Приложение 3
к макету ОПОП

Аннотации к рабочим программам дисциплин

Аннотация к рабочей программы дисциплины

«Криптография и сетевая безопасность»

1 Цели и задачи изучения дисциплины.

1.1 Цель освоения дисциплины.

Курс посвящен изучению современных концепций информационнойбезопасности и их применения в обеспечении защиты информации и безопасного использования программных средств в вычислительных системах. Цель курса – научить студента методам информационной безопасности и их использовании в области защиты информации. Задачей курса является изложение теории информационной безопасности и практики применения алгоритмов криптозащиты.

Воспитательной целью дисциплины является формирование у студентов научного, творческого подхода к освоению технологий, методов и средств производства и защиты программного обеспечения. Дать студентам математические основы защиты информации.

Отбор материала основывается на необходимости ознакомить студентов со следующей современной научной информацией: методы защиты информации; области применения защиты информации; о технологиях анализа шифров.

Содержательное наполнение дисциплины обусловлено общими задачами в подготовке магистра.

Научной основой для построения программы данной дисциплины является теоретико-прагматический подход в обучении.

Студент должен осуществлять профессиональную деятельность и уметь решать задачи, соответствующие программе дисциплины.

Студент в рамках курса должен знать области применения задач информационной безопасности; методы защиты информации; области применения различных методов информационной безопасности; этапы, методы и инструментальные средства информационной безопасности. принципы построения и функционирования систем информационной безопасности; классификацию шифров; основы организации идентификации и цифровой подписи; принципы построения и применения паролей; уметь проводить анализ и определять оптимальный метод защиты информации; формировать требования к предметно-ориентированной системе информационной безопасности и определять возможные пути их выполнения; формулировать и решать задачи организации процесса цифровой подписи; формулировать и решать задачи организации процесса идентификации; реализовать на языке программирования заданный метод защиты информации; решать задачи анализа шифра.

В качестве основной формы итогового контроля по рассматриваемой дисциплине предусмотрен экзамен.

1.2 Задачи дисциплины.

Основные задачи курса на основе системного подхода:

- Описать проблемную область информационной безопасности.

- Дать описание практического применения теории конечных полей в теории защиты информации.
- Расширить понятия о генерации псевдослучайных последовательностях.
- Расширить понятия о способах защиты информации.
- Расширить понятия о методах построения современных программных систем.
- Дать навыки практической работы с методами защиты информации.
- Дать навыки практической работы по решению задач идентификации.
- Дать навыки практической работы по решению задач цифровой подписи.

Содержательное наполнение дисциплины обусловлено общими задачами в подготовке магистра.

Научной основой для построения программы данной дисциплины является теоретико-прагматический подход в обучении.

1.3 Место дисциплины в структуре образовательной программы.

Курс «Криптография и сетевая безопасность» входит в вариативную часть Блока 1 «Дисциплины (модули)» дисциплин, формирующих знания и навыки в области разработки современного программного обеспечения. Курс опирается на знания в области дискретной математики, математической логики, программирования, базы данных. Курс расширяет знания студентов в области создания программных систем, защиты данных и знаний.

Дисциплина тесно связана с дисциплинами «История и методология прикладной математики и информатики», «Дискретные и вероятностные математические модели», «Технологии проектирования и сопровождения программных систем», «Распределенные системы обработки информации и управления данными».

К результатам обучения относятся: фундаментальная подготовка по основам профессиональных знаний; способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе; соблюдение основных требований информационной безопасности, в том числе защиты государственной тайны владение основными методами, способами и средствами получения, хранения, переработки информации, имеет навыки работы с компьютером как средством управления информацией способность к анализу и синтезу;

способность определения общих форм, закономерностей, инструментальных средств данной дисциплины; умение

понять поставленную задачу

умение грамотно пользоваться языком предметной области;

умение извлекать полезную научно-техническую информацию из электронных библиотек, реферативных журналов, сети Интернет знание

математических основ информатики как науки

знание проблемы современной информатики, ее категории и связи с другими научными дисциплинами; знание содержания, основных этапов и тенденции развития

программирования,

математического обеспечения и информационных технологий.

1.4 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.

Студент должен осуществлять профессиональную деятельность и уметь решать задачи, соответствующие программе дисциплины.

Знать	1) области применения задач информационной безопасности; 2) методы защиты информации; 3) области применения различных методов информационной безопасности; 4) этапы, методы и инструментальные средства информационной безопасности; 5) принципы построения и функционирования систем информационной безопасности; 6) методы разработки и анализа концептуальных и теоретических моделей; 7) классификацию шифров; 8) основы организации идентификации и цифровой подписи; 9) принципы построения и применения паролей;
	10) правовые и этические последствия при получении доступа к информации не санкционированными лицами
Уметь	11) проводить анализ и определять оптимальный метод защиты информации; 12) формировать требования к предметно-ориентированной системе информационной безопасности и определять возможные пути их выполнения; 13) анализировать модели шифрования при организации защиты данных 14) формулировать и решать задачи организации процесса цифровой подписи; 15) формулировать и решать задачи организации процесса идентификации; 16) реализовать на языке программирования заданный метод защиты информации; 17) решать задачи анализа шифра; 18) оценить последствия при компрометации ключа или шифра
Владеть	19) методологиями и парадигмами построение систем информационной безопасности; 20) методами проектирования систем защиты информации; 21) методами построения алгоритмов анализа; 22) методами построения систем идентификации; 23) методами определения требований и состава средств, мероприятий по системе информационной безопасности систем; 24) навыками оценки правовых и этических компрометации данных

№ п.п.	**Индекс компетенции**	**Содержание компетенции (или её части)**	**В результате изучения учебной дисциплины обучающиеся должны**		
			знать	**уметь**	**владеть**

1.	ПК-2	способностью разрабатывать и анализировать концептуальные и теоретические модели решаемых научных проблем и задач	1,2,3,4, 6,7,8,9	11, 13, 14, 15, 16, 17	19, 20,21, 22, 23
2.	ОПК-5	способностью использовать углубленные знания правовых и этических норм при оценке последствий своей профессиональной деятельности, при разработке и осуществлении социально значимых проектов	1,5,10	12, 18	23, 24

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 5зач.ед. (180 часов), их распределение по видам работ представлено в таблице (для студентов ОФО).

Вид учебной работы		**Всего часов**	**Семестры (часы)**			
			1	**___**		
Контактная работа, в том числе:						
Аудиторные занятия (всего):		**64**	**64**			
Занятия лекционного типа		32	32	-	-	-
Лабораторные занятия		32	32	-	-	-
Иная контактная работа:						
Промежуточная аттестация (ИКР)		0,3	0,3			
Самостоятельная работа, в том числе:						
Проработка учебного (теоретического) материала		35	35	-	-	-
Выполнение индивидуальных заданий		50	50	-	-	-
Подготовка к текущему контролю		4	4	-	-	-
Контроль:						
Подготовка к экзамену		26,7	26,7			
Общая трудоемкость	**час.**	**180**	**180**	**-**	**-**	**-**
	в том числе контактная работа	**64,3**	**64,3**			
	зач. ед	**5**	**5**			

2.2 Структура дисциплины: Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 1 семестре (очная форма).
Вид промежуточной аттестации: экзамен.

№	**Наименование разделов**	**Количество часов**				
		Всего	**Аудиторная работа**		**Внеаудиторная работа**	
			Л	**ЛР**	**СРС**	**контроль**
1	2	3	4	5	6	7

1.	Базовые понятия и история развития информационной безопасности.	18	4	4	10	4
2.	Конечные поля. Многочлены над конечным полем. Последовательности над конечным полем.	27	6	6	15	6,7
3.	Шифры замены. Шифры перестановки. Шифры гаммирования.	27	6	6	15	4
4.	Блочные системы шифрования.	31	6	6	19	4
5.	Поточные системы шифрования.	27	6	6	15	4
6.	Идентификация. Цифровые подписи.	23	4	4	15	4
7.	Промежуточная аттестация (ИКР)	0,3				
	Итого по дисциплине:	180	32	32	89	26,7

Курсовые работы: не предусмотрена

Форма проведения аттестации по дисциплине: зачёт

Автор Осипян В. О. проф., д. физ.-мат. наук, доцент