



МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ИГУ»
Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ
проф. Бучков Н.М.
28 *06* 2016 г.

Рабочая программа дисциплины (модуля)

Наименование дисциплины (модуля) Б1.Б.2 «Организационно-правовые механизмы обеспечения информационной безопасности»

Направление подготовки - 03.04.03 «Радиофизика»

Тип образовательной программы - академическая

Направленность (профиль) подготовки «Информационные процессы и системы»

Квалификация (степень) выпускника - Магистр

Форма обучения - очная

Согласовано с УМК физического факультета
Протокол № 3 от «28» 06 2016г.

Председатель _____

Рекомендовано кафедрой:

Протокол № 12
От «28» 06 2016г.
И.О.Зав. кафедрой _____

Жолесник С.Н.

Иркутск 2016 г.

Содержание

	Стр.
1. Цели и задачи дисциплины (модуля):.....	3
2. Место дисциплины в структуре ООП:.....	3
3. Требования к результатам освоения дисциплины (модуля):.....	3
4. Объем дисциплины (модуля) и виды учебной работы)	4
5. Содержание дисциплины (модуля)	5
5.1. Содержание разделов и тем дисциплины (модуля).....	5
5.2. Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами.....	5
5.3. Разделы и темы дисциплин (модулей) и виды занятий	5
6. Перечень семинарских, практических занятий и лабораторных работ.....	6
6.1. План самостоятельной работы студентов	7
6.2. Методические указания по организации самостоятельной работы студентов.....	7
7. Примерная тематика курсовых работ (проектов) (при наличии).....	8
8. Учебно-методическое и информационное обеспечение дисциплины (модуля):	8
9. Материально-техническое обеспечение дисциплины (модуля):	9
10. Образовательные технологии:	9
11. Оценочные средства (ОС):.....	9
11.1. Оценочные средства для входного контроля.....	9
11.2. Оценочные средства текущего контроля.....	9
11.3. Оценочные средства для промежуточной аттестации	10

1. Цели и задачи дисциплины (модуля):

Целями и задачами освоения дисциплины (модуля) «Организационно-правовые механизмы обеспечения информационной безопасности» являются знание и использование нормативных правовых документов в своей профессиональной деятельности, организация деятельности службы безопасности.

2. Место дисциплины в структуре ООП:

Учебная дисциплина «Организационно-правовые механизмы обеспечения информационной безопасности» входит в вариативную часть обязательных дисциплин.

3. Требования к результатам освоения дисциплины (модуля):

Процесс изучения дисциплины (модуля) направлен на формирование следующих компетенций:

общекультурной компетенции:

способностью к абстрактному мышлению, анализу, синтезу (ОК-1).

общепрофессиональной компетенции:

готовностью действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения (ОК-2);

готовностью руководить коллективом в сфере своей профессиональной деятельности, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия (ОПК-2);

способностью к свободному владению профессионально-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).

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).

В результате изучения дисциплины студент должен:

Знать:

Индекс компетенции	Индекс образовательного результата	Образовательный результат
ОК-1	З-1	правила оформления нормативных актов; правила использования нормативные правовые документы в деятельности; правила обеспечения информационной безопасности, изложенные в стандартах;
ОК-2	З-2	последствия, наступающие в результате утечки информации

Уметь:

Индекс компетенции	Индекс образовательного результата	Образовательный результат
ОК-1	У-1	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;
ОПК-2	У-2	организовать работу коллектива по защите информации
ОПК-4	У-3	использовать современные компьютерные сети, программные продукты и ресурсы информационно-телекоммуникационной сети «Интернет» для изучения организационно-правовых механизмов обеспечения информационной безопасности.
ПК-7	У-4	проводить занятия и инструктажи с персоналом, отвечающим за безопасность информации, проводить фрагмент занятия

Владеть:

Индекс компетенции	Индекс образовательного результата	Образовательный результат
ОК-1	В-1	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.

4. Объем дисциплины (модуля) и виды учебной работы (разделяется по формам обучения)

Вид учебной работы	Всего часов / зачетных единиц	Семестры			
		1	2	3	4
Аудиторные занятия (всего)	38/1.06	38/1.06	-	-	-
В том числе:	-	-	-	-	-
Лекции (Л)	18/0.5	18/0.5	-	-	-
Практические занятия (ПЗ)	18/0.5	18/0.5	-	-	-
Семинары (С)	-	-	-	-	-
Лабораторные работы (ЛР)	-	-	-	-	-
Контроль самостоятельной работы (КСР)	2/0.06	2/0.06	-	-	-
Самостоятельная работа (всего)	34/0.94	34/0.94	-	-	-
В том числе:	-	-	-	-	-
Курсовой проект (работа)	-	-	-	-	-
Расчетно-графические работы	-	-	-	-	-
Реферат (при наличии)	-	-	-	-	-
<i>Другие виды самостоятельной работы</i>					
Вид промежуточной аттестации: зачет	-	-	-	-	-
Контактная работа (всего)	41	41	-	-	-
Общая трудоемкость, часы	72	72	-	-	-
зачетные единицы	2	2	-	-	-

Примечание: Контактная работа с магистрантом включает аудиторную нагрузку, а также 2 часа консультаций перед экзаменом и 0,3 часа на прием экзамена из объема часов, отводимых на экзамен в учебном плане (36ч).

5. Содержание дисциплины (модуля)

5.1. Содержание разделов и тем дисциплины (модуля). Все разделы и темы нумеруются.

Т.1. Государственная политика в сфере обеспечения информационной безопасности: общие положения и проблемы законодательства.

Правовое обеспечение информационной безопасности. Основы информационного права. Государственная система правового обеспечения информационной безопасности. Законодательные и нормативные акты по защите информации.

Т.2. Защита информации с ограниченным доступом.

Институт правовой защиты государственной тайны. Институт правовой защиты коммерческой тайны. Институт правовой защиты профессиональная тайна. Служебная тайна. Институт правовой защиты частной жизни гражданина. Информационные аспекты интеллектуальной собственности. Правовое регулирование деятельности предприятий в области информационной безопасности. Правовая защита информации в сфере высоких технологий. Юридическая ответственность за правонарушения в области информационной безопасности.

Т.3. Организационно-техническая защита информации предприятия.

Организация внутриобъектового и пропускного режимов на предприятии. Организация охраны предприятия и физической защиты его объектов.

Т.4. Организационно-правовая защита информации предприятия.

Локальные нормативно-методические документы по защите информации.

Т.5. Технология защиты информации при отдельных видах деятельности.

Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам. Организация защиты информации при осуществлении рекламной и публикаторской деятельности.

Т.6. Аналитическая, контрольная и плановая деятельность по защите информации в организациях.

Организация контроля за состоянием защиты конфиденциальной информации на предприятии. Основные направления аналитической и плановой работы.

5.2 Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№ № разделов и тем данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин (вписываются разработчиком)						
		P1	P2	P3	P4	P5		
1.	НИР							

5.3. Разделы и темы дисциплин (модулей) и виды занятий

№ п/п	Наименование раздела Наименование темы	Виды занятий в часах					
		Лекц.	Практ. зан.	Семин	КСР	СРС	Всего
1	Т1. Государственная политика в сфере обеспечения	2				4	6

	информационной безопасности: общие положения и проблемы законодательства						
2	Т2. Защита информации с ограниченным доступом	6				10	16
3	Т3. Организационно-техническая защита информации предприятия	4				8	12
4	Т4. Организационно-правовая защита информации предприятия	2	8			4	14
5	Т5. Технология защиты информации при отдельных видах деятельности	2	4			4	10
6	Т6. Аналитическая, контрольная и плановая деятельность по защите информации в организациях	2	6		2	4	14

6. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы дисциплины	Наименование семинаров, практических и лабораторных работ	Трудоемкость (часы)	Оценочные средства	Формируемые компетенции
1	2	3	4	5	6
1	Т.4.	Пз1. Составление формы конфиденциальных документов	2	ПК, УК	ОК-1, ОК-2, ОПК-4, ПК-7
2	Т.4.	Пз2. Составление формы ценной информации	2	ПК, УК	ОК-1, ОПК-4, ПК-7
3	Т.4.	Пз3. Составление формы инструкции по обеспечению безопасности информации	2	ПК, УК	ОК-1, ОПК-4, ПК-7
4	Т.4.	Пз4. Составление формы правил обеспечения безопасности секретов в экстремальных ситуациях	2	ПК, УК	ОК-1, ОПК-4, ПК-7
5	Т.5.	Пз5. Составление документов, определяющих порядок доступа к конфиденциальной информации командированных лиц	2	ПК, УК	ОК-1, ОПК-2, ОПК-4, ПК-7
6	Т.5.	Пз6. Составление акта анализа объекта защиты	2	ПК, УК	ОК-1, ОПК-2, ОПК-4, ПК-7
7	Т.6.	Пз7. Составление формы плана мероприятий по защите конфиденциальной информации.	2	ПК, УК	ОК-1, ОПК-4
8	Т.6.	Пз8. Составление формы	2	ПК, УК	ОК-1, ОПК-4

		аналитического отчета по защите информации.			
9	Т.6.	Пз9. Оформление заключения о результатах проведенного служебного расследования.	2	ПК, УК	ОК-1, ОПК-4

ПК- письменный контроль, УК- устный контроль.

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1	Т1.	Работа с учебником, справочной литературой, первоисточниками, конспектом	Изучение, повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов	Источники 1 -3 из основной и 1-13 из дополнительной литературы; Самостоятельный поиск литературы на образовательных ресурсах, доступные по логину и паролю, предоставляемым Научной библиотекой ИГУ	4
2	Т2.				3
3	Т2.				3
4	Т2.				4
5	Т3.				4
6	Т3.				4
7	Т4.				4
8	Т5.				4
9	Т6.				4

6.2. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа магистров – индивидуальная учебная деятельность, осуществляемая без непосредственного руководства преподавателя (научного руководителя (консультанта)), в ходе которой магистр активно воспринимает, осмысливает полученную информацию, решает теоретические и практические задачи. В процессе проведения самостоятельной работы формируется компетенция ОПК-4.

На самостоятельную работу выносятся следующие вопросы по темам дисциплины:

Т1. Государственная система правового обеспечения информационной безопасности. Законодательные и нормативные акты по защите информации (3ч). Проработка лекционного материала (1ч).

Т2. Институт правовой защиты профессиональная тайна. Служебная тайна. Институт правовой защиты частной жизни гражданина. Информационные аспекты интеллектуальной собственности. Правовое регулирование деятельности предприятий в области информационной безопасности. Правовая защита информации в сфере высоких технологий. Юридическая ответственность за правонарушения в области информационной безопасности (8ч). Проработка лекционного материала (2ч).

Т3. Организация охраны предприятия и физической защиты его объектов (6ч). Проработка лекционного материала (2ч).

Т4. Локальные нормативно-методические документы по защите информации (2ч). Проработка лекционного материала и материала практических занятий (2ч).

Т5. Организация защиты информации при осуществлении рекламной и публикаторской деятельности (2ч). Проработка лекционного материала и материала практических занятий (2ч).

Т6. Основные направления аналитической и плановой работы по защите информации в организациях (2ч). Проработка лекционного материала и материала практических занятий (2ч).

Контроль самостоятельной работы проводится на практических занятиях и на КСР по окончании Т6.

7. Примерная тематика курсовых работ (проектов) (при наличии)

планом не предусмотрено

8. Учебно-методическое и информационное обеспечение дисциплины (модуля):

а) основная литература

1. Бойкова, Ольга Феоктистовна. Персональные данные: обработка, использование и защита/ О. Ф. Бойкова. – М.: Пашков дом, 2013. – 118 с.. – (Библиотека библиотекаря). – Библиогр.: с. 66-68 (1 экз.) ISBN 978-5-7510-0593-1
2. Ищейнов, Вячеслав Яковлевич. Защита конфиденциальной информации [Текст] : учеб. пособие для студ. вузов / В. Я. Ищейнов, М. В. Мещатунян. - М. : Форум, 2012. - 254 с. ; 21 см. - Библиогр.: с. 249-252. - ISBN 978-5-91134-336-1 (2 экз.)

Сверено с #БЧГУ

б) дополнительная литература

1. Глухих В. И. Информационная безопасность и защита данных: учеб. пособие для студ. вузов/ В. И. Глухих ; рец.: Б. В. Агалаков, Р. В. Мещеряков, Е. А. Черкашин; Иркут. гос. техн. ун-т. – Иркутск: Изд-во ИрГТУ, 2012. – 244 с.: а-ил.. – Библиогр.: с. 242-244. (1 экз.)
2. Мезенцев, Александр Владимирович. Технологии защищенной обработки информации: учеб. пособие/ А. В. Мезенцев, Н. И. Синадский, Д. А. Хорьков ; рец.: Ф. И. Иванов, О. Н. Соболев; Иркутский гос. ун-т, Ин-т мат., экон. и информ.. – Иркутск: Изд-во ИГУ, 2013. – 120 с.: а-ил. (3 экз.)
3. Мельников Д. А. Организация и обеспечение безопасности информационно-технологических сетей и систем: учеб. для студ. вузов, обуч. по спец. 080801 "Прикладная информатика (по обл.)" и др. экон. спец./ Д. А. Мельников. – М.: Университет. кн., 2012. – 598 (1 экз.)
4. Сердюк, Виктор Александрович. Организация и технология защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учеб. пособие/ В. А. Сердюк; Гос. ун-т - Высш. шк. экономики. – М.: Изд-во ГУ ВШЭ, 2011. – 572 с.: а-ил.. – Библиогр.: с. 541-567 (2 экз.)
5. Ярочкин В.И. Информационная безопасность - Гаудеамус, 2004. (1 экз.)
6. Мельников В.П. Информационная безопасность и защита информации : учеб. пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А. Клейменов. - 4-е изд., стер. - М. : Академия, 2009. - 331 с. ; 21 см. - (Высшее профессиональное образование : информатика и вычислительная техника). - ISBN 978-5-7695-6150-4. (1 экз.)
7. Корнеев И. К., Степанов Е. А. Защита информации в офисе. - М.: Проспект, 2010. (1 экз.)
8. Куприянов А. И., Шевцов В. А., Сахаров А. В. Основы защиты информации. - М.: Академия, 2006. (2 экз.)
9. Хорев П. Б. Программно-аппаратная защита информации: учебное пособие. - М.: Форум, 2009.

в) программное обеспечение

1. Microsoft PowerPoint

г) базы данных, информационно-справочные и поисковые системы

1. Поисковые системы Google, Yandex.

2. Электронные ресурсы доступные по логину и паролю, предоставляемые Научной библиотекой ИГУ.

9. Материально-техническое обеспечение дисциплины (модуля):

Чтение лекций сопровождается демонстрацией информации (мультимедийный проектор, офисное оборудование для оперативного размножения иллюстративного и раздаточного лекционного материалов).

10. Образовательные технологии:

На лекциях используются активные методы обучения (компьютерных симуляций, разбор конкретных ситуаций). Практические занятия 1-9 проводятся в интерактивной форме.

11. Оценочные средства (ОС):

11.1. Оценочные средства для входного контроля

Не предусмотрено.

11.2. Оценочные средства текущего контроля

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).

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.

Вопросы для письменного текущего контроля приведены ниже:

Пз.1. 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.

- Пз.2. 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.
- Пз.3. 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.
- Пз.4. 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.
- Пз.5. 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.
- Пз.6. 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.
- Пз.7. 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.
- Пз.8. Роль и место внутриобъектового 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.
- Пз.9. Контроль защиты конфиденциальной информации на предприятии. Служебное расследование по фактам нарушения защиты конфиденциальной информации. Организация аналитической работы в области защиты информации.
- КСР. Порядок доступа к конфиденциальной информации командированных лиц. Порядок допуска граждан к секретным сведениям. Порядок доступа граждан к коммерческой тайне.

11.3. Оценочные средства для промежуточной аттестации

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».

Разработчики:


(подпись)

доцент
(занимаемая должность)

Колесник С.Н.
(инициалы, фамилия)

(подпись)

(занимаемая должность)

(инициалы, фамилия)

Программа рассмотрена на заседании кафедры Радиофизики и радиоэлектроники
(наименование)

«28» 06 2016г.

Протокол № 12 И.О.Зав.кафедрой _____ Колесник С.Н.

Настоящая программа не может быть воспроизведена ни в какой форме без предварительного письменного разрешения кафедры-разработчика программы.