Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет»
(ФГБОУ ВО «ИГУ»)
Факультет (институт) физический
Кафедра радиофизики и радиоэлектроники

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине Б1.Б.2 «Организационно-правовые механизмы обеспечения информационной безопасности»

направление подготовки 03.04.03 «Радиофизика»

направленность (профиль) «Информационные процессы и системы»

Иркутск, 2016

Разработан в соответствии с ФГОС ВО по направлению подготовки 03.04.03 от 28 ноября 2014 г. N 1417

с учетом требований проф. стандарта: Научный работник (научная (научно-исследовательская) деятельность).

Одобрен
УМК физического факультета
Протокол №3 от «28.06.2016»

Председатель УМК декан, д.ф.-м.н., проф Буднев Н.М.
ФИО, должность, ученая степень, звание *подпись*

Разработчик Колесник С.Н. доц, к.ф.-м.н., доц
ФИО, должность, ученая степень, звание *подпись*

Декан, д.ф.-м.н., профессор Буднев Н.М.
ФИО, должность, ученая степень, звание *подпись*

ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине Б1.Б.2 «Организационно-правовые механизмы обеспечения информационной безопасности»
направление подготовки 03.04.03 «Радиофизика»
направленность (профиль) «Информационные процессы и системы»

1. **Компетенции (дескрипторы компетенций), формируемые в процессе изучения дисциплины** (курс 1 семестр 1):

Индекс и наименование компетенции (в соответствии с ФГОС ВО (ВПО)	Признаки проявления компетенции/ дескриптора (ов) в соответствии с уровнем формирования в процессе освоения дисциплины
способностью к абстрактному мышлению, анализу, синтезу (ОК-1).	Знать: правила оформления нормативных актов; правила использования нормативные правовые документы в деятельности; правила обеспечения информационной безопасности, изложенные в стандартах; Уметь: составлять и оформлять локальные нормативные акты, регулирующие и регламентирующую профессиональную деятельность; составлять и оформлять обзор по обеспечению информационной безопасности профессиональной деятельности; обеспечивать информационную безопасность на основе стандартов; Владеть: навыками использования общегосударственных и локальных нормативно-методических документов в профессиональной деятельности; способностью составления обзора по вопросам обеспечения информационной безопасности профессиональной деятельности; способностью анализа информационной безопасности систем, объектов с использованием стандартов.
готовностью действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения (ОК-2)	Знать: последствия, наступающие в результате утечки информации;
готовностью руководить коллективом в сфере своей профессиональной деятельности, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия (ОПК-2)	Уметь: организовать работу коллектива по защите информации
способностью к свободному владению профессионально-	Уметь: использовать современные компьютерные сети, программные продукты и ресурсы информационно-

профилированными знаниями в области информационных технологий, использованию современных компьютерных сетей, программных продуктов и ресурсов Интернет для решения задач профессиональной деятельности, в том числе находящихся за пределами профильной подготовки (ОПК-4)	телекоммуникационной сети «Интернет» для изучения организационно-правовых механизмов обеспечения информационной безопасности.
способностью к подготовке и проведению лабораторных и семинарских занятий (включая участие в разработке учебно-методических пособий), к руководству научной работой обучающихся младших курсов образовательных организаций высшего образования и общеобразовательных организаций в области физики и радиофизики (ПК-7)	Уметь: проводить занятия и инструктажи с персоналом, отвечающим за безопасность информации, проводить фрагмент занятия

2. В результате освоения дисциплины обучающийся должен

Знать: правила оформления нормативных актов; правила использования нормативные правовые документы в деятельности; правила обеспечения информационной безопасности, изложенные в стандартах; последствия, наступающие в результате утечки информации.

Уметь: составлять и оформлять локальные нормативные акты, регулирующие и регламентирующую профессиональную деятельность; составлять и оформлять обзор по обеспечению информационной безопасности профессиональной деятельности; обеспечивать информационную безопасность на основе стандартов; организовать работу коллектива по защите информации; использовать современные компьютерные сети, программные продукты и ресурсы информационно-телекоммуникационной сети «Интернет» для изучения организационно-правовых механизмов обеспечения информационной безопасности; проводить занятия и инструктажи с персоналом, отвечающим за безопасность информации, проводить фрагмент занятия.

Владеть: навыками использования общегосударственных и локальных нормативно-методических документов в профессиональной деятельности; способностью составления обзора по вопросам обеспечения информационной безопасности профессиональной деятельности; способностью анализа информационной безопасности систем, объектов с использованием стандартов.

3. Программа оценивания контролируемой компетенции:

Тема или раздел дисциплидины	Формируемый признак компетенции	Показатель	Критерий оценивания	Наименование ОС	
				ТК	ПА[4]
Т1. Государственная политика в сфере обеспечения информационной безопасности: общие положения и проблемы законодательства	**Знать** основы информационного права, законодательные и нормативные акты по защите информации	Знает основные положения законодательства и нормативные акты в сфере защиты информации	**Отлично (4балла).** Полностью и корректно выполнены все задания, получены ответы на все вопросы. **Хорошо (2.9 балла).** Полностью выполнены все задания, получены ответы на все вопросы. Допущены одна – две ошибки. **Удовлет-ворительно (1,5 балла).** Не полностью выполнены задания, не полные ответы на вопросы. Допущены одна – две ошибки. **Неудовлет-ворительно (0 баллов).** Задание не выполнено или задание выполнено не полностью, на вопросы не получены ответы. Допущено	ПК,УК	Зач
Т2. Защита информации с ограниченным доступом	**Знать** последствия за правонарушения в области информационной безопасности; порядок обеспечения информационной безопасности на основе стандартов; **Уметь** использовать современные информационные ресурсы для изучения вопросов информационной безопасности.	Знает о последствиях, возникающих при правонарушениях в области информационной безопасности; содержание стандартов по обеспечению информационной безопасности. Умеет получать информацию с помощью информационных ресурсов и их сети «Интернет»		ПК,УК	Зач
Т3. Организационно-техническая защита информации предприятия	**Знать** способы организации внутриобъектного и пропускного режима на предприятии; организацию работу коллектива по защите информации на предприятии; проводить инструктажи с персоналом по вопросу информационной безопасности.	Знает способы организации пропускного режима и внутреннего контроля на объектах предприятия; нормативную базу в сфере защиты информации для организации инструктажа персонала и деятельности сотрудников по защите		ПК,УК	Зач

		информации на предприятии.	более 3-х ошибок.		
Т4. Организационно-правовая защита информации предприятия	**Знать** правила оформления нормативных актов, регламентирующих деятельность по защите информации; последствия, наступающие в результате утечки информации. **Уметь** составлять локальные нормативные акты регламентирующие правовую деятельность по защите информации; составлять обзор нормативных актов по обеспечению информационной безопасности; хранить служебную тайну; **Владеть** способностью анализа информационной безопасности с использованием стандартов	Знает действующие правила оформления нормативных актов, умеет составлять локальные нормативные акты; какая наступит ответственность за утечку информации. Используя информационные ресурсы умеет составлять обзор нормативных актов по информационной безопасности. Владеет навыками анализа стандартов по информационной безопасности;		ПК,УК	Зач
Т5. Технология защиты информации при отдельных видах деятельности	**Знать** правила защиты информации при осуществлении публичной деятельности предприятия. **Уметь** организовать подготовку и проведение заседаний по конфиденциальным вопросам**.**	Знает правила защиты информации при организации рекламной, издательской деятельности предприятия. знает правила проведения заседаний по конфиденциаль-ным вопросам, умеет использовать эти правила при		ПК,УК	Зач

		организации заседаний и совещаний.			
Т6. Аналитическая, контрольная и плановая деятельность по защите информации в организациях	**Знать** нормативно правовые документы по защите информационной безопасности **Уметь** использовать ресурсы сети «Интернет» для изучения организационно-правовых механизмов обеспечения безопасности. Владеть способностью анализа направлений совершенствования информационной безопасности на предприятии;	Знает способы организации и контроля состояния защиты конфиденциальной информации в организации. Умеет использовать информационные ресурсы для получения информации об организационно-правовых механизмах обеспечения информационной безопасности. Владеет знаниями для определения основных направлений аналитической и плановой работы по защите информации в предприятиях.		ПК,УК	Зач

ПК – письменный контроль, УК – устный контроль.

Оценочные средства для проведения промежуточной аттестации[1]

Промежуточная аттестация направлена на проверку сформированности компетенций ОК-1, ОК-2, ОПК-2, ОПК-4, ПК-7 и проводится в форме зачета. Промежуточная аттестация проводится по оценочным средствам текущего контроля по окончании семестра.

Магистрант получает «зачет», который фиксируется в ведомости и зачетной книжке студента в том случае, если в течение семестра за текущую работу набрано более 40 баллов. В противном случае выставляется «незачет».

Оценочные средства для оценки текущей успеваемости студентов

1. Характеристика ОС для обеспечения текущего контроля по дисциплине

Раздел/ Тема	Индекс и уровень формируемой компетенции или дескриптора	ОС	Содержание задания
Т.4. Пз1. Составление формы конфиденциальных документов	ОК-1 (З-1), ОК-2 (З-2), ОПК-4 (У-3), ПК-7 (В-1).	ПК, УК	Понятие информационной безопасности. Принципы обеспечения информационной безопасности. Структура информационной безопасности. Типы отношений в сфере права информационной собственности, возникающих при реализации информационных процессов. Основные общие законы Российской Федерации в области информационной безопасности. Основные руководящие документы и стандарты по обеспечению информационной безопасности. Структура нормативной базы Российской Федерации по вопросам информационной безопасности.
Т.4. Пз2. Составление формы ценной информации	ОК-1 (З-1), ОК-2 (З-2), ОПК-4 (У-3), ПК-7 (В-1).	ПК, УК	Конституция Российской Федерации о защите прав граждан в информационной сфере. Организационная основа системы правового обеспечения информационной безопасности Российской Федерации. Методы правового обеспечения ИБ. Понятие «государственная тайна». Правовой режим защиты государственной тайны. Засекречивание информации. Основные принципы засекречивания информации.
Т.4. Пз3. Составление формы инструкции по обеспечению безопасности информации	ОК-1 (З-1), ОК-2 (З-2), ОПК-4 (У-3), ПК-7 (В-1).	ПК, УК	Порядок засекречивания информации, составляющей государственную тайну. Правовая защита персональных данных. Классификация персональных данных. Правовое регулирование защиты права на неприкосновенность частной жизни. Правовая база защиты коммерческой тайны. Порядок обеспечения защиты

			коммерческой тайны.
Т.4. Пз4. Составление формы правил обеспечения безопасности секретов в экстремальных ситуациях	ОК-1 (З-1), ОК-2 (З-2), ОПК-4 (У-3), ПК-7 (В-1).	ПК, УК	Коммерческая тайна. Признаки коммерческой тайны. Информация, которая не может относиться к коммерческой тайне. Служебная тайна. Информация, которая не может относиться к служебной тайне. Особенности регулирования информационных отношений институтом патентного права. Особенности регулирования информационных отношений институтом авторского права.
Т.5. Пз5. Составление документов, определяющих порядок доступа к конфиденциальной информации командированных лиц	ОК-1 (З-1), ОПК-2 (У-2), ОПК-4 (У-3), ПК-7 (У-4)	ПК, УК	Юридическая ответственность за правонарушения в области информационной безопасности. Правовое обеспечение защиты профессиональной тайны. Роль права в регулировании комплекса отношений в сфере защиты информации. Отрасли права, обеспечивающие законность в области защиты информации. Роль и место организационной защиты информации в системе комплексной защиты информации.
Т.6. Пз6. Составление акта анализа объекта защиты	ОК-1 (З-1), ОПК-4 (У-3)	ПК, УК	Задачи и функции, возлагаемые на руководителей и должностных лиц предприятия в решении задач по организационной защите информации. Организационно-техническая защита информации: определение, методы, средства защиты. Физическая защита информации: определение, средства защиты. Организационно-правовая защита информации фирмы: определение, методы, средства защиты.
Т.6. Пз7. Составление формы плана мероприятий по защите конфиденциальной информации.	ОК-1 (З-1), ОПК-4 (У-3)	ПК, УК	Перечень локальных нормативных актов предприятия по защите конфиденциальной информации, порядок создания. Мероприятия по защите информации в чрезвычайных ситуациях. Локальные нормативные акты по защите персональных данных работников. Понятие внутриобъектового режима на предприятии. Основные цели, подходы и принципы организации внутриобъектового режима.
Т.6. Пз8.	ОК-1 (З-1),	ПК,	Роль и место внутриобъектового

Составление формы аналитического отчета по защите информации.	ОПК-4 (У-3)	УК	режима на предприятии в общей системе защиты конфиденциальной информации. Организация защиты информации при проведении совещаний. Виды компьютерных преступлений. Классификация компьютерных злоумышленников. Ответственность. Организация защиты информации при осуществлении рекламной и публикаторской деятельности.
Т.6. Пз9. Оформление заключения о результатах проведенного служебного расследования.	ОК-1 (З-1), ОПК-4 (У-3)	ПК, УК	Контроль защиты конфиденциальной информации на предприятии. Служебное расследование по фактам нарушения защиты конфиденциальной информации. Организация аналитической работы в области защиты информации.
Т.6 КСР	ОК-1 (З-1), ОПК-4 (У-3)	ПК	Порядок доступа к конфиденциальной информации командированных лиц. Порядок допуска граждан к секретным сведениям. Порядок доступа граждан к коммерческой тайне.

Текущий контроль реализуется в виде письменного текущего контроля на ПЗ1-ПЗ9. Текущий контроль направлен на выявление сформированности компетенций ОК-1, ОК-2, ОПК-2, ОПК-4, ПК-7.

Для реализации текущего контроля используется балльно-рейтинговая система оценки.

Максимальное количество баллов за текущую работу в семестре ограничивается 60-ю баллами. За посещение одного вида занятия дается 0.5 балла (20 занятий (Л+Пз+СКР) * 0.8 балла = 16 баллов), максимальное количество баллов за письменный контроль на одном СКР или одном Пз – 4.4 балла (10 занятий (КСР+ПЗ)*4.4 балла = 44 балла).

Таблица 1. Параметры оценочного средства для письменного текущего контроля на ПЗ1-ПЗ9, КСР.

Критерии оценки	Оценка / баллы			
	Отлично 4 балла.	Хорошо 2.9 балла	Удовлетв. 1.5 балла.	Неудовл. 0 баллов
Выполнение заданий	Полностью и корректно выполнены все задания.	Полностью выполнены все задания, допущены одна – две ошибки.	Не полностью выполнены задания, допущены одна – две ошибки.	Задание не выполнено или задание выполнено не полностью и допущено более 3-х ошибок.

2. **Оценочные средства, обеспечивающие диагностику сформированности компетенций, заявленных в рабочей программе дисциплины (модуля)**

Результат диагностики сформированности компетенций ОК-1, ОК-2, ОПК-2, ОПК-4, ПК-7	**Показатели**	**Критерии**	**Соответствие/ несоответствие**	**Зачет**
ОК-1 знать правила оформления нормативных актов; правила использования нормативные правовые документы в деятельности; правила обеспечения информационной безопасности, изложенные в стандартах;	Показать знание порядка и правил оформления нормативных актов, правила использования нормативных документов в деятельности по защите информации; содержания стандартов и правил обеспечения информационной безопасности.	Смотри таблицу 1		
ОК-2 знать последствия, наступающие в результате утечки информации;	Показать знания о последствиях, наступающих при утечке информации; последствия при разглашении конфиденциальной информации.	Смотри таблицу 1		
ОК-1 уметь составлять и оформлять локальные нормативные акты, регулирующие и регламентирующую профессиональную деятельность; составлять и оформлять обзор по обеспечению информационной безопасности профессиональной деятельности; обеспечивать информационную безопасность на основе стандартов;	Продемонстрировать умения составлять и оформлять локальные нормативные акты, регулирующие и регламентирующие профессиональную деятельности; составлять и оформлять обзоры законодательных актов, инструкций по обеспечению информационной безопасности. Демонстрировать умения обеспечивать информационную безопасность на основе законодательных актов и стандартов.	Смотри таблицу 1		
ОПК-2 уметь организовать работу коллектива по защите	Показать умения организовывать работу коллектива по защите информации.	Смотри таблицу 1		

информации				
ОПК-4 уметь использовать современные компьютерные сети, программные продукты и ресурсы информационно-телекоммуникационной сети «Интернет» для изучения организационно-правовых механизмов обеспечения информационной безопасности.	Демонстрировать умения использовать современные информационные ресурсы, возможности сети Интернет для получения информации об организационно-правовых механизмах обеспечения информационной безопасности.	Смотри таблицу 1		
ПК-7 уметь проводить занятия и инструктажи с персоналом, отвечающим за безопасность информации, проводить фрагмент занятия.	Показать умения организовывать и проводить занятия и инструктажи с персоналом, обеспечивающим защиту информации.	Смотри таблицу 1		
ОК-1 владеть навыками использования общегосударственных и локальных нормативно-методических документов в профессиональной деятельности; способностью составления обзора по вопросам обеспечения информационной безопасности профессиональной деятельности; способностью анализа информационной безопасности систем, объектов с использованием стандартов.	Показать способность использования государственных нормативных актов в профессиональной деятельности. Демонстрировать владение навыками составления обзоров по вопросам обеспечения информационной безопасности. Показывать владение стандартами в сфере защиты информации для анализа информационной безопасности систем и объектов.	Смотри таблицу 1		