

Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность автоматизированных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очно-заочная

Рабочая программа дисциплины
ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

| | |
|--|---------------------------------|
| Блок: | Блок 1 «Дисциплины (модули)» |
| Часть образовательной программы: | Базовая |
| № дисциплины по учебному плану: | Б1.Б.29 |
| Трудоемкость в зачетных единицах: | 6 семестр - 4; |
| Часов (всего) по учебному плану: | 144 часа |
| Лекции | 6 семестр - 16 часов; |
| Практические занятия | 6 семестр - 32 часа; |
| Лабораторные работы | не предусмотрено учебным планом |
| Консультации | 6 семестр - 2 часа; |
| Самостоятельная работа | 6 семестр - 89,5 часа; |
| в том числе на КП/КР | 6 семестр - 20 часов; |
| Иная контактная работа | 6 семестр - 4 часа; |
| включая: Контрольная работа Семинар | |
| Промежуточная аттестация: | |
| Защита курсовой работы | 6 семестр - 0,3 часа; |
| Экзамен | 6 семестр - 0,2 часа; |
| | всего - 0,5 часа |

Москва 2017

ПРОГРАММУ СОСТАВИЛ:

Преподаватель

(должность)

| | | |
|--|---|------------------------------|
| | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» | |
| | Сведения о владельце ЦЭП МЭИ | |
| | Владелец | Туркина А.А. |
| | Идентификатор | R9001f342-TurkinaAA-3bcc47d9 |

(подпись)

А.А. Туркина

(расшифровка
подписи)

СОГЛАСОВАНО:

Руководитель
образовательной программы

(должность, ученая степень, ученое звание)

| | | |
|--|---|------------------------------|
| | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» | |
| | Сведения о владельце ЦЭП МЭИ | |
| | Владелец | Баронов О.Р. |
| | Идентификатор | R90d76356-BaronovOR-7bf8fd7e |

(подпись)

О.Р. Баронов

(расшифровка
подписи)

Заведующий выпускающей
кафедры

(должность, ученая степень, ученое звание)

| | | |
|--|---|-----------------------------|
| | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» | |
| | Сведения о владельце ЦЭП МЭИ | |
| | Владелец | Невский А.Ю. |
| | Идентификатор | R4bc65573-NevskyAY-0b6e493d |

(подпись)

А.Ю. Невский

(расшифровка
подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: освоение общекультурных и профессиональных компетенций, заключающихся в общей готовности и способности осуществлять мероприятия по правовой и организационной защите информации в интересах обеспечения информационной безопасности предприятия (организации).

Задачи дисциплины

- изучение теоретических основ обеспечения информационной безопасности на предприятии (в организации);
- формирование готовности и способности к активной профессиональной деятельности в условиях информационного противоборства;
- приобретение навыков правильного оформления результатов учебной деятельности..

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

| Код и наименование компетенции | Код и наименование индикатора достижения компетенции | Запланированные результаты обучения |
|---|--|--|
| ОПК-5 способностью использовать нормативные правовые акты в профессиональной деятельности | | уметь: - <input type="checkbox"/> использовать нормативные правовые документы в своей профессиональной деятельности. |
| ПК-7 способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений | | знать: - <input type="checkbox"/> виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз; уметь: - разрабатывать предложения по совершенствованию системы управления информационной безопасностью;. |
| ПК-9 способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности | | уметь: - <input type="checkbox"/> осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности;. |
| ПК-15 способностью организовывать | | уметь: - участвовать в работах по реализации |

| Код и наименование компетенции | Код и наименование индикатора достижения компетенции | Запланированные результаты обучения |
|---|--|---|
| технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю | | политики информационной безопасности; - <input type="checkbox"/> организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; |
| ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности | | знать: - <input type="checkbox"/> нормативные правовые документы по своей профессиональной деятельности; уметь: - формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности; |

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к обязательной части блока дисциплин основной профессиональной образовательной программе Безопасность автоматизированных систем (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Требования к входным знаниям и умениям:

- знать Дисциплина базируется на следующих дисциплинах: «Правоведение», «Основы информационной безопасности», «Теория информационной безопасности».

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, 144 часа.

| № п/п | Разделы/темы дисциплины/формы промежуточной аттестации | Всего часов на раздел | Семестр | Распределение трудоемкости раздела (в часах) по видам учебной работы | | | | | | | | | | Содержание самостоятельной работы/ методические указания |
|-------|--|-----------------------|---------|--|-----|----|--------------|---|-----|----|----|-------------------|-----------------------------------|---|
| | | | | Контактная работа | | | | | | | СР | | | |
| | | | | Лек | Лаб | Пр | Консультация | | ИКР | | ПА | Работа в семестре | Подготовка к аттестации /контроль | |
| КПР | ГК | ИККП | ТК | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 1 | Правовое обеспечение информационной безопасности Российской Федерации. Система права и система законодательства | 15 | 6 | 3 | - | 6 | - | - | - | - | - | 6 | - | <p><u>Подготовка к практическим занятиям:</u> Изучение материала по разделу "Правовое обеспечение информационной безопасности Российской Федерации. Система права и система законодательства" подготовка к выполнению заданий на практических занятиях</p> <p><u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Правовое обеспечение информационной безопасности Российской Федерации. Система права и система законодательства"</p> <p><u>Изучение материалов литературных источников:</u> [3], 1-43</p> |
| 1.1 | Правовое обеспечение информационной безопасности Российской Федерации. | 5 | | 1 | - | 2 | - | - | - | - | - | 2 | - | |
| 1.2 | Система права и система законодательства | 5 | | 1 | - | 2 | - | - | - | - | - | 2 | - | |
| 1.3 | Основные функции государственных органов в области информационной безопасности | 5 | | 1 | - | 2 | - | - | - | - | - | 2 | - | |
| 2 | Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная | 20 | | 4 | - | 8 | - | - | - | - | - | 8 | - | |

| | | | | | | | | | | | | | |
|-----|--|----|---|---|---|---|---|---|---|---|---|---|---|
| | информационной безопасности | | | | | | | | | | | | [1], 1-176 |
| 3.3 | Гражданско-правовая и дисциплинарная ответственности в области информационной безопасности | 5 | 1 | - | 2 | - | - | - | - | - | 2 | - | |
| 4 | Организация защиты информации на предприятии. Разработка системы защиты информации предприятия | 20 | 4 | - | 8 | - | - | - | - | - | 8 | - | <u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Организация защиты информации на предприятии. Разработка системы защиты информации предприятия" <u>Подготовка к практическим занятиям:</u> Изучение материала по разделу "Организация защиты информации на предприятии. Разработка системы защиты информации предприятия" подготовка к выполнению заданий на практических занятиях |
| 4.1 | Общая характеристика организации защиты информации на предприятии | 5 | 1 | - | 2 | - | - | - | - | - | 2 | - | Изучение материала по разделу "Организация защиты информации на предприятии. Разработка системы защиты информации предприятия" подготовка к выполнению заданий на практических занятиях |
| 4.2 | Сертификация средств защиты информации | 5 | 1 | - | 2 | - | - | - | - | - | 2 | - | <u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Организация защиты информации на предприятии. Разработка системы защиты информации предприятия" |
| 4.3 | Порядок организации аттестации объектов информатизации | 5 | 1 | - | 2 | - | - | - | - | - | 2 | - | <u>Изучение материалов литературных источников:</u> |
| 4.4 | Лицензирование деятельности в области информационной безопасности | 5 | 1 | - | 2 | - | - | - | - | - | 2 | - | [1], 1-176 |
| 5 | Корпоративная нормативная база по защите информации. Политика безопасности | 14 | 2 | - | 4 | - | - | - | - | - | 8 | - | <u>Подготовка к практическим занятиям:</u> Изучение материала по разделу "Корпоративная нормативная база по защите информации. Политика безопасности" подготовка к выполнению заданий на практических занятиях |
| 5.1 | Особенности работы с персоналом для обеспечения защиты информации | 4 | 1 | - | 1 | - | - | - | - | - | 2 | - | <u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Корпоративная нормативная база по защите информации" |
| 5.2 | Политика | 4 | 1 | - | 1 | - | - | - | - | - | 2 | - | |

| | | | | | | | | | | | | | |
|-----|---|--------------|-----------|----------|-----------|----------|----------|------------|-----------|-------------|-----------|-------------|--|
| | информационной безопасности | | | | | | | | | | | | информации. Политика безопасности" <u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Корпоративная нормативная база по защите информации. Политика безопасности" <u>Изучение материалов литературных источников:</u> [2], 1-77 |
| 5.3 | Основные организационно-распорядительные документы, определяющие порядок и особенности работы с конфиденциальной информацией на предприятии | 3 | - | - | 1 | - | - | - | - | - | 2 | - | |
| 5.4 | Особенности защиты информации при организации электронного документооборота | 3 | - | - | 1 | - | - | - | - | - | 2 | - | |
| | Экзамен | 35.7 | - | - | - | - | 2 | - | - | 0.2 | - | 33.5 | |
| | Курсовая работа (КР) | 24.3 | - | - | - | - | - | 4 | - | 0.3 | 20 | - | |
| | Всего за семестр | 144.0 | 16 | - | 32 | - | 2 | 4 | - | 0.5 | 56 | 33.5 | |
| | Итого за семестр | 144.0 | 16 | - | 32 | 2 | 4 | 0.5 | 56 | 89.5 | | | |

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПП – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Правовое обеспечение информационной безопасности Российской Федерации. Система права и система законодательства

1.1. Правовое обеспечение информационной безопасности Российской Федерации.

Предмет, задачи и содержание курса «Организационное и правовое обеспечение защиты информации». Место курса среди других дисциплин. Структура курса. Наименование тем и их распределение по видам аудиторных занятий. Форма проведения семинаров и практических занятий. Формы проверки знаний. Анализ нормативных источников и литературы по дисциплине. Методика самостоятельной работы студентов по изучению дисциплины. Компетенции студентов, которые должны быть получены в результате изучения дисциплины. Информационные технологии изучения дисциплины..

1.2. Система права и система законодательства

Понятие «право». Субъективное, объективное и естественное право. Формы и признаки позитивного права. Публичное и частное право. Нормы права, правоотношения, субъекты и объекты права, юридические факты. Источники права. Содержание и структура законодательства. Порядок принятия законодательных актов. Национальная безопасность Российской Федерации. Государственная политика в области обеспечения безопасности. Понятие информационной безопасности. Национальные интересы России в информационной сфере. Основные источники угроз информационной безопасности Российской Федерации. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации и первоочередные мероприятия по ее реализации..

1.3. Основные функции государственных органов в области информационной безопасности

Полномочия федеральных органов государственной власти, функции органов государственной власти субъектов Российской Федерации и органов местного самоуправления в области обеспечения безопасности. Статус Совета Безопасности. Составляющие национальной безопасности. Основные характеристики состояния национальной безопасности. Основные функции ФСТЭК и ФСБ России в области обеспечения информационной безопасности. Основные полномочия данных служб в области информационной безопасности, история их создания, структуры данных государственных органов. Функции ФСО, МВД, Роскомнадзора и других федеральных органов в области обеспечения информационной безопасности РФ. Организационная основа системы обеспечения информационной безопасности Российской Федерации..

2. Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д.

2.1. Законодательство в области государственной тайны.

Законодательство в области государственной тайны. Основные понятия и определения в области государственной тайны. Принципы отнесения сведений к государственной тайне и засекречивания этих сведений. Перечень сведений, составляющих государственную тайну. Степени секретности сведений и грифы секретности носителей этих сведений. Порядок рассекречивания сведений. Взаимная передача сведений, составляющих государственную тайну, органами государственной власти, предприятиями, учреждениями и организациями. Органы защиты государственной тайны. Допуск и доступ к информации, составляющей государственную тайну. Социальные гарантии лицам, допущенным к государственной тайне на постоянной основе. Государственная аттестация руководителей организаций. Организация доступа к сведениям, составляющим государственную тайну..

2.2. Правовое регулирование коммерческой тайны и служебной информации ограниченного распространения

Законодательство в области служебной тайны. Понятие служебной тайны. Порядок допуска сотрудников к информации, составляющей служебную тайну. Законодательство в области коммерческой тайны. Понятие коммерческой тайны и режима коммерческой тайны. Ответственность за нарушение законодательства Российской Федерации о коммерческой тайне..

2.3. Особенности защиты отдельных видов информации

Законодательство в области профессиональной тайны. Понятие профессиональной тайны. Виды профессиональных тайн. Порядок доступа к различным видам профессиональных тайн. Правовое регулирование банковской тайны.

2.4. Правовое регулирование объектов интеллектуальной собственности и их защита

Законодательство в области интеллектуальной собственности. Общие положения. Авторское право и смежные права. Права на программное обеспечение. Патентное право. Изобретение, полезная модель и промышленный образец, созданные в связи с выполнением служебного задания или при выполнении работ по договору. Получение патента. Защита прав авторов и патентообладателей. Право на топологии интегральных микросхем. Право на секрет производства (ноу-хау). Права на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий. Право использования результатов интеллектуальной деятельности в составе единой технологии..

3. Юридическая ответственность субъектов информационной сферы

3.1. Правовое регулирование уголовной ответственности в области информационной безопасности

Понятие юридической ответственности. Правовосстановительная ответственность. Публичная и частная ответственность. Уголовная ответственность. Порядок применения уголовной ответственности на территории РФ. Виды наказаний в УК РФ. Состав преступления: объект, субъект, объективная и субъективная сторона. Мотив к совершению преступления как важная часть для квалификации деяния. Основные составы преступлений в области информационной безопасности..

3.2. Правовое регулирование административной ответственности в области информационной безопасности

Административная ответственность. Порядок применения административной ответственности. Виды наказаний в КоАП РФ. Административная ответственность по законодательству субъектов РФ. Понятие длящегося правонарушения, неоднократность совершения административных правонарушений. Сроки в КоАП РФ. Основные составы административных правонарушений в области информационной безопасности..

3.3. Гражданско-правовая и дисциплинарная ответственности в области информационной безопасности

Гражданско-правовая ответственность. Порядок компенсации имущественного (реального) и морального вреда. Порядок оценки причиненного вреда. Дисциплинарная ответственность. Виды ответственности по трудовому законодательству. Порядок применения ответственности к работникам предприятия. Материальная ответственность. Суды общей юрисдикции, арбитражные суды, третейские суды, суд по интеллектуальным правам. Процедура обращения в суд за судебной защитой..

4. Организация защиты информации на предприятии. Разработка системы защиты информации предприятия

4.1. Общая характеристика организации защиты информации на предприятии

Организация пропускного режима. Организация внутриобъектового режима. Выявление и определение объектов информатизации, обрабатывающих информацию ограниченного доступа на предприятии. Порядок учета, хранения документов ограниченного доступа и обеспечение ограничений к их доступу..

4.2. Сертификация средств защиты информации

Понятие сертификации. Нормативные правовые акты Российской Федерации и национальные стандарты, регламентирующие порядок проведения сертификации средств защиты информации и использования технических средств защиты информации. Выбор средств защиты информации для обеспечения безопасности объектов информатизации..

4.3. Порядок организации аттестации объектов информатизации

Понятие аттестации объектов информатизации. Порядок проведения аттестации объектов информатизации. Иные виды оценки соответствия объектов информатизации..

4.4. Лицензирование деятельности в области информационной безопасности

Понятие лицензирования. Нормативные правовые акты Российской Федерации, регламентирующие порядок лицензирования в области защиты информации. Лицензируемые виды деятельности в области защиты информации. Требования к персоналу, осуществляющему лицензируемые виды деятельности. Требования к оборудованию и программному обеспечению необходимым для осуществления лицензируемых видов деятельности. Особенности и порядок получения литературы для осуществления лицензируемых видов деятельности..

5. Корпоративная нормативная база по защите информации. Политика безопасности

5.1. Особенности работы с персоналом для обеспечения защиты информации

Регулирование отношений по использованию информации ограниченного доступа с работниками организации. Обязанности работодателя по охране конфиденциальности информации в рамках трудовых отношений. Обязанности работников, получивших доступ к документам, содержащим информацию ограниченного доступа. Учёт лиц, получивших доступ к информации. Особенности оформления трудовых и гражданско-правовых отношений с лицами, получающими доступ к информации. Порядок проведения служебных расследований. Особенности определения взысканий при выявлении нарушений в области информационной безопасности..

5.2. Политика информационной безопасности

Установление порядка обращения с информацией ограниченного доступа на предприятии. Порядок определения перечня информации, составляющей коммерческую тайну или иной информации ограниченного доступа. Условия и организация доступа к информации. Понятие и состав грифа конфиденциальности документов. Порядок принятия решения об отнесении документов к информации ограниченного доступа..

5.3. Основные организационно-распорядительные документы, определяющие порядок и особенности работы с конфиденциальной информацией на предприятии

Определение и назначение ответственных лиц и подразделений. Определение перечня объектов на которых обрабатывается информация ограниченного доступа для определения режима. Формирование документов, описывающих технический процесс обработки информации и технических паспортов на объекты информатизации. Разработка инструкций, определяющих порядок отдельных видов защиты информации..

5.4. Особенности защиты информации при организации электронного документооборота
Организация внешнего и внутреннего электронного документооборота. Виды электронной подписи и правовые особенности ее применения. Удостоверяющий центр как основа организации электронного документооборота. Особенности создания внутреннего удостоверяющего центра. Требования к работникам, участвующих в процессе выпуска электронной подписи. Особенности хранения ключей электронной подписи..

3.3. Темы практических занятий

1. Основные функции государственных органов в области информационной безопасности;
2. Правовое регулирование отношений в области информации, информационных технологий и защиты информации;
3. Юридическая ответственность субъектов информационной сферы;
4. Особенности защиты информации на отдельных объектах информатизации.

3.4. Темы лабораторных работ не предусмотрено

3.5 Консультации

Аудиторные консультации по курсовому проекту/работе (КПР)

1. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Правовое обеспечение информационной безопасности Российской Федерации. Система права и система законодательства"
2. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д."
3. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Юридическая ответственность субъектов информационной сферы"
4. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Организация защиты информации на предприятии. Разработка системы защиты информации предприятия"
5. Консультации направлены на выполнение разделов курсового проекта под руководством наставника (преподавателя). В рамках часов на групповые консультации разбираются наиболее важные части расчетных заданий раздела "Корпоративная нормативная база по защите информации. Политика безопасности"

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Правовое обеспечение информационной безопасности Российской Федерации. Система права и система законодательства"
2. Обсуждение материалов по кейсам раздела "Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д."
3. Обсуждение материалов по кейсам раздела "Юридическая ответственность субъектов информационной сферы"
4. Обсуждение материалов по кейсам раздела "Организация защиты информации на предприятии. Разработка системы защиты информации предприятия"
5. Обсуждение материалов по кейсам раздела "Корпоративная нормативная база по защите информации. Политика безопасности"

Индивидуальные консультации по курсовому проекту /работе (ИККП)

1. Консультации проводятся по разделу "Правовое обеспечение информационной безопасности Российской Федерации. Система права и система законодательства"
2. Консультации проводятся по разделу "Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д."
3. Консультации проводятся по разделу "Юридическая ответственность субъектов информационной сферы"
4. Консультации проводятся по разделу "Организация защиты информации на предприятии. Разработка системы защиты информации предприятия"
5. Консультации проводятся по разделу "Корпоративная нормативная база по защите информации. Политика безопасности"

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Правовое обеспечение информационной безопасности Российской Федерации. Система права и система законодательства"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д."
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Юридическая ответственность субъектов информационной сферы"
4. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Организация защиты информации на предприятии. Разработка системы защиты информации предприятия"
5. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Корпоративная нормативная база по защите информации. Политика безопасности"

3.6 Тематика курсовых проектов/курсовых работ

6 Семестр

Курсовая работа (КР)

Темы:

- 1. Обзор нормативно-правовых актов по обеспечению защиты информации в организации
2. Основные направления государственной политики России в сфере информационной безопасности
3. Понятие информации и ее виды по порядку организации доступа к ней
4. Основные элементы организационной основы системы обеспечения информационной безопасности России
5. Полномочия в области информационной безопасности и история

создания ФСТЭК России. 6. Полномочия в области информационной безопасности и история создания ФСБ России 7. Полномочия МВД России, ФСО России, Службы внешней разведки и Федеральная служба войск национальной гвардии в области информационной безопасности 8. Организация лицензирования деятельности в области защиты информации, осуществляемое ФСТЭК России 9. Организация лицензирования деятельности в области защиты информации, осуществляемое ФСБ России 10. Понятие «коммерческая тайна», особенности ее установления на предприятии 11. Понятие «служебная информация», особенности определения режима её обработки 12. Информация, относимая к секрету производства, особенности ее правовой и организационной защиты 13. Особенности правового регулирования объектов интеллектуальной собственности и порядок их защиты 14. Банковская тайна и порядок ее определения и защиты 15. Профессиональная информация ограниченного доступа и порядок ее защиты 16. Персональные данные и иная личная информация ограниченного доступа и порядок ее защиты 17. Ответственность за нарушение законодательства в сфере защиты информации и особенности ее применения 18. Правовое регулирование применения электронной подписи 19. Понятие и виды электронной подписи, порядок применения электронной подписи во внутреннем (внешнем) документообороте 20. Особенности подтверждения соответствия средств защиты информации установленным нормативным требованиям. 21. Система сертификации средств защиты информации в России 22. Аттестация объектов информатизации, как способ подтверждения соответствия систем установленным требованиям 23. Порядок организации защиты информации на предприятии 24. Особенности разработки положения о пропускном режиме на предприятии 25. Особенности хранения материальных носителей, содержащих информацию ограниченного распространения 26. Организация доступа и допуска персонала к информации ограниченного распространения 27. Особенности защиты информации при проведении совещаний 28. Особенности организации публикации различной информации, на предприятиях, обрабатывающих информацию ограниченного распространения 29. Организация внутриобъектового режима на предприятии 30. Планирование мероприятий по защите информации на предприятии 31. Организация контроля за состоянием защиты информации на предприятии 32. Порядок подключения операторов к Единой Биометрической Системе (ЕБС) 33. Порядок защиты информации в государственной информационной системе на примере конкретной государственной информационной системы (ГИС) 34. Особенности обработки и защиты персональных данных при создании системы «Умный город» 35. Особенности привлечения к ответственности за киберпреступления в России 36. Правовое регулирования веб-приложений и программного обеспечения, обрабатывающего персональные данные 37. Сравнение законодательства России в области ПДн с европейским GDPR 38. Правовое регулирование интернета в России

График выполнения курсового проекта

| Неделя | 1 - 8 | 9 - 15 | Зачетная |
|---|-------|--------|--------------------------|
| Раздел курсового проекта | 1 | 2 | Защита курсового проекта |
| Объем раздела, % | 50 | 50 | - |
| Выполненный объем нарастающим итогом, % | 50 | 100 | - |

| Номер раздела | Раздел курсового проекта |
|---------------|--|
| 1 | Соблюдение графика выполнения работы |
| 2 | Применение при выполнении работы судебной практики и примеров из практической деятельности |

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

| Запланированные результаты обучения по дисциплине (в соответствии с разделом 1) | Коды индикаторов | Номер раздела дисциплины (в соответствии с п.3.1) | | | | | Оценочное средство (тип и наименование) |
|--|--------------------|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | |
| Знать: | | | | | | | |
| <input type="checkbox"/> виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз; | ПК-7(Компетенция) | + | | | | | Контрольная работа/Основные функции государственных органов в области информационной безопасности |
| <input type="checkbox"/> нормативные правовые документы по своей профессиональной деятельности; | ОК-4(Компетенция) | + | | | | | Контрольная работа/Основные функции государственных органов в области информационной безопасности |
| Уметь: | | | | | | | |
| <input type="checkbox"/> использовать нормативные правовые документы в своей профессиональной деятельности | ОПК-5(Компетенция) | | | | + | | Семинар/Особенности защиты информации на отдельных объектах информатизации |
| разрабатывать предложения по совершенствованию системы управления информационной безопасностью; | ПК-7(Компетенция) | | | | | + | Контрольная работа/Правовое регулирование отношений в области информации, информационных технологий и защиты информации |
| <input type="checkbox"/> осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности; | ПК-9(Компетенция) | | | | + | | Семинар/Особенности защиты информации на отдельных объектах информатизации |
| <input type="checkbox"/> организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и | ПК-15(Компетенция) | | + | | | | Семинар/Особенности защиты информации на отдельных объектах информатизации |

| | | | | | | | |
|--|--------------------|--|--|---|--|---|---|
| экспортному контролю; | | | | | | | |
| участвовать в работах по реализации политики информационной безопасности | ПК-15(Компетенция) | | | | | + | Контрольная работа/Правовое регулирование отношений в области информации, информационных технологий и защиты информации |
| формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности; | ОК-4(Компетенция) | | | + | | | Семинар/Юридическая ответственность субъектов информационной сферы |

4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

4.1. Текущий контроль успеваемости

6 семестр

Форма реализации: Письменная работа

1. Основные функции государственных органов в области информационной безопасности (Контрольная работа)
2. Особенности защиты информации на отдельных объектах информатизации (Семинар)
3. Правовое регулирование отношений в области информации, информационных технологий и защиты информации (Контрольная работа)

Форма реализации: Проверка задания

1. Юридическая ответственность субъектов информационной сферы (Семинар)

Балльно-рейтинговая структура дисциплины является приложением А.

Балльно-рейтинговая структура курсовой работы является приложением Б.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №6)

При формировании итоговой оценки учитывается как результат ответа на экзамене, так и текущая успеваемость студента

Курсовая работа (КР) (Семестр №6)

При выставлении итоговой оценки учитывается выполнение графика написания работы, содержание и оформление работы, а также качества доклада и умение студента аргументированно отстаивать свою точку зрения.

Примечание: Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Новиков В. К.- "Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации)", Издательство: "Горячая линия-Телеком", Москва, 2017 - (176 с.)
<https://e.lanbook.com/book/111084>;
2. Н. Б. Ельчанинова- "Правовые основы защиты информации с ограниченным доступом", Издательство: "Южный федеральный университет", Ростов-на-Дону, Таганрог, 2017 - (77 с.)
<https://biblioclub.ru/index.php?page=book&id=499598>;
3. Бахаров Л. Е.- "Информационная безопасность и защита информации", Издательство: "МИСИС", Москва, 2015 - (43 с.)
<https://e.lanbook.com/book/116711>.

5.2 Лицензионное и свободно распространяемое программное обеспечение:

1. СДО "Прометей";
2. Office;

3. Windows;
4. Майнд Видеоконференции.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:

1. ЭБС Лань - <https://e.lanbook.com/>
2. ЭБС "Университетская библиотека онлайн" - http://biblioclub.ru/index.php?page=main_ub_red
3. Научная электронная библиотека - <https://elibrary.ru/>
4. Национальная электронная библиотека - <https://rusneb.ru/>
5. ЭБС "Консультант студента" - <http://www.studentlibrary.ru/>
6. Электронная библиотека МЭИ (ЭБ МЭИ) - <http://elib.mpei.ru/login.php>
7. Информационно-справочная система «Кодекс/Техэксперт» - <Http://proinfosoft.ru;http://docs.cntd.ru/>

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

| Тип помещения | Номер аудитории, наименование | Оснащение |
|---|-------------------------------------|---|
| Учебные аудитории для проведения лекционных занятий и текущего контроля | К-601, Учебная аудитория | парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран |
| | А-300, Учебная аудитория "А" | кресло рабочее, парта, стеллаж, стол преподавателя, стол учебный, стул, трибуна, микрофон, мультимедийный проектор, экран, доска маркерная, колонки, техническая аппаратура, кондиционер, телевизор |
| Учебные аудитории для проведения практических занятий, КР и КП | М-510, Учебная аудитория | парта со скамьей, стол преподавателя, стул, доска меловая |
| Учебные аудитории для проведения промежуточной аттестации | М-510, Учебная аудитория | парта со скамьей, стол преподавателя, стул, доска меловая |
| | Ж-120, Машинный зал ИВЦ | сервер, кондиционер |
| Помещения для самостоятельной работы | НТБ-303, Компьютерный читальный зал | стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер |
| Помещения для консультирования | М-510, Учебная аудитория | парта со скамьей, стол преподавателя, стул, доска меловая |
| Помещения для хранения оборудования и учебного инвентаря | К-202/2, Склад кафедры БИТ | стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования |

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Организационное и правовое обеспечение информационной безопасности

(название дисциплины)

6 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

- КМ-1 Основные функции государственных органов в области информационной безопасности (Контрольная работа)
- КМ-2 Правовое регулирование отношений в области информации, информационных технологий и защиты информации (Контрольная работа)
- КМ-3 Юридическая ответственность субъектов информационной сферы (Семинар)
- КМ-4 Особенности защиты информации на отдельных объектах информатизации (Семинар)

Вид промежуточной аттестации – Экзамен.

| Номер раздела | Раздел дисциплины | Индекс КМ: | КМ-1 | КМ-2 | КМ-3 | КМ-4 |
|---------------|---|------------|------|------|------|------|
| | | Неделя КМ: | 4 | 8 | 12 | 15 |
| 1 | Правовое обеспечение информационной безопасности Российской Федерации. Система права и система законодательства | | | | | |
| 1.1 | Правовое обеспечение информационной безопасности Российской Федерации. | | + | | | |
| 1.2 | Система права и система законодательства | | + | | | |
| 1.3 | Основные функции государственных органов в области информационной безопасности | | + | | | |
| 2 | Правовое регулирование отдельных видов информации: государственная тайна, служебная информация, профессиональная тайна и т.д. | | | | | |
| 2.1 | Законодательство в области государственной тайны. | | | | | + |
| 2.2 | Правовое регулирование коммерческой тайны и служебной информации ограниченного распространения | | | | | + |
| 2.3 | Особенности защиты отдельных видов информации | | | | | + |
| 2.4 | Правовое регулирование объектов интеллектуальной собственности и их защита | | | | | + |
| 3 | Юридическая ответственность субъектов информационной сферы | | | | | |
| 3.1 | Правовое регулирование уголовной ответственности в области информационной безопасности | | | | + | |
| 3.2 | Правовое регулирование административной ответственности в области информационной безопасности | | | | + | |

| | | | | | |
|------------|---|----|----|----|----|
| 3.3 | Гражданско-правовая и дисциплинарная ответственности в области информационной безопасности | | | + | |
| 4 | Организация защиты информации на предприятии. Разработка системы защиты информации предприятия | | | | |
| 4.1 | Общая характеристика организации защиты информации на предприятии | | | | + |
| 4.2 | Сертификация средств защиты информации | | | | + |
| 4.3 | Порядок организации аттестации объектов информатизации | | | | + |
| 4.4 | Лицензирование деятельности в области информационной безопасности | | | | + |
| 5 | Корпоративная нормативная база по защите информации. Политика безопасности | | | | |
| 5.1 | Особенности работы с персоналом для обеспечения защиты информации | | + | | |
| 5.2 | Политика информационной безопасности | | + | | |
| 5.3 | Основные организационно-распорядительные документы, определяющие порядок и особенности работы с конфиденциальной информацией на предприятии | | + | | |
| 5.4 | Особенности защиты информации при организации электронного документооборота | | + | | |
| Вес КМ, %: | | 25 | 25 | 25 | 25 |

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА КУРСОВОГО ПРОЕКТА/РАБОТЫ ПО ДИСЦИПЛИНЕ

Организационное и правовое обеспечение информационной безопасности

(название дисциплины)

6 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по курсовой работе:

КМ-1 Срок КМ Соблюдение графика выполнения работы

КМ-2 Применение при выполнении работы судебной практики и примеров из практической деятельности

Вид промежуточной аттестации – защита КР.

| Номер раздела | Раздел курсового проекта/курсовой работы | Индекс КМ: | КМ-1 | КМ-2 |
|---------------|--|------------|------|------|
| | | Неделя КМ: | 8 | 15 |
| 1 | Соблюдение графика выполнения работы | | + | |
| 2 | Применение при выполнении работы судебной практики и примеров из практической деятельности | | | + |
| Вес КМ, %: | | | 50 | 50 |