

1. ЦЕЛИ ОСВОЕНИЯ

1.1	Цели освоения дисциплины: понимание моделей и стандартов информационной безопасности, усвоение методов защиты информационных систем, приобретение теоретических знаний и практических навыков по использованию современных программных средств для обеспечения информационной безопасности и защиты информации от несанкционированного использования.
1.2	
1.3	Задачи:
1.4	- изучить основные теоретические положения защиты информации, причины нарушений безопасности;
1.5	- получить практические навыки работы с современными сетевыми фильтрами и средствами криптографического преобразования информации.

2. МЕСТО В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Блок ОП:		Б1.В.ДВ.05
2.1	Требования к предварительной подготовке обучающегося:	
2.1.1	CASE-технологии	
2.1.2	Алгоритмы теории игр	
2.1.3	Базы данных	
2.1.4	Программная инженерия	
2.1.5	Проектный подход в технике	
2.1.6	Технологии программирования	
2.1.7	Численные методы	
2.1.8	Вычислительные системы, сети и телекоммуникации	
2.1.9	Информационные системы и технологии	
2.1.10	Начертательная геометрия и инженерная графика	
2.1.11	Теория вероятностей и математическая статистика	
2.1.12	Языки программирования	
2.1.13	Информатика	
2.2	Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
2.2.1	Безопасность жизнедеятельности	
2.2.2	Интеллектуальные технологии в металлургии	
2.2.3	Интеллектуальные технологии в энергетике	
2.2.4	Научно-исследовательская работа	
2.2.5	Подготовка к процедуре защиты и защита выпускной квалификационной работы	
2.2.6	Преддипломная практика	
2.2.7	Средства информатизации в металлургии	
2.2.8	Средства информатизации в энергетике	

3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ФОРМИРУЕМЫМИ КОМПЕТЕНЦИЯМИ

УК-6: Принятие решений (способен: определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений; управлять своей профессиональной деятельностью или проектами в соответствующей профессиональной сфере, брать на себя ответственность за принятие решений)

Знать:

УК-6-32 основные методы и модели обеспечения и управления информационной безопасностью, методы управления рисками информационной безопасности.

УК-6-31 задачи информационной безопасности, основные тенденции и направления формирования и функционирования комплексной системы защиты информации

УК-3: Проектирование и разработка (способен: проектировать и разрабатывать продукцию, процессы и системы, соответствующие профилю образовательной программы; выбирать и применять соответствующие методики проектирования и разработки, включая передовые методы и технологии)

Знать:

УК-3-31 принципы построения современных систем защиты информации в компьютерных сетях

ПК-2: Способен проектировать прикладные технологии и системы
Знать:
ПК-2-31 информационное обеспечение и принципы построения информационных систем управления технологическими процессами
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Знать:
ОПК-3-31 принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности
УК-6: Принятие решений (способен: определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений; управлять своей профессиональной деятельностью или проектами в соответствующей профессиональной сфере, брать на себя ответственность за принятие решений)
Уметь:
УК-6-У1 проводить анализ возможности применения моделей систем защиты информации различного назначения
УК-6-У2 проводить сравнительный анализ параметров систем защиты информации, определять оптимальные типы криптографических протоколов при передаче информации
УК-3: Проектирование и разработка (способен: проектировать и разрабатывать продукцию, процессы и системы, соответствующие профилю образовательной программы; выбирать и применять соответствующие методики проектирования и разработки, включая передовые методы и технологии)
Уметь:
УК-3-У1 определять применяемые методы несанкционированного доступа к данным
ПК-2: Способен проектировать прикладные технологии и системы
Уметь:
ПК-2-У1 использовать методы системного моделирования технологических процессов
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Уметь:
ОПК-3-У1 решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности
УК-6: Принятие решений (способен: определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений; управлять своей профессиональной деятельностью или проектами в соответствующей профессиональной сфере, брать на себя ответственность за принятие решений)
Владеть:
УК-6-В2 методами и средствами технической защиты информации, методами расчета и инструментального контроля показателей технической защиты информации
УК-6-В1 навыками обоснования решений по выбору и применению моделей систем защиты информации различного назначения
УК-3: Проектирование и разработка (способен: проектировать и разрабатывать продукцию, процессы и системы, соответствующие профилю образовательной программы; выбирать и применять соответствующие методики проектирования и разработки, включая передовые методы и технологии)
Владеть:
УК-3-В1 навыками отслеживания несанкционированного доступа к данным и установки защиты данных
ПК-2: Способен проектировать прикладные технологии и системы
Владеть:
ПК-2-В1 современными компьютерными методами математического моделирования технологических процессов
ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Владеть:

ОПК-3-В1 навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научноисследовательской работе с учетом требований информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Формируемые индикаторы компетенций	Литература и эл. ресурсы	Примечание	КМ	Выполняемые работы
	Раздел 1. Основы информационной безопасности и защиты информации							
1.1	Основные концептуальные положения системы защиты информации. Концептуальная модель информационной безопасности. Обзор и сравнительный анализ стандартов информационной безопасности. Понятие политики безопасности. Принципы организации системы защиты, направления, способы и методы защиты. /Лек/	4	1		Л1.3 Л1.4Л2.1 Л2.3 Л2.4 Э1 Э2 Э3 Э4			
1.2	Самостоятельное изучение учебного материала в LMS Canvas: Основные понятия и определения. Современное состояние и перспективы развития защиты информации. Исследование причин нарушений безопасности.Общая проблема информационной безопасности информационных систем. Защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение). Стандарты и нормативно-методические документы в области обеспечения информационной безопасности. Реализация и гарантирование политики безопасности. Состав и назначение должностных инструкций. /Ср/	4	26		Л1.3 Л1.4Л2.1 Л2.3 Л2.4 Э1 Э2 Э3 Э4			
1.3	Разработка и реализация алгоритма функционирования системы безопасности объектов. /Лаб/	4	2		Л1.3 Л1.4Л2.1 Л2.3 Л2.4Л3.1 Э1 Э2 Э3 Э4			
	Раздел 2. Модели безопасности в компьютерных системах							

2.1	<p>Модели безопасного субъектного взаимодействия в компьютерной системе. Процедура идентификации и аутентификации. Сопряжение защитных механизмов. Архитектура защищенных операционных систем. Модели сетевых сред. Создание механизмов безопасности в распределенной компьютерной системе. /Лек/</p>	4	1		<p>Л1.3 Л1.4Л2.1 Л2.4 Э1 Э2 Э3</p>			
2.2	<p>Самостоятельное изучение учебного материала в LMS Canvas: Аутентификация пользователей. Формализация задачи сопряжения. Методы сопряжения. Типизация данных, необходимых для обеспечения работы средств сопряжения. Понятие внешнего разделяемого сервиса безопасности. Постановка задачи. Понятие и свойства модуля реализации защитных функций. /Ср/</p>	4	24		<p>Л1.3 Л1.4Л2.1 Л2.4 Э1 Э2 Э3 Э4</p>			
2.3	<p>Разработка и реализация алгоритма функционирования системы безопасности субъектов. Проектирование модуля реализации защитных функций в среде гарантирования политики безопасности. /Лаб/</p>	4	4		<p>Л1.3 Л1.4Л2.1 Л2.4Л3.1 Э1 Э2 Э3 Э4</p>			
	<p>Раздел 3. Защита информации в компьютерных сетях</p>							
3.1	<p>Особенности обеспечения информационной безопасности в компьютерных сетях. Специфика средств защиты в компьютерных сетях. Сетевые модели передачи данных. Понятие протокола передачи данных. Принципы организации обмена данными в вычислительных сетях. Транспортный протокол TCP и модель TCP/IP. Модель взаимодействия открытых систем OSI/ISO. Современные средства построения защищенных виртуальных сетей. /Лек/</p>	4	2		<p>Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Э1 Э2 Э3 Э4</p>			

3.2	Самостоятельное изучение учебного материала в LMS Canvas: Классы удаленных угроз и их характеристика. Типовые удаленные атаки и их характеристика. Сравнение сетевых моделей передачи данных TCP/IP и OSI/ISO. Характеристика уровней модели OSI/ISO. Адресация в глобальных сетях. Основы IP-протокола. Классы адресов вычислительных сетей. Система доменных имен. Принципы защиты распределенных вычислительных сетей. /Ср/	4	24		Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Э1 Э2 Э3 Э4			
3.3	Разработка и реализация алгоритма сетевого фильтра. Построение защищенных виртуальных сетей. Безопасность удаленного доступа к локальной сети. /Лаб/	4	4		Л1.3 Л1.4Л2.1 Л2.2 Л2.4Л3.1 Э1 Э2 Э3 Э4			
	Раздел 4. Методы и системы защиты информации							
4.1	Защита информации от несанкционированного доступа. Каналы утечки информации. Системы анализа защищённости и обнаружения вторжений. Модели и источники каналов утечки информации. Способы несанкционированного доступа к информации. Компьютерные средства реализации защиты в информационных системах. Общие сведения по классической криптографии и алгоритмам блочного шифрования. Цифровая электронная подпись. /Лек/	4	2		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.4 Э1 Э2 Э3 Э4			
4.2	Самостоятельное изучение учебного материала в LMS Canvas: Причины нарушения целостности информации. Функции непосредственной защиты информации. Задачи защиты информации. Методы и системы защиты информации. Аппаратные средства защиты. Программные средства защиты. Криптографические средства защиты. Выполнение контрольной работы. Подготовка к зачету с оценкой. /Ср/	4	48		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.4 Э1 Э2 Э3 Э4			

4.3	Разработка и реализация алгоритма криптографического преобразования. /Лаб/	4	2		Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.4Л3.1 Э1 Э2 Э3 Э4			
4.4	Проведение зачета с оценкой /ЗачётСОц/	4	4		Э1 Э2 Э3 Э4			