п	0												
изучение учебного материала, вынесенного на самостоятельную проработку	49					49							
подготовка к лабораторным и/или практическим занятиям	20					20							
подготовка к сдаче зачета, экзамена	23					23							
иные виды работ обучающегося (при наличии)	0												
освоение on-line курса	0												
самостоятельная проектная деятельность (СПД)	0												
ИТОГО ПО ДИСЦИПЛИНЕ	108					108							

4. Содержание дисциплины

4.1. Темы (разделы) дисциплины и виды занятий (в часах)

Форма обучения: очная

(раздела)Номер темы	Название темы (раздела)	Семестр	Трудоемкость, часы					Шифр результата обучения
			Л	ПЗ	ЛР	СРО	Всего	
1	Инфор-	5	4	2	4	15	25	З(УК-и-

Номер темы	Назва- ние	Семес- тр	Трудоемкость, часы					Шифр ре-
			Л	ПЗ	ЛР	СРО	Всего	
	мацион- ная без- опас- ность и уровни ее обес- печения							11) У(УК-и- 11) В(УК-и- 11)
2	Про- граммно- техни- ческие аспекты обеспе- чения защиты инфор- мации	5	4	2	4	16	26	3(ОПК- 8-22Г.) У(ОПК- 8-22Г.) В(ОПК- 8-22Г.)
3	Основ- ные на- прав- ления по созда- нию си- стем комплек- сной за- щиты инфор- мацион- ной си- стемы пред- приятия	5	4	2	4	15	25	3(ОПК- 3-22Г.) У(ОПК- 3-22Г.) В(ОПК- 3-22Г.)
4	Основы управле- ния ин- форма- ционной безопас- ностью пред- приятия	5	4	2	6	14	26	3(ОПК- 2-22Г.) У(ОПК- 2-22Г.) В(ОПК- 2-22Г.)
	ИТОГО:		16	8	18	60	102	

Форма обучения: заочная

(раздела)Номер темы	Назва- ние темы (разде- ла)	Семестр	Трудоемкость, часы					Шифр ре- зульта- та обу- чения
			Л	ПЗ	ЛР	СРО	Всего	
1	Инфор- мацион- ная без- опас- ность и	5	1		2	22	25	3(УК-и- 11) У(УК-и- 11) В(УК-и-

Номер темы	Назва- ние	Семес- тр	Трудоемкость, часы					Шифр ре-
			Л	ПЗ	ЛР	СРО	Всего	
	уровни ее обеспе- чения							11)
2	Про- граммно- техни- ческие аспекты обеспе- чения защиты инфор- мации	5	1	2		20	23	З(ОПК- 8-22Г.) У(ОПК- 8-22Г.) В(ОПК- 8-22Г.)
3	Основ- ные напав- ления по созда- нию си- стем комплекс- ной за- щиты инфор- мацион- ной си- стемы пред- приятия	5	1		1	20	22	З(ОПК- 3-22Г.) У(ОПК- 3-22Г.) В(ОПК- 3-22Г.)
4	Основы управле- ния ин- формаци- онной безопас- ностью пред- приятия	5	1		1	30	32	З(ОПК- 2-22Г.) У(ОПК- 2-22Г.) В(ОПК- 2-22Г.)
	ИТОГО:		4	2	4	92	102	

4.2. Содержание лекционного курса

№ пп.	Номер раздела	Название темы	Трудоемкость, часы		
			очная	очно- заочная	заочная
1	1-Информационная безопасность и уров- ни ее обеспечения	Информацион- ная безопас- ность и ее основные со- ставляющие Информация и информацион- ный обмен; Ин- формация и ее за- щита; Компью- терные преступ-	4		1

		ления и способы их совершения; Пользователи и злоумышленники; Доктрины информационной безопасности			
2	2-Программно-технические аспекты обеспечения защиты информации	Программно-технические средства защиты информации от несанкционированного доступа Программно-технический уровень и сервисы информационной безопасности. Программно-технические средства защиты от несанкционированного доступа.	4		1
3	3-Основные направления по созданию систем комплексной защиты информационной системы предприятия	Комплексная система защиты информации на предприятии Подходы к проектированию систем защиты информации; Понятие и назначение комплексной системы защиты информации; Выработка политики безопасности предприятия; Основные требования, предъявляемые к комплексной системе защиты информации.	4		1
4	4-Основы управления информационной безопасностью предприятия	Инфраструктура и средства управления информационной безопасностью на предприятии Средства управления информационной безопасностью. Оценка рисков нарушения безопасно-	4		1

		сти. Факторы, необходимые для успешной реализации системы информационной безопасности в организации. Политика информационной безопасности. Документ о политике информационной безопасности.			
	-	ИТОГО:	16		4

4.3. Перечень лабораторных работ

Номер раздела	№ ЛР	Название лабораторной работы	Трудоемкость, часы		
			очная	очно-заочная	заочная
1-Информационная безопасность и уровни ее обеспечения	1	Оценка стойкости парольной защиты Подсистемы идентификации и аутентификации пользователя. Стойкость подсистемы идентификации и аутентификации пользователя в системе защиты информации. Методы парольной аутентификации. Требования к выбору пароля и к подсистеме парольной аутентификации пользователя. Количественная оценка стойкости парольной защиты	2		2
1-Информационная безопасность и уровни ее обеспечения	2	Реализация генератора паролей с заданными требова-	2		

		ниями Стойкость к взлому подсистемы парольной идентификации и аутентификации. Основные требования при выборе пароля пользователя. Реализация программы – генератор паролей.			
2-Программно-технические аспекты обеспечения защиты информации	3	Анализ рисков информационной безопасности Анализ рисков информационной безопасности Уязвимости и угрозы для организации. Идентификация и оценка рисков. Измерения рисков. Программные комплексы: CRAMM, RiskWatch, MSAT, ГРИФ, CORAS.	2		
2-Программно-технические аспекты обеспечения защиты информации	4	Оценка рисков информационной безопасности в Microsoft Security Assessment Tool (MSAT) Бизнес-модель компании, оценка риск для бизнеса, создание профиля риска для бизнеса (ПРБ). Защита инфраструктуры (защита периметра, аутентификация...), защита на уровне приложений, анализ безопасности операций (политика безопасности, политика резерв-	2		

		ного копирования и т.д.).			
3-Основные направления по созданию систем комплексной защиты информационной системы предприятия	5	Функциональная модель обеспечения информационной безопасности Функциональная декомпозиция процесса разработки внедрения и эксплуатации системы комплексной защиты информации (СКЗИ). Моделирование процессов СКЗИ с использованием методологии IDEF.	2		1
3-Основные направления по созданию систем комплексной защиты информационной системы предприятия	6	Визуальное моделирование систем информационной безопасности Определения требований к системе. Моделирование прецедентов и актеров. Семантические связи.	2		
4-Основы управления информационной безопасностью предприятия	7	Дискреционное управление доступом Права доступа пользователей-субъектов к объектам компьютерной системы. Матрица доступа. Множество пользователей и объектов	3		1
4-Основы управления информационной безопасностью предприятия	8	Реализация мандатной модели политики безопасности Многоуровневые модели.	3		

		Права доступа субъекта. Характеристики конфиденциальности объекта. Совокупности уровня конфиденциальности и набора категорий конфиденциальности			
-		ИТОГО:	18		4

4.4. Перечень практических занятий

Номер раздела	№ ПЗ	Тема практического занятия	Трудоемкость, часы		
			очная	очно-заочная	заочная
1-Информационная безопасность и уровни ее обеспечения	1	Проверка качества сгенерированного пароля Проверка паролей разной степени сложности, с помощью электронных ресурсов: Сервис 2ip, 2ip.online, измеритель сложности пароля passwordmeter, Касперский.	2		
2-Программно-технические аспекты обеспечения защиты информации	2	Пакеты антивирусных программ Антивирусные программные продукты. Наименования показателей для сравнения: Алгоритм нахождения вируса, Анализ поведения программ, Проверка макросов, Проверка скрипов, Структура программной системы, Число поддерживаемых	2		2

		мых семейств ОС, Объем дистрибутива (Мб).			
3-Основные направления по созданию систем комплексной защиты информационной системы предприятия	3	Оптимальное построение системы защиты для автоматизированных систем Свойства параметров исследуемых объектов. Внешние и внутренние параметра автоматизированных систем (АС). Размерность векторного критерия оптимальности, нормализация и свертка его компонент. Методы поиска решений внутри области компромиссов. Решение задачи оптимального проектирования СЗИ АС	2		
4-Основы управления информационной безопасностью предприятия	4	Политика информационной безопасности предприятия Изучение шаблонов документов, описывающих политику информационной безопасности организации, представленные в разделе "Политика безопасности" сайта SecurityPolicy.ru. Практические навыки разработки политики информационной безопасности с учетом нужд конкретной организа-	2		

		ции и приня- тых стан- дартов. Груп- повая полити- ка.			
-		ИТОГО:	8		2

4.5. Виды СРО

Номер раздела	Вид СРО	Трудоемкость, часы		
		очная	очно- заочная	заочная
1-Информационная безопасность и уровни ее обеспечения	подготовка к сда- че зачета, экзаме- на	5		5
1-Информационная безопасность и уровни ее обеспечения	подготовка к ла- бораторным и/или практиче- ским занятиям	5		5
1-Информационная безопасность и уровни ее обеспечения	изучение учебно- го материала, вы- несенного на самостоятельную проработку	5		12
2-Программно-технические аспекты обеспечения защиты информации	подготовка к сда- че зачета, экзаме- на	6		6
2-Программно-технические аспекты обеспечения защиты информации	подготовка к ла- бораторным и/или практиче- ским занятиям	5		5
2-Программно-технические аспекты обеспечения защиты информации	изучение учебно- го материала, вы- несенного на самостоятельную проработку	5		9
3-Основные направления по созданию систем комплекс- ной защиты информационной системы предприятия	подготовка к сда- че зачета, экзаме- на	6		6
3-Основные направления по созданию систем комплекс- ной защиты информационной системы предприятия	подготовка к ла- бораторным и/или практиче- ским занятиям	5		5
3-Основные направления по созданию систем комплекс- ной защиты информационной системы предприятия	изучение учебно- го материала, вы- несенного на самостоятельную	4		9

	проработку			
4-Основы управления информационной безопасностью предприятия	подготовка к сдаче зачета, экзамена	6		6
4-Основы управления информационной безопасностью предприятия	подготовка к лабораторным и/или практическим занятиям	5		5
4-Основы управления информационной безопасностью предприятия	изучение учебного материала, вынесенного на самостоятельную проработку	3		19
-	ИТОГО:	60		92

Темы для самостоятельной работы обучающихся

Раздел 1. Информационная безопасность и уровни ее обеспечения

Основные составляющие информационной безопасности; Доступность, целостность и конфиденциальность информационных ресурсов; Доктрина информационной безопасности Российской Федерации; Объектно-ориентированный подход к информационной безопасности. Основные направления информационной безопасности.

Раздел 2. Программно-технические аспекты обеспечения защиты информации

Специальные технические средства и программы для них; Организационные средства и средства администрирования; Средства антивирусной защиты; Системные средства резервного архивирования данных; Средства оценки уязвимости компьютерных систем; Средства детектирования попыток взлома и проникновения

Раздел 3. Основные направления по созданию систем комплексной защиты информационной системы предприятия

Подходы к проектированию систем защиты информации; Понятие комплексной системы защиты информации; Назначение комплексной системы защиты информации; Принципы построения комплексной системы защиты информации; Стратегии защиты информации; Выработка политики безопасности; Основные требования, предъявляемые к комплексной системе защиты информации

Раздел 4. Основы управления информационной безопасностью предприятия

Стандарты информационной безопасности ISO, COBIT, ITIL; Средства управления информационной безопасностью. Ключевые средства контроля. Группы требований к информационной безопасности организации; Оценка рисков нарушения безопасности. Факторы, необходимые для успешной реализации системы информационной безопасности в организации; Инфраструктура информационной безопасности

5. Формы текущего контроля успеваемости и проведения промежуточной аттестации

Перечень оценочных средств текущего контроля и промежуточной аттестации по дисциплине приведен Фонде оценочных средств (приложение Б).

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Учебно-методическое обеспечение

Сведения об обеспеченности дисциплины основной, дополнительной и учебно-методической литературой приведены в формах № 1-УЛ и № 2-УЛ (приложение А).

6.2. Перечень современных профессиональных баз данных и информационных справочных систем, рекомендуемых для освоения дисциплины

Названия современных профессиональных баз данных и информационных справочных систем, рекомендуемых для освоения дисциплины	Ссылки на официальные сайты
Консультант-плюс	http://www.consultant.ru/
Научная электронная библиотека eLibrary	http://elibrary.ru/
Национальный Открытый Университет "ИНТУИТ"	https://www.intuit.ru
ЭБС Znanium.com	http://znanium.com/
ЭБС Лань	https://e.lanbook.com/
Электронная библиотека УГНТУ	http://www.bibl.rusoil.net
	https://msdn.microsoft.com/ru-ru/

7. Материально-техническое обеспечение дисциплины

7.1. Перечень специальных аудиторий, кабинетов, лабораторий и пр., используемых при реализации дисциплины с перечнем основного оборудования

№ пп.	Номер помещения	Оснащенность помещения (перечень основного оборудования)	Наименование помещения
1	Учебный-102	Компьютер в сборе - 10 шт.; Принтер Canon LBP3000; Доступ к электронной информационно-образовательной среде (Корпоративная информационная система УГНТУ); Доступ в интернет;	Помещение для самостоятельной работы – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечено доступом в электронную информационно-образовательную среду организации.
2	Учебный-108	Компьютер в сборе - 16 шт.; Плоттер HP Designjet 500; Принтер HP DeskJet 1220C; Принтер hp LaserJet 5200; Сканер HP 4370; Доступ к электронной информационно-образовательной среде (Корпоративная информационная система УГНТУ); Доступ в интернет;	Помещение для самостоятельной работы – укомплектовано специализированной (учебной) мебелью, оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечено доступом в электронную информационно-образовательную среду организации.
3	Учебный-111	Шкаф(ы) для хранения	Помещения для хранения и профилактического обслуживания учебного оборудования
4	Учебный-214	Доска интерактивная SMART Boards; ПЭВМ DC 38CD 2 GB/160 SATA/DVD/19"; Учебно-наглядные пособия по дисциплине, набор демонстрационного оборудования; Столы, стулья;	Учебная аудитория для проведения занятий лекционного типа – укомплектована специализированной (учебной) мебелью, набором демонстрационного оборудования и учебно-наглядными пособиями, обеспечивающими тематические иллюстрации, соответствующие рабочим учебным программам дисциплин (модулей).
5	Учебный-310	Компьютер в сборе PowerCool (AMD Ryzen 5 1600X/ASRock A320M-DVS/8Gb2666/1Tb/GT710/PowerCool600W/LG 21.5" 22MK430H-B/Oklick 90M/CBR CM 104) - 20 шт.; Столы, стулья	Учебная аудитория для проведения занятий семинарского типа – укомплектована специализированной (учебной) мебелью, техническими средствами обучения.
6	Учебный-310	Компьютер в сборе PowerCool (AMD Ryzen 5 1600X/ASRock A320M-DVS/8Gb2666/1Tb/GT710/PowerCool600W/LG 21.5" 22MK430H-B/Oklick 90M/CBR CM 104) - 20 шт.; Столы, стулья	Учебная аудитория для проведения групповых и индивидуальных консультаций
7	Учебный-310	Компьютер в сборе PowerCool (AMD Ryzen 5 1600X/ASRock A320M-DVS/8Gb2666/1Tb/GT710/PowerCool600W/LG 21.5" 22MK430H-20	Учебная аудитория для текущего контроля и промежуточной аттестации – укомплектована специализированной (учебной) ме-

7.2. Перечень лицензионного и свободно распространяемого программного обеспечения, используемых в учебном процессе при освоении дисциплины

№ пп.	Наименование ПО	Лицензионная чистота (реквизиты лицензии, свидетельства о гос. регистрации и т.п., срок действия)
1	Java v8	Дата выдачи лицензии 01.01.2000, Поставщик: Свободное программное обеспечение
2	Microsoft Office	Дата выдачи лицензии 01.01.2007
3	Python	Дата выдачи лицензии 01.01.1991, Поставщик: Свободное программное обеспечение
4	RAD Studio XE Professional Academic Workstation ESD	Дата выдачи лицензии 29.07.2011
5	Visio Professional 2013	Дата выдачи лицензии 17.12.2013, Поставщик: ЗАО «СофтЛайн Трэйд»
6	Антивирус Kaspersky	Дата выдачи лицензии 27.10.2010

8. Организация обучения лиц с ограниченными возможностями здоровья

Для лиц с ограниченными возможностями здоровья, обучающихся по данной образовательной программе, разрабатывается индивидуальная программа освоения дисциплины с учетом особенностей их психофизического развития, их индивидуальных возможностей и состояния здоровья.

Приложение А

Форма № УЛ-1

СВЕДЕНИЯ

об обеспеченности дисциплины основной и дополнительной учебной литературой

Наименование дисциплины: (6724)(6724)Информационная безопасностьНаправление подготовки (специальность): 09.03.01 Информатика и вычислительная техникаНаправленность: профиль«Технологии искусственного интеллекта в нефтегазовой отрасли»Форма обучения: очная;заочная;Кафедра, обеспечивающая преподавание дисциплины: Информационных технологий (ИнТех);

Тип	Назначение учебных изданий	Семестр			Библиографическое описание	Кол-во экз.	Адрес нахождения электронного	Кoeffициент
		очная	очно-заочная	заочная				
1	2	3	4	5	6	7	8	9
Основная литература	Для выполнения СРО;Для изучения теории;	5		5	Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-46010-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/293009	1	http://www.e.lanbook.com	1.00

Основная литература	Для выполнения СРО; Для выполнения лабораторных работ; Для изучения теории;	5		5	Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6 . - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861657	1	http://www.znanium.com	1.00
Основная литература	Для выполнения СРО; Для изучения теории;	5		5	Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401	1	http://www.e.lanbook.com	1.00
Дополнительная литература	Для выполнения СРО; Для выполнения практических занятий; Для изучения теории;	5		5	Груздева, Л. М. Защита информации : учебное пособие / Л. М. Груздева. — Москва : РУТ (МИИТ), 2019. — 144 с. — ISBN 978-5-7876-0326-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/188703	1	http://www.e.lanbook.com	1.00

Дополнительная литература	Для выполнения СРО; Для выполнения лабораторных работ; Для выполнения практических занятий; Для изучения теории;	5		5	Филиппова, А. Г. Средства и методы защиты компьютерной информации : учебное пособие / А. Г. Филиппова, В. Н. Филиппов ; УГНТУ, каф. ВТИК. - Уфа : УГНТУ, 2022. - 2,74 Мб. - URL: http://bibl.rusoil.net/base_docs/UGNTU/VTIK/Filippov15509.pdf . - Текст : электронный.	1	http://bibl.rusoil.net	1.00
Дополнительная литература	Для выполнения лабораторных работ; Для выполнения практических занятий;	5		5	Информационная безопасность : учебное пособие / УГНТУ, каф. ВТИК ; сост.: В. Н. Филиппов [и др.]. - Уфа : УГНТУ, 2022. - 4,31 Мб. - URL: http://bibl.rusoil.net/base_docs/UGNTU/VTIK/Filippov15508.pdf . - Текст : электронный.	1	http://bibl.rusoil.net	1.00
Примечание – Графы 1-5,8 заполняются кафедрой, графы 7 и 9 - библиотекой								

Составил:

_____ ст. преподаватель, А.Г. Филиппова

_____ ст. преподаватель, Е.Ю Головина

Год приема 2023 г.

СВЕДЕНИЯ**об обеспеченности дисциплины учебно-методическими изданиями**

Наименование дисциплины: (6724)(6724)Информационная безопасность

Направление подготовки (специальность): 09.03.01 Информатика и вычислительная техника

Направленность профиль«Технологии искусственного интеллекта в нефтегазовой отрасли»

Форма обучения очная;заочная;

Кафедра, обеспечивающая преподавание дисциплины: Информационных технологий (ИнТех);

Назначение учебных изданий	Семестр			Библиографическое описание	Кол-во экз.		Адрес нахождения электронного	Коэффициент
	очная	очно-заочная	заочная		Всего	в том числе		
1	2	3	4	5	6	7	8	9
Для выполнения СРО;Для выполнения лабораторных работ;Для выполнения практических занятий;	5		5	Информационная безопасность : учебно-методическое пособие для выполнения практических, лабораторных работ и СРО / УГНТУ, Салават. фил., каф. ИнТех ; сост. Е. Ю. Головина. - Салават : УГНТУ, 2022. - 1,99 Мб. - Текст : электронный. http://bibl.rusoil.net/base_docs/UGNTU/Salawat/Golovina13697.pdf	1	0	http://bibl.rusoil.net	1.00

Для выполнения СРО;Для выполнения лабораторных работ;Для выполнения практических занятий;	5		5	Информационная безопасность : учебно-методическое пособие для проведения лабораторных работ и практических занятий / УГНТУ, ИЭС, каф. ЦТиМ ; сост. И. Р. Ахуннов. - Уфа : УГНТУ, 2018. - 9167 Кб.http://bibl.rusoil.net/base_docs/UGNTU/IES/Akhunov6.pdf	1	0	http://bibl.rusoil.net	1.00
Для выполнения лабораторных работ;Для выполнения практических занятий;	5		5	Информационная безопасность в информационных технологиях : учебно-методическое пособие для выполнения практических работ и СРО / УГНТУ, Салават. фил., каф. ИнТех ; сост. Е. Ю. Головина. - Салават, 2019. - 1,36 Мб. - URL: http://bibl.rusoil.net/base_docs/UGNTU/Salawat/Golovina6.pdf	1	0	http://bibl.rusoil.net	1.00
Примечание – Графы 1-5,8 заполняются кафедрой, графы 6,7 и 9 - библиотекой								

Составил:

ст. преподаватель, А.Г. Филиппова

—

ст. преподаватель, Е.Ю Головина

—

Год приема 2023 г.

Приложение Б

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Уфимский государственный нефтяной технический университет»

УТВЕРЖДАЮ

Директор СЛФЛ

_____ Н.Н. Лунева
29.06.2023

**Фонд оценочных средств по текущей успеваемости и промежуточной аттестации по дисциплине
(6724)Информационная безопасность**

Направление подготовки (специальность): 09.03.01 Информатика и вычислительная техника

Направленность: профиль «Технологии искусственного интеллекта в нефтегазовой отрасли»

Уровень высшего образования: бакалавриат

Форма обучения: очная;заочная;

Кафедра, обеспечивающая преподавание дисциплины: Информационных технологий (ИнТех);

Трудоемкость дисциплины: 3 з.е. (108час)

Салават 2023

ФОС по текущей успеваемости и промежуточной аттестации по дисциплине разработал (и):

_____ ст. преподаватель, А.Г. Филиппова

—

_____ ст. преподаватель, Е.Ю Головина

—

Рецензент

_____ доцент, канд.тех.наук Т.М. Левина

—

ФОС по текущей успеваемости и промежуточной аттестации по дисциплине рассмотрен и одобрен на заседании кафедры Информационных технологий (ИнТех);, обеспечивающей преподавание дисциплины 29.05.2023, протокол №6.

Заведующий кафедрой Информационных технологий (ИнТех); _____ Т.М. Левина

СОГЛАСОВАНО

Заведующий кафедрой ИнТех _____ Т.М. Левина

Год приема 2023 г.

ФОС по текущей успеваемости и промежуточной аттестации по дисциплине
зарегистрирован 08.06.2023 № 6 в отделе МСОП и внесен в электронную базу данных

1. Паспорт фонда оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины	Шифр результата обучения	Результат обучения	Индикатор достижения компетенций	Показатели достижения результатов освоения компетенций	Вид оценочного средства
1	Информационная безопасность и уровни ее обеспечения	В(УК-и-11)	подходы к организации деятельности в цифровом пространстве с учетом правовых и этических норм взаимодействия человека и искусственного интеллекта	УК-11.2 Использует технологии сбора, обработки, интерпретации, анализа и обмена информацией с учётом требований информационной безопасности	студент должен показать минимальное владение подходами организации деятельности в цифровом пространстве	Компьютерное тестирование Лабораторная работа Письменный и устный опрос Реферат
		З(УК-и-11)		УК-11.2 Использует технологии сбора, обработки, интерпретации, анализа и обмена информацией с учётом требований информационной безопасности	студент должен показать минимальные знания подходов к организации деятельности в цифровом пространстве	Компьютерное тестирование Лабораторная работа Письменный и устный опрос Реферат
		У(УК-и-11)		УК-11.2 Использует технологии сбора, обработки, интерпретации,	студент должен показать минимальные умения по организации	Компьютерное тестиро-

				анализа и обмена информацией с учётом требований информационной безопасности	своей деятельности в цифровом пространстве	вание Лабораторная работа Письменный и устный опрос Реферат
4	Программно-технические аспекты обеспечения защиты информации	В(ОПК-8-22Г.)	подходы интеграции программного модуля в инструментальные среды	ОПК 8.3 Интегрирует программные модули в инструментальные среды	студент должен показать минимальное владение вопросами интеграции программного модуля в инструментальные среды	Компьютерное тестирование Лабораторная работа Письменный и устный опрос Реферат
		З(ОПК-8-22Г.)		ОПК 8.3 Интегрирует программные модули в инструментальные среды	студент должен показать минимальные знания подходов интеграции программного модуля в инструментальные среды	Компьютерное тестирование Лабораторная работа Письменный и устный опрос Реферат

		У(ОПК-8-22Г.)		ОПК 8.3 Интегрирует программные модули в инструментальные среды	студент должен показать минимальные умения интеграции программного модуля в инструментальные среды	Компьютерное тестирование Лабораторная работа Письменный и устный опрос Реферат
7	Основные направления по созданию систем комплексной защиты информационной системы предприятия	В(ОПК-3-22Г.)	основные требования, применяемые к информационной безопасности	ОПК 3.1 Знает основные принципы, методы и средства решения стандартных задач профессиональной деятельности	студент должен показать минимальное владение решением стандартных задач профессиональной деятельности с учетом требований информационной безопасности	Компьютерное тестирование Лабораторная работа Письменный и устный опрос Реферат
		З(ОПК-3-22Г.)		ОПК 3.1 Знает основные принципы, методы и средства решения стандартных задач профессиональной деятельности	студент должен показать минимальные знания требований к информационной безопасности	Компьютерное тестирование Лабораторная работа Письмен-

						ный и устный опрос Реферат
		У(ОПК-3-22Г.)		ОПК 3.1 Знает основные принципы, методы и средства решения стандартных задач профессиональной деятельности	студент должен показать минимальные умения решения стандартных задач профессиональной деятельности	Компьютерное тестирование Лабораторная работа Письменный и устный опрос Реферат
10	Основы управления информационной безопасностью предприятия	В(ОПК-2-22Г.)	применимость современных информационных технологий и программных средств	ОПК 2.1 Знает современные информационные технологии и программные средства, в том числе отечественного производства, применяет их при решении задач профессиональной деятельности	студент должен показать минимальное владение по использованию современных ИТ при решении задач профессиональной деятельности	Компьютерное тестирование Лабораторная работа Письменный и устный опрос Реферат
		З(ОПК-2-22Г.)		ОПК 2.1 Знает современные информационные технологии и программные средства, в том чис-	студент должен показать минимальные знания применения ИТ и программных средств	Компьютерное тестирование

				ле отечественного производства, применяет их при решении задач профессиональной деятельности		Лабораторная работа Письменный и устный опрос Реферат
		У(ОПК-2-22Г.)		ОПК 2.1 Знает современные информационные технологии и программные средства, в том числе отечественного производства, применяет их при решении задач профессиональной деятельности	студент должен показать минимальные умения использования современных ИТ при решении задач профессиональной деятельности	Компьютерное тестирование Лабораторная работа Письменный и устный опрос Реферат

2. Перечень оценочных средств для текущего контроля и промежуточной аттестации по дисциплине

п/п	Вид оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде	Шкала оценки
1	2	3	4	5
1	Компьютерное тестирование	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося	Фонд тестовых заданий	оценка «отлично» выставляется обучающемуся, если правильно выполнено более 90% работы оценка «хорошо» выставляется обучающемуся, если правильно выполнено более 75% работы оценка «удовлетворительно» выставляется обучающемуся, если правильно выполнено более 60 % работы оценка «неудовлетворительно» выставляется обучающемуся, если правильно выполнено менее 60% работы
2	Лабораторная работа	Средство проверки умений при-	Темы, задания для выполне-	оценка «отлично» выставляется обучающемуся, если работа

		менять полученные знания по заранее определенной методике для решения задач или заданий по лабораторным исследованиям	ния ла-бораторных работ; вопросы и требования к их защите	выполнена полностью, использован правильный, оптимальный алгоритм решения; работа выполнена по плану и сделаны правильные выводы оценка «хорошо» выставляется обучающемуся, если работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя оценка «удовлетворительно» выставляется обучающемуся, если работа выполнена правильно не менее чем на половину или допущена одна существенная ошибка оценка «неудовлетворительно» выставляется обучающемуся, если не знает (отсутствие знаний)
3	Письменный и устный опрос	Оценочное средство для текущего контроля успеваемости и промежуточной аттестации. Позволяет выявить и восполнить пробелы в знаниях; повторить, закрепить, систематизировать материал; оценить знания, умения, теоретические и практические навыки; определить уровень сформированных у студентов компетенций по дисциплине (модулю)	Совокупность вопросов, заданий, упражнений, тестов для выполнения контрольных работ, домашних заданий, РГР и иных учебных работ. Комплект билетов для текущей и промежуточной аттестации	оценка «отлично» выставляется обучающемуся, если грамотно владеет знаниями об использовании программно-технического обеспечения информационной безопасности, проводит анализ предметной области, выявляет информационные потребности, разрабатывает требования к информационной безопасности и к прикладным и инструментальным средствам создания систем информационной безопасности оценка «хорошо» выставляется обучающемуся, если достаточно полно знает об использовании программно-технического обеспечения информационной безопасности, проводит анализ предметной области, выявляет информационные потребности, разрабатывает требования к информационной безопасности и к прикладным и инструментальным средствам создания систем информационной безопасности оценка «удовлетворительно» выставляется обучающемуся, если слабо знает понятия об использовании программно-технического обеспечения информационной безопасности, проводит анализ предметной области, выявляет информационные потребности, разрабатывает требования к информационной безопасности и к прикладным и инструментальным средствам создания систем информационной безопасности оценка «неудовлетворительно» выставляется обучающемуся, если не знает (отсутствие знаний)
4	Реферат	Продукт самостоятельной работы обучающегося, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приво-	Темы рефератов, требования к их защите	оценка «отлично» выставляется обучающемуся, если уверенно владеет методологией современных оценок угроз информационной безопасности для объекта информатизации, критической оценкой полученных результатов, эффективно и грамотно использует методы и средства защиты информации в автоматизированных системах, решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры, в совершенстве знает сущность и понятие информационной безопасности и характеристику ее составляющих оценка «хорошо» выставляется обучающемуся, если достаточно полно владеет методологией современных оценок угроз информационной безопасности для объекта информа-

		дит различные точки зрения, а также собственные взгляды на нее.		тизации, критической оценкой полученных результатов, использует методы и средства защиты информации в автоматизированных системах, решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры, знает сущность и понятие информационной безопасности и характеристику ее составляющих оценка «удовлетворительно» выставляется обучающемуся, если поверхностно владеет методологией для построения систем защиты информации по требованиям информационной безопасности, не достаточно полно систематизирует, классифицирует и анализирует информацию для построения систем защиты информации на предприятии и применяет основные средства и способы обеспечения информационной безопасности с учетом требований информационной безопасности оценка «неудовлетворительно» выставляется обучающемуся, если не знает (отсутствие знаний)
--	--	---	--	---

Приложение В

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Уфимский государственный нефтяной технический университет»

Письменный и устный опрос.

Перечень вопросов (задач, заданий, тем, комплекта тестовых заданий):

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ В ВИДЕ ПИСЬМЕННОГО И УСТНОГО ОПРОСА

1. Администрирование сетей в аспекте информационной безопасности.
2. Аудит информационной безопасности.
3. Безопасность баз данных.
4. Безопасность беспроводных сетей
5. Безопасность операционных систем.
6. Безопасность электронных платежей
7. Защита от инсайдеров и утечки информации
8. Защита от спама.
9. Защита персональных данных.
10. Защищенные системы электронной почты и документооборота.
11. Источники, риски и формы атак на информацию.
12. Киберугрозы и кибертерроризм.
13. Комплексные системы защиты информации (например, Программный комплекс ViPNet).
14. Математические основы и базовые процедуры формирования электронной цифровой подписи в соответствии с ГОСТ Р 34.10. 2001.
15. Многоуровневая защита корпоративных сетей.
16. Модели безопасности основных операционных систем.
17. Общая характеристика современных алгоритмов аутентификации пользователей.
18. Угрозы безопасности информации в компьютерных системах.
19. Инженерно-технические методы защиты информации.
20. Задача защиты сообщения от искажений.
21. Особенности защиты информации в вычислительной системе.
22. Основные угрозы безопасности вычислительной системы.
23. Наблюдение за каналами связи. Задержка, изменение, подмена сообщений.
24. Перехват побочных излучений. Установка “жучков”.
25. Получение конфиденциальных охраняемых сведений из базы данных.
26. Получение полномочий других пользователей и супервизора системы.
27. Анализ программного обеспечения с целью выявления слабых мест в защите.
28. Методы разграничения доступа. Требования к выбору и использованию паролей.
29. Методы поддержания целостности информации.
30. Методы поддержания конфиденциальности информации.
31. Физическая защита вычислительного центра и каналов связи.
32. Методы защиты программного обеспечения от копирования и анализа.
33. Организация работ с конфиденциальными информационными ресурсами.
34. Противодействие наблюдению в оптическом диапазоне.
35. Средства борьбы с закладными подслушивающими устройствами.
36. Защита от злоумышленных действий обслуживающего персонала и пользователей.
37. Методы защиты от побочных электромагнитных излучений и наводок.
38. Противодействие несанкционированному подключению устройств.
39. Система разграничения доступа к информации.
40. Защита программных средств от исследования.

41. Криптография с несколькими открытыми ключами.
42. Формальный анализ протоколов проверки подлинности и обмена ключами.
43. Разделение секрета. Совместное использование секрета.
44. Электронные деньги.
45. Шифрование коммуникационных каналов.
46. Протокол управления секретными ключами компании IBM.
47. Основные положения по обеспечению безопасности компьютерных баз данных.
48. Основы построения систем аутентификации с использованием интеллектуальных карт.
49. Сертификация и аттестация.
50. Системы централизованного управления корпоративной политикой безопасности.
51. Современные средства защиты программ от несанкционированного копирования.
52. Современные средства защиты компьютерной информации от программных закладок.
53. Средства анализа защищенности, реализуемые в современных компьютерных системах управления и обработки информации.
54. Средства защиты информации, построенные на основе технологии «туннелирования».
55. Управление доступом к компьютерной информации: принципы методы средства.
56. Характеристика современных средств идентификации и аутентификации пользователей.

Пример экзаменационного билета

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Уфимский государственный нефтяной технический университет» (ФГБОУ ВО «УГНТУ»)
(Институт нефтепереработки и нефтехимии ФГБОУ ВО УГНТУ в г. Салавате)

УТВЕРЖДАЮ

Зав. кафедрой ИнТех _____ Т.М. Левина
« _____ » _____ 2023 г.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

по дисциплине «Информационная безопасность

по направлению подготовки

09.03.01 Информатика и вычислительная техника

1 Безопасность беспроводных сетей.

2 Методы защиты от побочных электромагнитных излучений и наводок.

Экзаменатор _____

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Уфимский государственный нефтяной технический университет» (ФГБОУ ВО «УГНТУ»)
(Институт нефтепереработки и нефтехимии ФГБОУ ВО УГНТУ в г. Салавате)

УТВЕРЖДАЮ

Зав. кафедрой ИнТех _____ Т.М. Левина
« _____ » _____ 2023 г.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

по дисциплине «Информационная безопасность

по направлению подготовки

09.03.01 Информатика и вычислительная техника

1 Защита от спама.

2 Шифрование коммуникационных каналов.

Экзаменатор _____

Министерство науки и высшего образования Российской Федерации
 Федеральное государственное бюджетное образовательное учреждение высшего образования
 «Уфимский государственный нефтяной технический университет» (ФГБОУ ВО «УГНТУ»)
 (Институт нефтепереработки и нефтехимии ФГБОУ ВО УГНТУ в г. Салавате)

УТВЕРЖДАЮ

Зав. кафедрой ИнТех _____ Т.М. Левина
 «_____» _____ 2023 г.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 3

по дисциплине «Информационная безопасность

по направлению подготовки

09.03.01 Информатика и вычислительная техника

1 Киберугрозы и кибертерроризм.

2 Управление доступом к компьютерной информации: принципы методы средства.

Экзаменатор _____

Вопрос № 18 Угрозы безопасности информации в компьютерных системах. (примерный ответ)
 Угрозы информационной (компьютерной) безопасности — это различные действия, которые могут привести к нарушениям состояния защиты информации. Другими словами, это — потенциально возможные события, процессы или действия, которые могут нанести ущерб информационным и компьютерным системам. Угрозы ИБ можно разделить на два типа: естественные и искусственные. К естественным относятся природные явления, которые не зависят от человека, например ураганы, наводнения, пожары и т.д. Искусственные угрозы зависят непосредственно от человека и могут быть преднамеренными и непреднамеренными. Непреднамеренные угрозы возникают из-за неосторожности, невнимательности и незнания. Примером таких угроз может быть установка программ, не входящих в число необходимых для работы и в дальнейшем нарушающих работу системы, что и приводит к потере информации. Преднамеренные угрозы, в отличие от предыдущих, создаются специально. К ним можно отнести атаки злоумышленников как извне, так и изнутри компании. Результат реализации этого вида угроз — потери денежных средств и интеллектуальной собственности организации.

Классификация угроз информационной безопасности

В зависимости от различных способов классификации все возможные угрозы информационной безопасности можно разделить на следующие основные подгруппы:

Нежелательный контент.

Несанкционированный доступ.

Утечки информации. Потеря данных.

Мошенничество.

Кибервойны. Кибертерроризм.

Нежелательный контент — это не только вредоносный код, потенциально опасные программы и спам (т.е. то, что непосредственно создано для уничтожения или кражи информации), но и сайты, запрещенные законодательством, а также нежелательные ресурсы с информацией, не соответствующей возрасту потребителя.

Несанкционированный доступ — просмотр информации сотрудником, который не имеет разрешения пользоваться ею, путем превышения должностных полномочий. Несанкционированный доступ приводит к утечке информации. В зависимости от того, каковы данные и где они хранятся, утечки могут организовываться разными способами, а именно через атаки на сайты, взлом программ, перехват данных по сети, использование несанкционированных программ.

Утечки информации можно разделять на умышленные и случайные. Случайные утечки происходят из-за ошибок оборудования, программного обеспечения и персонала. Умышленные, в свою очередь, организовываются преднамеренно с целью получить доступ к данным, нанести ущерб. Потерю данных можно считать одной из основных угроз информационной безопасности. Нарушение целостности информации может быть вызвано неисправностью оборудования или умышленными действиями людей, будь то сотрудники или злоумышленники.

Не менее опасной угрозой является мошенничество с использованием информационных технологий («фрод»). К мошенничеству можно отнести не только манипуляции с кредитными картами («кардинг») и взлом онлайн-банка, но и внутренний фрод. Целями этих экономических преступлений являются обход законодательства, политики безопасности или нормативных актов, присвоение имущества. Ежегодно по всему миру возрастает террористическая угроза, постепенно перемещающаяся при этом в виртуальное пространство. На сегодняшний день никого не удивляет возможность атак на автоматизированные системы управления технологическими процессами (АСУ ТП) различных предприятий. Но подобные атаки не проводятся без предварительной разведки, для чего применяется кибершпионаж, помогающий собрать необходимые данные.

Существует также такое понятие, как «информационная война»; она отличается от обычной войны тем, что в качестве оружия выступает тщательно подготовленная информация. Источник угроз информационной безопасности. Нарушение режима информационной безопасности может быть вызвано как спланированными операциями злоумышленников, так и неопытностью сотрудников. Пользователь должен иметь хоть какое-то понятие об ИБ, вредоносном программном обеспечении, чтобы своими действиями не нанести ущерб компании и самому себе. Такие инциденты, как потеря или утечка информации, могут также быть обусловлены целенаправленными действиями сотрудников компании, которые заинтересованы в получении прибыли в обмен на ценные данные организации, в которой работают или работали. Основными источниками угроз являются отдельные злоумышленники («хакеры»), киберпреступные группы и государственные спецслужбы (киберподразделения), которые применяют весь арсенал доступных киберсредств, перечисленных и описанных выше. Чтобы пробиться через защиту и получить доступ к нужной информации, они используют слабые места и ошибки в работе программного обеспечения и веб-приложений, изъяны в конфигурациях сетевых экранов и настройках прав доступа, прибегают к прослушиванию каналов связи и использованию клавиатурных шпионов. То, чем будет производиться атака, зависит от типа информации, ее расположения, способов доступа к ней и уровня защиты. Если атака будет рассчитана на неопытность жертвы, то возможно, например, использование спам-рассылок. Оценивать угрозы информационной безопасности необходимо комплексно, при этом методы оценки будут различаться в каждом конкретном случае. Так, чтобы исключить потерю данных из-за неисправности оборудования, нужно использовать качественные комплектующие, проводить регулярное техническое обслуживание, устанавливать стабилизаторы напряжения. Далее следует устанавливать и регулярно обновлять программное обеспечение (ПО).

Вопрос № 39 Система разграничения доступа к информации. (примерный ответ)

Система разграничения доступа к информации должна содержать четыре функциональных блока:

- блок идентификации и аутентификации субъектов доступа;
- диспетчер доступа;
- блок криптографического преобразования информации при ее хранении и передаче;
- блок очистки памяти.

Идентификация и аутентификация субъектов осуществляется в момент их доступа к устройствам, в том числе и дистанционного доступа.

Диспетчер доступа реализуется в виде аппаратно-программных механизмов и обеспечивает необходимую дисциплину разграничения доступа субъектов к объектам доступа (в том числе и к аппа-

ратным блокам, узлам, устройствам). Диспетчер доступа разграничивает доступ к внутренним ресурсам КС субъектов, уже получивших доступ к этим системам. Необходимость использования диспетчера доступа возникает только в многопользовательских КС.

Запрос на доступ *i*-го субъекта и *j*-му объекту поступает в блок управления базой полномочий и характеристик доступа и в блок регистрации событий. Полномочия субъекта и характеристики объекта доступа анализируются в блоке принятия решения, который выдает сигнал разрешения выполнения запроса, либо сигнал отказа в допуске. Если число попыток субъекта допуска получить доступ к запрещенным для него объектам превысит определенную границу (обычно 3 раза), то блок принятия решения на основании данных блока регистрации выдает сигнал "НСДИ" администратору системы безопасности. Администратор может блокировать работу субъекта, нарушающего правила доступа в системе, и выяснить причину нарушений. Кроме преднамеренных попыток НСДИ диспетчер фиксирует нарушения правил разграничения, явившихся следствием отказов, сбоев аппаратных и программных средств, а также вызванных ошибками персонала и пользователей.

Следует отметить, что в распределенных КС криптографическое закрытие информации является надежным единственным способом защиты от НСДИ.

В СРД должна быть реализована функция очистки оперативной памяти и рабочих областей на внешних запоминающих устройствах после завершения выполнения программы, обрабатывающей конфиденциальные данные. Причем очистка должна производиться путем записи в освободившиеся участки памяти определенной последовательности двоичных кодов, а не удалением только учетной информации о файлах из таблиц ОС, как это делается при стандартном удалении средствами ОС.

Вопрос № 56 Характеристика современных средств идентификации и аутентификации пользователей. (примерный ответ)

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов.

Идентификация и аутентификация - это первая линия обороны, "проходная" информационного пространства организации.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова "аутентификация" иногда используют словосочетание "проверка подлинности".

Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной). Пример односторонней аутентификации - процедура входа пользователя в систему.

В сетевой среде, когда стороны идентификации/аутентификации территориально разнесены, у рассматриваемого сервиса есть два основных аспекта:

что служит аутентификатором (то есть используется для подтверждения подлинности субъекта); как организован (и защищен) обмен данными идентификации/аутентификации.

Субъект может подтвердить свою подлинность, предъявив по крайней мере одну из следующих сущностей:

нечто, что он знает (пароль, личный идентификационный номер, криптографический ключ и т.п.);

нечто, чем он владеет (личную карточку или иное устройство аналогичного назначения);

нечто, что есть часть его самого (голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики).

В открытой сетевой среде между сторонами идентификации/аутентификации не существует доверенного маршрута; это значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности. Необходимо обеспечить защиту от пассивного и активного прослушивания сети, то есть от перехвата, изменения и/или воспроизведения данных. Передача паролей в открытом виде, очевидно, неудовлетворительна; не спасает положение и шифрование паролей, так как оно не защищает от воспроизведе-

ния. Нужны более сложные протоколы аутентификации.

Надежная идентификация и затруднена не только из-за сетевых угроз, но и по целому ряду причин. Во-первых, почти все аутентификационные сущности можно узнать, украсть или подделать. Во-вторых, имеется противоречие между надежностью аутентификации, с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это не только хлопотно, но и повышает вероятность того, что кто-то может подсмотреть за вводом данных. В-третьих, чем надежнее средство защиты, тем оно дороже.

Современные средства идентификации/аутентификации должны поддерживать концепцию единого входа в сеть. Единый вход в сеть - это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформировались.

Таким образом, необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств идентификации и аутентификации.

Перечень вопросов (задач, заданий, тем, комплекта тестовых заданий):

Филиппова, А. Г. Средства и методы защиты компьютерной информации : учебное пособие / А. Г. Филиппова, В. Н. Филиппов ; УГНТУ, каф. ВТИК. - Уфа : УГНТУ, 2022. - 2,74 Мб. - URL: http://bibl.rusoil.net/base_docs/UGNTU/VTIK/Filippov15509.pdf. - Текст : электронный.

Реферат.

Перечень вопросов (задач, заданий, тем, комплекта тестовых заданий):

Перечень тем рефератов

1. Противодействие злоумышленникам. Системы антифрода. Основные принципы построения систем антифрода.
2. Противодействие злоумышленникам. Системы обнаружения и предотвращения вторжений. Принципы проектирования и использования.
3. Анализ и выявление APT (Advanced Persistent Threat) атак, методы их расследования и предотвращения.
4. Методы обеспечения информационной безопасности веб-технологий.
5. Использование технологий больших данных в области информационного противоборства. Анализ больших данных в целях выявления возможных угроз информационной безопасности.
6. Каналы утечки информации. Виды каналов, способы предотвращения утечки информации.
7. Методы обеспечения противодействия информационной разведке.
8. Принципы обеспечения информационной безопасности электронного банкинга.
9. Обеспечение безопасности операционных систем. Структура хранения и защита информации (операционные системы семейства Windows, Android, iOS, Linux).
10. Платежные инновации в РФ. Новые платежные технологии, электронные средства платежа и методы защиты информации. GAPb информационной безопасности.
11. Организация защиты использования сети Интернет и электронной почты. Основы организации защиты информации с использованием криптографических средств.
12. Принципы построения сетей передачи данных, использование сетевых протоколов, общего и специализированного программного обеспечения, для обеспечения информационной безопасности.
13. Обеспечение информационной безопасности в системах дистанционного обслуживания.
14. Программные и аппаратные комплексы защиты информации (DallasLock, «Соболь», SecretNet, электронные ключи и т.п.). Состав, назначение, функциональные возможности, приемы использо-

вания.

15. Средства анализа и методы исследования защищенности объектов информатизации, системы управления информационной безопасностью и инцидентами.
16. Обеспечение безопасности облачных сервисов.
17. Перспективы использования виртуальных валют и связанные с этим риски для финансовых систем.
18. Методология Security Development Life Cycle. Выстраивание процессов SDLC в классической проектной деятельности и Agile-проектах.
19. Автоматический анализ безопасности программного кода.
20. Современные модели и методы выявления (по выбору классов) уязвимостей и дефектов безопасности программ
21. Методы решения «проблемы больших данных» (big data) при мониторинге событий информационной безопасности.
22. Современные несигнатурные методы выявления целенаправленных компьютерных атак (APT- атак).
23. Современные проблемы цифровой криминалистики. 24.Образный анализ и защита и речевой информации
25. Методы и модели защиты информации на основе технологии «блокчейн».
26. Уровни ведения информационной войны. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети.
27. Цели информационной войны, её составные части и средства её ведения. Объекты воздействия в информационной войне.
28. Механизм заражения файловыми и загрузочными вирусами. Особенности макровирусов.
- 29.Методы защиты коммуникаций, основанные на принципах квантовой физики.
- 30.Защита программных средств КС от несанкционированного копирования и исследования.

Общий объем работы - 25—30 страниц печатного текста (с учетом титульного листа, содержания и списка литературы) на бумаге формата А4, на одной стороне листа. Реферат должен содержать: титульный лист,

оглавление, введение, основную часть (разделы, части), выводы (заключительная часть), приложения, пронумерованный список использованной литературы (не менее 5-ти источников) с указанием автора, названия, места издания, издательства, года издания.

Интервал межстрочный - полуторный. Цвет шрифта - черный.

Гарнитура шрифта основного текста — «Times New Roman». Кегль (размер) 14 пунктов. Размеры полей страницы (не менее): левое — 30 мм, верхнее, и нижнее, правое — 20 мм. Формат абзаца: полное выравнивание («по ширине»). Отступ красной строки одинаковый по всему тексту.

Расстояние между названием главы (подраздела) и текстом должно быть равно 2,5 интервалам.

Однако расстояние между подзаголовком и последующим текстом должно быть 2 интервала, а интервал между строками самого

текста — 1,5. Размер шрифта для названия главы — 16 (полужирный), подзаголовка

— 14 (полужирный), текста работы — 14. Точка в конце заголовка, располагаемого посередине листа, не ставится. Заголовки не подчеркиваются. Абзацы начинаются с новой строки и печатаются с отступом в 1,25 сантиметра.

Лабораторная работа.

Перечень вопросов (задач, заданий, тем, комплекта тестовых заданий):

ПРИМЕР ЛАБОРАТОРНОЙ РАБОТЫ

Тема 1. Реализация простейшего генератора паролей, обладающего требуемой стойкостью к взлому.

Подсистемы идентификации и аутентификации пользователя играют важную роль в системах за-

щиты информации.

Стойкость подсистемы идентификации и аутентификации пользователя в системе защиты информации (СЗИ) во многом определяет устойчивость к взлому самой СЗИ. Данная стойкость определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор или украв его.

Парольные системы идентификации/аутентификации являются одними из основных и наиболее распространенных в СЗИ методами пользовательской аутентификации. В данном случае информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только легальному пользователю.

Парольная аутентификация пользователя, как правило, передний край обороны СЗИ. В связи с этим модуль аутентификации по паролю наиболее часто подвергается атакам со стороны злоумышленника. Цель последнего в данном случае – подобрать аутентифицирующую информацию (пароль) легального пользователя.

Методы парольной аутентификации пользователя наиболее просты и при несоблюдении определенных требований к выбору пароля являются достаточно уязвимыми.

Основными минимальными требованиями к выбору пароля и к подсистеме парольной аутентификации пользователя являются следующие.

К паролю:

- 1) минимальная длина пароля должна быть не менее 6 символов;
- 2) пароль должен состоять из различных групп символов (малые и большие латинские буквы, цифры, специальные символы ‘(’, ‘)’, ‘#’ и т.д.);
- 3) в качестве пароля не должны использоваться реальные слова, имена, фамилии и т.д. К подсистеме парольной аутентификации:
 - 1) администратор СЗИ должен устанавливать максимальный срок действия пароля, после чего, пароль следует сменить;
 - 2) в подсистеме парольной аутентификации необходимо установить ограничение числа попыток ввода пароля (как правило, не более трёх);
 - 3) в подсистеме парольной аутентификации требуется установить временную задержку в случае ввода неправильного пароля.

Как правило, для генерирования паролей в СЗИ, удовлетворяющих перечисленным требованиям к паролям, используются программы – автоматические генераторы паролей пользователей.

При выполнении перечисленных требований к паролям и к подсистеме парольной аутентификации единственно возможным методом взлома данной подсистемы злоумышленником является прямой перебор паролей (brute forcing). В данном случае, оценка стойкости парольной защиты осуществляется следующим образом.

Количественная оценка стойкости парольной защиты

Пусть A – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля: если пароль состоит только из малых английских букв, то $A = 26$), L – длина пароля, $S = AL$ – число всевозможных паролей длины L , которые можно составить из символов алфавита A , V – скорость перебора паролей злоумышленником, T – максимальный срок действия пароля.

Тогда, вероятность P подбора пароля злоумышленником в течение срока его действия V определяется по следующей формуле:

$$P = (V \cdot T) / S = (V \cdot T) / AL.$$

Эту формулу можно использовать в обратную сторону для решения следующей задачи. Задача.

Определить минимальные мощность алфавита паролей A и длину паролей L , обеспечивающих вероятность подбора пароля злоумышленником не более заданной P , при скорости подбора паролей V , максимальном сроке действия пароля T .

Данная задача имеет неоднозначное решение. При исходных данных V , T , P однозначно можно

определить лишь нижнюю границу S^* числа всевозможных паролей. Целочисленное значение

нижней границы вычисляется по формуле

$$S^* = [V \cdot P / T], \quad (1)$$

где $[]$ – целая часть числа, взятая с округлением вверх.

После определения нижней границы S^* необходимо выбрать такие A и L для формирования $S = AL$, чтобы выполнялось следующее неравенство:

$$S^* \leq S = AL. \quad (2)$$

При выборе S , удовлетворяющего неравенству (2), вероятность подбора пароля злоумышленника (при заданных V и T) будет меньше, чем заданная P .

Следует отметить, что при осуществлении вычислений по формулам (1) и (2), величины должны быть приведены к одним размерностям.

Пример. Исходные данные: $P = 10^{-6}$, $T = 7$ дней = 1 неделя, $V = 10$ (паролей / минуту) = $10 \cdot 60 \cdot 24 \cdot 7 = 100800$ паролей в неделю. Тогда, $S^* = [(100800 \cdot 1) / 10^{-6}] = 108 \cdot 10^8$.

Условию $S^* \leq AL$ удовлетворяют, например, такие комбинации A и L , как $A = 26$, $L = 8$ (пароль состоит из восьми малых символов английского алфавита), $A = 36$, $L = 6$ (пароль состоит из шести символов, среди которых могут быть малые латинские буквы и произвольные цифры).

Задание на лабораторную работу

1. В таблице 1, найти для указанного варианта значения характеристик P , V , T .
2. Вычислить по формуле (1) нижнюю границу S^* для заданных P , V , T .
3. Выбрать некоторый алфавит с мощностью A и получить минимальную длину пароля L , при котором выполняется условие (2).
4. Реализовать программу для генерации паролей пользователей. Программа должна формировать случайную последовательность символов длины L , при этом должен использоваться алфавит из A символов.
5. Оформить отчет по лабораторной работе.

Коды символов:

1. Коды английских символов : «A» = 65, ..., «Z» = 90, «a» = 97, ..., «z» = 122. 2. Коды цифр : «0» = 48, «9» = 57.
3. «!» = 33, «“» = 34, «#» = 35, «\$» = 36, «%» = 37, «&» = 38, «'» = 39.
4. Коды русских символов : «А» – 128, ... «Я» – 159, «а» – 160, ..., «п» – 175, «р» – 224, ..., «я» – 239.

Таблица 1. Варианты заданий

Вариант	P	V	T
1	10-4	15 паролей/мин	2 недели
2	10-5	3 паролей/мин	10 дней
3	10-6	10 паролей/мин	5 дней
4	10-7	11 паролей/мин	6 дней
5	10-4	100 паролей/день	12 дней
6	10-5	10 паролей/день	1 месяц
7	10-6	20 паролей/мин	3 недели
8	10-7	15 паролей/мин	20 дней
9	10-4	3 паролей/мин	15 дней
10	10-5	10 паролей/мин	1 неделя
11	10-6	11 паролей/мин	2 недели
12	10-7	100 паролей/день	10 дней
13	10-4	10 паролей/день	5 дней
14	10-5	20 паролей/мин	6 дней
15	10-6	15 паролей/мин	12 дней
16	10-7	3 паролей/мин	1 месяц
17	10-4	10 паролей/мин	3 недели
18	10-5	11 паролей/мин	20 дней

19	10-6	100 паролей/день	15 дней
20	10-7	10 паролей/день	1 неделя
21	10-4	20 паролей/мин	2 недели
22	10-5	15 паролей/мин	10 дней
23	10-6	3 паролей/мин	5 дней
24	10-7	10 паролей/мин	6 дней
25	10-4	11 паролей/мин	12 дней
26	10-5	100 паролей/день	1 месяц
27	10-6	10 паролей/день	3 недели
28	10-7	20 паролей/мин	20 дней
29	10-4	15 паролей/мин	15 дней
30	10-5	3 паролей/мин	1 неделя

Порядок выполнения лабораторных работ и требования приведены в электронном издании: Информационная безопасность : учебное пособие / УГНТУ, каф. ВТИК ; сост.: В. Н. Филиппов [и др.]. - Уфа : УГНТУ, 2022. - 4,31 Мб. - URL: http://bibl.rusoil.net/base_docs/UGNTU/VTIK/Filippov15508.pdf. - Текст : электронный.

Компьютерное тестирование.

Перечень вопросов (задач, заданий, тем, комплекта тестовых заданий):

Перечень вопросов (задач, заданий, тем, комплекта тестовых заданий):

1. Что называют шифрованием?

- А) Алгоритм шифрования данных
- Б) Процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа
- В) Обратимое преобразование информации в целях сокрытия от неавторизованных лиц с предоставлением в это же время авторизованным пользователям доступа к ней
- Г) Все ответы верны

2. Можно ли использовать потоковый шифр в качестве генератора псевдослучайных последовательностей?

- А) Нет
- Б) Да
- В) Только потоковый шифр с нелинейной фильтрующей функцией

3. Алгоритм ГОСТ 28147-89 является:

- А) алгоритмом вычисления функции хеширования
- Б) блочным алгоритмом асимметричного шифрования
- В) блочным алгоритмом симметричного шифрования
- Г) алгоритмом формирования электронной цифровой подписи

4. RC4 – это...

- А) Алгоритм потокового шифрования (stream cipher)
- Б) Алгоритм блочного шифрования (block cipher)
- В) Алгоритм асимметричного шифрования (public key encryption)
- Г) Алгоритм хэширования (hash algorithm)

5. Данные, передаваемые без использования криптографии называются...?
- А) Исходный код
Б) Открытый текст
В) Телеграмма
Г) Дешифр
6. Криптосистема – это...?
- А) Семейство обратимых преобразований открытого текста в шифрованный
Б) Программа шифрования
В) Комплексная защита данных
Г) Система анализа методов шифрования
7. Что общего имеют все методы шифрования с закрытым ключом?
- А) в них для шифрования информации используется один ключ, а для расшифрования – другой ключ
Б) в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов
В) в них для операций шифрования и расшифрования используется два разных ключа – открытый и закрытый
Г) в них для шифрования и расшифрования информации используется один и тот же ключ
8. Чем шифрование отличается от кодирования?
- А) Цель шифрования – сокрытие информации, у кодирования иная цель (сжатие, к примеру)
Б) Шифрование применяется для бинарных данных, а кодирование – для человекочитаемых
В) Принципиально не отличаются
9. Как называется метод шифрования, в котором входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов?
- А) шифр асимметричного преобразования
Б) шифр замены
В) шифр многоалфавитной подстановки
Г) шифр перестановки
10. Зачем нужен паддинг при блочном шифровании?
- А) Для дополнения сообщений, длина которых не кратна длине блока
Б) Для сокрытия длины сообщения
В) Для усиления криптографических свойств блочного шифра
Г) Для шифрования сообщений, длина которых больше длины блока

вопрос 1 2 3 4 5 6 7 8 9 10
ответ Г Б В А Б А Г А Г А

Аннотация к рабочей программе дисциплины (6724)Информационная безопасность

Направление подготовки (специальность): 09.03.01 Информатика и вычислительная техника

Направленность: профиль«Технологии искусственного интеллекта в нефтегазовой отрасли»

Уровень высшего образования: бакалавриат

Форма обучения: очная;заочная;

Кафедра, обеспечивающая преподавание дисциплины: Информационных технологий (ИнТех);

Компетенции, формируемые в результате освоения дисциплины

ОПК-2-22Г. Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности:

-ОПК 2.1 Знает современные информационные технологии и программные средства, в том числе отечественного производства, применяет их при решении задач профессиональной деятельности

ОПК-3-22Г. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности:

-ОПК 3.1 Знает основные принципы, методы и средства решения стандартных задач профессиональной деятельности

ОПК-8-22Г. Способен разрабатывать алгоритмы и программы, пригодные для практического применения:

-ОПК 8.3 Интегрирует программные модули в инструментальные среды

УК-и-11 Способен планировать и организовывать свою деятельность в цифровом пространстве с учётом правовых и этических норм взаимодействия человека и искусственного интеллекта и требований информационной безопасности:

-УК-11.2 Использует технологии сбора, обработки, интерпретации, анализа и обмена информацией с учётом требований информационной безопасности

Результат обучения

Знать:

ОПК-2-22Г.-4 применимость современных информационных технологий и программных средств

ОПК-3-22Г.-5 основные требования, применяемые к информационной безопасности

ОПК-8-22Г.-3 подходы интеграции программного модуля в инструментальные среды

УК-и-11-2 подходы к организации деятельности в цифровом пространстве с учетом правовых и этических норм взаимодействия человека и искусственного интеллекта

Уметь:

ОПК-2-22Г.-4 использовать современные информационные технологии при решении задач профессиональной деятельности

ОПК-3-22Г.-5 способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры

ОПК-8-22Г.-3 осуществлять интеграцию программного модуля в инструментальные среды

УК-и-11-2 осуществлять планирование и организацию своей деятельности в цифровом пространстве

Владеть:

ОПК-2-22Г.-4 навыками использования современных информационных технологий при решении задач профессиональной деятельности

ОПК-3-22Г.-5 навыками решения стандартных задач профессиональной деятельности с учетом требований информационной безопасности

ОПК-8-22Г.-3 способностями интеграции программного модуля в инструментальные среды

УК-и-11-2 способностями по организации своей деятельности в цифровом пространстве с учетом правовых и этических норм взаимодействия человека и искусственного интеллекта

Краткая характеристика дисциплины

Информационная безопасность и уровни ее обеспечения; Программно-технические аспекты обеспечения защиты информации; Основные направления по созданию систем комплексной защиты информационной системы предприятия; Основы управления информационной безопасностью предприятия;

Трудоёмкость (з.е. / часы)

3 з.е. (108час)

Вид промежуточной аттестации

экзамен;

Разработчик(и):

ст. преподаватель, А.Г. Филиппова

ст. преподаватель, Е.Ю Головина

СОГЛАСОВАНО

Заведующий кафедрой ИнТех _____ Т.М. Левина