МИНОБРНАУКИ РОССИИ

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

Кафедра радиоэлектроники и защиты информации

Авторы-составители: **Лесникова Дарья Сергеевна**
Лунегов Игорь Владимирович

Рабочая программа дисциплины

АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Код УМК 81657

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

Пермь, 2020

1. Наименование дисциплины

Аппаратно-программные средства обеспечения информационной безопасности

2. Место дисциплины в структуре образовательной программы

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

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

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Аппаратно-программные средства обеспечения информационной безопасности** у обучающегося должны быть сформированы следующие компетенции:

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

ОПК.4 готовность к участию в проведении научных исследований

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

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

ПК.13 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы

ПК.14 способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы

ПК.15 способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации

ПК.16 способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем

ПК.23 способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности

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

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

ПК.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем

4. Объем и содержание дисциплины

Направления подготовки	10.05.03 Информационная безопасность автоматизированных систем (направленность: Безопасность открытых информационных систем)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	10
Объем дисциплины (з.е.)	6
Объем дисциплины (ак.час.)	216
Контактная работа с преподавателем (ак.час.), в том числе:	84
Проведение лекционных занятий	28
Проведение практических занятий, семинаров	0
Проведение лабораторных работ, занятий по иностранному языку	56
Самостоятельная работа (ак.час.)	132
Формы текущего контроля	Входное тестирование (1) Защищаемое контрольное мероприятие (2) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Экзамен (10 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Аппаратно-программные средства обеспечение информационной безопасности. Первый семестр.

Назначение и функции программно-аппаратных средств обеспечения безопасности
Задачи и программа курса. Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства:
экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства.

Методы защиты информации от несанкционированного доступа
Требования к средствам защиты информации от несанкционированного доступа. Контроль целостности системного и программного обеспечения и аппаратных средств. Организация виртуальных логических дисков. Шифрование пользовательских виртуальных дисков. Формирование ключевой информации.

Методы обеспечения целостности аппаратного обеспечения автоматизированных систем
Средства обеспечения целостности составных частей компьютера. Защита узлов и блоков компьютеров от несанкционированного доступа. Средства контроля
доступа к рабочему месту пользователя. Программные средства выявления фактов физического доступа к системному блоку и узлам автоматизированной системы.

Анализ уязвимости программного обеспечения автоматизированных систем
Типовая структура подсистемы безопасности ОС и выполняемые ей функции: идентификация и аутентификация, разграничение доступа, аудит, подотчетность
действий, повторное использование объектов, точность и надежность обслуживания, защита обмена данных. Реализация подсистем безопасности и
средства обеспечения безопасности в ОС семейств UNIX и Windows. Домены безопасности критерии защищенности ОС. Понятие вредоносного кода. Программные закладки. Классификация программных закладок. Предпосылки к внедрению программных закладок. Уязвимости программного обеспечения. Принципы построения политики безопасности. Уязвимости политики безопасности. Человеческий фактор. Сокрытие программных
закладок.

Методы защиты от вредоносных программ
Сигнатурное и эвристическое сканирование. Аппаратные средства противодействия вредоносному коду. Контроль целостности программного обеспечения. Мониторинг информационных потоков. Изолированная программная среда. Цифровая подпись исполняемого кода. Шифрование исполняемого кода.
Средства анализа уязвимостей

Средства авторизации и аутентификации пользователей автоматизированных систем
Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях протоколы аутентификации при удаленном доступе
средства и методы обеспечения целостности и конфиденциальности защита серверов и рабочих станций средства защиты локальных сетей при подключении к
Интернет защитные экраны защита виртуальных локальных сетей. Применение парольных систем. Аутентификация с помощью физических
предметов хранящихся у пользователя. Электронные ключи. Пластиковые карты.

Итоговое контрольное мероприятие

Итоговое контрольное мероприятие по предмету (экзамен)

6. Методические указания для обучающихся по освоению дисциплины

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

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

Самостоятельная работа преследует следующие цели:

– закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;

- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;

- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;

- самоконтроль освоения программного материала.

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

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

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

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

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

При самостоятельной работе обучающимся следует использовать:

– конспекты лекций;

– литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);

– текст лекций на электронных носителях;

– ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;

– лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;

– методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Спицын, В. Г. Информационная безопасность вычислительной техники : учебное пособие / В. Г. Спицын. — Томск : Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011. — 148 с. — ISBN 978-5-4332-0020-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/13936

2. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : учебно-методическое пособие / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 218 с. — ISBN 978-5-4487-0297-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/77317.html

Дополнительная:

1. Помешкин, А. А. Система защиты информации от несанкционированного доступа на основе программно-аппаратного комплекса «SECRET NET 5.0» : учебно-методическое пособие / А. А. Помешкин, И. В. Коротких. — Новосибирск : Новосибирский государственный технический университет, 2012. — 47 с. — ISBN 978-5-7782-1990-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/45015.html

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // ЭБС Юрайт [сайт]. https://urait.ru/bcode/449548

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

https://www.mascom.ru/equipment/sredstva-zashchity-informatsii/programmno-apparatnye-kompleksy/ Группа компаний Маском

https://www.tssltd.ru/company Сайт компании ТСС

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

Образовательный процесс по дисциплине **Аппаратно-программные средства обеспечения информационной безопасности** предполагает использование следующего программного обеспечения и информационных справочных систем:
Образовательный процесс по дисциплине предполагает использование следующего информационных технологий, программного обеспечения и информационных справочных систем:
- презентационные материалы (слайды по темам лекционных и практических занятий);
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательной среду университета (ЕТИС ПГНИУ);
- интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии и т.д.).
Перечень используемого программного обеспечения:
- открытая система "ALT Linux"
- офисный пакет приложений "Libre office";
- приложение позволяющее просматривать и воспроизводить медиа контент PDF-файлов "Adobe Acrobat Reader DC";
- программы демонстрации видео материалов (проигрыватель) "Windows Media Plaer";
- программа просмотра интернет контента (браузер) "Google Chrome"
Операционная система "Microsoft Windows 7"
Средство защиты информации от несанкционированного доступа "Dallas Lock 8.0-K"
Средство защиты информации от несанкционированного доступа "Secret Net 7 (автономный)"
Средство защиты информации от несанкционированного доступа "Аккорд"
Средство защиты конфиденциальной информации "Secret Disk"

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

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

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

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

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

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

Лекционные занятия, групповые (индивидуальные) консультации, мероприятия текущего контроля и промежуточной аттестации проводятся в аудитории, оснащенной презентационной техникой (проектор, экран для проектора, компьютер/ноутбук), а также меловой (и) или маркерной доской. Для реализации дисциплины требуется наличие компьютерного класса с предустановленной операционной системой "Microsoft Windows 7".

Аудитория для лабораторных занятий.
Лабораторные занятия проводятся в лаборатории радиотехнических средств зашиты информации с техническим оснащением, представленным в паспорте лаборатории .

Аудитория для самостоятельной работы: Лаборатория радиотехнических средств зашиты информации кафедры, помещения Научной библиотеки ПГНИУ, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченные доступом в электронную информационно-образовательную среду университета

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.
2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.
5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.
6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

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

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

Фонды оценочных средств для аттестации по дисциплине
Аппаратно-программные средства обеспечения информационной безопасности

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

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.7 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем	Знать основную нормативно-методическую документацию по обеспечению безопасности автоматизированных систем. Уметь классифицировать основные виды автоматизированных систем и определять требования по защите этих систем. Владеть терминологией в области программно-аппаратной защиты информации, а также методологией классификации автоматизированных систем.	**Неудовлетворител** Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков **Удовлетворительн** Общие, но не структурированные знания основной нормативно-методической документации по обеспечению безопасности автоматизированных систем. Частично сформированное умение классифицировать основные виды автоматизированных систем и определять требования по защите этих систем. Фрагментарное применение навыков владения терминологией в области программно-аппаратной защиты информации, а также методологией классификации автоматизированных систем. **Хорошо** Сформированное, но содержащее отдельные пробелы знание основной нормативно-методической документации по обеспечению безопасности автоматизированных систем. В целом успешное, но содержащее отдельные пробелы умение классифицировать основные виды автоматизированных систем и определять требования по защите этих систем. В целом успешное, но содержащее отдельные пробелы владение терминологией в области программно-аппаратной защиты информации, а также методологией классификации автоматизированных систем. **Отлично** Сформированные и систематические знания

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично основной нормативно-методической документацию по обеспечению безопасности автоматизированных систем. Сформированные умения классифицировать различные виды автоматизированных систем и определять требования по защите этих систем. Успешное и систематическое применение терминологии в области программно-аппаратной защиты информации, методологии классификации автоматизированных систем, а также навыками работы с нормативно-методической документацией.
ПК.15 способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Знать основные средства обеспечения защиты информации. Уметь применять средства защиты информации исходя из требований предъявляемых к конкретной автоматизированной системе. Владеть практическими навыками по применению способов и средств защиты информации.	**Неудовлетворител** Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков **Удовлетворительн** Общие, но не структурированные знания основных средств обеспечения защиты информации. Частично сформированное умение применять средства защиты информации исходя из требований предъявляемых к конкретной автоматизированной системе Фрагментарное применение навыков работы со средствами защиты информации. **Хорошо** Сформированные, но содержащие отдельные пробелы знания основных средства обеспечения защиты информации. В целом успешные, но содержащие отдельные пробелы умения применять средства защиты информации исходя из требований предъявляемых к конкретной автоматизированной системе. В целом успешные, но содержащие отдельные пробелы владения практическими навыками по применению способов и средств защиты информации. **Отлично**

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично Сформированные систематические знания основных средства обеспечения защиты информации. Сформированное умение применять средства защиты информации исходя из требований предъявляемых к конкретной автоматизированной системе. Успешное владение практическими навыками по применению способов и средств защиты информации.
ПК.9 способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем	Знать основные проектные решения по обеспечению безопасности автоматизированных систем. Уметь применять проектные решения, комбинировать их, а также анализировать эффективность различных решений и обосновывать их выбор. Владеть основными понятиями практической реализации проектных решений по обеспечению безопасности автоматизированных систем.	**Неудовлетворител** Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков **Удовлетворительн** Общие, но не структурированные знания основных проектных решения по обеспечению безопасности автоматизированных систем. Частично сформированное умение применять проектные решения, комбинировать их, а также анализировать эффективность различных решений и обосновывать их выбор. Фрагментарное применение навыков практической реализации проектных решений по обеспечению безопасности автоматизированных систем. **Хорошо** Сформированное, но содержащее отдельные пробелы знание основные проектные решения по обеспечению безопасности автоматизированных систем. В целом успешное, но содержащее отдельные пробелы умение применять проектные решения, комбинировать их, а также анализировать эффективность различных решений и обосновывать их выбор. В целом успешное, но содержащее отдельные пробелы применения навыков

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо практической реализации проектных решений по обеспечению безопасности автоматизированных систем. **Отлично** Сформированные и систематические знания основных проектных решений по обеспечению безопасности автоматизированных систем. Сформированное умение применять проектные решения, комбинировать их, а также анализировать эффективность различных решений и обосновывать их выбор. Успешное и систематическое применение навыков практической реализации проектных решений по обеспечению безопасности автоматизированных систем.
ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Знать классификацию угроз безопасности автоматизированной системы, а также основную нормативно-методическую документацию по построение модели угроз и модели нарушителя. Уметь разрабатывать модель угроз и модель нарушителя информационной безопасности автоматизированной системы. Владеть навыками оценки актуальности угроз информационной безопасности и создания модели нарушителя.	**Неудовлетворител** Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков **Удовлетворительн** Общие, но не структурированные знания классификации угроз безопасности автоматизированной системы, а также основных нормативно-методических документов по построение модели угроз и модели нарушителя. Частично сформированное умение разрабатывать модель угроз и модель нарушителя информационной безопасности автоматизированной системы. Фрагментарное применение навыков оценки актуальности угроз информационной безопасности и создания модели нарушителя. **Хорошо** Сформированное, но содержащее отдельные пробелы, знание классификации угроз безопасности автоматизированной системы, а также основных нормативно-методических

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо документов по построение модели угроз и модели нарушителя. В целом успешное, но содержащее отдельные пробелы, умение разрабатывать модель угроз и модель нарушителя информационной безопасности автоматизированной системы. В целом успешное, но содержащее отдельные пробелы, владение навыками оценки актуальности угроз информационной безопасности и создания модели нарушителя. **Отлично** Сформированные и систематические знания классификации угроз безопасности автоматизированной системы, а также основных нормативно-методический документов по построение модели угроз и модели нарушителя. Сформированное умение разрабатывать модель угроз и модель нарушителя информационной безопасности автоматизированной системы. Успешное и систематическое применение навыков оценки актуальности угроз информационной безопасности и создания модели нарушителя.
ПК.23 способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере	Знать перечень организационно-распорядительной документации по защите информации, обрабатываемой в автоматизированной системе и требования по содержанию этой документации. Уметь разрабатывать организационно-распорядительную документацию по защите информации, обрабатываемой в автоматизированной системе. Владеть навыками анализа информационных потоков, циркулирующих в	**Неудовлетворител** Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков **Удовлетворительн** Общие, но не структурированные, знания перечня организационно-распорядительной документации по защите информации, обрабатываемой в автоматизированной системе и требований к содержанию этой документации. Частично сформированное умение разрабатывать организационно-распорядительную документацию по защите информации, обрабатываемой в

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
профессиональной деятельности	автоматизированной системе.	**Удовлетворительн** автоматизированной системе. Фрагментарное применение навыков анализа информационных потоков, циркулирующих в автоматизированной системе. **Хорошо** Сформированное, но содержащее отдельные пробелы, знание перечня организационно-распорядительной документации по защите информации, обрабатываемой в автоматизированной системе и требований к содержанию этой документации. В целом успешное, но содержащее отдельные пробелы, умение разрабатывать организационно-распорядительную документацию по защите информации, обрабатываемой в автоматизированной системе. В целом успешное, но содержащее отдельные пробелы, владение навыками анализа информационных потоков, циркулирующих в автоматизированной системе. **Отлично** Сформированные и систематические знания перечня организационно-распорядительной документации по защите информации, обрабатываемой в автоматизированной системе и требований к содержанию этой документации. Сформированное умение разрабатывать организационно-распорядительную документацию по защите информации, обрабатываемой в автоматизированной системе. Успешное и систематическое применение навыков анализа информационных потоков, циркулирующих в автоматизированной системе.
ПК.16 способность участвовать в проведении экспериментально-исследовательских	Знать типы средств защиты информации, циркулирующей в автоматизированных системах, порядок сертификации средств защиты информации, а также классификацию средств защиты	**Неудовлетворител** Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
работ при сертификации средств защиты автоматизированных систем	информации в соответствии с требованиями к сертификации. Уметь определять класс средств защиты информации в соответствии с требованиями к защите информации, циркулирующей в конкретной автоматизированной системе. Владеть навыками подбора средств защиты информации для конкретной автоматизированной системы.	**Удовлетворительн** Общие, но не структурированные, знания типов средств защиты информации, циркулирующей в автоматизированных системах, порядка сертификации средств защиты информации, а также классификаций средств защиты информации в соответствии с требованиями к сертификации. Частично сформированное умение определять класс средств защиты информации в соответствии с требованиями к защите информации, циркулирующей в конкретной автоматизированной системе. Фрагментарное применение навыков подбора средств защиты информации для конкретной автоматизированной системы. **Хорошо** Сформированное, но содержащее отдельные пробелы, знание типов средств защиты информации, циркулирующей в автоматизированных системах, порядка сертификации средств защиты информации, а также классификации средств защиты информации в соответствии с требованиями к сертификации. В целом успешное, но содержащее отдельные пробелы, умение определять класс средств защиты информации в соответствии с требованиями к защите информации, циркулирующей в конкретной автоматизированной системе. В целом успешное, но содержащее отдельные пробелы, применение навыков подбора средств защиты информации для конкретной автоматизированной системы. **Отлично** Сформированные и систематические знания типов средств защиты информации, циркулирующей в автоматизированных системах, порядка сертификации средств защиты информации, а также классификации средств защиты информации в соответствии с требованиями к сертификации. Сформированное умение определять класс средств защиты информации в соответствии

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично с требованиями к защите информации, циркулирующей в конкретной автоматизированной системе. Успешное и систематическое применение навыков подбора средств защиты информации для конкретной автоматизированной системы.
ПК.13 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Знать требования, предъявляемые к системе управления информационной безопасностью автоматизированной системы. Уметь применять требования, предъявляемые к системе управления информационной безопасностью автоматизированной системы, и управлять инцидентами информационной безопасности, возникающими при обработки информации, циркулирующей в автоматизированной системе. Владеть навыками обработки инцидентов информационной безопасности, возникающих при обработки информации, циркулирующей в автоматизированной системе.	**Неудовлетворител** Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков **Удовлетворительн** Общие, но не структурированные, знания требований, предъявляемые к системе управления информационной безопасностью автоматизированной системы. Частично сформированное умение применять требования, предъявляемые к системе управления информационной безопасностью автоматизированной системы, и управлять инцидентами информационной безопасности, возникающими при обработки информации, циркулирующей в автоматизированной системе. Фрагментарное применение навыков обработки инцидентов информационной безопасности, возникающих при обработки информации, циркулирующей в автоматизированной системе. **Хорошо** Сформированное, но содержащее отдельные пробелы, знание требований, предъявляемые к системе управления информационной безопасностью автоматизированной системы. В целом успешное, но содержащее отдельные пробелы, умение применять требования, предъявляемые к системе управления информационной безопасностью автоматизированной системы, и управлять инцидентами информационной

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо безопасности, возникающими при обработки информации, циркулирующей в автоматизированной системе. В целом успешное, но содержащее отдельные пробелы, применение навыков обработки инцидентов информационной безопасности, возникающих при обработки информации, циркулирующей в автоматизированной системе. **Отлично** Сформированные и систематические знания требований, предъявляемые к системе управления информационной безопасностью автоматизированной системы. Сформированное умение применять требования, предъявляемые к системе управления информационной безопасностью автоматизированной системы, и управлять инцидентами информационной безопасности, возникающими при обработки информации, циркулирующей в автоматизированной системе. Успешное и систематическое применение навыков обработки инцидентов информационной безопасности, возникающих при обработки информации, циркулирующей в автоматизированной системе.
ПК.14 способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы	Знать требования предъявляемые к функционалу средств защиты информации и средств контроля защищенности, необходимому для обеспечения безопасности автоматизированных систем. Уметь определять необходимый и достаточных функционал средств защиты информации и средств контроля защищенности для обеспечения безопасности автоматизированных систем. Владеть навыками применения различных средств для	**Неудовлетворител** Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков **Удовлетворительн** Общие, но не структурированные, знания требований предъявляемых к функционалу средств защиты информации и средств контроля защищенности, необходимых для обеспечения безопасности автоматизированных систем. Частично сформированное умение определять необходимый и достаточных функционал средств защиты информации и

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
	автоматизированных систем.	**Удовлетворительн** средств контроля защищенности для обеспечения безопасности автоматизированных систем. Фрагментарное применение навыков использования применения различных средств для автоматизированных систем. **Хорошо** Сформированное, но содержащее отдельные пробелы, знание требований предъявляемых к функционалу средств защиты информации и средств контроля защищенности, необходимых для обеспечения безопасности автоматизированных систем. В целом успешное, но содержащее отдельные пробелы, умение определять необходимый и достаточных функционал средств защиты информации и средств контроля защищенности для обеспечения безопасности автоматизированных систем. В целом успешное, но содержащее отдельные пробелы, применение навыков использования различных средств для автоматизированных систем. **Отлично** Сформированные и систематические знания требований предъявляемый к функционалу средств защиты информации и средств контроля защищенности, необходимых для обеспечения безопасности автоматизированных систем. Сформированное умение определять необходимый и достаточных функционал средств защиты информации и средств контроля защищенности для обеспечения безопасности автоматизированных систем. Успешное и систематическое применение навыков использования различных средств для автоматизированных систем.
ПК.10 способность участвовать в разработке защищенных автоматизированных	Знать типы автоматизированных систем и комплекс мер, необходимый для обеспечения безопасности информации, обрабатываемой в этих автоматизированных	**Неудовлетворител** Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
систем по профилю своей профессиональной деятельности	системах.. Уметь классифицировать автоматизированные системы, а также определять перечень мер, необходимых для защиты информации, обрабатываемой в этих автоматизированных системах. Владеть навыками разработки комплекса мер по защите автоматизированных систем.	**Удовлетворительн** Общие, но не структурированные, знания типов автоматизированных систем и комплекса мер, необходимых для обеспечения безопасности информации, обрабатываемой в этих автоматизированных системах. Частично сформированное умение классифицировать автоматизированные системы, а также определять перечень мер, необходимых для защиты информации, обрабатываемой в этих автоматизированных системах. Фрагментарное применение навыков разработки комплекса мер по защите автоматизированных систем. **Хорошо** Сформированное, но содержащее отдельные пробелы, знание типов автоматизированных систем и комплекса мер, необходимого для обеспечения безопасности информации, обрабатываемой в этих автоматизированных системах. В целом успешное, но содержащее отдельные пробелы, умение классифицировать автоматизированные системы, а также определять перечень мер, необходимых для защиты информации, обрабатываемой в этих автоматизированных системах. В целом успешное, но содержащее отдельные пробелы, применение навыков разработки комплекса мер по защите автоматизированных систем. **Отлично** Сформированные и систематические знания типов автоматизированных систем и комплекса мер, необходимый для обеспечения безопасности информации, обрабатываемой в этих автоматизированных системах. Сформированное умение классифицировать автоматизированные системы, а также определять перечень мер, необходимых для защиты информации, обрабатываемой в этих

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично автоматизированных системах. Успешное и систематическое применение навыков разработки комплекса мер по защите автоматизированных систем.
ПК.11 способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности	Знать типы и основные компоненты автоматизированных систем. Уметь классифицировать автоматизированные системы, а также разрабатывать компоненты автоматизированных систем. Владеть навыками анализа автоматизированных систем в рамках профессиональной деятельности.	**Неудовлетворител** Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков **Удовлетворительн** Общие, но не структурированные, знания типов и основных компонентов автоматизированных систем. Частично сформированное умение классифицировать автоматизированные системы, а также разрабатывать компоненты автоматизированных систем. Фрагментарное применение навыков анализа автоматизированных систем в рамках профессиональной деятельности. **Хорошо** Сформированное, но содержащее отдельные пробелы, знание типов и основных компонентов автоматизированных систем. В целом успешное, но содержащее отдельные пробелы, умение классифицировать автоматизированные системы, а также разрабатывать компоненты автоматизированных систем. В целом успешное, но содержащее отдельные пробелы, применение навыков анализа автоматизированных систем в рамках профессиональной деятельности. **Отлично** Сформированные и систематические знания типов и основных компонентов автоматизированных систем. Сформированное умение классифицировать автоматизированные системы, а также разрабатывать компоненты автоматизированных систем. Успешное и систематическое применение

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично навыков анализа автоматизированных систем в рамках профессиональной деятельности.
ОПК.4 готовность к участию в проведении научных исследований	Знать способы разработки планов и программ проведения научных исследований в сфере средств защиты информации. Уметь проводить научные исследования и оценивать полученные результаты в сфере средств защиты информации. Владеть навыками представления результатов научной деятельности в сфере средств защиты информации.	**Неудовлетворител** Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков **Удовлетворительн** Общие, но не структурированные, знания способов разработки планов и программ проведения научных исследований в сфере средств защиты информации. Частично сформированное умение проводить научные исследования и оценивать полученные результаты в сфере средств защиты информации. Фрагментарное применение навыков представления результатов научной деятельности в сфере средств защиты информации. **Хорошо** Сформированное, но содержащее отдельные пробелы, знание способов разработки планов и программ проведения научных исследований в сфере средств защиты информации. В целом успешное, но содержащее отдельные пробелы, умение проводить научные исследования и оценивать полученные результаты в сфере средств защиты информации. В целом успешное, но содержащее отдельные пробелы, применение навыков представления результатов научной деятельности в сфере средств защиты информации. **Отлично** Сформированные и систематические знания способов разработки планов и программ проведения научных исследований в сфере средств защиты информации. Сформированное умение проводить научные

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично исследования и оценивать полученные результаты в сфере средств защиты информации. Успешное и систематическое применение навыков представления результатов научной деятельности в сфере средств защиты информации.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

Вид мероприятия промежуточной аттестации : Экзамен
Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.
Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 43 до 60
«неудовлетворительно» / «незачтено» менее 43 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Назначение и функции программно-аппаратных средств обеспечения безопасности **Входное тестирование**	Проверяются базовые знания в области информационной безопасности и защиты информации

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.5 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы **ПК.7** способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем **ПК.23** способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности	Методы защиты информации от несанкционированного доступа **Защищаемое контрольное мероприятие**	Умение разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы.Умение проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем.Умение разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности.

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.14 способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы **ПК.15** способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации **ПК.16** способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем	Методы защиты от вредоносных программ **Защищаемое контрольное мероприятие**	Умение проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.Умение проводить экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем.Принимать участие в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы.

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.4 готовность к участию в проведении научных исследований **ПК.5** способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы **ПК.7** способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем **ПК.9** способность проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем **ПК.10** способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности **ПК.11** способность участвовать в разработке компонентов автоматизированных систем в сфере профессиональной деятельности **ПК.13** способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы **ПК.14** способность участвовать в проектировании средств защиты информации и средств контроля защищенности	Итоговое контрольное мероприятие **Итоговое контрольное мероприятие**	Умение проводить синтез и анализ проектных решений по обеспечению безопасности автоматизированных систем.Принимать участие в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности. Принимать участие в разработке компонентов автоматизированных систем в сфере профессиональной деятельности.Принимать участие в проектировании системы управления информационной безопасностью автоматизированной системы.

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
автоматизированной системы **ПК.15** способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации **ПК.16** способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты автоматизированных систем **ПК.23** способность разрабатывать проекты нормативных и методических материалов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности		

Спецификация мероприятий текущего контроля

Назначение и функции программно-аппаратных средств обеспечения безопасности

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**
Проходной балл: **0**

Показатели оценивания	Баллы
Отсутствие ошибок при входном контроле	100
Одна ошибка при входном контроле	81
Две ошибки при входном контроле	61
Три ошибки при входном контроле	41

Методы защиты информации от несанкционированного доступа

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **13**

Показатели оценивания	Баллы
Умеет разрабатывать модель угроз и модель нарушителя информационной безопасности автоматизированной системы, классифицировать основные виды автоматизированных систем и определять требования по защите этих систем, разрабатывать организационно-распорядительную документацию по защите информации, обрабатываемой в автоматизированной системе.	10
Владеет терминологией в области программно-аппаратной защиты информации, а также методологией классификации автоматизированных систем, навыками оценки актуальности угроз информационной безопасности и создания модели нарушителя, навыками анализа информационных потоков, циркулирующих в автоматизированной системе.	10
Знает классификацию угроз безопасности автоматизированной системы, основную нормативно-методическую документацию по обеспечению безопасности автоматизированных систем, а также перечень организационно-распорядительной документации по защите информации, обрабатываемой в автоматизированной системе и требования по содержанию этой документации.	10

Методы защиты от вредоносных программ

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **13**

Показатели оценивания	Баллы
Знает основные средства обеспечения защиты информации, типы средств защиты информации, порядок сертификации средств защиты информации, а также классификацию средств защиты информации в соответствии с требованиями к сертификации, требования предъявляемые к функционалу средств защиты информации и средств контроля защищенности, необходимому для обеспечения безопасности автоматизированных систем.	10
Владеет практическими навыками по применению способов и средств защиты информации, навыками подбора средств защиты информации для конкретной автоматизированной системы, навыками применения различных средств для автоматизированных систем.	10
Умеет применять средства защиты информации исходя из требований предъявляемых к конкретной автоматизированной системе, определять класс средств защиты информации в соответствии с требованиями к защите информации, циркулирующей в конкретной автоматизированной системе, определять необходимый и достаточных функционал средств защиты информации и средств контроля защищенности для обеспечения безопасности автоматизированных систем.	10

Итоговое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **3 часа**

Условия проведения мероприятия: **в часы самостоятельной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **17**

Показатели оценивания	**Баллы**
Умеет применять проектные решения, комбинировать их, а также анализировать эффективность различных решений и обосновывать их выбор, классифицировать автоматизированные системы, а также определять перечень мер, необходимых для защиты информации, обрабатываемой в этих автоматизированных системах, разрабатывать компоненты автоматизированных систем, применять требования, предъявляемые к системе управления информационной безопасностью автоматизированной системы, и управлять инцидентами информационной безопасности, возникающими при обработки информации, циркулирующей в автоматизированной системе.	14
Владеет основными понятиями практической реализации проектных решений по обеспечению безопасности автоматизированных систем, навыками разработки комплекса мер по защите автоматизированных систем, навыками анализа автоматизированных систем в рамках профессиональной деятельности, навыками обработки инцидентов информационной безопасности, возникающих при обработки информации, циркулирующей в автоматизированной системе.	13
Знает основные проектные решения по обеспечению безопасности автоматизированных систем, типы автоматизированных систем и комплекс мер, необходимый для обеспечения безопасности информации, обрабатываемой в этих автоматизированных системах, требования, предъявляемые к системе управления информационной безопасностью автоматизированной системы.	13