

МИНОБРНАУКИ РОССИИ

**Федеральное государственное бюджетное образовательное
учреждение высшего образования "Пермский
государственный национальный исследовательский
университет"**

Кафедра радиоэлектроники и защиты информации

Авторы-составители: **Сеник Кирилл Александрович
Лунегов Игорь Владимирович**

Рабочая программа дисциплины

**ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Код УМК 94428

Утверждено
Протокол №4
от «24» июня 2020 г.

Пермь, 2020

1. Наименование дисциплины

Правовые и организационные основы обеспечения информационной безопасности

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.03** Информационная безопасность автоматизированных систем
направленность Безопасность открытых информационных систем

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Правовые и организационные основы обеспечения информационной безопасности** у обучающегося должны быть сформированы следующие компетенции:

10.05.03 Информационная безопасность автоматизированных систем (направленность : Безопасность открытых информационных систем)

ОПК.7 способность применять нормативные правовые акты в профессиональной деятельности

ПК.10 способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности

ПК.11 способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности

ПК.22 способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности

ПК.4 способность проводить анализ защищенности автоматизированных систем

ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем

ПК.8 способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ

4. Объем и содержание дисциплины

Направления подготовки	10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	14
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	42
Проведение лекционных занятий	28
Проведение практических занятий, семинаров	14
Самостоятельная работа (ак.час.)	66
Формы текущего контроля	Входное тестирование (1) Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (5)
Формы промежуточной аттестации	Экзамен (14 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Правовые и организационные основы обеспечения информационной безопасности

Раздел 1. Информация как объект правового регулирования

Информация как объект правового регулирования. Структура информационной сферы и характеристика ее элементов. Виды информации. Формирование информационных ресурсов и их квалификация. Конституционные гарантии прав на информацию и механизм их реализации

Раздел 2. Законодательство РФ в области информационной безопасности

Понятие и структура информационной безопасности. Информационная сфера и информационная среда. Субъекты и объекты правоотношений в области информационной безопасности. Понятие и виды защищаемой информации по законодательству РФ. Отрасли законодательства, регламентирующие деятельность по защите информации. Перспективы развития законодательства в области информационной безопасности

Раздел 3. Правовой режим защиты государственной тайны

Понятие правового режима защиты государственной тайны. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Реквизиты носителей сведений, составляющих государственную тайну. Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Порядок допуска и доступа к государственной тайне. Система контроля за состоянием защиты государственной тайны. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная)

Раздел 4. Правовые режимы защиты конфиденциальной информации

Понятие правового режима защиты государственной тайны. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Реквизиты носителей сведений, составляющих государственную тайну. Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Порядок допуска и доступа к государственной тайне. Система контроля за состоянием защиты государственной тайны. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная)

Раздел 5. Лицензирование и сертификация в сфере информационной безопасности

Понятия лицензирования по российскому законодательству. Виды деятельности в информационной сфере, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области защиты информации. Объекты лицензирования в сфере защиты информации. Участники лицензионных отношений в сфере защиты информации. Специальные экспертизы и государственная аттестация руководителей. Органы лицензирования и их полномочия. Контроль за соблюдением лицензиатами условий ведения деятельности.

Понятие сертификации по российскому законодательству. Правовая регламентация сертификационной деятельности в области защиты информации. Режимы сертификации. Объекты сертификационной деятельности (сертификации). Органы сертификации и их полномочия.

Правовые основы защиты информации с использованием технических средств (защиты от технических разведок, применения и разработки шифровальных средств, применения электронно-цифровой подписи и т.д.).

Раздел 6. Защита интеллектуальной собственности

Законодательство РФ об интеллектуальной собственности. Понятие интеллектуальной собственности. Объекты и субъекты авторского права. Исключительные авторские права. Смежные права. Правовая

охрана программ для ЭВМ, баз данных и топологий интегральных микросхем. Защита авторских и смежных прав. Основы патентных правоотношений. Условия патентоспособности. Объекты изобретения, связанные с электронно-вычислительной техникой и информационными технологиями. Авторы изобретений и патентообладатели. Механизм патентования. Защита прав патентообладателей и авторов. Особенности договорных отношений в области информационной безопасности. Правовое регулирование взаимоотношений администрации и персонала в области обеспечения информационной безопасности. Особенности трудовых отношений

Раздел 7. Компьютерные правонарушения

Преступления в сфере компьютерной информации. Признаки и элементы состава преступления. Криминалистическая характеристика компьютерных преступлений. Расследование компьютерного преступления. Особенности основных следственных действий. Криминалистические аспекты проведения расследования Сбор доказательств. Экспертиза преступлений в области компьютерной информации. Проблемы судебного преследования за преступления в сфере компьютерной информации.

Раздел 8. Международное законодательство в области защиты информации

Законодательство РФ об участии в международном информационном обмене Правовой режим участия в международном обмене. Субъекты и объекты международного информационного обмена. Национальные законодательства о компьютерных правонарушениях и защите информации. Международное сотрудничество в области борьбы с компьютерной преступностью

Раздел 9. Концептуальные положения организационного обеспечения информационной безопасности

Цели и задачи организационной защиты информации, ее связь с правовой и инженерно-технической защитой информации. Виды угроз информационной безопасности на объекте защиты и их характеристика. Модели нарушителей информационной безопасности на объекте. Формы преступного посягательства. Оценка ущерба вследствие организационных нарушений информационной безопасности на объекте. Основные направления организационной защиты на объекте. Структура сил и средств организационной защиты информации

Раздел 10. Организация службы безопасности объекта

Функции, задачи и особенности службы безопасности объекта. Принципы организации службы безопасности объекта. Типовая структура службы безопасности. Основные документы, регламентирующие деятельность службы безопасности объекта. Способы и формы участия сотрудников в организационной защите информации. Особенности действий сотрудников службы безопасности в чрезвычайных ситуациях и в условиях чрезвычайного положения. Способы и формы взаимодействия службы безопасности объекта с контрразведывательными и правоохранными органами.

Раздел 11. Подбор сотрудников и работа с кадрами

Роль персонала (кадров) в обеспечении информационной безопасности объекта. Требования к сотрудникам организации, допущенных к конфиденциальной информации. Основные критерии приема на работу, связанную с сохранением тайны. Состав документов, необходимых при подборе и приеме сотрудников на работу. Методы проверки кандидатов на должности. Организация обучения персонала, ее методы и формы. Организация контроля выполнения сотрудниками требований режима и секретности. Цели, задачи и процедуры служебного расследования нарушения режима и секретности. Меры по защите информации при увольнении сотрудника.

Раздел 12. Организация и обеспечение режима секретности (конфиденциальности) на объекте

12.1. Организация и обеспечение конфиденциального делопроизводства

Требования режима конфиденциальности при работе с секретными документами. Назначение и задачи секретного делопроизводства. Порядок разработки, учета, хранения, размножения и уничтожения конфиденциальных документов. Режим конфиденциальности при обработке документов с применением средств вычислительной техники.

12.2. Допуск к конфиденциальной информации

Понятия допуска к конфиденциальной информации и доступа к конфиденциальным работам, документам и изделиям. Номенклатура должностей работников, подлежащих оформлению на допуск. Формы допусков. Оформление, учет и уничтожение справок о допуске. Организация работы по обеспечению контроля за допуском сотрудников организации и посетителей

12.3. Обеспечение режима конфиденциальности при деятельности объекта

Обеспечение режима секретности при проведении НИОКР по конфиденциальной тематике, при разработке и изготовлении изделий, их опытной эксплуатации и серийном производстве, хранении и транспортировке. Основные требования, предъявляемые к подготовке служебного совещания. Организация обеспечения режима при проведении служебного совещания. Требования к помещениям проведения совещания. Организация работ по защите информации при опубликовании открытых материалов. Порядок создания и функционирования экспертных комиссий организации. Порядок организации информационной безопасности объекта при осуществлении международного научно-технического и экономического сотрудничества.

Раздел 13. Организация внутри объектового режима

Назначение и требования внутри объектового режима. Порядок определения перечня предметов, запрещенных к проносу/провозу на территорию организации. Требования к помещениям, в которых циркулирует защищаемая информация. Категорирование помещений. Обеспечение режима в выделенных помещениях. Определение границ контролируемых зон. Порядок передвижения сотрудников и перевозки охраняемых изделий по территории организации. Порядок пребывания и организация контроля выполнения посетителями требований режима на территории организации и в помещениях. Обеспечение защиты информации в экстремальных ситуациях и в условиях чрезвычайного положения

Раздел 14. Охрана объектов

14.1. Организация охраны объекта

Цели и задачи охраны. Объекты охраны. Виды и способы охраны. Посты охраны, связь, взаимодействие с местными органами правопорядка. Использование собак и борьба с собаками нарушителя. Прием и сдача объекта под охрану. Средства и методы физической защиты объектов. Технические средства охраны и видеонаблюдения объекта. Оружие, используемое для охраны объектов. Индивидуальная защита от оружия нападения. Оборона объекта в случае нападения. Организация охраны объектов защиты в процессе их транспортировки. Противопожарная охрана

14.2. Организация пропускного режима

Понятие пропускного режима. Цели и задачи пропускного режима. Организация пропускного режима. Атрибутные и биометрические идентификаторы людей. Порядок оформления и выдачи пропусков. Контрольно-пропускные пункты людей и автотранспорта, их оборудование и организация. Порядок вывоза/выноса, ввоза/вывоза материальных ценностей и документации на/с территории организации

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

- закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;
- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;
- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;
- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

- конспекты лекций;
- литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);
- текст лекций на электронных носителях;
- ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;
- лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;
- методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Ковалёва Н. Н. Информационное право России: учебное пособие / Н. Н. Ковалёва. - Москва: Дашков и К°, 2010, ISBN 978-5-394-00482-7. - 352. - Библиогр.: с. 348-350
2. Попов Л. Л., Мигачев Ю. И., Тихомиров С. В. Информационное право: учебник / Л. Л. Попов, Ю. И. Мигачев, С. В. Тихомиров. - Москва: Норма, 2010, ISBN 978-5-91768-054-5. - 495.
3. Правовое обеспечение информационной безопасности: учеб. пособие / С. Я. Казанцев [и др.] ; ред. Казанцев С. Я.. - 2-е изд., испр. и доп.. - М.: Академия, 2007, ISBN 5-7695-3635-9. - 240.
4. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. <https://urait.ru/bcode/451933>

Дополнительная:

1. Курушин Владимир Александрович, Минаев Владимир Дмитриевич Компьютерные преступления и информационная безопасность: Справ. / Владимир Александрович Курушин, Владимир Дмитриевич Минаев. - М.: Новый Юрист, 1998, ISBN 5-7969-0022-6. - 256.
2. Бачило И. Л. Информационное право: учебник для вузов : [специальный курс] / И. Л. Бачило. - Москва: Юрайт, 2009, ISBN 978-5-9692-0462-1. - 454. - Библиогр. в конце гл.
3. Серго А. Г., Пушин В. С. Основы права интеллектуальной собственности для ИТ-специалистов: учебное пособие / А. Г. Серго, В. С. Пушин. - Москва: БИНОМ, Лаборатория знаний, 2011, ISBN 978-5-9963-0494-3. - 239. - Библиогр.: с. 239

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

<http://center-bereg.ru/> Юридический портал Center Bereg

<http://window.edu.ru/> Единое окно доступа к информационным ресурсам

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Правовые и организационные основы обеспечения информационной безопасности** предполагает использование следующего программного обеспечения и информационных справочных систем:

Образовательный процесс по дисциплине предполагает использование следующего информационных технологий, программного обеспечения и информационных справочных систем:

- презентационные материалы (слайды по темам лекционных и практических занятий);
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательную среду университета (ЕТИС ПГНИУ);
- интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии и т.д.).

Перечень используемого программного обеспечения:

- открытая система "ALT Linux"
- офисный пакет приложений "Libreoffice";
- приложение позволяющее просматривать и воспроизводить медиа контент PDF-файлов "AdobeAcrobatReader DC";
- программы демонстрации видео материалов (проигрыватель) "WindowsMediaPlaer";
- программа просмотра интернет контента (браузер) "GoogleChrome".

Дополнительно могут использоваться :

Справочная система "Консультант плюс", "Гарант" онлайн версия .

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (student.psu.ru).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (<https://bigbluebutton.org/>).

система LMS Moodle (<http://e-learn.psu.ru/>), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (<https://indigotech.ru/>).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия, практические занятия, групповые (индивидуальные) консультации, мероприятия текущего контроля и промежуточной аттестации проводятся в аудитории, оснащенной презентационной техникой (проектор, экран для проектора, компьютер/ноутбук), а также меловой (и) или маркерной доской.

Самостоятельная работа:

помещения Научной библиотеки ПГНИУ ,оснащенные компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченные доступом в электронную информационно-образовательную среду университета.

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.

5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

Фонды оценочных средств для аттестации по дисциплине
Правовые и организационные основы обеспечения информационной безопасности

Планируемые результаты обучения по дисциплине для формирования компетенции.
Индикаторы и критерии их оценивания

ОПК.7

способность применять нормативные правовые акты в профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ОПК.7 способность применять нормативные правовые акты в профессиональной деятельности</p>	<p>Знать как проводить анализ правовых и организационных методов защиты в автоматизированных системах. Уметь применить правовые основы информационной безопасности для анализа защищенности автоматизированных систем. Владеть анализом организационных мер защиты в информационных системах.</p>	<p style="text-align: center;">Неудовлетворител</p> <p>Не знает как проводить анализ правовых и организационных методов защиты в автоматизированных системах. Не умеет применить правовые основы информационной безопасности для анализа защищенности автоматизированных систем. Не владеет анализом организационных мер защиты в информационных системах.</p> <p style="text-align: center;">Удовлетворительн</p> <p>Знаком как проводить анализ правовых и организационных методов защиты в автоматизированных системах. Частично умеет применить правовые основы информационной безопасности для анализа защищенности автоматизированных систем. Частично владеет анализом организационных мер защиты в информационных системах.</p> <p style="text-align: center;">Хорошо</p> <p>Знает как проводить анализ правовых и организационных методов защиты в автоматизированных системах, с небольшими пробелами в знаниях. Умеет применить правовые основы информационной безопасности для анализа защищенности автоматизированных систем, с небольшими пробелами в знаниях. Владеет анализом организационных мер защиты в информационных системах с небольшими пробелами в знаниях.</p> <p style="text-align: center;">Отлично</p> <p>Хорошо знает как проводить анализ правовых и организационных методов защиты в автоматизированных системах. Умеет применить правовые основы информационной безопасности для анализа</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично защищенности автоматизированных систем. Владеет анализом организационных мер защиты в информационных системах.

ПК.22

способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.22 способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности	Знать содержание основных понятий по правовому обеспечению информационной безопасности. Уметь контролировать состояние организационной защиты информации на объекте и определять рациональные меры по обеспечению организационной защиты на нем. Иметь навыки работы с нормативно-правовыми документами	<p>Неудовлетворител Отсутствие знаний содержания основных понятий по правовому обеспечению информационной безопасности Отсутствие умений контролировать состояние организационной защиты информации на объекте и определять рациональные меры по обеспечению организационной защиты на нем Отсутствие навыков работы с нормативно- правовыми документами</p> <p>Удовлетворительн Общие, но не структурированные знания основных понятий по правовому обеспечению информационной безопасности. Частично сформированное умение контролировать состояние организационной защиты информации на объекте и определять рациональные меры по обеспечению организационной защиты на нем. Фрагментарное применение навыков работы с нормативно-правовыми документами</p> <p>Хорошо Сформированные, но содержащие отдельные пробелы знания основных понятий по правовому обеспечению информационной безопасности. В целом успешные, но содержащие отдельные пробелы умения контролировать состояние организационной защиты информации на объекте и определять рациональные меры по обеспечению</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Хорошо организационной защиты на нем. В целом успешное, но содержащее отдельные пробелы применение навыков навыков работы с нормативно-правовыми документами</p> <p>Отлично Сформированные систематические знания основных понятий по правовому обеспечению информационной безопасности. Сформированное умение контролировать состояние организационной защиты информации на объекте и определять рациональные меры по обеспечению организационной защиты на нем. Успешное и систематическое применение навыков работы с нормативно-правовыми документами</p>

ПК.4

способность проводить анализ защищенности автоматизированных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.4 способность проводить анализ защищенности автоматизированных систем	Знать: основы конфиденциальной информации и ее правовые режимы, юридическую ответственность за нарушение правового режима. Уметь применять действующую законодательную базу в области информационной безопасности и защиты интересов личности, общества и государства	<p>Неудовлетворител Не знает основ информационного законодательства Российской Федерации, основ конфиденциальной информации и ее правовые режимы, основ юридической ответственности за нарушение правового режима. Не умеет применять действующую законодательную базу в области информационной безопасности</p> <p>Удовлетворительн Общие, но не структурированные знания основ информационного законодательства Российской Федерации, основ конфиденциальной информации и ее правовые режимы, основ юридической ответственности за нарушение правового режима. Частично сформированное умение применять действующую законодательную</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Удовлетворительн базу в области информационной безопасности</p> <p>Хорошо Сформированные, но содержащие отдельные пробелы знания основ информационного законодательства Российской Федерации, основ конфиденциальной информации и ее правовые режимы, основ юридической ответственности за нарушение правового режима. В целом успешные, но содержащие отдельные пробелы умения применять действующую законодательную базу в области информационной безопасности</p> <p>Отлично Сформированное знание основ информационного законодательства Российской Федерации, основ конфиденциальной информации и ее правовые режимы, основ юридической ответственности за нарушение правового режима. Полное понимание значимости информационной безопасности. Сформированное умение применять действующую законодательную базу в области информационной безопасности и защиты интересов личности, общества и государства</p>

ПК.7

способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем	Знать набор решений в области организационных мер защиты автоматизированных систем. Уметь выбирать критерии оценки эффективности мер защиты в автоматизированных системах. Владеть навыками анализа, предлагать и обосновывать выбор решений по обеспечению требуемого уровня	<p>Неудовлетворител Не знает набор решений в области организационных мер защиты автоматизированных систем. Не умеет выбрать критерии оценки эффективности мер защиты в автоматизированных системах. Не владеет навыками проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
	<p>эффективности применения автоматизированных систем в защищенном исполнении.</p>	<p>Неудовлетворител автоматизированных систем в защищенном исполнении.</p> <p>Удовлетворительн Частично сформированные знания решений в области организационных мер защиты автоматизированных систем. Частично сформированные умения выбирать критерии оценки эффективности мер защиты в автоматизированных системах. Частично сформированные навыки анализа, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем в защищенном исполнении.</p> <p>Хорошо Сформированные, но содержащие пробелы знания решений в области организационных мер защиты автоматизированных систем. Сформированные, но содержащие пробелы умения выбирать критерии оценки эффективности мер защиты в автоматизированных системах. Сформированные, но содержащие пробелы навыки анализа, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем в защищенном исполнении.</p> <p>Отлично Сформированные знания решений в области организационных мер защиты автоматизированных систем. Сформированные умения выбирать критерии оценки эффективности мер защиты в автоматизированных системах. Сформированные навыки анализа, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем в защищенном исполнении.</p>

ПК.5

способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Знать цели и задачи организационной защиты информации, ее связь с правовой и инженерно- технической защитой информации; виды угроз, модели нарушителей ИБ, основные направления организационной защиты АС. Уметь оценить ущерб вследствие организационных нарушений информационной безопасности; иметь навыки выявления угроз информационной безопасности объекта	Неудовлетворител Не понимает цели и задачи организационной защиты информации, ее связи с правовой и инженерно-технической защитой информации; не знает виды угроз, модели нарушителей ИБ, основные направления организационной защиты АС. Не умеет оценить ущерб вследствие организационных нарушений информационной безопасности; Не имеет навыков выявления угроз информационной безопасности объекта Удовлетворительн Частично понимает цели и задачи организационной защиты информации, ее связи с правовой и инженерно-технической защитой информации. Общие, но не структурированные знания видов угроз, модели нарушителей ИБ, основных направлений организационной защиты АС. Частично сформированное умение оценить ущерб вследствие организационных нарушений информационной безопасности. Фрагментарное применение навыков выявления угроз информационной безопасности объекта. Хорошо Понимает цели и задачи организационной защиты информации, ее связь с правовой и инженерно-технической защитой информации. Сформированные, но содержащие отдельные пробелы знания виды угроз, моделей нарушителей ИБ, основных направлений организационной защиты АС. В целом успешное, но содержащее отдельные пробелы применение навыков выявления угроз информационной безопасности объекта. Отлично Четкое понимание цели и задачи организационной защиты информации, ее связь с правовой и инженерно-технической

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Отлично</p> <p>защитой информации. Сформированные знания видов угроз и моделей нарушителей ИБ. Сформированное умение оценить ущерб вследствие организационных нарушений информационной безопасности. Успешное применение навыков выявления угроз информационной безопасности объекта.</p>

ПК.8

способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.8</p> <p>способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ</p>	<p>Уметь разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ</p>	<p>Неудовлетворител</p> <p>Не умеет разрабатывать техническую и организационную документацию, готовить отчеты, инструкции, акты, протоколы службы информационной безопасности организации.</p> <p>Удовлетворительн</p> <p>Имеет представление о том, как разрабатывать техническую и организационную документацию, готовить отчеты, инструкции, акты, протоколы службы информационной безопасности организации</p> <p>Хорошо</p> <p>В целом умеет разрабатывать техническую и организационную документацию, готовить отчеты, инструкции, акты, протоколы службы информационной безопасности организации.</p> <p>Отлично</p> <p>Сформировано представление о том, как разрабатывать техническую и организационную документацию, готовить отчеты, инструкции, акты, протоколы службы информационной безопасности организации.</p>

ПК.10

способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.10 способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности	Знать организационные процедуры создания защищенных автоматизированных систем, уметь применять набор правил и регламентов для создания защищенных автоматизированных систем, владеть навыками контроля соблюдения требований организационного регламента.	<p>Неудовлетворител не знает организационные процедуры создания защищенных автоматизированных систем, не умеет применять набор правил и регламентов для создания защищенных автоматизированных систем, не владеет навыками контроля соблюдения требований организационного регламента.</p> <p>Удовлетворительн частично сформированные знания организационных процедур создания защищенных автоматизированных систем, частично сформированные умения применять набор правил и регламентов для создания защищенных автоматизированных систем, сформированные навыки контроля соблюдения требований организационного регламента.</p> <p>Хорошо сформированные, но содержащие пробелы знания организационных процедур создания защищенных автоматизированных систем, сформированные, но содержащие пробелы умения применять набор правил и регламентов для создания защищенных автоматизированных систем, сформированные, но содержащие пробелы навыки контроля соблюдения требований организационного регламента.</p> <p>Отлично Полностью сформированные знания организационных процедур создания защищенных автоматизированных систем, сформированные умения применять набор правил и регламентов для создания защищенных автоматизированных систем, сформированные навыки контроля соблюдения требований организационного регламента.</p>

ПК.11

способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.11 способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности	Знать организационные меры, применяемые для защиты автоматизированных систем. Уметь выбрать критерии оценки эффективности мер защиты в автоматизированных системах. Владеть навыками проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем в защищенном исполнении.	Неудовлетворител Не знает набор решений в области организационных мер защиты автоматизированных систем. Не умеет выбрать критерии оценки эффективности мер защиты в автоматизированных системах. Не владеет способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем в защищенном исполнении. Удовлетворительн Частично знает набор решений в области организационных мер защиты автоматизированных систем. Частично умеет выбрать критерии оценки эффективности мер защиты в автоматизированных системах. Частично владеет способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем в защищенном исполнении. Хорошо Знает с небольшими неточностями набор решений в области организационных мер защиты автоматизированных систем. Уметь с небольшими неточностями выбрать критерии оценки эффективности мер защиты в автоматизированных системах. Владеет способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем в защищенном исполнении. Отлично Полностью сформированные знания в области организационных мер защиты

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично автоматизированных систем. Умеет выбрать критерии оценки эффективности мер защиты в автоматизированных системах. В совершенстве владеет способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем в защищенном исполнении.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

Вид мероприятия промежуточной аттестации : Экзамен

Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.

Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100

«хорошо» - от 61 до 80

«удовлетворительно» - от 46 до 60

«неудовлетворительно» / «незачтено» менее 46 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Раздел 1. Информация как объект правового регулирования Входное тестирование	Понимание основ теории информации. Знание основ правоведения.
ОПК.7 способность применять нормативные правовые акты в профессиональной деятельности	Раздел 3. Правовой режим защиты государственной тайны Письменное контрольное мероприятие	Знание правового обеспечения режима государственной тайны. Понимание основ организационного обеспечения защиты государственной тайны
ОПК.7 способность применять нормативные правовые акты в профессиональной деятельности ПК.8 способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	Раздел 6. Защита интеллектуальной собственности Письменное контрольное мероприятие	правовые основы информационной безопасности,

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ОПК.7 способность применять нормативные правовые акты в профессиональной деятельности</p> <p>ПК.10 способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности</p>	<p>Раздел 7. Компьютерные правонарушения</p> <p>Письменное контрольное мероприятие</p>	<p>Знание законодательства в сфере компьютерных правонарушений и ответственности за них.</p>
<p>ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем</p> <p>ПК.8 способность разрабатывать научно-техническую документацию, готовить научно- технические отчеты, обзоры, публикации по результатам выполненных работ</p> <p>ПК.10 способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности</p>	<p>Раздел 9. Концептуальные положения организационного обеспечения информационной безопасности</p> <p>Письменное контрольное мероприятие</p>	<p>Понимание возможности и необходимости применения организационных мер защиты информации в организации. Знание документационного обеспечения организационной защиты информационных систем.</p>

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p>ПК.10 способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности</p> <p>ПК.22 способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности</p>	<p>12.3. Обеспечение режима конфиденциальности при деятельности объекта</p> <p>Письменное контрольное мероприятие</p>	<p>Знание последовательности организации и эксплуатации конфиденциального делопроизводства, документации разрабатываемой при конфиденциальном документообороте.</p>

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ПК.4 способность проводить анализ защищенности автоматизированных систем</p> <p>ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы</p> <p>ОПК.7 способность применять нормативные правовые акты в профессиональной деятельности</p> <p>ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем</p> <p>ПК.8 способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ</p> <p>ПК.10 способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности</p> <p>ПК.11 способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности</p> <p>ПК.22 способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с</p>	<p>14.2. Организация пропускного режима</p> <p>Итоговое контрольное мероприятие</p>	<p>Знание- основы информационного законодательства Российской Федерации;- основы системы защиты государственной тайны;- основы правил лицензирования и сертификации в области защиты информации;- основы международного законодательства в области защиты информации; - о компьютерных преступлениях;- правовых способов защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности;</p> <p>Умение работать с нормативно-правовыми актами; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов;</p>

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
учетом требований информационной безопасности		

Спецификация мероприятий текущего контроля

Раздел 1. Информация как объект правового регулирования

Продолжительность проведения мероприятия промежуточной аттестации: **.5 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**

Проходной балл: **0**

Показатели оценивания	Баллы
Одна ошибка при входном контроле	81
Две ошибки при входном контроле	61
Отсутствие ошибок при входном контроле	41
Три ошибки при входном контроле	0

Раздел 3. Правовой режим защиты государственной тайны

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**

Проходной балл: **5**

Показатели оценивания	Баллы
Знать законодательство, открытые нормативно-правовые акты в области государственной тайны в РФ	5
Знать виды ответственности за нарушения правового режима государственной тайны.	5

Раздел 6. Защита интеллектуальной собственности

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**

Проходной балл: **5**

Показатели оценивания	Баллы
Знать виды интеллектуальной собственности. Уметь применить статьи Гражданского кодекса для решения конкретных задач в области интеллектуальной собственности.	10
Знать виды интеллектуальной собственности. Частично уметь применить статьи Гражданского кодекса для решения конкретных задач в области интеллектуальной собственности.	8
Знать частично виды интеллектуальной собственности. Частично уметь применить статьи Гражданского кодекса для решения конкретных задач в области интеллектуальной собственности.	7

Раздел 7. Компьютерные правонарушения

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**

Проходной балл: **5**

Показатели оценивания	Баллы
Студент знает виды правонарушений и ответственность в сфере компьютерных преступлений.	10
Студент частично знает виды правонарушений и ответственность в сфере компьютерных преступлений.	5
Студент не знает виды правонарушений и ответственность в сфере компьютерных преступлений.	0

Раздел 9. Концептуальные положения организационного обеспечения информационной безопасности

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **15**

Проходной балл: **7**

Показатели оценивания	Баллы
Уметь разработать документацию по результатам реализации организационных мер в информационной системе в соответствии с требованиями нормативных документов.	15
Уметь разработать документацию по результатам реализации организационных мер в информационной системе в соответствии с требованиями нормативных документов с неточностями	10
Уметь разработать документацию по результатам реализации организационных мер в информационной системе без соответствия с требованиями нормативных документов.	7
Не умеет разработать документацию по результатам реализации организационных мер в информационной системе в соответствии с требованиями нормативных документов.	0

12.3. Обеспечение режима конфиденциальности при деятельности объекта

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **15**

Проходной балл: **7**

Показатели оценивания	Баллы
Знать конфиденциальное делопроизводство, особенности конфиденциального документооборота, документы разрабатываемые при конфиденциальном делопроизводстве. Уметь организовать конфиденциальное делопроизводство в организации. Владеть навыками составления документов свойственных закрытому документообороту.	15
Не полностью знать конфиденциальное делопроизводство, особенности конфиденциального документооборота, документы разрабатываемые при конфиденциальном делопроизводстве. Уметь организовать конфиденциальное	10

делопроизводство в организации. Владеть навыками составления документов свойственных закрытом документообороте не для всех документов.	
Частично знать конфиденциальное делопроизводство, особенности конфиденциального документооборота, документы разрабатываемые при конфиденциальном делопроизводстве. Частично уметь организовать конфиденциальное делопроизводство в организации. Частично владеть навыками составления документов свойственных закрытом документообороте.	7
Не знает конфиденциальное делопроизводство, особенности конфиденциального документооборота, документы разрабатываемые при конфиденциальном делопроизводстве. Не умеет организовать конфиденциальное делопроизводство в организации. Не владеет навыками составления документов свойственных закрытом документообороте.	0

14.2. Организация пропускного режима

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы самостоятельной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**

Проходной балл: **17**

Показатели оценивания	Баллы
Сформированные знания в области организационного обеспечения информационной безопасности организации. Владение правовыми нормами защиты информации. Знание законов и нормативно-методических документов в области информационной безопасности и интеллектуальной собственности.	40
Хорошо разбирается в Законодательстве РФ в области информационной безопасности	40
Достаточные знания в области организационного обеспечения информационной безопасности организации. Владение правовыми нормами защиты информации. Знание законов и нормативно-методических документов в области информационной безопасности и интеллектуальной собственности.	30
Неполные знания в области организационного обеспечения информационной безопасности организации. Не полное владение правовыми нормами защиты информации. Знание законов и нормативно-методических документов в области информационной безопасности и интеллектуальной собственности.	17