МИНОБРНАУКИ РОССИИ

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

Кафедра радиоэлектроники и защиты информации

Авторы-составители: **Лунегов Игорь Владимирович**
Сеник Кирилл Александрович
Лесникова Дарья Сергеевна

Рабочая программа дисциплины

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Код УМК 81660

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

Пермь, 2020

1. Наименование дисциплины

Управление информационной безопасностью

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 **Управление информационной безопасностью** у обучающегося должны быть сформированы следующие компетенции:

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

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

ПК.31 способность управлять информационной безопасностью автоматизированной системы

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.)	5
Объем дисциплины (ак.час.)	180
Контактная работа с преподавателем (ак.час.), в том числе:	70
Проведение лекционных занятий	28
Проведение практических занятий, семинаров	14
Проведение лабораторных работ, занятий по иностранному языку	28
Самостоятельная работа (ак.час.)	110
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

Управление информационной безопасностью. Первый семестр

Тема 1. 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.

Тема 2. Введение. Базовые вопросы управления ИБ
Процессный подход Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний. Сущность и функции управления. Наука управления. Принципы, подходы и виды управления. Цели и задачи управления ИБ. Понятие системы управления. Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием. Стандартизация в области построения систем управления. История развития. Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИБ). Основные процессы СУИБ и требования, предъявляемые к ним каждым из стандартов.

Тема 3. 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».

Тема 4. 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

Тема 5. Стандартизация системы управления информационной безопасности
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.

Тема 6. 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.

Тема 7. 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.

Тема 8. Частные политики информационной безопасности
Процессы СУИБ. Политики безопасности применительно к процессам СУИБ. Примеры реализации. Применение стандарта ГОСТ Р ИСО/МЭК 17799

Тема 9. Управление инцидентами информационной безопасности автоматизированных систем
Цели и задачи процесса «Управления инцидентами ИБ, важность процесса с точки зрения управления ИБ Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ

Тема 10. Процесс Обеспечение непрерывности ведения бизнеса
Цели и задачи процесса «Обеспечение непрерывности ведения бизнеса». Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ. Стандарты планирования и управления непрерывностью бизнеса. ГОСТ Р ИСО/МЭК ТО 18044-2007. ГОСТ Р 53647.1,2,3- 2009. Построение СОНБ.

Тема 11. Управление аттестованными объектами информатизации
Требования к аттестованным объектам информатизации. Управление изменениями. Управление непрерывностью работы объектов. Взаимодействие с органами аттестации и лицензиатами, регуляторами в процессе эксплуатации объектов.

Тема 12. Управление системой криптографической защиты информации в автоматизированных системах
Требования к средствам криптографической защиты в организации. Эксплуатация системы криптографии. Управление ключевой информацией. Расследование инцидентов.

Тема 13. Управление системой защиты персональных данных (СЗИПДн) в информационных системах обработки персональных данных (ИСПДн)
Порядок создания СЗИПДн. Эксплуатация ИСПДн. Внесение изменений. Система управления информационной безопасностью ПДн в организации. Устойчивость ИСПДн к внешним воздействиям.

Тема 14. Управление системой защиты в государственных информационных системах (ГИС). Порядок создания ГИС. Эксплуатация ГИС. Внесение изменений. Система управления информационной безопасностью ГИС.

Тема 15. Конфиденциальное делопроизводство

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

Итоговое контрольное мероприятие. Экзамен.

Экзамен проводится в устной форме, по билетам, содержащим два теоретических вопроса по всему курсу дисциплины

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. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 c. — ISBN 978-5-4497-0675-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/97562

2. 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 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/72158.html

3. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1 : учебное пособие / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 244 с. — ISBN 978-5-9912-0271-8. — Текст : электронный // Лань : электронно-библиотечная система. https://elis.psu.ru/node/619854

4. Милославская, Н.Г. Технические, организационные и кадровые аспекты управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 4 : учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 214 с. — ISBN 978-5-9912-0274-9. — Текст : электронный // Лань : электронно-библиотечная система. https://elis.psu.ru/node/619856

5. Анисимов А. А. Менеджмент в сфере информационной безопасности: Учебное пособие / А.А. Анисимов. — М.: Интернет-Университет Информационных технологий: БИНОМ. Лаборатория знаний. 2009. — 176 с.: ил. табл. — (Основы информационных технологий). — ISBN 9778-5-9963-0237-6. — Текст : электронный // Электронно-библиотечная система БиблиоТех : [сайт]. https://psu.bibliotech.ru/Reader/Book/8807

6. 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://elis.psu.ru/node/619855

Дополнительная:

1. Информационное право. Информационная безопасность и защита информации:сб. нормативно - правовых актов/Перм. гос. ин-т искусства и культуры.-Пермь:[б. и.],2004.-328.

2. Суглобов, А. Е. Экономическая безопасность предприятия : учебное пособие для студентов вузов, обучающихся по специальности «Экономическая безопасность» / А. Е. Суглобов, С. А. Хмелев, Е. А. Орлова. — Москва : ЮНИТИ-ДАНА, 2013. — 271 c. — ISBN 978-5-238-02378-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/21011

3. 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://searchinform.ru/informatsionnaya-bezopasnost/ сайт компании SearchInform
https://www.croc.ru/ Сайт компании Крок

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

Образовательный процесс по дисциплине **Управление информационной безопасностью** предполагает использование следующего программного обеспечения и информационных справочных систем:
Образовательный процесс по дисциплине Управление информационной безопасности предполагает использование следующего программного обеспечения и информационных справочных систем:
Программное обеспечение:
-Операционная система ALT Linux;
-Офисный пакет приложений «LibreOffice».
- MS Windows 7, 8, 10
- Средство Microsoft Baseline Security Analyzer (MBSA) версии 1.2.1 свободно распространяемая версия
- ПО "Гриф", "Кондор" компании Digital Security академическая лицензия
- ПО SIEM Splunk свободно распространяемая версия
- СЗИ "Secret Net"
- СЗИ "Dallas Lock"
- ПО "Wingdocs"свободно распространяемая версия
- ПО оценки рисков "RA 2A" свободно распространяемая версия.
Справочная система "Консультант плюс", "Гарант" онлайн версия .

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

1. 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.
2. Лабораторные и практические занятия проводятся в Компьютерном классе кафедры радиоэлектроники и защиты информации с техническим оснащением, указанным в паспорте компьютерного класса
3. Самостоятельная работа:
Компьютерный класс кафедры радиоэлектроники и защиты информации;

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
Управление информационной безопасностью

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

Компетенция	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: основные методы управления информационной безопасностью организаций, объектов и систем. • основные стандарты, регламентирующие управление ИБ; • принципы построения СУИБ; • принципы разработки процессов управления ИБ; • взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ; • подходы к интеграции СУИБ в общую систему управления предприятие Уметь находить современные подходы к управлению ИБ.	**Неудовлетворител** Не знает основ управления ИБ. Отсутствие знаний основных методов управления информационной безопасностью организаций, объектов и автоматизированных систем; основных стандартов, регламентирующие управление ИБ; принципов построения и разработки процессов СУИБ; Отсутствие умений находить современные подходы к управлению ИБ, практически решать задачи формализации разрабатываемых процессов управления ИБ; осуществлять мониторинг безопасности автоматизированной системы Отсутствие навыков владения анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ **Удовлетворительн** Общие, но не структурированные знания основ управления ИБ. Имеет представление об основных методах управления информационной безопасностью организаций, объектов и автоматизированных систем; основных стандартах, регламентирующие управление ИБ; принципах построения и разработке процессов СУИБ; Частично сформированное умение находить современные подходы к управлению ИБ, практически решать задачи формализации разрабатываемых процессов управления ИБ; осуществлять мониторинг безопасности автоматизированной системы. Имеет представление о принципах управления ИБ организации с помощью DLP-решений.

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн Имеет фрагментарное применение навыков владения анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ **Хорошо** Сформированные, но содержащие отдельные пробелы знания основ управления ИБ, основных методов управления информационной безопасностью организаций, объектов и автоматизированных систем; основных стандартов, регламентирующие управление ИБ; принципов построения и разработке процессов СУИБ; В целом успешные, но содержащие отдельные пробелы умения находить современные подходы к управлению ИБ, практически решать задачи формализации разрабатываемых процессов управления ИБ; осуществлять мониторинг безопасности автоматизированной системы. В целом успешное, но содержащее отдельные пробелы применение навыков владения анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ **Отлично** Сформированные систематические знания основ управления ИБ, основных методов управления информационной безопасностью организаций, объектов и автоматизированных систем; основных стандартов, регламентирующие управление ИБ; принципов построения и разработке процессов СУИБ; Сформированное умение находить современные подходы к управлению ИБ, практически решать задачи формализации разрабатываемых процессов управления ИБ; осуществлять мониторинг безопасности автоматизированной системы; знает как управлять ИБ организации с помощью DLP-решений.

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично Успешное и систематическое применение навыков владения анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ
ПК.31 способность управлять информационной безопасностью автоматизированной системы	Знать структуру и процессы системы управления ИБ (СУИБ) автоматизированных систем. Понимать политику СУИБ, механизмы реализации информационной безопасности. Средства управления информационной безопасностью. Средства поддержки процессов управления информационной безопасностью АС. Знать основы управления системой криптографической защиты информации в автоматизированных системах. Владеть навыками управления информационной безопасностью простых объектов; терминологией и процессным подходом построения систем управления ИБ; Уметь работать с документацией по ИСПДн с помощью средств автоматизации. Уметь делать проверку дискреционных прав доступа в информационной системе. Уметь использовать DLP систем и ERP систем для управления ИБ .	**Неудовлетворител** Отсутствие знаний о структуре и процессах системы управления ИБ (СУИБ) автоматизированных систем, средствах управления информационной безопасностью, средствах поддержки процессов управления информационной безопасностью АС. Не понимает политику СУИБ, механизмы реализации информационной безопасности. Не знает основ управления системой криптографической защиты информации в автоматизированных системах. Отсутствие умений работать с документацией по ИСПДн с помощью средств автоматизации, делать проверку дискреционных прав доступа в информационной системе, использовать DLP систем и ERP систем для управления ИБ. Отсутствие владения навыками управления информационной безопасностью простых объектов; терминологией и процессным подходом построения систем управления ИБ, построения как отдельных процессов управления ИБ, так и системы процессов в целом **Удовлетворительн** Общие, но не структурированные знания о структуре и процессах системы управления ИБ (СУИБ) автоматизированных систем, средствах управления информационной безопасностью, средствах поддержки процессов управления информационной безопасностью АС. Имеет представление о принципах политики СУИБ и механизмах реализации информационной безопасности. Общие знания основ управления системой

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн криптографической защиты информации в автоматизированных системах. Частично сформированное умение работать с документацией по ИСПДн с помощью средств автоматизации, делать проверку дискреционных прав доступа в информационной системе, использовать DLP систем и ERP систем для управления ИБ. Фрагментарное применение навыков управления информационной безопасностью простых объектов; терминологией и процессным подходом построения систем управления ИБ, построения как отдельных процессов управления ИБ, так и системы процессов в целом. **Хорошо** Сформированные, но содержащие отдельные пробелы знания о структуре и процессах системы управления ИБ (СУИБ) автоматизированных систем, средствах управления информационной безопасностью, средствах поддержки процессов управления информационной безопасностью АС. Понимание политики СУИБ и механизмы реализации информационной безопасности. В целом успешные, но содержащие отдельные пробелы умения работать с документацией по ИСПДн с помощью средств автоматизации, делать проверку дискреционных прав доступа в информационной системе, использовать DLP систем и ERP систем для управления ИБ. В целом успешное, но содержащее отдельные пробелы применение навыков управления информационной безопасностью простых объектов; терминологией и процессным подходом построения систем управления ИБ, построения как отдельных процессов управления ИБ, так и системы процессов в целом **Отлично** Сформированные систематические знания о структуре и процессах системы управления

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично ИБ (СУИБ) автоматизированных систем, средствах управления информационной безопасностью, средствах поддержки процессов управления информационной безопасностью АС. Полное понимание политики СУИБ и механизмы реализации информационной безопасности. Хорошие знания основ управления системой криптографической защиты информации в автоматизированных системах. Сформированное умение работать с документацией по ИСПДн с помощью средств автоматизации, делать проверку дискреционных прав доступа в информационной системе, использовать DLP систем и ERP систем для управления ИБ. Успешное и систематическое применение навыков управления информационной безопасностью простых объектов; терминологией и процессным подходом построения систем управления ИБ, построения как отдельных процессов управления ИБ, так и системы процессов в целом
ПК.25 способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Знать современные подходы к управлению ИБ и направлениях их развития;основы конфиденциального делопроизводства;требования к средствам криптографической защиты в организации. Уметь анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; использовать современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;уметь оценивать	**Неудовлетворител** Отсутствие знаний современных подходов к управлению ИБ и направлениях их развития. Не знает основ конфиденциального делопроизводства;требования к средствам криптографической защиты в организации Отсутствие умений анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; использовать современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; оценивать риски ИБ на предприятии, уметь их анализировать. Отсутствие навыков управления информационной безопасностью простых объектов;

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
	риски ИБ на предприятии, уметь их анализировать; Владеть навыками управления информационной безопасностью простых объектов; • терминологией и процессным подходом построения систем управления ИБ; • навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ;	**Неудовлетворител** • владения терминологией и процессным подходом построения систем управления ИБ; • навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ; **Удовлетворительн** Общие, но не структурированные знания основ современных подходов к управлению ИБ и направлениях их развития, конфиденциального делопроизводства; требования к средствам криптографической защиты в организации. Частично сформированное умение анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; использовать современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; оценивать риски ИБ на предприятии, умения их анализировать. Фрагментарное применение навыков управления информационной безопасностью простых объектов; • владения терминологией и процессным подходом построения систем управления ИБ; • навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ **Хорошо** Сформированные, но содержащие отдельные пробелы знания современных подходов к управлению ИБ и направлениях их развития, требования безопасности при эксплуатации объектов; конфиденциального делопроизводства; требований к средствам криптографической защиты в организации. В целом успешные, но содержащие отдельные пробелы умения анализировать

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; использовать современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; оценивать риски ИБ на предприятии, умения их анализировать В целом успешное, но содержащее отдельные пробелы применение навыков управления информационной безопасностью простых объектов; • владения терминологией и процессным подходом построения систем управления ИБ; • навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ **Отлично** Четко сформированные систематические знания современных подходов к управлению ИБ и направлениях их развития, требования безопасности при эксплуатации объектов; конфиденциального делопроизводства; требований к средствам криптографической защиты в организации. Сформированное умение анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; использовать современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; оценивать риски ИБ на предприятии, умения их анализировать Успешное и систематическое применение навыков управления информационной безопасностью простых объектов;

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично • владения терминологией и процессным подходом построения систем управления ИБ; • навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ

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 44 до 60
«неудовлетворительно» / «незачтено» менее 44 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Тема 1. Введение. Основные понятия в области теории управления. Менеджмент. **Входное тестирование**	Проверяются остаточные знания ранее пройденных дисциплин: «Правовое и организационное обеспечение информационной безопасности автоматизированных систем», «Технические средства защиты информации"
ПК.30 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг безопасности автоматизированной системы	Тема 3. Система управления информационной безопасностью. **Письменное контрольное мероприятие**	Понимание базовых вопросов системы управления ИБ.

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
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	Тема 8. Частные политики информационной безопасности **Письменное контрольное мероприятие**	понимание политики информационной безопасности. Риски ИБ. Система управления рисками ИБ.
ПК.31 способность управлять информационной безопасностью автоматизированной системы	Тема 13. Управление системой защиты персональных данных (СЗИПДн) в информационных системах обработки персональных данных (ИСПДн) **Письменное контрольное мероприятие**	Знание требований к средствам криптографической защиты в организации. Порядок создания СЗИПДн.
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 **ПК.31** способность управлять информационной безопасностью автоматизированной системы	Итоговое контрольное мероприятие. Экзамен. **Итоговое контрольное мероприятие**	Оценивается понимание вопроса о системе управления информационной безопасностью, ее функции, процессах СУИБ. Оценивается умение практически решать задачи формализации разрабатываемых процессов управления ИБ; • разрабатывать и внедрять СУИБ и оценивать ее эффективность. Также оценивается самостоятельное лабораторное задание, выполняемое студентом на протяжении всего курса обучения и на основании которого студент допускается до итоговой контрольной точки

Спецификация мероприятий текущего контроля

Тема 1. Введение. Основные понятия в области теории управления. Менеджмент.

Продолжительность проведения мероприятия промежуточной аттестации: **.5 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

Тема 3. Система управления информационной безопасностью.

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **9**

Показатели оценивания	Баллы
Знание основных функций управления.	5
Знание процессов СУИБ	5
Знание функций СУИБ	5
Знание общего подхода в принятии управленческого решения	5

Тема 8. Частные политики информационной безопасности

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **9**

Показатели оценивания	Баллы
Знание политики информационной безопасности, требования к Политике ИБ. Создание Политики ИБ. Реализация Политики ИБ Частные Политики ИБ.	10
Знание основных задач , этапов управление рисками ИБ.	10

Тема 13. Управление системой защиты персональных данных (СЗИПДн) в информационных системах обработки персональных данных (ИСПДн)

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**
Проходной балл: **9**

Показатели оценивания	Баллы
Умение управлять системой защиты персональных данных, создание организационной документации по ИСПДн с помощью средств автоматизации. Управление изменениями	10

системы защиты ПДн в ИСПДн.	
Знание требований к средствам криптографической защиты в организации. Эксплуатация системы криптографии. Управление ключевой информацией.	10

Итоговое контрольное мероприятие. Экзамен.

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**
Условия проведения мероприятия: **в часы самостоятельной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **17**

Показатели оценивания	Баллы
Студент дает полный, исчерпывающий ответ на второй вопрос билета	10
По первому вопросу студент показывает хорошие знания в области системы управления информационной безопасностью. На поставленный вопрос дает исчерпывающий ответ.	10
Ответ на дополнительный вопрос	10
Ответ на дополнительный вопрос	10