

**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**

*(цифр, название направления)*

Направленность (профиль) подготовки

**Открытые информационные системы**

Форма обучения

**очная, очно-заочная**

*(очная, заочная, очно-заочная и др.)*

## 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
<b>ПК-6</b> 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.	<b>ИПК-6.1.</b> Знает основы проектирования и элементы архитектурных решений информационных систем. <b>ИПК-6.2.</b> Умеет применять в практической деятельности профессиональные стандарты в области информационных технологий. <b>ИПК-6.3.</b> Имеет практический опыт составления технического задания на разработку	<b>знать:</b> <ul style="list-style-type: none"><li>- понятие информации, способы ее представления, основные приемы получения, хранения, обработки информации;</li><li>- основные понятия информационной безопасности, критерии оценки защищенности систем;</li><li>- основные Федеральные законы и нормативно-правовые акты в области защиты информации, их сферу действия и основные положения;</li><li>- правовые акты в области защиты государственной тайны и информационной безопасности;</li><li>- правовые основы организации защиты государственной тайны и конфиденциальной информации;</li><li>основные принципы организации и алгоритмы функционирования систем безопасности в современных операционных системах и оболочках; стандарты безопасности информационных технологий;</li><li>- типовые подсистемы безопасности информационных систем и принципы их функционирования, примеры средств их реализации;</li><li>- основные принципы организации и алгоритмы функционирования операционных систем и оболочек;</li><li>- возможности применения в работе современных системных программных средств: операционных систем, операционных оболочек, обслуживающих программ;</li><li>- угрозы в процессе проектирования и разработки программного обеспечения и принципы безопасного программирования;</li><li>- стандартные программные средства набора текста и баз данных; проблемы и направления развития системных программных средств.</li><li>- о проблемах и направлениях развития аппаратных и программных средств защиты информации;</li></ul>

		<p>– о современных криптографических системах.</p> <p><b>уметь:</b>  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:</p> <ul style="list-style-type: none"> <li>– использовать программные и аппаратные средства персонального компьютера;</li> <li>– ориентироваться в современной системе источников информации;</li> <li>– применять средства антивирусной защиты;</li> <li>– анализировать информационную безопасность многопользовательских систем;</li> <li>– пользоваться программными средствами, реализующими основные криптографические функции - системы публичных ключей, цифровую подпись, разделение доступа;</li> <li>– 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.</li> </ul> <p><b>владеть (иметь навыки, опыт практической работы):</b></p> <ul style="list-style-type: none"> <li>- обеспечения безопасной работы на компьютере;</li> <li>- поиска информации в глобальной информационной сети Интернет, работы с базами данных и Интернет-ресурсами;</li> <li>- современной терминологией и методологией в области информационной безопасности;</li> <li>- 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.</li> <li>- участия в разработке программного обеспечения для решения задач защиты информации.</li> </ul>
<p><b>ПК-7</b> Способность к анализу требований и разработке вариантов реализации информационной системы; способность к оценке качества, надежности и эффективности информационной системы в конкретной профессиональной сфере.</p>	<p><b>ИПК-7.1.</b> Знает методику анализа требований и вариантов реализации информационных систем.</p> <p><b>ИПК-7.2.</b> Умеет оценивать качество, надежность и эффективность информационной системы.</p> <p><b>ИПК-7.3.</b> Имеет практический опыт разработки вариантов реализации информационных систем.</p>	<p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- принципы построения информационной безопасности;</li> <li>- экономические предпосылки внедрения информационной безопасности;</li> <li>- методы и средства выявления уязвимостей информационных систем;</li> <li>- способы исследования программного обеспечения на отсутствие недекларированных возможностей;</li> <li>- понятие политики информационной безопасности, типовые организационные меры защиты информации;</li> <li>- типовые сервисы безопасности операционных систем;</li> <li>- типовые программные средства защиты информации от несанкционированного доступа в</li> </ul>

		<p>компьютерную среду, средства антивирусной защиты и средства обеспечения безопасности при сетевом взаимодействии.</p> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- проводить экспериментальный анализ защищённости в компьютерной среде с применением специализированного программного обеспечения;</li> <li>- осуществлять выбор средств и методов для решения конкретных задач;</li> <li>- пользоваться специальной литературой в изучаемой предметной области;</li> <li>- использовать международные и отечественные стандарты;</li> </ul> <p><b>владеть (иметь навыки, опыт практической работы):</b></p> <ul style="list-style-type: none"> <li>- навыками чтения и перевода технической документации на английском языке;</li> <li>- методикой оценки стойкости парольной защиты;</li> <li>- навыками организационного регулирования защиты процессов переработки информации.</li> </ul>
<p><b>ПК-8</b> Способность к установке, администрированию программных систем; к реализации технического сопровождения информационных систем; к интеграции информационных систем с используемыми аппаратно-программными комплексами.</p>	<p><b>ИПК-8.1.</b> Знает методику установки и администрирования программных систем.</p> <p><b>ИПК-8.2.</b> Умеет реализовывать техническое сопровождение информационных систем.</p> <p><b>ИПК-8.3.</b> Имеет практический опыт разработки интеграции информационных систем с использованием аппаратно-программных комплексов.</p>	<p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- требования к защите информации в автоматизированных (информационных) системах различных классов защищённости;</li> <li>- 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;</li> <li>- основы языков разметки (язык HTML, XHTML, XML, CSS);</li> <li>- основы программирования приложений для Web;</li> <li>- технологии работы с реляционными базами данных через WEB-интерфейс;</li> <li>- проблемы и направления развития отечественных и зарубежных информационных ресурсов;</li> <li>- основные понятия, термины и определения в области информационной безопасности и защиты информации;</li> <li>- основные виды угроз безопасности в информационных системах, их классификацию, понятие модели угроз, методы определения актуальных угроз и оценки рисков информационной безопасности</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- ориентироваться в современных web-технологиях, их возможностях, перспективах развития;</li> <li>- проводить анализ существующих узлов и разрабатывать новые web-узлы;</li> <li>- владеть навыками работы в современной программно-технической среде в различных операционных системах.</li> </ul> <p><b>устанавливать средства защиты информации при сетевом взаимодействии и анализировать корректность их функционирования</b></p> <p>настраивать стандартные сервисы безопасности операционных систем и анализировать корректность их функционирования</p>

		<p><b>владеть (иметь навыки, опыт практической работы):</b></p> <ul style="list-style-type: none"> <li>- приобретение практических навыков безопасной работы с информацией, включая работу в локальных и глобальных компьютерных сетях.</li> </ul>
<p><b>ПК-9</b> Способность применять в профессиональной деятельности современные языки программирования и методы параллельной обработки данных, операционные системы, электронные библиотеки и пакеты программ, сетевые технологии.</p>	<p><b>ИПК-9.1.</b> Знает современные языки программирования и методы параллельной обработки данных. Знаком с содержанием Единого Реестра Российских программ для электронных вычислительных машин и баз данных.</p> <p><b>ИПК-9.2.</b> Умеет реализовывать численные методы решения прикладных задач в профессиональной сфере деятельности, пакеты программного обеспечения, операционные системы, электронные библиотеки, сетевые технологии.</p> <p><b>ИПК-9.3.</b> Имеет практический опыт разработки интеграции информационных систем.</p>	<p><b>знать:</b></p> <ul style="list-style-type: none"> <li>- написание и аббревиатуру специальных терминов на иностранном языке.</li> <li>- международные и отечественные правовые и нормативные акты обеспечения ИБ процессов переработки информации;</li> <li>- ответственность за нарушение законодательства в информационной сфере;</li> <li>- модель ISO/OSI и стек протоколов TCP/IP;</li> <li>- проблемы безопасности IP- сетей;</li> <li>- угрозы и уязвимости проводных корпоративных сетей;</li> <li>- угрозы и уязвимости беспроводных сетей;</li> <li>- способы обеспечения информационной безопасности;</li> <li>- проблемы обеспечения безопасности ОС;</li> <li>- правила разграничения доступа;</li> <li>- функции межсетевых экранов;</li> <li>- протоколы формирования защищенных каналов;</li> <li>- протоколы формирования каналов на сеансовом уровне;</li> <li>- протокол SOCKS;</li> <li>- базы данных SAD и SPD;</li> <li>- протоколы аутентификации удаленных пользователей;</li> <li>- концепции адаптивного управления безопасностью;</li> <li>- классификации вирусов.</li> </ul> <p><b>уметь:</b></p> <ul style="list-style-type: none"> <li>- оценить выбор программного обеспечения ОС и СУБД в контексте требований по защите информации; в ОС UNIX переводить ман инструкции на английском языке;</li> <li>- проводить исследование подсистемы парольной аутентификации пользователей.</li> <li>- использовать международные правовые и нормативные акты обеспечения ИБ;</li> <li>- анализировать угрозы сетевой безопасности;</li> <li>- решать проблемы защиты информации в сетях;</li> <li>- использовать основные функции подсистемы защиты операционной системы;</li> <li>- разграничивать доступ к объектам операционной системы;</li> <li>- особенности функционирования межсетевых экранов на различных уровнях модели OSI;</li> <li>- схемы сетевой защиты на базе межсетевых экранов;</li> <li>- управлять идентификацией и доступом;</li> <li>- построить систему антивирусной защиты сети.</li> </ul> <p><b>владеть (практический опыт):</b></p> <ul style="list-style-type: none"> <li>- 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</li> </ul>

		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.