МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Беловский институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования
«Кемеровский государственный университет» (БИФ КемГУ)
Кафедра экономических наук и информационных технологий

УТВЕРЖДАЮ
Директор БИФ КемГУ
_____ В.А. Саркисян
«27» февраля 2019г.

Аннотация
рабочей программы дисциплины модуля
Профессиональный цикл

Информационная безопасность и защита информации

Направление подготовки
02.03.02 Фундаментальная информатика и информационные технологии
(шифр, название направления)

Направленность (профиль) подготовки
Открытые информационные системы

Форма обучения
очная, очно-заочная
(очная, заочная, очно-заочная и др.)

Белово *20* ***19***

1. *Цели и задачи дисциплины*

Цели преподавания дисциплины:

Целью изучения дисциплины «Информационная безопасность и защита информации» является ознакомление студентов с тенденцией развития информационной безопасности, с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации, а так же с нормативными документами.

Задачами дисциплины являются: ознакомление студентов с терминологией информационной безопасности, развитие мышления студентов, изучение методов и средств обеспечения информационной безопасности, обучение определению причин, видов, каналов утечки и искажения информации.

2. *Требования к результатам освоения дисциплины (табл. из п.1 РП)*

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения**
ПК-6 Способность собирать, обрабатывать и интерпретировать экспериментальные данные, необходимые для проектной и производственно-технологической деятельности; способность к разработке новых алгоритмических, методических и технологических решений в конкретной сфере профессиональной деятельности.	**ИПК-6.1.** Знает основы проектирования и элементы архитектурных решений информационных систем. **ИПК-6.2.** Умеет применять в практической деятельности профессиональные стандарты в области информационных технологий. **ИПК-6.3.** Имеет практический опыт составления технического задания на разработку	**знать:** - понятие информации, способы ее представления, основные приемы получения, хранения, обработки информации; - основные понятия информационной безопасности, критерии оценки защищенности систем; - основные Федеральные законы и нормативно-правовые акты в области защиты информации, их сферу действия и основные положения; - правовые акты в области защиты государственной тайны и информационной безопасности; - правовые основы организации защиты государственной тайны и конфиденциальной информации; основные принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах и оболочках; стандарты безопасности информационных технологий; - типовые подсистемы безопасности информационных систем и принципы их функционирования, примеры средств их реализации; - основные принципы организации и алгоритмы функционирования операционных систем и оболочек; - возможности применения в работе современных системных программных средств: операционных систем, операционных оболочек, обслуживающих программ; - угрозы в процессе проектирования и разработки программного обеспечения и принципы безопасного программирования; - стандартные программные средства набора текста и баз данных; проблемы и направления развития системных программных средств. – о проблемах и направлениях развития аппаратных и программных средств защиты информации;

		– о современных криптографических системах. **уметь:** применять действующие нормативно-правовые акты по защите персональных данных, государственных информационных систем, объектов критической информационной инфраструктуры при проектировании, разработке, внедрении и эксплуатации программного обеспечения и информационных систем: – использовать программные и аппаратные средства персонального компьютера; – ориентироваться в современной системе источников информации; – применять средства антивирусной защиты; – анализировать информационную безопасность многопользовательских систем; – пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа; – - категорировать проектируемые и разрабатываемые информационные системы по классам (уровням); видеть и формулировать проблему, видеть конкретную ситуацию, прогнозировать и предвидеть, рассчитывать риски, ставить цели и задачи. **владеть (иметь навыки, опыт практической работы):** - обеспечения безопасной работы на компьютере; - поиска информации в глобальной информационной сети Интернет, работы с базами данных и Интернет-ресурсами; - современной терминологией и методологией в области информационной безопасности; – применения аппаратных и программных средств обеспечения информационной безопасности; противостояния типовым удаленным атакам, формирование навыков построения комплексной защиты информационных сервисов и ресурсов, применения стандартных программно-аппаратных средств обеспечения информационной безопасности. - участия в разработке программного обеспечения для решения задач защиты информации.
ПК-7 Способность к анализу требований и разработке вариантов реализации информационной системы; способность к оценке качества, надежности и эффективности информационной системы в конкретной профессиональной сфере.	**ИПК-7.1.** Знает методику анализа требований и вариантов реализации информационных систем. **ИПК-7.2.** Умеет оценивать качество, надежность и эффективность информационной системы. **ИПК-7.3.** Имеет практический опыт разработки вариантов реализации информационных систем.	**знать:** - принципы построения информационной безопасности; - экономические предпосылки внедрения информационной безопасности; - методы и средства выявления уязвимостей информационных систем; - способы исследования программного обеспечения на отсутствие недекларированных возможностей; - понятие политики информационной безопасности, типовые организационные меры защиты информации; - типовые сервисы безопасности операционных систем; - типовые программные средства защиты информации от несанкционированного доступа в

		компьютерную среду, средства антивирусной защиты и средства обеспечения безопасности при сетевом взаимодействии. **уметь:** - проводить экспериментальный анализ защищённости в компьютерной среде с применением специализированного программного обеспечения; - осуществлять выбор средств и методов для решения конкретных задач; - пользоваться специальной литературой в изучаемой предметной области; - использовать международные и отечественные стандарты; **владеть (иметь навыки, опыт практической работы):** - навыками чтения и перевода технической документации на английском языке; - методикой оценки стойкости парольной защиты; - навыками организационного регулирования защиты процессов переработки информации.
ПК-8 Способность к установке, администрированию программных систем; к реализации технического сопровождения информационных систем; к интеграции информационных систем с используемыми аппаратно-программными комплексами.	**ИПК-8.1.** Знает методику установки и администрирования программных систем. **ИПК-8.2.** Умеет реализовывать техническое сопровождение информационных систем. **ИПК-8.3.** Имеет практический опыт разработки интеграции информационных систем с использованием аппаратно-программных комплексов.	**знать:** - требования к защите информации в автоматизированных (информационных) системах различных классов защищённости; - основные модели дискреционного, мандатного и ролевого управления доступом, их сравнительные возможности и примеры применения в подсистемах безопасности операционных систем и баз данных; инструкции man для функций ОС Linux; - основы языков разметки (язык HTML, XHTML, XML, CSS); - основы программирования приложений для Web; - технологии работы с реляционными базами данных через WEB-интерфейс; - проблемы и направления развития отечественных и зарубежных информационных ресурсов; - основные понятия, термины и определения в области информационной безопасности и защиты информации; - основные виды угроз безопасности в информационных системах, их классификацию, понятие модели угроз, методы определения актуальных угроз и оценки рисков информационной безопасности **уметь:** - ориентироваться в современных web-технологиях, их возможностях, перспективах развития; - проводить анализ существующих узлов и разрабатывать новые web-узлы; владеть навыками работы в современной программно-технической среде в различных операционных системах. **устанавливать средства защиты информации при сетевом взаимодействии и анализировать корректность их функционирования** настраивать стандартные сервисы безопасности операционных систем и анализировать корректность их функционирования

		владеть (иметь навыки, опыт практической работы): - приобретение практических навыков безопасной работы с информацией, включая работу в локальных и глобальных компьютерных сетях.
ПК-9 Способность применять в профессиональной деятельности современные языки программирования и методы параллельной обработки данных, операционные системы, электронные библиотеки и пакеты программ, сетевые технологии.	**ИПК-9.1.** Знает современные языки программирования и методы параллельной обработки данных. Знаком с содержанием Единого Реестра Российских программ для электронных вычислительных машин и баз данных. **ИПК-9.2.** Умеет реализовывать численные методы решения прикладных задач в профессиональной сфере деятельности, пакеты программного обеспечения, операционные системы, электронные библиотеки, сетевые технологии. **ИПК-9.3.** Имеет практический опыт разработки интеграции информационных систем.	**знать:** - написание и аббревиатуру специальных терминов на иностранном языке. - международные и отечественные правовые и нормативные акты обеспечения ИБ процессов переработки информации; - ответственность за нарушение законодательства в информационной сфере; - модель ISO/OSI и стек протоколов TCP/IP; - проблемы безопасности IP- сетей; - угрозы и уязвимости проводных корпоративных сетей; - угрозы и уязвимости беспроводных сетей; - способы обеспечения информационной безопасности; - проблемы обеспечения безопасности ОС; - правила разграничения доступа; - функции межсетевых экранов; - протоколы формирования защищенных каналов; - протоколы формирования каналов на сеансовом уровне; - протокол SOCKS; - базы данных SAD и SPD; - протоколы аутентификации удаленных пользователей; - концепции адаптивного управления безопасностью; - классификации вирусов. **уметь:** - оценить выбор программного обеспечения ОС и СУБД в контексте требований по защите информации; в ОС UNIX переводить man инструкции на английском языке; - проводить исследование подсистемы парольной аутентификации пользователей. - использовать международные правовые и нормативные акты обеспечения ИБ; - анализировать угрозы сетевой безопасности; - решать проблемы защиты информации в сетях; - использовать основные функции подсистемы защиты операционной системы; - разграничивать доступ к объектам операционной системы; - особенности функционирования межсетевых кранов на различных уровнях модели OSI; - схемы сетевой защиты на базе межсетевых экранов; - управлять идентификацией и доступом; - построить систему антивирусной защиты сети. **владеть (практический опыт):** - навыками категорирования объектов и защиты информационной собственности; сетевого информационного обмена; использования сетей интернет; идентификации, аутентификации и авторизации субъектов доступа; администрирования, регистрации событий и генерации отчетов; защиты

		беспроводных сетей; организации защищенного удаленного доступа; использования антивирусных программ и комплексов; защиты информации при взаимодействии абонентов с сетями общего пользования.

3. Общая трудоемкость дисциплины – 3 з.е., 108 часов

4. Содержание дисциплины (дидактические единицы)

Информационная безопасность (ИБ) деятельности общества и её основные положения. Организационное и правовое обеспечение ИБ. Методологические основы обеспечения ИБ жизнедеятельности общества и его структур. Методологическое и техническое обеспечение ИБ функционирования предприятий. Программно-аппаратные средства обеспечения ИБ функционирования организаций.