МИНОБРНАУКИ РОССИИ

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

Институт компьютерных наук и технологий

Авторы-составители: **Черников Арсений Викторович**

Рабочая программа дисциплины

ТРЕК «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМАХ ПЕРЕДАЧИ ДАННЫХ» (УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ)

Код УМК 100491

Утверждено
Протокол №1
от «28» августа 2023 г.

Пермь, 2023

1. Наименование дисциплины

Трек «Информационная безопасность в системах передачи данных» (Управление информационной безопасностью)

2. Место дисциплины в структуре образовательной программы

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

Направление подготовки: **11.03.02** Инфокоммуникационные технологии и системы связи направленность Инфокоммуникационные технологии в сервисах и услугах связи

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Трек «Информационная безопасность в системах передачи данных» (Управление информационной безопасностью)** у обучающегося должны быть сформированы следующие компетенции:

11.03.02 Инфокоммуникационные технологии и системы связи (направленность : Инфокоммуникационные технологии в сервисах и услугах связи)

ПК.1 Способен к развитию коммутационных подсистем и сетевых платформ, сетей передачи данных, транспортных сетей и сетей радиодоступа, спутниковых систем связи

Индикаторы

ПК.1.1 Делает выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи

ПК.1.2 Производит анализ существующих сетей и систем связи, вносит предложения по улучшению качества работы сетей и систем связи

ПК.1.3 Осуществляет развитие сетей и систем связи

ПК.5 Способен к оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью

Индикаторы

ПК.5.1 Применяет на практике теоретические основы информационной безопасности систем передачи данных, нормативно-правовую базу по защите информации, методы и средства по защите информации в системах передачи данных

ПК.5.2 Организовывает экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью

ПК.5.3 Проводит самостоятельную экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью

4. Объем и содержание дисциплины

Направление подготовки	11.03.02 Инфокоммуникационные технологии и системы связи (направленность: Инфокоммуникационные технологии в сервисах и услугах связи)
форма обучения	очная
№№ семестров, выделенных для изучения дисциплины	7
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	51
Проведение лекционных занятий	17
Проведение лабораторных работ, занятий по иностранному языку	34
Самостоятельная работа (ак.час.)	57
Формы текущего контроля	Защищаемое контрольное мероприятие (7)
Формы промежуточной аттестации	Зачет (7 семестр)

5. Аннотированное описание содержания разделов и тем дисциплины

1 семестр

Введение. Основные понятия в области теории управления. Менеджмент.
Основные понятия, термины и определения. Предмет и задачи дисциплины. Цели и задачи курса и его место в подготовке магистров. Взаимосвязь курса с другими дисциплинами учебного плана. Методические материалы. Периодические издания. Обязательная и дополнительная литература. Определение входных данных оценки. Роли и обязанности по проведению оценивания. Модель оценки процесса. Мероприятия процесса оценивания и выходные данные оценивания. Факторы успешной оценки процесса.

Система управления информационной безопасностью.
Область деятельности СУИБ. Ролевая структура СУИБ. Политика СУИБ. Понятие области деятельности СУИБ. Механизм выбора области деятельности. Состав области деятельности (процессы, структурные подразделения организации, кадры). Описание области деятельности (структура и содержание документа). Понятие роли. Использование ролевого принципа в рамках СУИБ. Преимущества использования ролевого принципа. Ролевая структура СУИБ (основные и дополнительные роли). Роль высшего руководства организации в СУИБ. Этапы разработки и функционирования СУИБ, на которых важно участие руководства организации. Суть участия руководства организации на этих этапах (утверждение документов, результатов анализа рисков и т.д.).
Основные процессы СУИБ. Обязательная документация СУИБ Процессы «Управление документами» и «Управление записями» (цели и задачи процессов, входные/выходные данные, роли участников, обязательные этапы процессов, связи с другими процессами СУИБ). Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»). Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса». Процесс «Анализ со стороны высшего руководства». Процесс «Обучение и обеспечение осведомленности».

Риски ИБ. Система управления рисками ИБ.
Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Разработка Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации, как открытые, так и закрытые. Выбор и анализ угроз ИБ (технических, программных, программно-аппаратных, организационных, в том числе социальной инженерии) и уязвимостей (связанных с техническими, программными, программно-аппаратными средствами, а также с персоналом) для выделенных на этапе инвентаризации активов. Оценка рисков ИБ, в том числе связанных с социальной инженерией. Планирование мер по обработке выявленных рисков ИБ, как защитных, так и превентивных. Проведение исследований по определению устойчивости информационной системы к внешним воздействиям. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ.

Стандартизация системы управления информационной безопасности. Нормативные документы.
Серия стандартов ГОСТ Р ИСО/МЭК 27000. ГОСТ Р ИСО/МЭК 13335. Общие критерии ИСО 15408, ИСО 18045. Стандарт ИСО 17799. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации. Стандарты серии NIST, BSI, BS.

Политика информационной безопасности.
Политика безопасности автоматизированных систем. Политика СУИБ. Разработка Политики

безопасности СУИБ. Стандарт управления информационной безопасностью ГОСТ Р ИСО 17799.Понятие Политики СУИБ. Цели Политики СУИБ. Структура и содержание Политики СУИБ. Источники информации для разработки Политики СУИБ.

Механизмы реализации системы управления информационной безопасности.
Средства управления информационной безопасностью Средства поддержки процессов управления информационной безопасностью АС. Программные реализации. Использование DLP систем и ERP систем для управления ИБ в информационной сфере организации.
Порядок создания СЗИПДн. Эксплуатация ИСПДн. Внесение изменений. Система управления информационной безопасностью ПДн в организации. Устойчивость ИСПДн к внешним воздействиям. Порядок создания ГИС. Эксплуатация ГИС. Внесение изменений. Система управления информационной безопасностью ГИС.

Конфиденциальное делопроизводство.
Управление организацией информационной безопасности в конфиденциальном документообороте. Использование DLP-систем. Автоматизация конфиденциального документооборота. Управление системами защиты информации в конфиденциальных сетях.

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. Голиков, А. М. Основы проектирования защищенных телекоммуникационных систем : учебное пособие для специалитета: 10.05.02 Информационная безопасность телекоммуникационных систем. Курс лекций, компьютерный практикум, компьютерные лабораторные работы и задание на самостоятельную работу / А. М. Голиков. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2016. — 396 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/72158.html

2. Милославская, Н.Г. Управление рисками информационной безопасности. Серия «Вопросы управление информационной безопасностью". Выпуск 2 : учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 130 с. — ISBN 978-5-9912-0272-5. — Текст : электронный // Лань : электронно-библиотечная система. https://e.lanbook.com/book/5179

Дополнительная:

1. Гребешков А. Ю. Техническая эксплуатация и управление телекоммуникационными сетями и системами:Учебное пособие/Гребешков А. Ю..-Самара:Поволжский государственный университет телекоммуникаций и информатики,2017.-199. http://www.iprbookshop.ru/75415.html

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

https://www.securityvision.ru/info/upravlenie-ib/ Управление ИБ

https://ru.wikipedia.org/wiki/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1% Управление ИБ

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

Образовательный процесс по дисциплине **Трек «Информационная безопасность в системах передачи данных» (Управление информационной безопасностью)** предполагает использование следующего программного обеспечения и информационных справочных систем:
Образовательный процесс по дисциплине предполагает использование следующего программного обеспечения и информационных справочных систем:
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательной среду университета.

Необходимое лицензионное и (или) свободно распространяемое программное обеспечение:
- приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов «Adobe Acrobat Reader DC»;
- офисный пакет приложений «LibreOffice», Alt Linux.
- СЗИ от НСД.

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

Лекционная аудитория - Проектор, ноутбук/компьютер, экран для проектора, маркерная или меловая доска.
Аудитория для лабораторных работ - Лаборатория Информационной безопасности: аппаратные и программные средства определены паспортом лаборатории.
Аудитория для практических работ - Лаборатория Информационной безопасности: аппаратные и программные средства определены паспортом лаборатории.
Помещение для самостоятельной работы - Помещения Научной библиотеки ПГНИУ, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченные доступом в электронную информационно-образовательную среду университета и с доступом к ЭБС.

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
Трек «Информационная безопасность в системах передачи данных» (Управление информационной безопасностью)

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

ПК.1

Способен к развитию коммутационных подсистем и сетевых платформ, сетей передачи данных, транспортных сетей и сетей радиодоступа, спутниковых систем связи

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.1.1 Делает выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи	Знает технические особенности ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи. Умеет делать выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи.	**Неудовлетворител** Не знает технические особенности ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи. Не умеет делать выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи. **Удовлетворительн** Знает частично технические особенности ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи. Не умеет делать выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи. **Хорошо** Знает технические особенности ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи. Умеет

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо частично делать выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи. **Отлично** Знает технические особенности ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи. Умеет делать выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи.
ПК.1.3 Осуществляет развитие сетей и систем связи	Знает стандарты систем связи. Умеет осуществлять развитие сетей и систем связи.	**Неудовлетворител** Не знает стандарты систем связи. Не умеет осуществлять развитие сетей и систем связи. **Удовлетворительн** Знает частично стандарты систем связи. Не умеет осуществлять развитие сетей и систем связи. **Хорошо** Знает стандарты систем связи. Частично умеет осуществлять развитие сетей и систем связи. **Отлично** Знает стандарты систем связи. Умеет осуществлять развитие сетей и систем связи.
ПК.1.2 Производит анализ существующих сетей и систем связи, вносит предложения по улучшению качества работы сетей и систем связи	Знает стандарты сетей связи. Умеет производить анализ существующих сетей и систем связи, вносит предложения по улучшению качества работы сетей и систем связи.	**Неудовлетворител** Не знает стандарты сетей связи. Не умеет производить анализ существующих сетей и систем связи, вносит предложения по улучшению качества работы сетей и систем связи. **Удовлетворительн** Знает частично стандарты сетей связи. Не умеет производить анализ существующих

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн сетей и систем связи, вносит предложения по улучшению качества работы сетей и систем связи. **Хорошо** Знает стандарты сетей связи. Умеет частично производить анализ существующих сетей и систем связи, вносит предложения по улучшению качества работы сетей и систем связи. **Отлично** Знает стандарты сетей связи. Умеет производить анализ существующих сетей и систем связи, вносит предложения по улучшению качества работы сетей и систем связи.

ПК.5

Способен к оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.5.2 Организовывает экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью	Знает методики и параметры оценки безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. Умеет организовывать экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью.	**Неудовлетворител** Не знает методики и параметры оценки безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. Не умеет организовывать экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. **Удовлетворительн** Знает частично методики и параметры оценки безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. Не умеет организовывать экспертизу по оценке параметров безопасности и защиты программного

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. **Хорошо** Знает методики и параметры оценки безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. Умеет частично организовывать экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. **Отлично** Знает методики и параметры оценки безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. Умеет организовывать экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью.
ПК.5.1 Применяет на практике теоретические основы информационной безопасности систем передачи данных, нормативно-правовую базу по защите информации, методы и средства по защите информации в системах передачи данных	Знает теоретические основы информационной безопасности систем передачи данных, нормативно-правовую базу по защите информации, методы и средства по защите информации в системах передачи данных и умеет применять их на практике.	**Неудовлетворител** Не знает теоретические основы информационной безопасности систем передачи данных, нормативно-правовую базу по защите информации, методы и средства по защите информации в системах передачи данных и не умеет применять их на практике. **Удовлетворительн** Знает частично теоретические основы информационной безопасности систем передачи данных, нормативно-правовую базу по защите информации, методы и средства по защите информации в системах

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн передачи данных и не умеет применять их на практике. **Хорошо** Знает теоретические основы информационной безопасности систем передачи данных, нормативно-правовую базу по защите информации, методы и средства по защите информации в системах передачи данных и умеет частично применять их на практике. **Отлично** Знает теоретические основы информационной безопасности систем передачи данных, нормативно-правовую базу по защите информации, методы и средства по защите информации в системах передачи данных и умеет применять их на практике.
ПК.5.3 Проводит самостоятельную экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью	Знает методики оценки параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. Умеет проводить самостоятельную экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью.	**Неудовлетворител** Не знает методики оценки параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. Не умеет проводить самостоятельную экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. **Удовлетворительн** Знает частично методики оценки параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. Не умеет проводить самостоятельную экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо Знает методики оценки параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. Частично умеет проводить самостоятельную экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. **Отлично** Знает методики оценки параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью. Умеет проводить самостоятельную экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Базовая

Вид мероприятия промежуточной аттестации : Зачет
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 41 до 60
«неудовлетворительно» / «незачтено» менее 41 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.1.1 Делает выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи	Введение. Основные понятия в области теории управления. Менеджмент. **Защищаемое контрольное мероприятие**	Знание основных понятий в области теории управления. Менеджмент ИБ.
ПК.5.2 Организовывает экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью	Система управления информационной безопасностью. **Защищаемое контрольное мероприятие**	Знание систем управления информационной безопасностью.
ПК.5.1 Применяет на практике теоретические основы информационной безопасности систем передачи данных, нормативно-правовую базу по защите информации, методы и средства по защите информации в системах передачи данных	Риски ИБ. Система управления рисками ИБ. **Защищаемое контрольное мероприятие**	Знание рисков ИБ, систем управления рисками ИБ.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.1.3 Осуществляет развитие сетей и систем связи	Стандартизация системы управления информационной безопасности. Нормативные документы. **Защищаемое контрольное мероприятие**	Знание стандартов систем управления информационной безопасности, нормативных документов.
ПК.5.3 Проводит самостоятельную экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью	Политика информационной безопасности. **Защищаемое контрольное мероприятие**	Знание политик информационной безопасности.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.1.1 Делает выборку необходимого для решения задачи ПО, оборудования и технологий, применяемых в коммутационных подсистемах, сетевых платформах, сетях передачи данных, транспортных сетях и сетях радиодоступа, спутниковых системах связи **ПК.1.2** Производит анализ существующих сетей и систем связи, вносит предложения по улучшению качества работы сетей и систем связи **ПК.1.3** Осуществляет развитие сетей и систем связи **ПК.5.2** Организовывает экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью **ПК.5.3** Проводит самостоятельную экспертизу по оценке параметров безопасности и защиты программного обеспечения и сетевых устройств, администрируемой сети с помощью специальных средств управления безопасностью **ПК.5.1** Применяет на практике теоретические основы информационной безопасности систем передачи данных, нормативно-правовую базу по защите информации, методы и	Механизмы реализации системы управления информационной безопасности. **Защищаемое контрольное мероприятие**	Знание механизмов реализации системы управления информационной безопасности. Умение ими пользоваться.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
средства по защите информации в системах передачи данных		
ПК.1.2 Производит анализ существующих сетей и систем связи, вносит предложения по улучшению качества работы сетей и систем связи	Конфиденциальное делопроизводство. **Защищаемое контрольное мероприятие**	Знание как вести конфиденциальное делопроизводство.

Спецификация мероприятий текущего контроля

Введение. Основные понятия в области теории управления. Менеджмент.

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**
Проходной балл: **4.1**

Показатели оценивания	Баллы
Выполненное задание.	6
Отчет.	4

Система управления информационной безопасностью.

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**
Проходной балл: **4.1**

Показатели оценивания	Баллы
Выполненное задание.	6
Отчет.	4

Риски ИБ. Система управления рисками ИБ.

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**
Проходной балл: **4.1**

Показатели оценивания	Баллы
Выполненное задание.	6
Отчет.	4

Стандартизация системы управления информационной безопасности. Нормативные документы.

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

Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**
Проходной балл: **4.1**

Показатели оценивания	Баллы
Выполненное задание.	6
Отчет.	4

Политика информационной безопасности.

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**
Проходной балл: **4.1**

Показатели оценивания	Баллы
Выполненное задание.	6
Отчет.	4

Механизмы реализации системы управления информационной безопасности.

Продолжительность проведения мероприятия промежуточной аттестации: **12 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **16.4**

Показатели оценивания	Баллы
Выполненная работа.	20
Отчет.	20

Конфиденциальное делопроизводство.

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**
Проходной балл: **4.1**

Показатели оценивания	Баллы
Выполненное задание,	6
Отчет.	4