

**Аннотация рабочей программы дисциплины (модуля)
Б1.В.05 «Информационная безопасность»**

Цель дисциплины (модуля) – формирование базовых знаний в области обеспечения информационной безопасности личности, общества и государства.

Задачи дисциплины (модуля):

- ознакомление студентов с современными системами информационной безопасности, технологическими защиты информации, организационными мерами по информационной защите, правовыми принципами их функционирования;
- изучение возможностей использования защиты в работе с информационными ресурсами в различных областях жизнедеятельности.

Формируемые компетенции и индикаторы их достижения по дисциплине (модулю)

Коды компетенции	Содержание компетенций	Код и наименование индикатора достижения компетенции
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. знать: – методы критического анализа и оценки современных научных достижений; основные принципы критического анализа; – методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа. УК-1.2. уметь: – получать новые знания на основе анализа, синтеза и других методов; собирать данные по сложным научным проблемам, относящимся к профессиональной области; осуществлять поиск информации и решений на основе экспериментальных действий; – выявлять в процессе анализа проблематичность ситуации, определяет этапы ее разрешения с учетом вариативных контекстов; – находить, критически анализировать и выбирать информацию, необходимую для выработки стратегии действий по разрешению проблемной ситуации; – рассматривать различные варианты решения проблемной ситуации на основе системного подхода, оценивать их преимущества и риски; – грамотно, логично, аргументировано формулировать собственные суждения и оценки; предлагать стратегию действий; – определять и оценивать практические последствия реализации действий по разрешению проблемной ситуации; – применять методики поиска, сбора и обработки информации; – осуществлять критический анализ и синтез информации, полученной из разных источников; – предвидеть проблемную ситуацию и моделировать умения и навыки выхода из нее; – применять системный подход для решения поставленных задач. УК-1.3. владеть: – исследованием проблем профессиональной деятельности с применением анализа, синтеза и

		других методов интеллектуальной деятельности; – выявлением научных проблем и использованием адекватных методов для их решения; – демонстрацией оценочных суждений в решении проблемных профессиональных ситуаций; – методами поиска, сбора и обработки, критического анализа и синтеза информации; методикой системного подхода для решения поставленных задач; – способностью выхода из проблемной ситуации в профессиональной деятельности.
ПК-3	Способен оценивать риск и определять меры по обеспечению безопасности разрабатываемой техники	ПК-3.1. знать: – научные и организационные основы безопасности производственных процессов и устойчивости производств в чрезвычайных ситуациях; – специфику производственных потоков и зоны наибольшей опасности в них; – основные принципы анализа и моделирования надежности технических систем и определения приемлемого риска; – методы и способы оценки риска и может определять меры по обеспечению безопасности разрабатываемой техники; ПК-3.2. уметь: – проводить расчеты деталей машин по критериям работоспособности и надежности; – идентифицировать основные опасности среды обитания человека, оценивать риск их реализации, выбирать методы защиты от опасностей и способы обеспечения комфортных условий жизнедеятельности; – проводить расчеты надежности и работоспособности основных видов механизмов; – прогнозировать аварии и катастрофы; ПК-3.3. владеть: – способами и технологиями защиты в чрезвычайных ситуациях; – методами оценки экологической ситуации; – методами математического моделирования надежности и безопасности работы отдельных звеньев реальных технических систем и технических объектов в целом; – приемами и методами оценки риска, а также способен определять меры по обеспечению безопасности разрабатываемой техники.
ПК-4	Способен использовать методы расчетов элементов технологического оборудования по критериям работоспособности и надежности	ПК-4.1. знать: – основы проектирования технических объектов; – основные виды механизмов методы исследования и расчета из кинетических и динамических характеристик; – методы расчета на прочность и жесткость типовых элементов различных конструкций. ПК-4.2. уметь: – применять действующие стандарты, положения и инструкции по оформлению технической

		документации; – применять методы анализа и синтеза исполнительных механизмов; – применять методы расчета и конструирования деталей и узлов механизмов; – проводить расчеты деталей машин, оборудования по критериям работоспособности и надежности; ПК-4.3. владеть: – навыками использования методов теоретической механики, теории механизмов и машин, сопротивления материалов, деталей машин и основ конструирования при решении практических задач; – методами теоретического и экспериментального исследования в механике, электротехнике и электронике. – методами математического моделирования надежности и безопасности работы отдельных звеньев реальных технических систем и технических объектов в целом.
--	--	--

Содержание дисциплины (модуля)

Раздел 1. Информационная безопасность: содержание и структура понятия

Содержание и структура понятия «безопасность». Содержание и структура понятия «информационная безопасность». Содержание и структура понятия «обеспечение информационной безопасности». Содержание и структура понятия «угроза». Классификация угроз.

Раздел 2. Правовое обеспечение информационной безопасности

Направления обеспечения безопасности. Основные статьи российского законодательства о компьютерных преступлениях. Основы правовой защиты информации. Структура законодательства России в области защиты информации. Основы правовой защиты информации.

Раздел 3. Организационное обеспечение информационной безопасности. Компьютерные преступления

Структура законодательства России в области защиты информации. Основы организационных средств обеспечения информационной безопасности. Классификация средств и методов организационной защиты. Понятие компьютерного преступления. Причины совершения. Признаки. Классификация компьютерных преступлений. Понятие «хакер». Виды хакеров. Способы подготовки к действиям компьютерных преступников. Методы незаконного проникновения.

Раздел 4. Инженерно-технические средства обеспечения информационной безопасности. Защита от компьютерных вирусов

Основы инженерно-технических средств обеспечения информационной безопасности. Классификация средств инженерно-технической защиты. Понятие компьютерного вируса. Классификация компьютерных вирусов. Основные этапы жизненного цикла вирусов. Основные каналы распространения компьютерных вирусов. Методы и средства антивирусной защиты. Методы обнаружения вирусов. Антивирусные программы. Виды и структура. Основные критерии качества антивируса. Построение системы антивирусной защиты корпоративной сети.

Раздел 5. Способы защиты информации. Противодействие несанкционированному доступу к информационным ресурсам

Физические средства защиты информации. Аппаратные средства защиты информации. Программные средства защиты информации. Сферы программной защиты. Средства защиты данных и программ. Криптографические средства защиты. Общая технология шифрования.

Раздел 6. Тайна как правовая категория

Понятие конфиденциальной информации. Виды конфиденциальной информации. Коммерческая тайна. Формы защиты коммерческой тайны.