

МИНОБРНАУКИ РОССИИ

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

Кафедра радиоэлектроники и защиты информации

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

Рабочая программа дисциплины

**РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ ЗАЩИЩЕННЫХ
АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

Код УМК 68682

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

Пермь, 2020

1. Наименование дисциплины

Разработка и эксплуатация защищенных автоматизированных систем

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную 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 **Разработка и эксплуатация защищенных автоматизированных систем** у обучающегося должны быть сформированы следующие компетенции:

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

ОПК.5 Способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности

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

ПК.25 способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации

ПК.27 способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности

ПК.28 способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы

ПК.29 способность администрировать подсистему информационной безопасности автоматизированной системы

ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы

ПК.31 способность управлять информационной безопасностью автоматизированной системы

ПК.32 способность обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций

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	13
Объем дисциплины (з.е.)	6
Объем дисциплины (ак.час.)	216
Контактная работа с преподавателем (ак.час.), в том числе:	84
Проведение лекционных занятий	42
Проведение лабораторных работ, занятий по иностранному языку	42
Самостоятельная работа (ак.час.)	132
Формы текущего контроля	Входное тестирование (1) Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (3)
Формы промежуточной аттестации	Экзамен (13 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Разработка и эксплуатация защищенных автоматизированных систем. Первый семестр

Тема 1. Компоненты комплексной системы информационной безопасности

Системный подход к защите информации. Методология формирования задач защиты, интеграция средств информационной безопасности в технологическую среду.

Системный подход к защите информации

Введение в дисциплину. Основные понятия и положения защиты информации в автоматизированных системах. Этапы развития информационных и автоматизированных систем. Классификация задач, решаемых с использованием автоматизированных систем. Модели данных, систем и процессов защиты информации в автоматизированных системах. Требования к моделям защиты информации в автоматизированных системах.

Методология формирования задач защиты, интеграция средств информационной безопасности в технологическую среду

Определение научно-методологического базиса защиты информации, состоящего из трех уровней. Определение и рассмотрение проблемы защиты информации с точки зрения общеметодологических принципов формирования науки. Определение и рассмотрение вопроса интеграции средств информационной безопасности в технологическую среду.

Тема 2. Проектирование системы информационной

Основные этапы проектирования СИБ, требования к ним. Порядок и особенности проведения испытаний и внедрения в эксплуатацию СИБ.

Основные этапы проектирования СИБ, требования к ним

Описание этапов проектирования СИБ: аудит, выявление информационных ресурсов, определение угроз безопасности информации, определение методов и средств защиты информации, внедрение методов и средств защиты информации, обучение персонала по работе с СИБ. А также определение требований к этим этапам.

Порядок и особенности проведения испытаний и внедрения в эксплуатацию СИБ.

Определение порядка и особенностей проведения испытаний СИБ:

- Контроль выполнения требований, предъявляемых к персоналу, допущенного к конфиденциальной информации;
 - Контроль организации и обеспечения работы с конфиденциальной информацией;
 - Контроль соответствия размещения, охраны, специального оборудования помещений требованиям информационной безопасности;
 - Контроль порядка учёта, хранения, использования и уничтожения документов;
 - Проверка организации и осуществления контроля за обеспечением информационной безопасности;
- Рассмотрение порядка и особенностей внедрения СИБ в эксплуатацию.

Тема 3. Управление системой информационной безопасности

Мониторинг окружающей среды, выявление каналов несанкционированного доступа. Методика построения административного управления СИБ.

Мониторинг окружающей среды, выявление каналов несанкционированного доступа

Общие сведения поисковых мероприятий. Перечень поисковых работ для контроля каналов несанкционированного доступа. Варианты комплектации поисковых подразделений.

Методика построения административного управления СИБ

Общие подходы по управлению проектами, включающими в себя:

- Сетевое планирование;
- Управление стоимостью;
- Управление проектными рисками.

Возможность планирование систем для бизнеса (требования и рекомендации).

Тема 4 Методика построения административного управления СИБ

Оценка качества системы информационной безопасности. Оценка качества СИБ методом экспертных структурных анкет. Оценка качества СИБ методом оценки уязвимости информации Хоффмана. Оценка качества СИБ методом оценки риска Фишера.

Оценка качества системы информационной безопасности

Общие сведения об оценке качества СИБ. Методы оценки качества СИБ. В качестве примера метод экспертных оценок.

Оценка качества СИБ методом экспертных структурных анкет

Определение:

1. общей характеристики метода;
2. этапов экспертного оценивания такие как:
 - Постановка цели исследования.
 - Выбор формы исследования, определение бюджета проекта.
 - Подготовка информационных материалов, бланков анкет, модератора процедуры.
 - Подбор экспертов.
 - Проведение экспертизы.
 - Статистический анализ результатов.
 - Подготовка отчета с результатами экспертного оценивания.
3. морфологический анализ.

Оценка качества СИБ методом оценки уязвимости информации Хоффмана

Общая характеристика угроз информации. Оценка уязвимостей по Дж. Хоффману с построением таблицы угроз, уязвимостей и общей оценки уязвимостей.

Оценка качества СИБ методом оценки риска Фишера

Общие характеристики метода Фишера. Метод оценки рисков по двум факторам – вероятности происшествий и цены потерь. Метод оценки рисков по трем факторам – угроза, уязвимость и цена потери.

Тема 5 Сопровождение системы информационной безопасности автоматизированной системы

Эксплуатационная документация СИБ автоматизированных систем. Аттестация объектов по требованиям информационной безопасности. Особенности эксплуатации СИБ на объекте защиты. Особенности проектирования на современном уровне и синтез СИБ.

Эксплуатационная документация СИБ автоматизированных систем

Весь жизненный цикл любой технической системы, в том числе и КСИБ, начиная от разработки технического задания на проектирование и заканчивая утилизацией после списания, сопровождается ведением документации. Перед созданием СИБ разрабатывается проектно-конструкторская документация. В ходе создания системы руководствуются технологической документацией, в том числе технологическими картами выполнения различных технологических операций. Перечень (комплект) документов, поставляемых предприятием-изготовителем СИБ. Документация, разрабатываемую на

месте эксплуатации СИБ.

Аттестация объектов по требованиям информационной безопасности

Порядок работ по подготовке и проведению аттестации объектов информатизации (АС), включающий 3 основных этапа и руководствуясь при этом.

Особенности эксплуатации СИБ на объекте защиты

Основы, направления и этапы защиты информации

- Законодательная, нормативно-методическая и научная база.
- Организационно-технические и режимные меры.
- Программно-технические методы и средства защиты информации.
- Структура и задачи органов (подразделений), осуществляющих комплексную защиту информации.

Правовые аспекты защиты информации:

- Подсистема организационно-правовой защиты;
- Промышленный шпионаж и законодательство;
- Защита программного обеспечения авторским правом;

Стандарты и рекомендации по защите информации:

- Недостатки существующих стандартов и рекомендаций;
- Требования к содержанию нормативно-методических документов по ЗИ

Особенности проектирования на современном уровне и синтез СИБ

Вопрос многокритериального синтеза применительно к системам защиты информации.

«Критериальный» подход описания выбора на примере задачи оптимизации. Оценку вклада функциональных подсистем в эффективность целостной системы. Возможность синтеза систем на основе качественных классификационных признаков. Метод морфологического древовидного синтеза, морфологический метод лабиринтного синтеза.

Контрольное итоговое мероприятие

Итоговое контрольное мероприятие - 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. Чипига Александр Федорович Информационная безопасность автоматизированных систем: учебное пособие для студентов высших учебных заведений, обучающихся по специальности 090105 - "Комплексное обеспечение информационной безопасности автоматизированных систем"/А. Ф. Чипига.- Москва: Гелиос АРВ, 2010, ISBN 978-5-85438-183-3.-3342.-Библиогр.: с. 323-324
2. Пелешенко, В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В. С. Пелешенко, С. В. Говорова, М. А. Лапина. — Ставрополь : Северо-Кавказский федеральный университет, 2017. — 86 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/69405.html>
3. Информационная безопасность и защита информации : учебно-методический комплекс / составители С. А. Омарова, К. А. Искакова, Н. А. Тойганбаева. — Алматы : Нур-Принт, 2012. — 98 с. — ISBN 9965-756-05-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/67055.html>
4. 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. Карпов, В. В. Технология построения защищенных автоматизированных систем : учебное пособие / В. В. Карпов, В. А. Мельник. — Москва : Российский новый университет, 2009. — 232 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/21326>
2. Торокин А. А. Инженерно-техническая защита информации: учеб. пособие/А. А. Торокин.-М.:Гелиос АРВ, 2005, ISBN 5-85438-140-0.-960.-Библиогр.: с. 934-949

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

<https://cyberleninka.ru/> научная библиотека

<https://ru.wikibooks.org/> Вики учебник

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

Образовательный процесс по дисциплине **Разработка и эксплуатация защищенных автоматизированных систем** 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-образовательную 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 "Libreoffice";
- приложение позволяющее просматривать и воспроизводить медиа контент PDF-файлов "AdobeAcrobatReader DC";
- программы демонстрации видео материалов (проигрыватель) "WindowsMediaPlaer";
- программа просмотра интернет контента (браузер) "GoogleChrome
- SecretNet 6.0.
- Accord
- Dallas Lock

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

Материально-техническая база обеспечивается наличием:

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.

Лабораторные занятия проводятся в лаборатории радиотехнических средств защиты информации с

техническим оснащением, представленным в паспорте лаборатории

Аудитория для самостоятельной работы: лаборатория радиотехнических средств защиты информации и помещения библиотеки с персональными компьютерами с доступом к локальной и глобальной сетям

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютерами 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
Разработка и эксплуатация защищенных автоматизированных систем

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

ОПК.5

Способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.5 Способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности	Знать способы применения языков, систем и инструментов программирования, при эксплуатации и оценке защищенности автоматизированных систем. Уметь применять системы и инструменты программирования, при эксплуатации и оценке защищенности автоматизированных систем. Владеть навыками разработки для оценки защищенности автоматизированных систем.	<p style="text-align: center;">Неудовлетворител</p> Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков <p style="text-align: center;">Удовлетворительн</p> Общие, но не структурированные, знания способов применения языков, систем и инструментов программирования, при эксплуатации и оценке защищенности автоматизированных систем. Частично сформированное умение применять системы и инструменты программирования, при эксплуатации и оценке защищенности автоматизированных систем. Фрагментарное применение навыков разработки для оценки защищенности автоматизированных систем. <p style="text-align: center;">Хорошо</p> Сформированное, но содержащее отдельные пробелы, знание способов применения языков, систем и инструментов программирования, при эксплуатации и оценке защищенности автоматизированных систем. В целом успешное, но содержащее отдельные пробелы, применять системы и инструменты программирования, при эксплуатации и оценке защищенности автоматизированных систем. В целом успешное, но содержащее отдельные пробелы, применение навыков разработки для оценки защищенности автоматизированных систем.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Отлично</p> <p>Знать способы применения языков, систем и инструментов программирования, при эксплуатации и оценке защищенности автоматизированных систем.</p> <p>Уметь применять системы и инструменты программирования, при эксплуатации и оценке защищенности автоматизированных систем.</p> <p>Владеть навыками разработки для оценки защищенности автоматизированных систем.</p>

ПК.29

способность администрировать подсистему информационной безопасности автоматизированной системы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.29</p> <p>способность администрировать подсистему информационной безопасности автоматизированной системы</p>	<p>Знать особенности администрирования подсистем информационной безопасности автоматизированных систем.</p> <p>Уметь реализовывать подсистему информационной безопасности автоматизированных систем.</p> <p>Владеть навыками администрирования автоматизированных систем, в том числе в части информационной безопасности.</p>	<p>Неудовлетворител</p> <p>Отсутствие знаний</p> <p>Не знает основ дисциплины, необходимых при формировании компетенции</p> <p>Отсутствие умений</p> <p>Отсутствие навыков</p> <p>Удовлетворительн</p> <p>Общие, но не структурированные, знания особенностей администрирования подсистем информационной безопасности автоматизированных систем.</p> <p>Частично сформированное умение реализовывать подсистему информационной безопасности автоматизированных систем.</p> <p>Фрагментарное применение навыков администрирования автоматизированных систем, в том числе в части информационной безопасности.</p> <p>Хорошо</p> <p>Сформированное, но содержащее отдельные пробелы, знание особенностей администрирования подсистем информационной безопасности автоматизированных систем</p> <p>В целом успешное, но содержащее отдельные пробелы, умение реализовывать подсистему информационной безопасности</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Хорошо автоматизированных систем. В целом успешное, но содержащее отдельные пробелы, применение навыков администрирования автоматизированных систем, в том числе в части информационной безопасности.</p> <p>Отлично Сформированные и систематические знания особенностей администрирования подсистем информационной безопасности автоматизированных систем. Сформированное умение реализовывать подсистему информационной безопасности автоматизированных систем. Успешное и систематическое применение навыков администрирования автоматизированных систем, в том числе в части информационной безопасности.</p>

ПК.30

способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы	Знать требования предъявляемые к политике информационной безопасности автоматизированной системы. Уметь разрабатывать частную политику информационной безопасности автоматизированной системы. Владеть навыками мониторинга безопасности автоматизированной системы.	<p>Неудовлетворител Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков</p> <p>Удовлетворительн Общие, но не структурированные, знания требований, предъявляемых к политике информационной безопасности автоматизированной системы. Частично сформированное умение разрабатывать частную политику информационной безопасности автоматизированной системы. Фрагментарное применение навыков мониторинга безопасности автоматизированной системы.</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Хорошо</p> <p>Сформированное, но содержащее отдельные пробелы, знание требований, предъявляемых к политике информационной безопасности автоматизированной системы.</p> <p>В целом успешное, но содержащее отдельные пробелы, умение разрабатывать частную политику информационной безопасности автоматизированной системы.</p> <p>В целом успешное, но содержащее отдельные пробелы, применение навыков мониторинга безопасности автоматизированной системы.</p> <p>Отлично</p> <p>Сформированные и систематические знания требований предъявляемых к политике информационной безопасности автоматизированной системы.</p> <p>Сформированное умение разрабатывать частную политику информационной безопасности автоматизированной системы.</p> <p>Успешное и систематическое применение навыков мониторинга безопасности автоматизированной системы.</p>

ПК.32

способность обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.32 способность обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций	<p>Знать порядок действий при возникновении инцидентов безопасности.</p> <p>Уметь реагировать на инциденты информационной безопасности и восстанавливать работоспособность автоматизированной системы.</p> <p>Владеть навыками обработки инцидента информационной безопасности.</p>	<p>Неудовлетворител</p> <p>Отсутствие знаний</p> <p>Не знает основ дисциплины, необходимых при формировании компетенции</p> <p>Отсутствие умений</p> <p>Отсутствие навыков</p> <p>Удовлетворительн</p> <p>Общие, но не структурированные, знания порядка действий при возникновении инцидентов безопасности.</p> <p>Частично сформированное умение реагировать на инциденты информационной безопасности и восстанавливать работоспособность автоматизированной системы.</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Удовлетворительн Фрагментарное применение навыков обработки инцидента информационной безопасности.</p> <p>Хорошо Сформированное, но содержащее отдельные пробелы, знание порядка действий при возникновении инцидентов безопасности. В целом успешное, но содержащее отдельные пробелы, умение реагировать на инциденты информационной безопасности и восстанавливать работоспособность автоматизированной системы. В целом успешное, но содержащее отдельные пробелы, применение навыков обработки инцидента информационной безопасности.</p> <p>Отлично Сформированные и систематические знания порядка действий при возникновении инцидентов безопасности. Сформированное умение реагировать на инциденты информационной безопасности и восстанавливать работоспособность автоматизированной системы. Успешное и систематическое применение навыков обработки инцидента информационной безопасности.</p>

ПК.27

способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.27 способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований	Знать требования предъявляемые к информационно-техническим средствам, применяемым для защиты автоматизированных систем. Уметь выбирать информационно-технические средства в соответствии с требованиями защиты	<p>Неудовлетворител Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков</p> <p>Удовлетворительн Общие, но не структурированные, знания требований предъявляемых к информационно-техническим средствам,</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
информационной безопасности	автоматизированных систем. Владеть навыками работы с основными информационно-техническими средствами.	<p>Удовлетворительн применяемым для защиты автоматизированных систем. Частично сформированное умение выбирать информационно-технические средства в соответствии с требованиями защиты автоматизированных систем. Фрагментарное применение навыков работы с основными информационно-техническими средствами.</p> <p>Хорошо Сформированное, но содержащее отдельные пробелы, знание требований предъявляемых к информационно-техническим средствам, применяемым для защиты автоматизированных систем. В целом успешное, но содержащее отдельные пробелы, умение выбирать информационно-технические средства в соответствии с требованиями защиты автоматизированных систем. В целом успешное, но содержащее отдельные пробелы, применение навыков работы с основными информационно-техническими средствами.</p> <p>Отлично Сформированные и систематические знания требований предъявляемых к информационно-техническим средствам, применяемым для защиты автоматизированных систем. Сформированное умение выбирать информационно-технические средства в соответствии с требованиями защиты автоматизированных систем. Успешное и систематическое применение навыков работы с основными информационно-техническими средствами.</p>

ПК.28

способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.28	Знать требования	Неудовлетворител

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы</p>	<p>предъявляемые к средствам защиты информации, применяемым для защиты автоматизированных систем. Уметь выбирать средства защиты информации в соответствии с требованиями защиты автоматизированных систем. Владеть навыками работы с основными средствами защиты информации.</p>	<p>Неудовлетворител Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков</p> <p>Удовлетворительн Общие, но не структурированные, знания требований предъявляемых к средствам защиты информации, применяемым для защиты автоматизированных систем. Частично сформированное умение выбирать средства защиты информации в соответствии с требованиями защиты автоматизированных систем. Фрагментарное применение навыков работы с основными средствами защиты информации.</p> <p>Хорошо Сформированное, но содержащее отдельные пробелы, знание требований предъявляемых к средствам защиты информации, применяемым для защиты автоматизированных систем. В целом успешное, но содержащее отдельные пробелы, умение выбирать средства защиты информации в соответствии с требованиями защиты автоматизированных систем. В целом успешное, но содержащее отдельные пробелы, применение навыков работы с основными средствами защиты информации.</p> <p>Отлично Сформированные и систематические знания требований предъявляемых к средствам защиты информации, применяемым для защиты автоматизированных систем. Сформированное умение выбирать средства защиты информации в соответствии с требованиями защиты автоматизированных систем. Успешное и систематическое применение навыков работы с основными средствами защиты информации.</p>

ПК.31

способность управлять информационной безопасностью автоматизированной системы

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.31 способность управлять информационной безопасностью автоматизированной системы	Знать основы менеджмента информационной безопасности автоматизированной системы. Уметь разрабатывать политику информационной безопасности автоматизированной системы организации. Владеть навыками управления информационной безопасности автоматизированных систем.	<p>Неудовлетворител</p> Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков <p>Удовлетворительн</p> Общие, но не структурированные, знания основ менеджмента информационной безопасности автоматизированной системы. Частично сформированное умение разрабатывать политику информационной безопасности автоматизированной системы организации. Фрагментарное применение навыков управления информационной безопасности автоматизированных систем. <p>Хорошо</p> Сформированное, но содержащее отдельные пробелы, знание основ менеджмента информационной безопасности автоматизированной системы. В целом успешное, но содержащее отдельные пробелы, умение разрабатывать политику информационной безопасности автоматизированной системы организации. В целом успешное, но содержащее отдельные пробелы, применение навыков управления информационной безопасности автоматизированных систем. <p>Отлично</p> Сформированные и систематические знания основ менеджмента информационной безопасности автоматизированной системы. Сформированное умение разрабатывать политику информационной безопасности автоматизированной системы организации. Успешное и систематическое применение навыков управления информационной безопасности автоматизированных систем.

ПК.14

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
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 автоматизированных систем.	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 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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Отлично</p> <p>средств защиты информации и средств контроля защищенности, необходимых для обеспечения безопасности автоматизированных систем.</p> <p>Сформированное умение определять необходимый и достаточных функционал средств защиты информации и средств контроля защищенности для обеспечения безопасности автоматизированных систем.</p> <p>Успешное и систематическое применение навыков использования различных средств для автоматизированных систем.</p>

ПК.25

способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.25</p> <p>способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации</p>	<p>Знать основы менеджмента информационной безопасности предприятия.</p> <p>Уметь разрабатывать политику информационной безопасности предприятия.</p> <p>Владеть навыками управления информационной безопасности предприятия.</p>	<p>Неудовлетворител</p> <p>Отсутствие знаний</p> <p>Не знает основ дисциплины, необходимых при формировании компетенции</p> <p>Отсутствие умений</p> <p>Отсутствие навыков</p> <p>Удовлетворительн</p> <p>Общие, но не структурированные, знания основ менеджмента информационной безопасности предприятия.</p> <p>Частично сформированное умение разрабатывать политику информационной безопасности предприятия.</p> <p>Фрагментарное применение навыков управления информационной безопасностью предприятия.</p> <p>Хорошо</p> <p>Сформированное, но содержащее отдельные пробелы, знание основ менеджмента информационной безопасности предприятия.</p> <p>В целом успешное, но содержащее отдельные пробелы, умение разрабатывать политику информационной безопасности предприятия.</p> <p>В целом успешное, но содержащее отдельные пробелы, применение навыков</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p>Хорошо управления информационной безопасности предприятия.</p> <p>Отлично Сформированные и систематические знания основ менеджмента информационной безопасности предприятия. Сформированное умение разрабатывать политику информационной безопасности предприятия. Успешное и систематическое применение навыков управления информационной безопасности предприятия.</p>

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : СУОС

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 44 до 60

«неудовлетворительно» / «незачтено» менее 44 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Системный подход к защите информации Входное тестирование	проверяются остаточные знания по дисциплинам "Программно-аппаратные средства ЗИ" , "Технические средства ЗИ", "Сети и системы передачи информации"
ПК.25 способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы	Порядок и особенности проведения испытаний и внедрения в эксплуатацию СИБ. Письменное контрольное мероприятие	Формирование политики информационной безопасности организации и контроль эффективности ее реализации.Выполнение полного объема работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ПК.29 способность администрировать подсистему информационной безопасности автоматизированной системы</p> <p>ПК.32 способность обеспечить восстановление работоспособности систем защиты информации при возникновении нештатных ситуаций</p>	<p>Методика построения административного управления СИБ</p> <p>Письменное контрольное мероприятие</p>	<p>Администрирование подсистемы информационной безопасности автоматизированной системы.</p> <p>Обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций.</p>
<p>ПК.27 способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности</p> <p>ПК.31 способность управлять информационной безопасностью автоматизированной системы</p>	<p>Оценка качества СИБ методом оценки риска Фишера</p> <p>Письменное контрольное мероприятие</p>	<p>Обеспечение эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности. Управление информационной безопасностью автоматизированной системы</p>
<p>ОПК.5 Способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности</p> <p>ПК.14 способность участвовать в проектировании средств защиты информации и средств контроля защищенности автоматизированной системы</p> <p>ПК.28 способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы</p>	<p>Особенности проектирования на современном уровне и синтез СИБ</p> <p>Итоговое контрольное мероприятие</p>	<p>Обеспечение эффективного применения средств защиты информационно-технологических ресурсов автоматизированной системы.</p> <p>Проектирование средств защиты информации и средств контроля защищенности автоматизированной системы.</p>

Спецификация мероприятий текущего контроля

Системный подход к защите информации

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставаемый 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

Порядок и особенности проведения испытаний и внедрения в эксплуатацию СИБ.

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставаемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **9**

Показатели оценивания	Баллы
Умение разрабатывать политику информационной безопасности предприятия, а также разрабатывать частную политику информационной безопасности автоматизированной системы.	7
Владение навыками управления информационной безопасности предприятия, а также навыками мониторинга безопасности автоматизированной системы.	7
Знание основ менеджмента информационной безопасности предприятия, а также требований, предъявляемых к политике информационной безопасности автоматизированной системы.	6

Методика построения административного управления СИБ

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы самостоятельной работы**

Максимальный балл, выставаемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **9**

Показатели оценивания	Баллы
Умение реализовывать подсистему информационной безопасности автоматизированных систем, а также реагировать на инциденты информационной безопасности и восстанавливать работоспособность автоматизированной системы.	7
Владение навыками администрирования автоматизированных систем, в том числе в части информационной безопасности, а также навыками обработки инцидента информационной безопасности.	7
Знание особенностей администрирования подсистем информационной безопасности автоматизированных систем, а также порядка действий при возникновении инцидентов безопасности.	6

Оценка качества СИБ методом оценки риска Фишера

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**

Условия проведения мероприятия: **в часы самостоятельной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **9**

Показатели оценивания	Баллы
Умение разрабатывать политику информационной безопасности автоматизированной системы организации, а также выбирать информационно-технические средства в соответствии с требованиями защиты автоматизированных систем.	7
Владение навыками управления информационной безопасности автоматизированных систем, а также навыками работы с основными информационно-техническими средствами.	7
Знание основ менеджмента информационной безопасности автоматизированной системы, а также требований, предъявляемых к информационно-техническим средствам, применяемым для защиты автоматизированных систем.	6

Особенности проектирования на современном уровне и синтез СИБ

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**

Проходной балл: **17**

Показатели оценивания	Баллы
Владеет навыками работы и применения средств защиты информации.	14
Знает требования предъявляемые к средствам защиты информации, применяемым для защиты автоматизированных систем, а также требования предъявляемые к функционалу средств защиты информации и средств контроля защищенности, необходимому для обеспечения безопасности автоматизированных систем.	13
Умеет выбирать средства защиты информации в соответствии с требованиями, а также определять необходимый и достаточных функционал средств защиты информации и средств контроля защищенности для обеспечения безопасности автоматизированных систем.	13