Аннотация к рабочей программе дисциплины

«Криптографические протоколы»

Рабочая программа дисциплины «Криптографические протоколы» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана Б1.Б.12.06.

Трудоёмкость дисциплины составляет 5 зачетных единиц, в академических часах – 180 часов. Среди них на лекции выделено 36 часов, практические занятия 54 часов, лабораторные работы 36 часов, самостоятельная работа 18 часов, а также 36 часов на подготовку к экзамену. Дисциплина реализуется на 3 курсе в 6 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Криптографические протоколы» логически и содержательно связана с такими курсами, как «Математическая логика и теория алгоритмов», «Дискретная математика», «Криптографические методы защиты информации».

Цель изучения дисциплины «Криптографические протоколы» заключается в формировании у студентов представления об использовании криптографических протоколов для защиты информации, о принципах применения совершенных информационных технологий.

Задачи дисциплины:

– дать основы знаний об основных криптографических протоколах;

– познакомить с методикой выбора и оценки их качества.

Для успешного изучения дисциплины «Криптографические протоколы» у обучающихся должны быть сформированы следующие предварительные компетенции:

– способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);

– способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8);

– способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах (ОПК-10).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные, профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
ОПК-2 – способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов	Знает	основные понятия и задачи векторной алгебры и аналитической геометрии; основные свойства алгебраических структур; основы линейной алгебры над произвольными полями; основы теории групп и теории групп подстановок; свойства векторных пространств; свойства кольца многочленов; основные понятия и методы дискретной математики; основные понятия математической логики и теории алгоритмов; основные понятия и методы теории вероятностей, математической статистики и теории случайных процессов; основные понятия и методы информации
	Умеет	решать основные задачи векторной алгебры и аналитической геометрии; решать системы линейных уравнений над полями; использовать математический аппарат дискретной математики, в том числе применять аппарат производящих функций и рекуррентных соотношений для решения перечисленных задач; находить представление и исследовать

		свойства булевых и многозначных функций формулами в различных базисах; определять возможность применения методов математического анализа
	Владеет	навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике; навыками решения систем линейных уравнений над полем и кольцом вычетов; основами построения математических моделей текстовой информации и моделей систем передачи информации
ОПК-9 – способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знает	основные виды политик управления доступом и информационными потоками в компьютерных системах
	Умеет	основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков
	Владеет	разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками

Для формирования вышеуказанных компетенций в рамках дисциплины «Криптографические протоколы» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: лабораторные работы (ПР-6), конспект (ПР-6), собеседование (ОУ-1), коллоквиум (ОУ-2).