АННОТАЦИЯ
дисциплины «Б1.В.02 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ»

Объем трудоемкости: 4 зачетные единицы (144 часа, из них – 64,3 часа контактной работы (32 часов лекций, 32 часа лабораторные работы, 0,3 часа ИКР); 53 часов самостоятельной работы, 26,7 часов контроль).

Цель дисциплины:

Цель освоения дисциплины – знакомство с задачами и методами защиты информации математическими методами. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук. Ее значение возрастает в свете ведущейся информационной войны против Российской Федерации.

Задачи дисциплины:

Задачи освоения дисциплины «Теоретические основы компьютерной безопасности»: обучить магистров принципам и методам защиты информации, комплексного проектирования, построения, обслуживания и анализа защищенных автоматизированных систем (АС), а также содействовать фундаментализации образования, формированию научного мировоззрения и развитию системного мышления. Знания и практические навыки, полученные из курса «Теоретические основы компьютерной безопасности», используются обучаемыми при изучении естественнонаучных дисциплин.

Знания и умения, приобретенные в ходе изучения курса «Теоретические основы компьютерной безопасности» используются обучаемыми при разработке выпускных работ.

Задачи дисциплины – дать основы:

устройства и принципов функционирования, защищенных АС,

методологии проектирования и построения, защищенных АС,

критериев и методов оценки защищенности АС,

средств и методов несанкционированного доступа (НСД) к информации АС.

Место дисциплины в структуре ООП ВО

Дисциплина «Теоретические основы компьютерной безопасности» относится к вариативной части блока Б1 Дисциплины и модули и является обязательной дисциплиной.

Данная дисциплина как составная часть науки «Информационное право» - правового фундамента информационного общества, а также как раздел дискретной математики и теории управления, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления магистров.

Требования к уровню освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ПК-1	Способен формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики	Основные теоремы алгебры, теории чисел и других разделов теоретической математики	Применять стандартные алгоритмы фундаментальной и прикладной математики	Методами анализа математических Моделей, возникающих в области информационных технологий и защиты информации

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
2	ПК-4	Способен ориентироваться в современных алгоритмах компьютерной математики; обладать способностями к эффективному применению и реализации математически сложных алгоритмов в современных программных комплексах	О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа.	Применять основные математические методы, используемые в анализе типовых алгоритмов.	использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в области символьных вычислений.

Основные разделы дисциплины:

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Структура теории компьютерной безопасности.		10		6	13
2	Методология построения систем защищенных АС		8		8	16
3	Политика безопасности.		8		8	14
4	Основные критерии защищенности АС. Классы защищенности АС.		6		10	10
	Итого по дисциплине:		32		32	53

Курсовые работы: не предусмотрены.

Форма проведения аттестации по дисциплине: экзамен

Основная литература:

1. Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. 3-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2015. – URL: https://e.lanbook.com/book/70724
2. Нестеров С.А. Основы информационной безопасности, 4-е изд. [Электронный ресурс]. - СПб.: Лань, 2018. URL: https://e.lanbook.com/book/103908

Дополнительная литература:

1. Никифоров С.Н. Методы защиты информации. Защита от внешних вторжений. [Электронный ресурс] – СПб.: Лань, 2018. URL: https://e.lanbook.com/book/107306

2. Никифоров С.Н. Методы защиты информации. Пароли, скрытие, шифрование. [Электронный ресурс] – СПб.: Лань, 2018. URL: https://e.lanbook.com/book/107307

Интернет-ресурсы:

1. Клиентская ОС Debian 9.5. Официальный сайт https://www.debian.org/
2. Система аудита и обнаружения вторжений Kali Linux 2018.3. Официальный сайт http://www.kali.org/
3. http://www.pravo.gov.ru – официальный портал правовой информации
4. http://minsvyaz.ru/ru - сайт Минкомсвязи РФ
5. http://www.rsoc.ru - сайт Федеральной службы Роскомнадзор
6. http://www.scrf.gov.ru – сайт Совета безопасности РФ
7. http://base.consultant.ru – сайт правовой информации «Консультант+»

Автор РПД, д.ф.-м.н, профессор Рожков А.В.