МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

_____ Филиппович А.Ю.

"01" сентября 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Организационное и правовое обеспечение информационной безопасности»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль)
«Обеспечение информационной безопасности распределенных информационных систем»

Квалификация (степень) выпускника
Специалист

Форма обучения
Очная
Год приема - 2019

Москва 2019 г.

1. Цели освоения дисциплины.

К **основным целям** освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» следует отнести:

- приобретение студентами знаний по организационному обеспечению защиты информации и формирование практических навыков работы в конкретных условиях, необходимых для комплексного обеспечения безопасности информации;
- обеспечение основ правовой подготовки специалистов в области защиты информации, развитие навыков работы с нормативно-правовыми документами, приобретение знаний и навыков, необходимых для комплексного обеспечения безопасности информации.

К **основным задачам** освоения дисциплины «Организационное и правовое обеспечение информационной безопасности» следует отнести:

- овладение студентами практическими навыками использования организационных и правовых принципов и норм для защиты информации.

2. Место дисциплины в структуре ООП специалитета.

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к числу профессиональных учебных дисциплин базовой части базового цикла (Б1.1.13) основной образовательной программы специалитета.

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Основы информационной безопасности» (основными понятиями и терминологией в области информационной безопасности).

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	**В результате освоения образовательной программы обучающийся должен обладать**	**Перечень планируемых результатов обучения по дисциплине**
ОК - 4	Способностью использовать основы правовых знаний в различных сферах деятельности	**владеть:** - навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.

ОПК - 6	Способностью применять нормативные правовые акты в профессиональной деятельности	**Знать:** - основные отечественные и зарубежные стандарты в области информационной безопасности. **Уметь:** Применять действующую законодательную базу в области обеспечения информационной безопасности. **Владеть:** навыками работы с нормативными правовыми актами.
ПК - 11	Способностью разрабатывать политику информационной безопасности автоматизированной системы	**знать:** - принципы формирования политики информационной безопасности

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет **4**зачетных единицы, т.е. **144**академических часа (лекции - 36часов, практические занятия - 0 часов, лабораторные занятия- 36 час, самостоятельная работа – 72 часов, форма контроля - экзамен) во 2 семестре.

Структура и содержание дисциплины «Организационное и правовое обеспечение информационной безопасности» по срокам и видам работы отражены в приложении.

Содержание разделов дисциплины

Тема 1. *Понятие "Организационная защита информации".* Сущность организационных методов защиты информации. Соотношение организационных методов защиты информации с правовыми и техническими. Организационные методы как реализация полномочий и их распределение между уровнями управления организацией. Понятия организационная защита информации и режим защиты информации. Различные подходы к определению понятия организация защиты информации. Определение понятия по целям, по функциям, по структуре т.д. Понятие режим защиты информации. Режим защиты информации как составная часть организационной защиты информаци; субъекты и объекты системы организационной защиты информации.

Тема 2. *Организационные источники и каналы утечки информации. Силы, средства и условия организационной защиты информации.* Комуникационный процесс и его базовые элементы: источник информации, отправитель,

сообщение, канал, получатель. Источники конфиденциальной информации: люди, документы, изделия, технические носители и средства коммуникации. Организационные каналы передачи информации и каналы утечки информации и несанкционированного доступа к ней. Классификация организационных каналов утечки конфиденциальной информации. Основания классификации: по каналам коммуникации и источникам конфиденциальной информации; по источникам угроз; времени воздействия и места их возникновения; по направлениям деятельности организации и характеру конфиденциальной информации; по характеру взаимоотношений с партнерами; по способам и средствам несанкционированного доступа к конфиденциальной информации; по способам, средствам и методам защиты информации от утечки и несанкционированного доступа к ней; по степени формализации каналов утечки и т.д. Основные организационные каналы утечки и несанкционированного доступа к информации: разглашение информации персоналом организации: разглашение информации при осуществлении сотрудничества с другими организациями, в частности в ходе переговоров, при поведении совещаний, при приеме в организации посетителей; при осуществлении рекламной и публикаторской деятельности. Соотношение организационных и правовых методов защиты информации при взаимоотношениях с государственными и муниципальными организациями (налоговой инспекцией, санитарной и пожарной службами, органами статистики, правоохранительными органами и т.п.), с другими организациями на основе договоров (банками, адвокатскими конторами, аудиторскими фирмами, страховыми компаниями, службами связи, охранными агентствами и т.п.). Соотношение организационных и технических методов защиты информации при использовании технических, в том числе, электронных средств передачи, обработки, хранения конфиденциальной информации. Совокупности каждого из методов защиты информации, используемых для перекрытия каналов утечки информации, как основные направления организационной защиты информации.

Тема 3. *Порядок засекречивания и рассекречивания конфиденциальных сведений, документов и изделий.*
Установление и изменение степени секретности сведений, содержащихся в работах, документах и изделиях. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности. Присвоение грифа и изменение грифа секретности работам, документам и изделиям. Понятие рассекречивание сведений. Основания для рассекречивания конфиденциальных сведений, документов и изделий.

Тема 4. *Подбор персонала на должности, связанные с работой с конфиденциальной информацией.*
Персонал организации как источник конфиденциальной информации и один из основных каналов ее разглашения. Особенности подбора персонала на должности, связанные с работой с конфиденциальной информацией. Должности, составляющие с точки зрения защиты информации группы риска : руководящий состав организации, средний управленческий персонал, исполнители, сотрудники, осуществляющие технологические процессы передачи, обработки и хранения информации и др. Оценка кандидатов на должности, связанные с доступом к конфиденциальной информации. Основные критерии оценки: уровень профессиональной подготовки, знаний, умений и наличие практического опыта работы; личностные характеристики. Методы проверки кандидатов на должности. Состав документов, необходимых при подборе и приеме сотрудников на должности, связанные с доступом к конфиденциальной информации. Особенности документирования трудовых отношений с персоналом, обладающим конфиденциальной информацией.

Тема 5. *Организация доступа и допуска к информации ограниченного доступа.*
Понятие допуск. Формы допусков, их назначение и классификация. Основные принципы допускной работы. Понятие доступ к защищаемой информации. Условия правомерного доступа.

Задачи режима защиты информации, решаемые в процессе регулирования доступа. Понятие разрешительной системы доступа, основные требования, предъявляемые к ней.

Тема 6. *Текущая работа с персоналом, обладающим конфиденциальной информацией.* Профессиональная ориентация и обучение персонала. Ознакомление сотрудника с правилами, процедурами и методами защиты информации. Организация обучения персонала. Основные формы обучения и методы контроля знаний. Мотивация персонала к выполнению требований по защите информации. Основные формы воздействия на персонал как методы мотивации: использование различных форм вознаграждения, управление карьерой, привлечение к участию в прибылях, воспитание фирменного патриотизма и др. Организация контроля за соблюдением персоналом требований режима защиты информации. Методы проверки персонала. Основные меры по защите информации при увольнении сотрудника. Документирование процедуры увольнения сотрудника.

Тема 7. *Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.* Понятие служебное расследование по фактам разглашения информации. Цели и задачи служебного расследования. Основания для проведения служебного расследования. Процедура служебного расследования. Меры, принимаемые по результатам расследования. Документирование хода и результатов служебного расследования.

Тема 8. *Организация охраны территории, зданий, помещений и персонала.* Понятие охрана. Цели и задачи охраны. Объекты охраны: территория, здания, помещения, персонал, информационные ресурсы и другие материальные и финансовые ценности. Особенности их охраны. Виды и способы охраны. Понятие о рубежах охраны. Многорубежная система охраны. Факторы выбора приемов и средств охраны.

Тема 9. *Организация пропускного и внутриобъектового режимов.* Понятие пропускной режим. Цели и задачи пропускного режима. Организация пропускного режима. Основные положения инструкции об организации пропускного режима и работе бюро пропусков. Понятие пропуска. Виды пропусков и отличительных шифров. Порядок оформления и выдачи пропусков. Контрольно-пропускные пункты, их оборудование и организация работы. Порядок прохода и проезда на территорию организации. Порядок вывоза (выноса), ввоза (вывоза) материальных ценностей и документации на/с территории организации. Понятие внутриобъектовый режим. Его основное назначение при ведении конфиденциальных работ и обращении с охраняемыми изделиями и документами. Порядок определения перечня предметов, запрещенных к проносу/провозу на режимную территорию. Общие требования внутриобъектового режима. Порядок передвижения работников и перевозки охраняемых изделий по режимной территории объекта. Порядок допуска работников в помещения, где ведутся конфиденциальные работы. Организация контроля за выполнением распорядка дня лицами, работающими на режимных объектах. Создание отдельных (выделенных) производственных зон (зон доступа) по типу и степени конфиденциальности работ с самостоятельными системами организации и контроля доступа. Методика проектирования системы пропускного и внутриобъектового режимов и оценки эффективности их функционирования.

Тема 10. *Требования к помещениям и хранилищам в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия.* Понятие режимных помещений и требования, предъявляемые к ним. Особенности оборудования помещения, где ведутся конфиденциальные работы. Порядок назначения комиссии для аттестации помещений на пригодность их для ведения конфиденциальных работ. Порядок лицензирования. Документальное оформление после обследования помещений на пригодность. Назначение

ответственных лиц, имеющих право вскрывать и опечатывать режимные помещения. Оборудование специальных хранилищ, сейфов и металлических а, предназначенных для хранения конфиденциальных изделий и документов. Порядок приема-сдачи под охрану режимные помещения.

Тема 11. *Организация защиты информации при взаимодействии со сторонними организациями.* Организация подготовки и проведения совещаний и переговоров по конфиденциальнымвопросам. Организация защиты информации при приеме в организации посетителей и командированных лиц. Организация защиты информации при приеме в организации иностранных представителей. Организация защиты информации при осуществлении рекламной и выставочной деятельности. Организация защиты информации при подготовке материалов к открытому опубликованию.

Тема 12. *Контроль функционирования системы организационной защиты информации.* Сущность контроля как функции управления. Цели контроля. Функции контроля: сбор , обработка и анализ информации о фактических результатах деятельности по защите информации , сравнение их с планами , выявление отклонений и анализ причин отклонений ; разработка мероприятий, необходимых для достижения целей ОЗИ. Учет и отчетность по ОЗИ , как основа контроля . Объекты контроля . Методы контроля : анализ , наблюдение , проверка, сравнение , учет и др. Формы контроля : предварительный , текущий и заключительный . Технология контроля : выработка стандартов и критериев ОЗИ , сопоставление с ними полученных результатов и принятие необходимых корректирующих действий . Выбор методов контроля , используемых на различных его этапах в зависимости от объектов контроля. Методика оценки эффективности контроля. Документирование процесса и результатов контроля как основа анализа, планирования и организационного- правового регулирования структур и процессов ОЗИ.

Тема 13. *Характеристика правоотношений в сфере защиты информации.* Информация и окружающий мир. Свойства информации. Влияние информации на общество. Информация и право. Правовое определение понятия "информация". Документирование информации. Понятие информационных ресурсов. Виды информации по категориям доступа. Общедоступная информация. Информация ограниченного доступа. Информационные технология. Информационные системы и средства их обеспечения. Правовая характеристика информационной сферы. Модель сферы защиты информации. Объекты и субъекты сферы защиты информации. Принципы регулирования правоотношений, возникающих в сфере защиты информации. Правовые нормы, используемые в сфере защиты информации. Правовое закрепление необходимости принятия мер по защите информации. Составление правовых понятий информационной безопасности и защиты информации.

Тема 14. *Структура системы организационно-правового обеспечения информационной безопасности в России.* Исторические аспекты и обеспечение безопасности информации в России. Угрозы информационной безопасности. Внутренние и внешние угрозы. Доктрина информационной безопасности Российской Федерации об угрозах информационной безопасности и мерах противодействия. Система правовой защиты информации в Российской Федерации. Отрасли права, обеспечивающие законность в сфере защиты информации. Органы государственной власти, ответственные за защиту информации в стране. Нормативно-правовые акты, определяющие права и обязанности органов государственной власти, юридических и физических лиц по защите информации.

Тема 15. *Содержание основных нормативно-правовых актов, направленных на защиту информации ограниченного доступа.*
Конституционное законодательство о защите информации. Обзор законодательных актов общего характера, содержащих положения о защите информации. Специальное законодательство по защите информации. Особая роль законов об информации, информационных технологиях и защите информации, О коммерческой тайне, О государственной тайне, "О персональных данных", "Об электронной цифровой подписи", "Об оперативно-розыскной деятельности", "О техническом регулировании". Законы субъектов РФ, регламентирующие вопросы защиты информации. Подзаконные правовые акты, регулирующие процессы защиты информации. Роль подзаконных нормативных документов ФСТЭК и ФСБ. Международные правовые акты по защите информации. Открытые критерии. Технологические регламенты.

Тема 16. *Правовой порядок установления и поддержание режима ограничения доступа к информации.*
Правовые основания для введения режима ограничения доступа к информации. Виды тайн, правовые цели принципы введения режима ограничения доступа. Правовые нормы - запреты, не допускающие возможность введения режима ограничения доступа к информации. Порядок введения режима конфиденциальности информации. Реквизиты, используемые для населения на носители информации с ограниченным доступом и доступ к их носителем. Порядок представления информации ограниченного доступа государственным органам и общественным организациям. Органы государственного контроля за выполнением требований по защите информации ограниченного доступа. Использование договорных отношений дляподдержание режим ограничения доступа.

Тема 17. *Лицензирование и сертификация, как методы правового регулирования отношений в сфере защиты информации.*
Закон "О лицензировании отдельных деятельности". Виды деятельности в сфере защиты информации, подлежащие лицензированию. Подзаконные правовые акты, определяющие порядок лицензирования. Особый порядок лицензирования предприятий на право работы с документами, составляющими государственную тайну. Требования, которые должны удовлетворять предприятия-лицензиаты. Органы государственной власти, наделенные полномочиями лицензирования в сфере защиты информации. Сертификация. Нормативно-правовые акты, определяющие порядок сертификации средств защиты информации. Роль Федерального закона "О техническом регулировании". Методы оценки соответствия, используемые в сфере защиты информации. Современные системы сертификации. Обязательная и добровольная сертификация. Порядок проведения обязательной и добровольной сертификации. Правовые санкции и нарушителям порядка лицензирования и сертификации.

Тема 18. *Правовые последствия введения режима ограничения доступа для субъектов защиты информации. Сферы.*
Обязанность субъектов информационной сферы по соблюдению режима охраны сведений ограниченного доступа. Законодательное закрепление необходимости принятия субъектами информационной сферы мер по защите информации. Принципы допуска и доступа граждан к информации ограниченного доступа. Основание для отказа должному лицу или гражданину в допуске к информации с ограниченным доступом. Социальные гарантии, предоставляемые гражданам при допуске к информации ограниченного доступа. Правовое регулирование отношений между работодателями и работниками в сфере защиты информации. Виды и условия применения правовых норм дисциплинарной, гражданско-правовой, административно-правовой и уголовной ответственности за разглашение информации и нарушение правил её защиты.

Тема 19. *Государственная система правовой защиты сведений, составляющих государственную тайну.*
Законодательство РФ в области защиты государственной тайны. Принципы обеспечения защиты государственной тайны. Органы государственной власти и должностные лица, отвечающие за сохранность гостайны. Роль межведомственной комиссии РФ по защите гостайны. Перечни сведений, составляющих государственную тайну, отнесенных к государственной тайне и подлежащих засекречиванию. Обеспечение режима секретности. Порядок засекречивания и рассекречивания сведений, составляющих государственную тайну. Распоряжение сведениями, составляющими государственную тайну. Правовая оценка ущерба, наносимого безопасности РФ, вследствие разглашения информации, составляющей государственную тайну.

Тема 20. *Особенности правовой защиты сведений, составляющих различные виды тайн.*
Защита сведений о частной жизни гражданина. Персональные данные. Личная и семейная тайна. Тайна голосования. Тайна исповеди. Тайна усыновления. Служебная тайна. Защита сведений, составляющих тайну следствия и судопроизводства. Налоговая тайна. Таможенная тайна. Защита профессиональной тайны. Журналистская тайна. Нотариальная тайна. Страховая тайна. Врачебная тайна. Тайна аудита. Тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Защита сведений, связанных с коммерческой деятельностью. Банковская тайна. Практические аспекты защиты конфиденциальной информации. Основных документы ФСТЭК России определяющие требования по защите информации. Профили по защите конфиденциальной информации.

Тема 21. *Правовая защита информации, составляющей интеллектуальную собственность.*
Понятие интеллектуальной собственности. Объекты и субъекты отношений в сфере защиты интеллектуальной собственности. Авторское право и смежные права. Патентное право. Изобретения, полезные модели, промышленные образцы. Защита авторских прав на программы для ЭВМ и базы данных. Защита авторских прав на топологию интегральных схем. Защита средств индивидуализации участников гражданского оборота и производимой ими продукции. Фирменные наименования и товарные знаки. Ноу-хау. Договорное право. Авторские и лицензионные договоры. Меры пресечения нарушений в сфере интеллектуальной собственности.

Тема 22. *Правовое обеспечение безопасности информационных и телекоммуникационных систем.*
Доктрина информационной безопасности России об угрозах безопасности информационным системам. Особенности правовой защиты информационных и телекоммуникационных систем. Гражданско-правовые, уголовно-правовые и административно-правовые нормы защиты информации в информационных и телекоммуникационных системах. Ключевые (критические) технологии. Особенности правовой защиты ключевых (критических) технологий. Проблемы защиты информации в сети Интернет. Закон Об электронной подписи.

4. Образовательные технологии.

Методика преподавания дисциплины «Организационное и правовое обеспечение информационной безопасности» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- проведение интерактивных лекционных и практических занятий в форме видео уроков;
- обсуждение и защита домашних заданий по дисциплине;
- подготовка, представление и обсуждение презентаций на семинарских занятиях.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов.

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- домашние задания и их защита;
- экзамен.

Темы домашних заданий, контрольных вопросов и заданий для проведения текущего контроля, экзаменационных билетов приведены в приложении 2.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ОК - 4	Способностью использовать основы правовых знаний в различных сферах деятельности
ОПК - 6	способностью применять нормативные правовые акты в профессиональной деятельности
ПК - 11	Способностью разрабатывать политику информационной безопасности автоматизированной системы

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимисядисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю)

ОПК-6 - способностью применять нормативные правовые акты в профессиональной деятельности

Показатель	Критерии оценивания			
	2	3	4	5
знать: - основные отечественные и зарубежные стандарты в области информационной безопасности.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: основные отечественные и зарубежные стандарты в области информационной безопасности.	Обучающийся демонстрирует неполное соответствие следующих знаний: основные отечественные и зарубежные стандарты в области информационной безопасности. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний: основные отечественные и зарубежные стандарты в области информационной безопасности, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: основные отечественные и зарубежные стандарты в области информационнй безопасности, свободно оперирует приобре-тенными знаниями.
уметь: - Применять действующую законодательну ю базу в области обеспечения информационной безопасности	Обучающийся не умеет или в недостаточной степени умеетприменять действующую законодательную базу в области обеспечения информационной безопасности	Обучающийся демонстрирует неполное соответствие следующих умений: применять действующую законодательную базу в области обеспечения информационной безопасности. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: применять действующую законодательную базу в области обеспечения информационной безопасности. Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие следующих умений: применять действующую законодательнн ую базу в области обеспечения информационнй безопасности. Свободно оперирует приобретенны ми умениями, применяет их в ситуациях повышенной сложности.
владеть: - навыками работы с нормативными правовыми актами	Обучающийся не владеет или в недостаточной степени владеет навыками работы с нормативными правовыми актами	Обучающийся владеет навыками работы с нормативными правовыми актами.допускаются значительные ошибки, проявляется недостаточность владения навыками.	Обучающийся частично владеет навыками работы с нормативными правовыми актами. Навыки освоены, но допускаются незначительные ошибки,	Обучающийся в полном объеме владеет навыками работы с нормативными правовыми актами, свободно

			неточности, затруднения.	применяет полученные навыки в ситуациях повышенной сложности.
ОК-4 - Способностью использовать основы правовых знаний в различных сферах деятельности				
владеть: навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности..	Обучающийся не владеет или в недостаточной степени владеет навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.	Обучающийся владеет навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.	Обучающийся частично владеет навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности. Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения.	Обучающийся в полном объеме владеет навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности, свободно применяет полученные навыки в ситуациях повышенной сложности.
ПК-11 Способностью разрабатывать политику информационной безопасности автоматизированной системы				
знать: принципы формирования политики информационной безопасности	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: принципы формирования политики информационной безопасности	Обучающийся демонстрирует неполное соответствие следующих знаний: принципы формирования политики информационной безопасности Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации	Обучающийся демонстрирует частичное соответствие следующих знаний: принципы формирования политики информационной безопасности Допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: принципы формирования политики информационной безопасности, свободно оперирует приобре-тенными знаниями.

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен.

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонды оценочных средств представлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины.

а) основная литература:

1. Семененко В.А. Информационная безопасность : учеб.пособие для вузов. - М.: МГИУ, 2010 Гриф УМО
2. Правовое обеспечение информационной безопасности :учеб. для вузов. / авт.- ред. Минаев В.А., Фисун А.П., Скрыль С.В. и др - М.: Маросейка, 2008
3. Малюк, А. А. Информационная безопасность: концептуальные и методологичесские основы защиты информации : учеб.пособие для вузов / А. А. Малюк. - М. : Горячая линия-Телеком, 2004. - 280 с. : ил.
4. Ярочкин, В. И. Информационная безопасность : учеб.для вузов / В. И. Ярочкин. - 4-е изд. - М. : Академ. проект, 2006. - 543 с.
5. Основы организационного обеспечения информационной безопасности объектов информатизации : учеб.пособие / С. Н. Сёмкин, Э. В. Беляков, С. В. Гребнев, В. И. Козачок. - М. : Гелиос АРВ, 2005. - 186 с.

б) дополнительная литература:

1. Основы информационной безопасности : учеб.пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. - М. : Горячая линия-Телеком, 2006. - 544 с. : ил.
2. Правовое обеспечение информационной безопасности: Учебное пособие, 2-е издание. / Под ред. С.Я.Казанцева. М.: Издательский центр "Академия", 2007. – 240 с.

в) Нормативные документы:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // Российская газета. № 237. 25.12.1993.
2. Семейный кодекс Российской Федерации от 29.12.1995 № 223-ФЗ // СЗ РФ. 1996. № 1. ст. 16.
3. Гражданский кодекс Российской Федерации (Часть вторая) от 26.01.1996 № 14-ФЗ (ред. от 01.02.2008) // СЗ РФ. 1996. № 5. ст. 410.
4. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СЗ РФ. 1996. № 25. ст. 2954.
5. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // СЗ РФ. 2001. № 52 (ч. I).ст. 4921.
6. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ // Российская газета. № 256., 31.12.2001.
7. Гражданский кодекс Российской Федерации (Часть четвертая) от 18.12.2006 № 230-ФЗ // СЗ РФ. 2006. № 52 (1 ч.).ст. 5496.
8. Основы законодательства Российской Федерации о нотариате // Российская газета. № 49. 13.03.1993.
9. Основы законодательства Российской Федерации об охране здоровья граждан (утв. ВС РФ 22.07.1993 № 5487-1) // Ведомости СНД и ВС РФ. 1993. № 33. ст. 1318.
10. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» // СЗ РФ. 1997. № 41. стр. 8220-8235.
11. Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» // СЗ РФ.1996. № 6. ст. 492.
12. Федеральный закон от 07.08.2001 № 119-ФЗ «Об аудиторской деятельности» // СЗ РФ. 2001. № 33 (часть I).ст. 3422.
13. Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной подписи» // СЗ

РФ. 2002. № 2. ст. 127.

14. Федеральный закон от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации // СЗ РФ. 2002. № 23. ст. 2102.

15. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // СЗ РФ. 2003. № 28. ст. 2895.

16. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // СЗ РФ. 2004. № 32. ст. 3283.

17. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.).ст. 3448.

18. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (1 ч.).ст. 3451.

19. Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» // СЗ РФ. 1997. № 10. ст. 1127.

20. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // Российская газета. № 187. 28.09.2000.

в) программное обеспечение и интернет-ресурсы:

Операционная система Windows 7(или ниже) - MicrosoftOpenLicense Лицензия № 61984214, 61984216,61984217, 61984219, 61984213, 61984218, 61984215

Офисные приложения, MicrosoftOffice 2013(или ниже) – MicrosoftOpenLicense Лицензия № 61984042

8. Материально-техническое обеспечение дисциплины.

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются *лекции.*

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

Практические занятия проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на лекциях и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста по ИБ. *Практические занятия* проводятся по теоретическим и проблемным вопросам ИБ. Практическое занятие предполагает творческие дискуссии, активный обмен мнениями по поставленным *вопросам,* заслушивание и обсуждение докладов по предложенным преподавателем темам.

При проведении практического занятия преподаватель *выполняет, в основном,* функции ведущего - следит за регламентом времени, помогает уточнить формулировки, обобщает результаты дискуссии, подводит итог занятию в целом. При высоком уровне подготовки студенческой группы отдельные функции ведущего можно поручить одному из студентов. В

случае необходимости, преподаватель оказывает ему поддержку, а при подведении итогов - дает оценку работе ведущего.

Активная работа студента на практическом занятии учитывается при определении итоговой оценки его знаний по дисциплине на зачете.

Самостоятельная работа по дисциплине предполагает: выполнение студентами домашних заданий. Домашние задания являются, как правило, продолжением практических занятий и содействуют овладению практическими навыками по основным разделам дисциплины. Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, использование справочной литературы и др..

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Самостоятельная работа осуществляется индивидуально.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки специалистов **10.05.03 «Информационная безопасность автоматизированных систем».**

Программу составил: Ст. преподаватель Пашина А.Д.

Программа утверждена на заседании кафедры “Информационная безопасность” «29» августа 2019 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

Приложение

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.05.03«Информационная безопасность автоматизированных систем»

ОП (профиль): «Обеспечение информационной безопасности распределенных информационных систем»

Форма обучения: очная

Вид профессиональной деятельности: научно-исследовательская; проектно-конструкторская; контрольно-аналитическая; организационно-управленческая; эксплуатационная.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Организационное и правовое обеспечение информационной безопасности»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Домашние задания

Экзамен

Составитель: Ст. преподаватель Пашина А.Д.

Москва, 2019 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Организационное и правовое обеспечение информационной безопасности					
ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетенций**	**Форма оценочного средств**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				
ОПК – 6	Способностью применять нормативные правовые акты в профессиональной деятельности	**Знать:** - основные отечественные и зарубежные стандарты в области информационной безопасности. **Уметь:** Применять действующую законодательную базу в области обеспечения информационной безопасности. **Владеть:** навыками работы с нормативными правовыми актами.	лекции, самостоятельная работа, практические занятия	ДЗ, экзамен	**Базовый уровень:** способенприменять нормативные правовые акты в профессиональной деятельности **Повышенный уровень:** способенприменять нормативные правовые акты в профессиональной деятельности, свободно применяет полученные навыки в ситуациях повышенной сложности.

ОК-4	Способностью использовать основы правовых знаний в различных сферах деятельности	**владеть:** - навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности.	лекции, самостоятельная работа, практические занятия	ДЗ, экзамен	**Базовый уровень:** Способностью использовать основы правовых знаний в различных сферах деятельности **Повышенный уровень:** Способностью использовать основы правовых знаний в различных сферах деятельности, свободно применяет полученные навыки в ситуациях повышенной сложности

ПК-11	Способностью разрабатывать политику информационной безопасности автоматизированной системы	**знать:** - принципы формирования политики информационной безопасности	лекции, самостоятельная работа, практические занятия	ДЗ, экзамен	**Базовый уровень:** способенразрабатывать политику информационной безопасности автоматизированной системы **Повышенный уровень:** Способен разрабатывать политику информационной безопасности автоматизированной системы, свободно применяет полученные навыки в ситуациях повышенной сложности

Приложение 2

к рабочей программе

Оценочные средства для текущей аттестации

Примерный перечень вопросов для домашнего задания.

Домашнее задание 1.Характеристика каналов утечки информации и методов организационного противодействия этим каналам.

Организация охраны предприятий, обрабатывающих конфиденциальную информацию.

Организация пропускного режима на предприятии.

Домашнее задание 2.Обеспечение безопасности информации при чрезвычайных ситуациях.
Организация защиты информации при ведении переговоров.

Организация работ по защите информации в информационных системах и сетях.

Домашнее задание 3. Использование лицензирования и сертификации в целях защиты информации.
Организация режима секретности государственной тайны в РФ.

Виды информации ограниченного доступа и способы её правовой защиты.

Домашнее задание 4. Порядок введения режима конфиденциальности информации.
Роль закона "Об информации, информационных технологиях и о защите информации" в упорядочении отношений субъектов информационной сферы.

Правовые основы защиты коммерческой тайны.

Домашнее задание 5. Защита сведений, связанных с коммерческой деятельностью. Банковская тайна.

Органы государственного контроля за выполнением требований по защите информации ограниченного доступа.

Административно-правовая и дисциплинарная ответственность за утечку информации ограниченного доступа

Оценочные средства для промежуточной аттестации

Экзамен

Список вопросов для экзамена по дисциплине

1. Организационная и правовая защита информации как составные части системы комплексного противодействия информационным угрозам.
2. Структура и задачи органов власти и управления, отвечающих за организацию защиты информации в стране.
3. Основные цели и задачи организационного обеспечения информационной безопасности на предприятии.
4. Угрозы информационной безопасности. Виды угроз.
5. Утечка информации. Каналы утечки информации. Разглашение информации. Несанкционированный доступ.
6. Структура и содержание документа «Политика информационной безопасности предприятия».
7. Концепция информационной безопасности предприятия как составная часть «Политики информационной безопасности предприятия».
8. Служба информационной безопасности предприятия. Состав, задачи службы информационной безопасности предприятия.
9. Служба информационной безопасности предприятия. Состав, основные направления деятельности службы информационной безопасности предприятия.
10. Порядок засекречивания и рассекречивания сведений, составляющих информацию ограниченного доступа.
11. Порядок учета и хранения сведений, составляющих информацию ограниченного доступа.
12. Кадровая политика предприятия. Возможные источники пополнения предприятия кадрами для работы с конфиденциальной информацией.
13. Кадровая политика предприятия. Этапы подбора кадров для работы с конфиденциальной информацией.
14. Отражение вопросов информационной безопасности в трудовых договорах.
15. Организация доступа и допуска сотрудников к конфиденциальной информации.
16. Текущая работа с персоналом, допущенным к конфиденциальной информации. Дисциплинарная ответственность.
17. Основные направления деятельности при текущей работе с персоналом, допущенным к конфиденциальной информации.
18. Организация служебного расследования по фактам утраты конфиденциальной информации.
19. Организация охраны объектов информатизации. Составные элементы системы охраны.
20. Организация режима охраны объекта. Факторы, влияющие на выбор приёмов и средств охраны.
21. Организация внутриобъектового и пропускного режимов на объектах информатизации.
22. Атрибутивный и биометрический способы идентификации сотрудников. Их преимущества и недостатки.
23. Общие требования к помещениям и хранилищам, в которых ведутся закрытые работы и хранятся конфиденциальные документы.
24. Аттестация помещений, в которых обрабатывается конфиденциальная информация.
25. Организация защиты информации при взаимодействии со сторонними организациями. Отражение вопросов защиты информации при подготовке договоров о сотрудничестве.
26. Организация защиты информации при взаимодействии со сторонними организациями. Порядок отбора и подготовки информации к оглашению.
27. Контроль функционирования системы защиты информации. Формы контроля.
28. Аудит информационной безопасности.

29. Закон «Об информации информационных технологиях и о защите информации». Информация как объект правовых отношений.
30. Правовое определение понятий: «информация», «информационные технологии», «информационные системы» и «информационно-телекоммуникационные сети»
31. Закон «Об информации информационных технологиях и о защите информации».Обладатель информации.
32. Закон «Об информации информационных технологиях и о защите информации». Общедоступная информация.
33. Закон «Об информации информационных технологиях и о защите информации». Право на доступ к информации.
34. Закон «Об информации информационных технологиях и о защите информации». Ограничение доступа к информации.
35. Закон «Об информации информационных технологиях и о защите информации». Распространение информации или предоставление информации.
36. Закон «Об информации информационных технологиях и о защите информации». Защита информации.
37. Закон «Об информации информационных технологиях и о защите информации». Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.
38. Закон «О персональных данных». Согласие субъекта персональных данных на обработку его персональных данных.
39. Закон «О персональных данных». Меры по обеспечению безопасности персональных данных при их обработке.
40. Закон «О персональных данных». Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных.
41. Закон «О персональных данных». Принципы обработки персональных данных.
42. Перечень сведений, составляющих государственную тайну.
43. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию.
44. Закон «О государственной тайне». Ограничение прав собственности предприятий, учреждений, организаций и граждан Российской Федерации на информацию в связи с ее засекречиванием.
45. Допуск должностных лиц и граждан к государственной тайне.
46. Передача сведений, составляющих государственную тайну, в связи с выполнением совместных и других работ.
47. Условия прекращения допуска должностного лица или гражданина к государственной тайне.
48. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне.
49. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну.
50. Правовое определение понятий: «коммерческая тайна», «информация, составляющая коммерческую тайну», «обладатель информации, составляющей коммерческую тайну», «разглашение информации, составляющей коммерческую тайну».
51. Сведения, которые не могут составлять коммерческую тайну в соответствии с законом «О коммерческой тайне».
52. Правовое определение понятий: «доступ к информации, составляющей коммерческую тайну», «передача информации, составляющей коммерческую

тайну», «контрагент», «предоставление информации, составляющей коммерческую тайну».

53. Права обладателя информации, составляющей коммерческую тайну.
54. Закон «О коммерческой тайне». Охрана конфиденциальности информации.
55. Охрана конфиденциальности информации, составляющей коммерческую тайну, в рамках трудовых отношений.
56. Предоставление информации, составляющей коммерческую тайну. Охрана конфиденциальности информации при ее предоставлении

Пример билета

1. Предоставление информации, составляющей коммерческую тайну. Охрана конфиденциальности информации при ее предоставлении
2. Аудит информационной безопасности.

Структура и содержание дисциплины «Организационное и правовое обеспечение информационной безопасности»

по направлению подготовки

10.05.03 «Информационная безопасность автоматизированных систем»

(Специалитет)

Год приема – 2019

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб	СРС	КСР	К.Р.	К.П.	ДЗ	Реферат	К/р	Э	З
	Седьмой семестр														
1.1	Понятие «Организационная защита информации»	2	1-2	2											
1.2	Организационные источники и каналы утечки информации. Силы, средства и условия организационной защиты информации	2	2-3			2	4								
1.3	Порядок засекречивания и рассекречивания конфиденциальных сведений, документов и	2	3-4	2		**2**	4								

	изделий														
1.4	Подбор персонала на должности, связанные с работой с конфиденциальной информацией.	2	5			2	4				+				
1.5	Организация доступа и допуска к информации ограниченного доступа.	2	5	2		2	4								
1.6	Текущая работа с персоналом, обладающим конфиденциальной информацией	2	6	2			4								
1.7	Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.	2	6	2			4								
1.8	Организация охраны территории, зданий, помещений и персонала.	2	7	2		2	4								
1.9	Организация пропускного и внутриобъектового режимов	2	8-9	2		2	4								
1.10	Требования к помещениям и хранилищам в которых ведутся закрытые работы и хранятся конфиденциальные документы и изделия.	2	10	2		2	4								
1.11	Организация защиты информации при взаимодействии со сторонними организациями	2	10	2		2	4				+				
1.12	Контроль функционирования системы организационной защиты информации.	2	11	2		2	4								

1.13	Характеристика правоотношений в сфере защиты информации.	2	12	2		2									
1.14	Структура системы организационно-правового обеспечения информационной безопасности в России.	2	12	2		2	4				+				
1.15	Содержание основных нормативно-правовых актов, направленных на защиту информации ограниченного доступа.	2	13	2		2									
1.16	Правовой порядок установления и поддержание режима ограничения доступа к информации.	2	14	2			4								
1.17	Лицензирование и сертификация, как методы правового регулирования отношений в сфере защиты информации.	2	15	2		2	4				+				
1.18	Правовые последствия введения режима ограниченния доступа для субъектов защиты информации.	2	15			2	4								
1.19	Государственная система правовой защиты сведений, составляющих государственную тайну.	2	16	2		2									
1.20	Особенности правовой защиты сведений,	2	16			2	4								

	составляющих различные виды тайн.														
1.21	Правовая защита информации, составляющей интеллектуальную собственность.	2	17	2		2	4				+				
1.22	Правовое обеспечение безопасности информационных и телекоммуникационных систем.	2	17			2	4								
	Форма аттестации		18-20											**Э**	
	Всего часов по дисциплине В первом семестре			36		36	72								
	Всего часов по дисциплине			36		36	72								