

***Лист регистрации изменений и дополнений***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Раздел РПД  (модуля) | Краткое содержание изменения/дополнения | Дата, № протокола заседания кафедры | Подпись зав. кафедрой |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. **Цели освоения дисциплины**

Целью дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» является формирование профессиональных навыков администрирования подсистем информационной безопасности автоматизированной системы и подготовка к деятельности, связанной с эксплуатацией и обслуживанием современных программно-аппаратных СЗИ в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» рассматривает базовые теоретические понятия, лежащие в основе программно-аппаратной защиты информации.

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

Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» входит в цикл дисциплин Б1.Б.32 образовательной программы по специальности 10.05.03 Информационная безопасность автоматизированных систем.

Успешное усвоение материала предполагает знание обучающимися основных положений курсов «Организация ЭВМ и вычислительных систем», «Введение в специальность», «Информатика», «Основы радиотехники», «Теория информации», «Основы информационной безопасности», «Технологии и методы программирования».

Дисциплина является предшествующей для изучения дисциплин: «Управление информационной безопасностью», «Разработка и эксплуатация защищенных автоматизированных систем», «Информационная безопасность распределенных информационных систем».

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

В результате освоения дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» обучающийся должен обладать следующими компетенциями:

| **Структурный элемент  компетенции** | | | **Планируемые результаты обучения** |
| --- | --- | --- | --- |
| ОПК-8 - способностью к освоению новых образцов программных, технических средств и информационных технологий. | | | |
| *Знать:* | *Классификацию современных программных и программно-аппаратных СЗИ.*  *Состав, назначение функциональных компонентов и программного обеспечения программных и программно-аппаратных средств ЗИ.*  *Типовые структуры и принципы организации программных и программно-аппаратных СЗИ.* | | |
| *Уметь:* | *Осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области программных и программно-аппаратных средств ЗИ и систем с применением современных информационных технологий.*  *Основные принципы работы всех подсистем системы ИБ АС.* | | |
| *Владеть:* | *Навыками работы с подсистемами системы информационной безопасности автоматизированной системы.*  *Навыками администрирования системы ИБ АС.* | | |
| **ПК-10 *-*** способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности***.*** | | | |
| *Знать:* | | *Способы и средства защиты информации с использованием программно-аппаратных средств обеспечения ИБ.*  *Способы контрольных проверок работоспособности и эффективности применяемых программно-аппаратных СЗИ.* | |
| *Уметь:* | | *Исследовать эффективность контрольных проверок работоспособности применяемых программно-аппаратных средств защиты информации.*  *Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей ИБ АС.* | |
| *Владеть:* | | *Навыками анализа основных характеристик и возможностей телекоммуникационных систем по передаче информации.*  *Навыками использования программно-аппаратных средств обеспечения ИБ АС.*  *Навыками анализа программных, архитектурно-технических и схемотехнических решении компонентов АС с целью выявления потенциальных уязвимостей ИБ АС.* | |
| **ПК-14 -** способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации**.** | | | |
| *Знать:* | | *Виды программных и программно-аппаратных средств защиты информации.*  *Принципы администрирования системы ИБ АС.*  *Способы контрольных проверок работоспособности и эффективности применяемых программных и программно-аппаратных СЗИ.* | |
| *Уметь:* | | *Самостоятельно настраивать программные и программно-аппаратные средства обеспечения ИБ.*  *Исследовать эффективность контрольных проверок работоспособности применяемых программных и программно-аппаратных СЗИ.*  *Применять программные и программно-аппаратные средства обеспечения ИБ.* | |
| *Владеть:* | | *Техникой настройки программных и программно-аппаратных средств обеспечения ИБ.*  *Навыками использования программных и программно-аппаратных средств обеспечения ИБ АС.*  *Навыками анализа архитектурно-технических и схемотехнических решений компонентов АС с целью выявления потенциальных уязвимостей ИБ АС.* | |

1. **Структура и содержание дисциплины**

*Общая трудоемкость дисциплины составляет 5 зачетных единицы 180 акад. часов, в том числе:*

– контактная работа – 89 акад. часов:

– аудиторная – 85 акад. часов;

– внеаудиторная – 4 акад. часов;

– самостоятельная работа – 55,3 акад. часов;

– подготовка к экзамену – 35,7 акад. часа.

*Форма аттестации* – Экзамен.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Раздел дисциплины** | | | **Аудиторная**  **контактная работа**  **(в акад. часах)** | | | **Вид самостоятельной работы** | **Формы текущего и промежуточного контроля успеваемости** | **Код и структурный элемент компетенции** |
| **Л** | **ЛЗ** | **СР** |
| **Раздел 1**  **Общие положения защиты информации программно-аппаратными средствами.** | **Семестр** | **Тема 1.1.** Предмет и содержание дисциплины. Принципы работы систем обработки и передачи информации. | **2** | **1/ 1И** | **1** | Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к КТ. | **КТ-1** | ОПК-8 з |
| **4** | **Тема 1.2.** Задачи и методы защиты информации программно-аппаратными средствами. | **2** | **1/ 1И** | **1** |
| **Раздел 2**  **Задачи и методы защиты информации от НСД.** | **4** | **Тема 2.1.** Применение СЗИ от НСД для организации защищенных компьютерных систем. | **4** | **3/ 2И** | **3** | Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР и ИДЗ. | **ИДЗ-1** | ОПК-8 зув  ПК-14 зув  ПК-10 зув |
| **Тема 2.2.** Электронные ключи и идентификаторы. | **2** | **4/ 2И** | **4** |
| **Раздел 3**  **СЗИ от НСД «СТРАЖ NT».** | **4** | **Тема 3.1.** Механизмы системы защиты СЗИ «СТРАЖ NT». Администрирование СЗИ. Аварийное снятие и восстановление системы защиты. | **8** | **15/ 7И** | **15** | Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к АКР. | **АКР-1** | ПК-14 зув  ПК-10 зув |
| **Тема 3.2.** Редактирование параметров системного аудита. Установка параметров целостности. Назначение грифа. Контроль устройств. | **8** | **10/ 5И** | **10** |
| **Раздел 4**  **Обеспечение разграничения и контроля доступа пользователей различными способами.** | **4** | **Тема 4.1.** Обеспечение безопасности доступа к данным и приложениям ИС на основе продуктов MicroSoft, Oracle и Aladdin. | **4** | **12/ 8И** | **15** | Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к ИДЗ. | **ИДЗ-2** | ПК-10 зув  ПК-14 зув |
| **Тема 4.2** Обеспечение разграничения и контроля доступа пользователей к техническим средствам вычислительной сети, на которых будет обрабатываться информация с использованием изделий семейства АПМДЗ «КРИПТОН-ЗАМОК». | **4** | **5/ 4И** | **6,3** |
|  | **4** | **Экзамен** |  |  | **35,7** | Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к экзамену. | **Экзамен** | ПК-10 зув  ПК-14 зув  ОПК-8 зув |
|  |  | **Итого по курсу** | **34** | **51/ 30И** | **55,3+35,7** |  | **Экзамен** | **180** |

Л – лекции, ПЗ – практические занятия, ЛР – лабораторные занятия, СР – самостоятельная работа, АКР – аудиторная контрольная работа, ИДЗ – индивидуальное задание, КТ – контрольное 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*.

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

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде докладов и выполнения индивидуальных заданий, которые определяет преподаватель для обучающегося.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде чтения литературы по соответствующему разделу с проработкой материала и выполнения домашних заданий с консультациями преподавателя.

**Тема 1-4**

**Вопросы:**

1. Разновидности ключей Rutoken.
2. Отличия ключей eToken от Rutoken.
3. Особенности ключей Guardant.
4. Методы защиты информации от НСД.
5. Обеспечение разграничения и контроля доступа пользователей к техническим средствам вычислительной сети на примере АПМДЗ «КРИПТОН-ЗАМОК».
6. Предмет и задачи программно-аппаратной защиты информации.
7. Идентификация и аутентификация пользователя.
8. Типовые схемы идентификации и аутентификации пользователя.
9. Управление доступом к информации в КС.
10. Основные механизмы систем защиты информации в ИС на примере СЗИ «Страж NT».
11. Обеспечение безопасности доступа к данным и приложениям ИС на основе продуктов MicroSoft, Oracle и Aladdin. Сравнительный анализ.
12. Обеспечение целостности и доступности информации в КС.

**Задания:**

1. В СЗИ «Страж NT» создать пользователей user1 и user2. Присвоить пользователю user1 пароль, назначить допуск «Сов.секретно» и сформировать идентификатор типа Guardant ID. Не присваивать пользователю user2 пароль, назначить допуск «Секретно» и сформировать идентификатор типа ruToken. Сформировать ЗПС. Настроить управление защитными атрибутами ресурсов. Продемонстрировать различия в работе этих двух пользователей.
2. В СЗИ «Страж NT» создать иерархию ресурсов, назначить им разные дискреционные списки контроля доступа, назначить им разные грифы. Продемонстрировать различия в работе пользователей с различными правами доступа при осуществлении попытки доступа к созданным ресурсам.
3. В СЗИ «Страж NT» зарегистрировать несколько внешних носителей информации, настроить права доступа к ним, отредактировать политику доступа к ним по умолчанию. Затем необходимо настроить политику использования пользователями групп устройств. Продемонстрировать различия в работе зарегистрированных внешних носителей информации.
4. В СЗИ «Страж NT» на документы, расположенные в КС, установить контроль целостности, а также настроить дополнительный аудит. Осуществить пользователями с различными правами доступа попытки доступа к документам. Продемонстрировать журнал событий, отфильтровать события и заархивировать его.
5. В СЗИ «Страж NT» настроить приложение для работы с грифованными ресурсами, исходя из записей аудита в журнале событий. Продемонстрировать различия работы с ресурсами, имеющими различные грифы. Создать шаблон настройки приложения для использования грифованных носителей и применить его для всех пользователей.
6. Провести тестирование СЗИ «Страж NT». Осуществить переидентификацию пользователей без перезагрузки операционной системы. Произвести маркировку документов и продемонстрировать различия печати нескольких документов с разными грифами. Продемонстрировать блокировку и разблокировку системы.
7. Произвести аварийное снятие системы защиты. Затем восстановить подсистему идентификации и работоспособность основных служб СЗИ «Страж NT».
8. **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-8 - способностью к освоению новых образцов программных, технических средств и информационных технологий. | | |
| Знать | *Классификацию современных программных и программно-аппаратных СЗИ.*  *Состав, назначение функциональных компонентов и программного обеспечения программных и программно-аппаратных средств ЗИ.*  *Типовые структуры и принципы организации программных и программно-аппаратных СЗИ.* | Вопросы к экзамену:  1. Разновидности ключей Rutoken.  2. Отличия ключей eToken от Rutoken.  3. Особенности ключей Guardant.  4. Методы защиты информации от НСД.  5. Классификация программных и программно-аппаратных СЗИ. |
| Уметь | *Осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области программных и программно-аппаратных средств ЗИ и систем с применением современных информационных технологий.*  *Основные принципы работы всех подсистем системы ИБ АС.* | В СЗИ «Страж NT» создать пользователей user1 и user2. Присвоить пользователю user1 пароль, назначить допуск «Сов.секретно» и сформировать идентификатор типа Guardant ID. Не присваивать пользователю user2 пароль, назначить допуск «Секретно» и сформировать идентификатор типа ruToken. Сформировать ЗПС. Настроить управление защитными атрибутами ресурсов. Продемонстрировать различия в работе этих двух пользователей. |
| Владеть | *Навыками работы с подсистемами системы информационной безопасности автоматизированной системы.*  *Навыками администрирования системы ИБ АС.* | В СЗИ «Страж NT» создать иерархию ресурсов, назначить им разные дискреционные списки контроля доступа, назначить им разные грифы. Продемонстрировать различия в работе пользователей с различными правами доступа при осуществлении попытки доступа к созданным ресурсам. |
| **ПК-10 *-*** способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности***.*** | | |
| Знать | *Способы и средства защиты информации с использованием программно-аппаратных средств обеспечения ИБ.*  *Способы контрольных проверок работоспособности и эффективности применяемых программно-аппаратных СЗИ.* | Вопросы к экзамену:  1. Подсистемы СЗИ автоматизированной системы.  2. Концепция MBR и GPT.  3. Обеспечение безопасности доступа к данным и приложениям ИС на основе продуктов MicroSoft, Oracle и Aladdin. Сравнительный анализ.  4. Обеспечение целостности и доступности информации в КС. |
| Уметь | *Исследовать эффективность контрольных проверок работоспособности применяемых программно-аппаратных средств защиты информации.*  *Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей ИБ АС.* | В СЗИ «Страж NT» зарегистрировать несколько внешних носителей информации, настроить права доступа к ним, отредактировать политику доступа к ним по умолчанию. Затем необходимо настроить политику использования пользователями групп устройств. Продемонстрировать различия в работе зарегистрированных внешних носителей информации. |
| Владеть | *Способы и средства защиты информации с использованием программно-аппаратных средств обеспечения ИБ.*  *Способы контрольных проверок работоспособности и эффективности применяемых программно-аппаратных СЗИ.* | В СЗИ «Страж NT» на документы, расположенные в КС, установить контроль целостности, а также настроить дополнительный аудит. Осуществить пользователями с различными правами доступа попытки доступа к документам. Продемонстрировать журнал событий, отфильтровать события и заархивировать его. |
| **ПК-14 -** способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации**.** | | |
| Знать | *Виды программных и программно-аппаратных средств защиты информации.*  *Принципы администрирования системы ИБ АС.*  *Способы контрольных проверок работоспособности и эффективности применяемых программных и программно-аппаратных СЗИ.* | Вопросы к экзамену:  1. Обеспечение разграничения и контроля доступа пользователей к техническим средствам вычислительной сети на примере АПМДЗ «КРИПТОН-ЗАМОК».  2. Предмет и задачи программно-аппаратной защиты информации.  3. Идентификация и аутентификация пользователя.  4. Типовые схемы идентификации и аутентификации пользователя.  5. Управление доступом к информации в КС.  6. Основные механизмы систем защиты информации в ИС на примере СЗИ «Страж NT». |
| Уметь | *Самостоятельно настраивать программные и программно-аппаратные средства обеспечения ИБ.*  *Исследовать эффективность контрольных проверок работоспособности применяемых программных и программно-аппаратных СЗИ.*  *Применять программные и программно-аппаратные средства обеспечения ИБ.* | В СЗИ «Страж NT» настроить приложение для работы с грифованными ресурсами, исходя из записей аудита в журнале событий. Продемонстрировать различия работы с ресурсами, имеющими различные грифы. Создать шаблон настройки приложения для использования грифованных носителей и применить его для всех пользователей. |
| Владеть | *Техникой настройки программных и программно-аппаратных средств обеспечения ИБ.*  *Навыками использования программных и программно-аппаратных средств обеспечения ИБ АС.*  *Навыками анализа архитектурно-технических и схемотехнических решений компонентов АС с целью выявления потенциальных уязвимостей ИБ АС.* | Провести тестирование СЗИ «Страж NT». Осуществить переидентификацию пользователей без перезагрузки операционной системы. Произвести маркировку документов и продемонстрировать различия печати нескольких документов с разными грифами. Продемонстрировать блокировку и разблокировку системы.  Произвести аварийное снятие системы защиты. Затем восстановить подсистему идентификации и работоспособность основных служб СЗИ «Страж NT». |

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

**Показатели и критерии оценивания экзамена:**

– на оценку **«отлично»** – обучающийся должен показать высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку **«хорошо»** – обучающийся должен показать средний уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач;

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

– на оценку **«неудовлетворительно»** – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать навыки решения типовых задач.

1. **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.
    2. Программно-аппаратная защита информации [Электронный ресурс]: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - 352 с.: ил.; - (Высшее образование). - Режим доступа: <http://znanium.com/bookread.php?book=169345> - ISBN 978-5-91134-353-8.

***б) Дополнительная литература:***

* + 1. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс]. - М.: ДМК Пресс, 2014. — 702 с. Режим доступа: <http://e.lanbook.com/view/book/50578> - Загл. с экрана. – ISBN 978-5-94074-768-0.
    2. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс]. - М.: ДМК Пресс, 2012. - 474 с. - Режим доступа: <http://e.lanbook.com/view/book/39990/> - Загл. с экрана. – ISBN 978-5-94074-647-8.
    3. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс]. - М.: ДМК Пресс, 2012. - 592 с. - Режим доступа: <http://e.lanbook.com/view/book/3032/> - Загл. с экрана. – ISBN 978-5-94074-637-9.
    4. Информационная безопасность и защита информации [Текст]: учеб.пособ. / Ю. Ю. Громов, В. О. Драчёв, О. Г. Иванова, Н. Г. Шахов. - Старый Оскол: ТНТ, 2010.

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

* + 1. Журнал Information Security. Информационная безопасность: периодич. интернет-изд. URL: <http://www.itsec.ru/articles2/allpubliks> – Загл. с экрана. Яз. рус.
    2. Журнал «Безопасность информационных технологий» : периодич. интернет-изд. URL: <http://www.pvti.ru/articles_14.htm> – Загл. с экрана. Яз. рус.
    3. Журнал «Вопросы кибербезопасности»: периодич. интернет-изд. URL: http://cyberrus.com/ – Загл. с экрана. Яз. рус.
    4. «Журнал сетевых решений LAN»: периодич. интернет-изд. URL: http://www.osp.ru/lan/ Издательство "Открытые системы. СУБД".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>, свободный.– Загл. с экрана. Яз. рус.
    6. Российская национальная библиотека. [Электронный ресурс] / –URL: <http://www.nlr.ru>. Яз. рус.
    7. Безопасник [Электронный ресурс] – Режим доступа: <http://www.безопасник.рф> .– Загл. с экрана. Яз. рус.
    8. Компьютерра: 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

| Тип и название аудитории | Оснащение аудитории |
| --- | --- |
| Компьютерный класс (ауд. 372, ауд. 245, ауд. 247, ауд. 144, ауд. 142 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 (Microsoft Open License 42649837, бессрочная);  Выход в Интернет и доступ в электронную информационно-образовательную среду университета. |
| Лаборатория программно-аппаратных средств защиты информации, ауд. 2124 | Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021).  СЗИ от НСД Страж NT 3.0 № лицензии: D1B4D8C0F28854B0, бессрочная;  СЗИ от НСД Страж NT 3.0 № лицензии: 49F19FCF20457E46, бессрочная;  СЗИ от НСД Страж NT 3.0 № лицензии: B0CE6203861DE71A, бессрочная;  СЗИ от НСД Страж NT 3.0 № лицензии: 3DDCF2F25EB5446D, бессрочная;  СЗИ от НСД Страж NT 3.0 № лицензии: 0F984E80A43783D3, бессрочная;  СЗИ от НСД Страж NT 3.0 № лицензии: Е5593458ВВ84ВВ40, бессрочная;  СЗИ от НСД Страж NT 3.0 № лицензии: FEFFCC97CAE0DCF5, бессрочная;  СЗИ от НСД Страж NT 3.0 № лицензии: 58PE4EEF00376D64, бессрочная;  СЗИ от НСД Страж NT 3.0 № лицензии: E6F42E5B5704A2D7, бессрочная;  СЗИ от НСД Страж NT 3.0 N° лицензии: 42D08B0C46D41EA3, бессрочная;  СЗИ от НСД Страж NT 3.0 N° лицензии: 14АВ5ЕВ9СС9С3790, бессрочная;  СЗИ от Нед Страж NT 3.0 № лицензии: D6125FCAB3A84B9F, бессрочная. |
| Лаборатория радиомониторинга и контроля утечек информации, ауд. 226 | КРИПТОН-ЗАМОК/У (АПМДЗ-У, М-526 Б); |
| 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. |

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ПрООП ВО для специальности *10.05.03* *Информационная безопасность автоматизированных систем. Специализация «Обеспечение информационной безопасности распределенных информационных систем».*