

 ******

1. **Цели освоения дисциплины**

Целью дисциплины «Основы информационной безопасности» является понимание социальной значимости своей будущей профессии в соответствии с доктриной информационной безопасности Российской Федерации. Формирование у студентов навыков их практического применения в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем». Дисциплина «Основы информационной безопасности» рассматривает основные принципы и основные направления обеспечения информационной безопасности Российской Федерации.

1. **Место дисциплины в структуре ООП подготовки специалиста**

Дисциплина «Основы информационной безопасности» относится к базовой части образовательной программы по специальности 10.05.03 «Информационная безопасность автоматизированных систем».

Успешное усвоение материала предполагает знание обучающимися основных положений курса «Основы информационной безопасности».

Дисциплина является предшествующей для изучения дисциплин: «Организационно – правовое обеспечение информационной безопасности», «Информационная безопасность распределенных ИС», «Методы проектирования распределенных приложений» и др.

1. **Компетенции обучающегося, формируемые в результате освоения дисциплины и планируемые результаты обучения**

В результате освоения дисциплины «Основы информационной безопасности» обучающийся должен обладать следующими компетенциями:

| **Структурный элемент  компетенции** | | | | **Планируемые результаты обучения** |
| --- | --- | --- | --- | --- |
| **ОПК-6** способностью применять нормативные правовые акты в профессиональной деятельности | | | | |
| Знать | Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации.  Системы регулирования возникающих общественных отношений в информационной сферы.  Составляющие информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации.  Влияние информационной сферы на состояние политической, экономической, оборонной и других составляющих безопасности РФ. | | | |
| Уметь: | Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем.  Использовать инфраструктуру единого информационного пространства РФ в личных целях.  Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем. | | | |
| Владеть: | Методами разработки проектов нормативных документов, регламентирующих работу по защите информации.  Способами использования информационной инфраструктуры в интересах общественного развития.  Методами разработки проектов нормативных документов, регламентирующих работу по защите информации. | | | |
| **ПК-3** способностью проводить анализ защищенности автоматизированных систем | | | | |
| Знать: | | Основы методологии научных исследований.  Технические средства контроля эффективности мер защиты информации.  Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем  Классификацию современных компьютерных систем.  Современные способы использования компьютерных технологий для проведения исследований.  Технические средства контроля эффективности мер защиты информации.  Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. | | |
| Уметь: | | Пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет.  Анализировать основные узлы и устройства современных автоматизированных систем.  Пользоваться сетевыми информационными ресурсами для подбора необходимых современных компьютерных систем и правил работы в этих системах.  Эффективно использовать современные компьютерные технологии для изучения предмета исследования. | | |
| Владеть: | | Представлением о возможности использования информационных технологий для решения профессиональных задач.  Представлением использования информационных технологий для проведения исследовательской работы в профессиональной деятельности.  Навыками пользования библиотеками прикладных программ для проведения исследовательской работы в профессиональной деятельности.  Представлением о способах и методах анализа защищенности информационной инфраструктуры автоматизированной системы. | | |
| **ПК-6** способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности | | | | |
| Знать: | | | Основные информационные технологии, используемые в автоматизированных системах.  Сущность и понятие информационной безопасности и характеристику ее составляющих.  Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах. | |
| Уметь: | | | Пользоваться современной научно-технической информацией по рассматриваемым в рамках дисциплины проблемам и задачам.  Принимать участие в исследованиях и анализе современной научно-технической информации по информационной безопасности.  Анализировать современную научно-техническую информацию по информационной безопасности.  Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе | |
| Владеть: | | | Основными методами научного познания в области защиты информации.  Навыками участия в проведении исследовательских работ по информационной безопасности.  Профессиональной терминологией в области информационной безопасности.  Разрабатывать предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах | |
| **ПК-18** способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности | | | | |
| Знать: | | | Основные меры по защите информации в автоматизированных системах.  Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.  Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.  Принципы организации работы малых коллективов исполнителей. | |
| Уметь: | | | Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности.  Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.  Определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации. | |
| Владеть: | | | Профессиональной терминологией в области информационной безопасности.  Навыками участия в проведении исследовательских работ по информационной безопасности.  Методами синтеза структурных и функциональных схем защищенных автоматизированных систем. | |

1. **Структура и содержание дисциплины**

Общая трудоемкость дисциплины составляет 3 зачетных единицы 108 акад. часов, в том числе:

–контактная работа – 69,8 акад. часов:

–аудиторная – 68 акад. часов;

–внеаудиторная – 1,8 акад. часов

–самостоятельная работа – 38,2 акад. часов.

Форма аттестации – Зачет.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Раздел дисциплины** | | | **Аудиторная**  **контактная работа**  **(в акад. часах)** | | | **Вид самостоятельной работы** | **Формы текущего и промежуточного контроля успеваемости** | **Код и структурный элемент компетенции** |
| **Л** | **ПЗ** | **СР** |
| **Раздел 1**  **Место и роль информационной безопасности в системе национальной безопасности РФ.** | **Семестр** | **Тема 1.1.** Сущность и понятие информации. Понятие национальной безопасности. Основы государственной информационной политики. | **4** | **4** | **4** | Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к КТ. | **КТ-1** | ОПК-6 з |
| **4** | **Тема 1.2.**  Угрозы национальной безопасности страны во всех сферах деятельности государства все осуществляемые через информационную среду. | **4** | **4/ 2И** | **4** | ОПК-6 з |
| **Раздел 2**  **Классификация защищаемой информации и угроз информационной безопасности** | **4** | **Тема 2.1.** Классификация защищаемой информации по видам тайны и степеням конфиденциальности. | **4** | **4/ 2И** | **4** | Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР и ИДЗ. | **ИДЗ-1** | ОПК-6 зув  ПК-3 зув |
| **4** | **Тема 2.2.** Источники и классификация угроз информационной безопасности для объекта информатизации. | **4** | **4/ 2И** | **4** | ОПК-6 зув  ПК-3 зув |
| **Раздел 3**  **Способы обеспечения информационной безопасности автоматизированных систем.** | **4** | **Тема 3.1.** Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. | **6** | **6/ 4И** | **4** | Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР. | **АКР-1** | ПК-6 зув |
| **4** | **Тема 3.2.** Классификация средств и способов обеспечения информационной безопасности, принципы построения систем защиты информации. | **4** | **4/ 2И** | **4** | ПК-3 зув  ПК-6 зув |
| **Раздел 4** | **4** | **Тема 4.1.**  Анализ существующих методов и средств, применяемых для защиты информации. | **4** | **4/ 4И** | **5** | Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к ИДЗ. | **ИДЗ-2** | ПК-6 зув |
| **Методы формирования требований по защите информации.** | **4** | **Тема 4.2.** Разработка предложений по совершенствованию существующих методов и средств, применяемых для контроля и защиты информации и повышению их эффективности. | **4** | **4/ 4И** | **5** | ПК-18 зув |
|  | **4** | **Зачет** |  |  | **6** | Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к зачету. | **Зачет** | ПК-3 зув  ПК-6 зув  ПК-18 зув  ОПК-6 зув |
|  |  | **Итого** | **34** | **34/ 20И** | **38** |  |  |  |

Л – лекции, ПЗ – практические занятия, СР – самостоятельная работа, АКР – аудиторная контрольная работа, ИДЗ – индивидуальное задание, КТ – аудиторное компьютерное тестирование.

1. **Образовательные технологии**

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

1. **Традиционная технология**, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. Формы учебных занятий с использованием традиционных технологий:
   1. ***Вводная лекция*** – для целостного представления об учебном предмете и анализа учебно-методической литературы;
   2. ***Обзорные лекции*** – для систематизации научных знаний на высоком уровне с использованием ассоциативных связей в процессе представления и осмысления информации;
   3. ***Информационная лекция*** – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя);
   4. ***Семинар*** – беседа преподавателя и обучающихся, обсуждение заранее подготовленных сообщений по каждому вопросу плана занятия с единым для всех перечнем рекомендуемой обязательной и дополнительной литературы;
   5. ***Практическое занятие***, посвященное освоению конкретных умений и навыков по предложенному алгоритму;
   6. ***Лабораторная работа*** – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.
2. **Разделно-компетентностная технология**, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками домашних заданий, контрольных работ и тестированием по каждой теме содержания курса. Формы учебных занятий с использованием Разделно-компетентностной технологии:
   1. ***Кейс-методы*** – для овладения системой знаний и умений и творческого их использования в профессиональной деятельности и самообразовании; для квалифицированного и независимого решения профессиональных задач; для ориентации в многообразии учебных программ, пособий, литературы и выбора наиболее эффективных в применении к конкретной ситуации; для осуществления саморефлексии для дальнейшего профессионального, творческого роста и социализации личности.
3. **Интерактивные технологии –** организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе личностно значимого для них образовательного результата. Наряду со специализированными технологиями такого рода принцип интерактивности прослеживается в большинстве современных образовательных технологий. Интерактивность подразумевает субъект-субъектные отношения в ходе образовательного процесса и, как следствие, формирование саморазвивающейся информационно-ресурсной среды. Формы учебных занятий с использованием интерактивных технологий:
   1. ***Case-study*** – для анализа реальных проблемных ситуаций и поиска лучших вариантов решений, разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения проблемы.
   2. ***Методы IT*** – для применения компьютеров в процессе освоения дисциплины и доступа к ЭОР кафедры и Интернет-ресурсам.
   3. ***Лекция «обратной связи»*** – лекция–провокация (изложение материала с заранее запланированными ошибками), лекция-беседа, лекция-дискуссия, лекция-прессконференция.
   4. ***Семинар-дискуссия*** – коллективное обсуждение какого-либо спорного вопроса, проблемы, выявление мнений в группе (межгрупповой диалог, дискуссия как спор-диалог).
   5. ***Контекстное обучение*** – для мотивации обучающихся к усвоению знаний путем выявления связей между конкретным знанием и его применение. Овладев в рамках изучения дисциплины навыками обеспечения безопасности информации с помощью типовых программных средств, обучающийся приобретет способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности;
   6. ***Междисциплинарное обучение*** – для использования знаний из различных областей, их группировки и концентрации в контексте решаемой задачи. Для реализации данного метода обучения обучающимся выдаются задания по решения задач из другой предметной области.
4. **Технологии проблемного обучения** – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности обучающихся. Формы учебных занятий с использованием технологий проблемного обучения:
   1. ***Проблемная лекция*** – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала.
   2. ***Лекция «вдвоем» (бинарная лекция)*** – изложение материала в форме диалогического общения двух преподавателей (например, реконструкция диалога представителей различных научных школ, «ученого» и «практика» и т.п.).
   3. ***Практическое занятие в форме практикума*** – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от обучающегося применения как научно-теоретических знаний, так и практических навыков.
   4. ***Практическое занятие на основе кейс-метода*** – обучение в контексте моделируемой ситуации, воспроизводящей реальные условия научной, производственной, общественной деятельности. Обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации. разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения учебной проблемы.
5. **Игровые технологии** – организация образовательного процесса, основанная на реконструкции моделей поведения Формы учебных занятий с использованием предложенных сценарных условий. Формы учебных занятий с использованием игровых технологий:
   1. ***Учебная игра*** – форма воссоздания предметного и социального содержания будущей профессиональной деятельности специалиста, моделирования таких систем отношений, которые характерны для этой деятельности как целого.
   2. ***Деловая игра*** – моделирование различных ситуаций, связанных с выработкой и принятием совместных решений, обсуждением вопросов в режиме «мозгового штурма», реконструкцией функционального взаимодействия в коллективе и т.п.
   3. ***Ролевая игра*** – имитация или реконструкция моделей ролевого поведения в предложенных сценарных условиях.
6. **Технологии проектного обучения** – организация образовательного процесса в соответствии с алгоритмом поэтапного решения проблемной задачи или выполнения учебного задания. Проект предполагает совместную учебно-познавательную деятельность группы обучающихся, направленную на выработку концепции, установление целей и задач, формулировку ожидаемых результатов, определение принципов и методик решения поставленных задач, планирование хода работы, поиск доступных и оптимальных ресурсов, поэтапную реализацию плана работы, презентацию результатов работы, их осмысление и рефлексию. Основные типы проектов:
   1. ***Исследовательский проект*** – структура приближена к формату научного исследования (доказательство актуальности темы, определение научной проблемы, предмета и объекта исследования, целей и задач, методов, источников, выдвижение гипотезы, обобщение результатов, выводы, обозначение новых проблем).
   2. ***Творческий проект***, как правило, не имеет детально проработанной структуры; учебно-познавательная деятельность обучающихся осуществляется в рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия и т.п.).
   3. ***Информационный проект*** – учебно-познавательная деятельность с ярко выраженной эвристической направленностью (поиск, отбор и систематизация информации о каком-то объекте, ознакомление участников проекта с этой информацией, ее анализ и обобщение для презентации более широкой аудитории).
7. **Информационно-коммуникационные образовательные технологии** – организация образовательного процесса, основанная на применении специализированных программных сред и технических средств работы с информацией. Формы учебных занятий с использованием информационно-коммуникационных технологий:
   1. ***Лекция-визуализация*** – изложение содержания сопровождается презентацией (демонстрацией учебных материалов, представленных в различных знаковых системах, в т.ч. иллюстративных, графических, аудио- и видеоматериалов).
   2. ***Практическое занятие в форме презентации*** – представление результатов проектной или исследовательской деятельности с использованием специализированных программных сред.

**6. Учебно-методическое обеспечение самостоятельной работы обучающихся**

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для студента с использованием *методов IT* .

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде чтения литературы по соответствующему разделу с проработкой материала и выполнения домашних заданий с консультациями преподавателя, а так же с применением *кейс-технологий*.

**Контрольные вопросы и задания для проведения текущего контроля**

**Темы для ИДЗ:**

1. Стратегия развития информационного общества в России
2. Правовая охрана программ и данных. Защита информации.
3. Методы защиты информации
4. Системы защиты информации
5. Защита баз данных
6. Угрозы национальной безопасности страны в экономической сфере, осуществляемые через информационную среду.
7. Угрозы национальной безопасности страны в политической сфере, осуществляемые через информационную среду.
8. Угрозы национальной безопасности страны в военной сфере, осуществляемые через информационную среду.
9. Угрозы национальной безопасности страны в духовной сфере, осуществляемые через информационную среду.

**Задания и вопросы по разделам**

**Раздел 1-4**

Вопросы:

1. Понятие информационной безопасности государства.
2. Источники угроз информационной безопасности для объекта информатизации.
3. Классификация угроз информационной безопасности для объекта информатизации.
4. Требования защиты информации.
5. Угрозы национальной безопасности страны в экономической сфере, осуществляемые через информационную среду.
6. Угрозы национальной безопасности страны в политической сфере, осуществляемые через информационную среду.
7. Угрозы национальной безопасности страны в военной сфере, осуществляемые через информационную среду.
8. Угрозы национальной безопасности страны в духовной сфере, осуществляемые через информационную среду.
9. Классификация защищаемой информации по видам тайны.
10. Классификация защищаемой информации по степеням конфиденциальности.

**7. Оценочные средства для проведения промежуточной аттестации**

**а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:**

| Структурный элемент  компетенции | Планируемые результаты обучения | Оценочные средства |
| --- | --- | --- |
| **ОПК-6** способностью применять нормативные правовые акты в профессиональной деятельности | | |
| Знать | Нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации.  Системы регулирования возникающих общественных отношений в информационной сферы.  Составляющие информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации.  Влияние информационной сферы на состояние политической, экономической, оборонной и других составляющих безопасности РФ. | Вопросы для зачета:  1. Понятие информационной безопасности государства.  2. Источники угроз информационной безопасности для объекта информатизации.  3. Классификация угроз информационной безопасности для объекта информатизации.  4. Требования защиты информации.  5. Стратегия развития информационного общества в России. |
| Уметь | Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем.  Использовать инфраструктуру единого информационного пространства РФ в личных целях.  Определять структуру системы защиты информации автоматизированной системы в соответствии с требованиями нормативных правовых документов в области защиты информации автоматизированных систем. | 1. Найти перечень нормативно-правовых документов в области защиты информации автоматизированных систем.  2. Провести анализ нормативно-правовых документов в области защиты информации автоматизированных систем. |
| Владеть | Методами разработки проектов нормативных документов, регламентирующих работу по защите информации.  Способами использования информационной инфраструктуры в интересах общественного развития.  Методами разработки проектов нормативных документов, регламентирующих работу по защите информации | 1. На основе проведенного анализа нормативно-правовых документов в области защиты информации автоматизированных систем найти слабые места в системе управления безопасностью информации в автоматизированных системах на современном уровне развития общества. |
| **ПК-3** способностью проводить анализ защищенности автоматизированных систем | | |
| Знать | Основы методологии научных исследований.  Технические средства контроля эффективности мер защиты информации.  Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.  Классификацию современных компьютерных систем.  Современные способы использования компьютерных технологий для проведения исследований.  Технические средства контроля эффективности мер защиты информации.  Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем. | 1. Понятие информационной безопасности государства.  2. Источники угроз информационной безопасности для объекта информатизации.  3. Классификация угроз информационной безопасности для объекта информатизации.  4. Требования защиты информации. |
| Уметь | Пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет.  Анализировать основные узлы и устройства современных автоматизированных систем.  Пользоваться сетевыми информационными ресурсами для подбора необходимых современных компьютерных систем и правил работы в этих системах.  Эффективно использовать современные компьютерные технологии для изучения предмета исследования. | 1. Определить угрозы национальной безопасности страны в экономической сфере, осуществляемые через информационную среду.  2. Определить угрозы национальной безопасности страны в политической сфере, осуществляемые через информационную среду. |
| Владеть | Представлением о возможности использования информационных технологий для решения профессиональных задач.  Представлением использования информационных технологий для проведения исследовательской работы в профессиональной деятельности.  Навыками пользования библиотеками прикладных программ для проведения исследовательской работы в профессиональной деятельности.  Представлением о способах и методах анализа защищенности информационной инфраструктуры автоматизированной системы. | 1. Составить перечень программного обеспечения, позволяющего автоматизировать работу в области ИБ.  2. Составить перечень сертифицированных средств ЗИ от НСД.  3. Составить перечень средств СКЗИ. |
| **ПК-6** способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности | | |
| Знать | Основные информационные технологии, используемые в автоматизированных системах.  Сущность и понятие информационной безопасности и характеристику ее составляющих.  Основные проблемы обеспечения безопасности информации в компьютерных и автоматизированных системах. | Вопросы для зачета  8. Угрозы национальной безопасности страны в духовной сфере, осуществляемые через информационную среду.  9. Классификация защищаемой информации по видам тайны.  10. Классификация защищаемой информации по степеням конфиденциальности.  11. Стратегия развития информационного общества в России. |
| Уметь | Пользоваться современной научно-технической информацией по рассматриваемым в рамках дисциплины проблемам и задачам.  Принимать участие в исследованиях и анализе современной научно-технической информации по информационной безопасности.  Анализировать современную научно-техническую информацию по информационной безопасности.  Определять методы управления доступом, типы доступа и правила разграничения доступа к объектам доступа, подлежащим реализации в автоматизированной системе | 1. Определить угрозы национальной безопасности страны в духовной сфере, осуществляемые через информационную среду.  2. Определить угрозы национальной безопасности страны в военной сфере, осуществляемые через информационную среду. |
| Владеть | Основными методами научного познания в области защиты информации.  Навыками участия в проведении исследовательских работ по информационной безопасности.  Профессиональной терминологией в области информационной безопасности.  Разрабатывать предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах | 1. На основе проведенного анализа нормативно-правовых документов в области защиты информации автоматизированных систем разработать предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах на современном уровне развития общества. |
| **ПК-18** способностью организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности | | |
| Знать | Основные меры по защите информации в автоматизированных системах.  Принципы организации и структура систем защиты информации программного обеспечения автоматизированных систем.  Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.  Принципы организации работы малых коллективов исполнителей. | Вопросы для зачета  4. Требования защиты информации.  5. Угрозы национальной безопасности страны в экономической сфере, осуществляемые через информационную среду.  6. Угрозы национальной безопасности страны в политической сфере, осуществляемые через информационную среду.  7. Угрозы национальной безопасности страны в военной сфере, осуществляемые через информационную среду. |
| Уметь | Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности.  Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.  Определять виды и типы средств защиты информации, обеспечивающих реализацию технических мер защиты информации. | 1. Классифицировать защищаемую информацию по видам тайны.  2. Классифицировать защищаемую информацию по степеням конфиденциальности.  3. Составить перечень средств ЗИ для обеспечения защиты от утечки по акустическому каналу. |
| Владеть | Профессиональной терминологией в области информационной безопасности.  Навыками участия в проведении исследовательских работ по информационной безопасности.  Методами синтеза структурных и функциональных схем защищенных автоматизированных систем. | 1. Составить глоссарий по терминологии в области информационной безопасности.  2. Исследовать угрозы национальной безопасности страны в военной сфере.  3. Исследовать стратегия развития информационного общества в России. |

**б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:**

**Показатели и критерии оценивания зачета:**

**«зачтено»** – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации, навыки решения типовых задач.

**«не зачтено»** – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

**8. Учебно-методическое и информационное обеспечение дисциплины**

***а) Основная литература:***

1. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с.- Режим доступа: <http://znanium.com/bookread.php?book=405000> . - Загл. с экрана. - ISBN 978-5-369-01178-2.
   * 1. Информационная безопасность и защита информации: [Электронный ресурс]: учеб. пособие / Баранова Е.К., Бабаш А.В. - 3-е изд., перераб. и доп. - М. : РИОР: ИНФРА-М, 2017. - 322 с. - Режим доступа: <http://znanium.com/bookread2.php?book=763644>. - Загл. с экрана. – ISBN 978-5-369-01450-9.
     2. Информационная безопасность и защита информации: [Электронный ресурс]: Учебное пособие / Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 336 с. - Режим доступа:<http://znanium.com/bookread2.php?book=957144>. - Загл. с экрана. – ISBN 978-5-369-01761-6.

***б) Дополнительная литература:***

1. Ажмухамедов И.М. Основы организационно-правового обеспечения информационной безопасности: [Электронный ресурс]: учеб. пособие / И.М. Ажмухамедов, О.М. Князева. - СПб.: Издательский центр «Интермедия», 2017. – 264 с. - Режим доступа: <https://ibooks.ru/product.php?productid=356930> - Загл. с экрана. - ISBN: 978-5-4383-0160-8.

2. Унижаев Н.В. Информационно-аналитическое обеспечение безопасности организации: [Электронный ресурс]: учеб. пособие / Н.В. Унижаев - СПб.: Издательский центр «Интермедия», 2018. – 408с. - Режим доступа: <https://ibooks.ru/product.php?productid=356934>. - Загл. с экрана. - ISBN: 978-5-4383-0158-5.

3. Царегородцев А.В. Методы и средства защиты информации в государственном управлении: [Электронный ресурс]: учеб. пособие / А.В. Царегородцев, М.М. Тараскин. - Москва: Проспект, 2017. - 208 с. - Режим доступа: <https://ibooks.ru/product.php?productid=356008> . - Загл. с экрана. - ISBN: 978-5-392-20353-6.

4. Баркалов С.А. Информационная безопасность при управлении техническими системами: [Электронный ресурс]: учеб. пособие /, О.М. Барсуков, В.Е. Белоусов, К.В. Славнов. – СПб.: ИЦ «Интермедия», 2016. – 528с.: илл. - 208 с. - Режим доступа: <https://ibooks.ru/product.php?productid=356935> - Загл. с экрана. - ISBN: 978-5-4383-0133-2.

***с)* Программное обеспечение** и **Интернет-ресурсы:**

* + 1. Журнал Information Security. Информационная безопасность [Электронный ресурс]: периодич. интернет-изд. – Режим доступа: <http://www.itsec.ru/articles2/allpubliks> – Загл. с экрана. Яз. рус.
    2. Журнал «Безопасность информационных технологий» [Электронный ресурс]: периодич. интернет-изд. – Режим доступа: <http://www.pvti.ru/articles_14.htm> . – Загл. с экрана. Яз. рус.
    3. Журнал «Вопросы кибербезопасности» [Электронный ресурс]: периодич. интернет-изд. – Режим доступа: http://cyberrus.com/ – Загл. с экрана. Яз. рус.
    4. «Журнал сетевых решений LAN»: [Электронный ресурс]: периодич. интернет-изд. URL: http://www.osp.ru/lan/ Издательство "Открытые системы. СУБД". – Режим доступа: <http://www.osp.ru/os/> – Загл. с экрана. Яз. рус.
    5. Государственная публичная научно-техническая библиотека России [Электронный ресурс] / – Режим доступа: [http://www.gpntb.ru](http://www.gpntb.ru/) , свободный.– Загл. с экрана. Яз. рус.
    6. Российская национальная библиотека. [Электронный ресурс] / – Режим доступа: <http://www.nlr.ru> . Яз. рус.
    7. Безопасник [Электронный ресурс]. – Режим доступа: <http://www.безопасник.рф> .– Загл. с экрана. Яз. рус.
    8. Компьтерра: все новости про компьютеры, железо, новые технологии, информационные технологии [Электронный ресурс]. – Периодическое электронное Интернет-издание – Режим доступа: <http://www.computerra.ru/> – Загл. с экрана. Яз. рус.
    9. ФСТЭК России [Электронный ресурс] – Режим доступа: <http://fstec.ru/>.– Загл. с экрана. Яз. рус.

**9. Материально-техническое обеспечение дисциплины**

Материально-техническое обеспечение дисциплины включает:

| Тип и название аудитории | Оснащение аудитории |
| --- | --- |
| *Лекционные аудитории* (ауд. 2124, ауд. 226, ауд. 365, ауд. 388 и т.д.) | Мультимедийные средства хранения, передачи и представления информации |
| *Компьютерные классы* (ауд. 372, 133, 247 и т.д.) | Персональные компьютеры с ПО:  Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021);  Пакет MS Office 2007 (Microsoft Open License 42649837, бессрочная);  Выход в Интернет и доступ в электронную информационно-образовательную среду университета. |
| *Аудитории для самостоятельной работы (ауд. 132а): компьютерные классы; читальные залы библиотеки.* | Персональные компьютеры с ПО:  Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021);  Пакет MS Office 2007 (Microsoft Open License 42649837, бессрочная);  Выход в Интернет и доступ в электронную информационно-образовательную среду университета. |