

**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 93160

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 вариативную часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.01** Компьютерная безопасность  
специализация Разработка защищенного программного обеспечения

### 3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Управление информационной безопасностью** у обучающегося должны быть сформированы следующие компетенции:

**10.05.01** Компьютерная безопасность (специализация : Разработка защищенного программного обеспечения)

**ПК.10** Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах

**ПК.11** способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи

**ПК.14** способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения

**ПК.15** Способность оценивать эффективность системы защиты информации в компьютерных системах

**ПК.17** Способность разрабатывать планы работы первичных подразделений

**ПК.18** способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы

**ПК.19** Способность принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем

**ПК.2** способность осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем

**ПК.4** способность проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности

**ПК.5** Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций

**ПК.9** Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем

#### 4. Объем и содержание дисциплины

<b>Направления подготовки</b>	10.05.01 Компьютерная безопасность (направленность: Разработка защищенного программного обеспечения)
<b>форма обучения</b>	очная
<b>№№ триместров, выделенных для изучения дисциплины</b>	14
<b>Объем дисциплины (з.е.)</b>	3
<b>Объем дисциплины (ак.час.)</b>	108
<b>Контактная работа с преподавателем (ак.час.), в том числе:</b>	42
<b>Проведение лекционных занятий</b>	14
<b>Проведение лабораторных работ, занятий по иностранному языку</b>	28
<b>Самостоятельная работа (ак.час.)</b>	66
<b>Формы текущего контроля</b>	Входное тестирование (1) Защищаемое контрольное мероприятие (3) Итоговое контрольное мероприятие (1)
<b>Формы промежуточной аттестации</b>	Зачет (14 триместр)

## **5. Аннотированное описание содержания разделов и тем дисциплины**

### **Управление информационной безопасностью**

#### **Введение. Основные понятия в области теории управления**

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.

#### **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.

#### **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 безопасностью**

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 безопасностью**

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.

### **Частные политики информационной безопасности**

Процессы СУИБ. Политики безопасности применительно к процессам СУИБ. Примеры реализации. Применение стандарта ГОСТ Р ИСО/МЭК 17799

### **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

### **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.

### **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.

### **Управление системой криптографической защиты информации в автоматизированных системах**

Требования к средствам криптографической защиты в организации. Эксплуатация системы криптографии. Управление ключевой информацией. Расследование инцидентов.

### **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.

### **Управление системой защиты в государственных информационных системах (ГИС).**

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

### **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 аудиторские 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. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/87995.html>
2. Анисимов, А. А. Менеджмент в сфере информационной безопасности : учебное пособие / А. А. Анисимов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 211 с. — ISBN 978-5-4497-0328-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/89443>

### Дополнительная:

1. 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>
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://elis.psu.ru/node/619855>

## **9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины**

<https://www.securitycode.ru/> сайт компании код безопасности

<https://searchinform.ru/informatsionnaya-bezopasnost/> сайт компании SearchInform

## **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](http://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 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  
Управление информационной безопасностью**

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

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p><b>ПК.14</b> способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения</p>	<p>Знать основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; Уметь разрабатывать модели угроз и модели нарушителя объекта информатизации.</p>	<p align="center"><b>Неудовлетворител</b> не знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; не умеет разрабатывать модели угроз и модели нарушителя объекта информатизации.</p> <p align="center"><b>Удовлетворительн</b> частично сформированные знания основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; частично сформированные умения разрабатывать модели угроз и модели нарушителя объекта информатизации.</p> <p align="center"><b>Хорошо</b> сформированные, но содержащие пробелы знания основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; сформированные, но содержащие пробелы умения разрабатывать модели угроз и модели нарушителя объекта информатизации.</p> <p align="center"><b>Отлично</b> Полностью сформированные знания основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; сформированные умения разрабатывать модели угроз и модели нарушителя объекта информатизации.</p>
<p><b>ПК.5</b> Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности</p>	<p>Знать основные проектные решения по обеспечению безопасности автоматизированных систем. Уметь применять проектные решения, комбинировать их, а также анализировать эффективность различных</p>	<p align="center"><b>Неудовлетворител</b> Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков</p> <p align="center"><b>Удовлетворительн</b></p>

<b>Компетенция</b>	<b>Планируемые результаты обучения</b>	<b>Критерии оценивания результатов обучения</b>
компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций	решений и обосновывать их выбор. Владеть основными понятиями практической реализации проектных решений по обеспечению безопасности автоматизированных систем.	<p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Общие, но не структурированные знания основных проектных решения по обеспечению безопасности автоматизированных систем. Частично сформированное умение применять проектные решения, комбинировать их, а также анализировать эффективность различных решений и обосновывать их выбор. Фрагментарное применение навыков практической реализации проектных решений по обеспечению безопасности автоматизированных систем.</p> <p style="text-align: center;"><b>Хорошо</b></p> <p>Сформированное, но содержащее отдельные пробелы знание основные проектные решения по обеспечению безопасности автоматизированных систем. В целом успешное, но содержащее отдельные пробелы умение применять проектные решения, комбинировать их, а также анализировать эффективность различных решений и обосновывать их выбор. В целом успешное, но содержащее отдельные пробелы применения навыков практической реализации проектных решений по обеспечению безопасности автоматизированных систем.</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Сформированные и систематические знания основных проектных решений по обеспечению безопасности автоматизированных систем. Сформированное умение применять проектные решения, комбинировать их, а также анализировать эффективность различных решений и обосновывать их выбор. Успешное и систематическое применение навыков практической реализации проектных решений по обеспечению безопасности автоматизированных систем.</p>
<b>ПК.2</b>	Знать средства поиска научно-	<b>Неудовлетворител</b>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>способность осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем</p>	<p>технической информации, нормативных и методических материалов в сфере информационной безопасности, в том числе на иностранном языке, уметь искать, анализировать научно-техническую информацию, в сфере информационной безопасности, владеть навыками обобщения научно-технической информации в сфере информационной безопасности</p>	<p><b>Неудовлетворител</b> не знает средства поиска научно-технической информации, нормативных и методических материалов в сфере информационной безопасности, в том числе на иностранном языке; не умеет искать, анализировать научно-техническую информацию, в сфере информационной безопасности; не владеет навыками обобщения научно-технической информации в сфере информационной безопасности</p> <p><b>Удовлетворительн</b> Частично сформированные знания средств поиска научно-технической информации, нормативных и методических материалов в сфере информационной безопасности, в том числе на иностранном языке; частично сформированные умения искать, анализировать научно-техническую информацию, в сфере информационной безопасности; посредственное владение навыками обобщения научно-технической информации в сфере информационной безопасности</p> <p><b>Хорошо</b> Сформированные, но содержащие пробелы знания средств поиска научно-технической информации, нормативных и методических материалов в сфере информационной безопасности, в том числе на иностранном языке; сформированные, но содержащие пробелы умения искать, анализировать научно-техническую информацию, в сфере информационной безопасности, неуверенное владение навыками обобщения научно-технической информации в сфере информационной безопасности</p> <p><b>Отлично</b> Сформированные знания средств поиска научно-технической информации, нормативных и методических материалов в сфере информационной безопасности, в том числе на иностранном языке; сформированные умения искать, анализировать научно-техническую</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p align="center"><b>Отлично</b></p> <p>информацию, в сфере информационной безопасности, уверенное владение навыками обобщения научно-технической информации в сфере информационной безопасности</p>
<p><b>ПК.11</b> способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи</p>	<p>знать методы оценки надежности механизмов обеспечения безопасности информационной системы; уметь оценивать надежность принимаемых защитных мер; владеть навыками тестирования безопасности компьютерных систем</p>	<p align="center"><b>Неудовлетворител</b></p> <p>не знает методы оценки надежности механизмов обеспечения безопасности информационной системы; не умеет оценивать надежность принимаемых защитных мер; не владеет навыками тестирования безопасности компьютерных систем</p> <p align="center"><b>Удовлетворительн</b></p> <p>частично сформированные знания методов оценки надежности механизмов обеспечения безопасности информационной системы; частично сформированное умение оценивать надежность принимаемых защитных мер; посредственное владение навыками тестирования безопасности компьютерных систем</p> <p align="center"><b>Хорошо</b></p> <p>сформированные, но содержащие пробелы знания методов оценки надежности механизмов обеспечения безопасности информационной системы; сформированное, но содержащие пробелы умение оценивать надежность принимаемых защитных мер; неуверенное владение навыками тестирования безопасности компьютерных систем</p> <p align="center"><b>Отлично</b></p> <p>сформированные знания методов оценки надежности механизмов обеспечения безопасности информационной системы; сформированное умение оценивать надежность принимаемых защитных мер; уверенное владение навыками тестирования безопасности компьютерных систем</p>
<p><b>ПК.15</b> Способность оценивать эффективность системы защиты информации в компьютерных</p>	<p>Знать место анализа рисков в общей системе обеспечения информационной безопасности, уметь оценивать информационные риски в</p>	<p align="center"><b>Неудовлетворител</b></p> <p>не знает место анализа рисков в общей системе обеспечения информационной безопасности, не умеет оценивать информационные риски в</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
системах	автоматизированных системах, владеть методами количественной и качественной оценки информационных рисков	<p><b>Неудовлетворител</b> автоматизированных системах, не владеет методами количественной и качественной оценки информационных рисков</p> <p><b>Удовлетворительн</b> частично сформированные знания места анализа рисков в общей системе обеспечения информационной безопасности, частично сформированное умение оценивать информационные риски в автоматизированных системах, посредственное владение методами количественной и качественной оценки информационных рисков</p> <p><b>Хорошо</b> сформированные, но содержащие пробелы знания места анализа рисков в общей системе обеспечения информационной безопасности, сформированное, но содержащие пробелы умение оценивать информационные риски в автоматизированных системах, неуверенное владение методами количественной и качественной оценки информационных рисков</p> <p><b>Отлично</b> сформированные знания места анализа рисков в общей системе обеспечения информационной безопасности, сформированное умение оценивать информационные риски в автоматизированных системах, уверенное владение методами количественной и качественной оценки информационных рисков</p>
<b>ПК.19</b> Способность принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем	Знать требования предъявляемые к средствам защиты информации, применяемым для защиты автоматизированных систем. Уметь выбирать средства защиты информации в соответствии с требованиями защиты автоматизированных систем.	<p><b>Неудовлетворител</b> Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков</p> <p><b>Удовлетворительн</b> Общие, но не структурированные, знания требований предъявляемых к средствам защиты информации, применяемым для</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
	<p>Владеть навыками работы с основными средствами защиты информации.</p>	<p><b>Удовлетворительн</b> 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><b>Хорошо</b> 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><b>Отлично</b> 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>
<p><b>ПК.9</b> Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем</p>	<p>Знать основные проектные решения по обеспечению безопасности автоматизированных систем. Уметь применять проектные решения, комбинировать их, а также анализировать эффективность различных решений и обосновывать их</p>	<p><b>Неудовлетворител</b> Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков</p> <p><b>Удовлетворительн</b> Общие, но не структурированные знания</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
	<p>выбор.            Владеть основными понятиями практической реализации проектных решений по обеспечению безопасности автоматизированных систем.</p>	<p><b>Удовлетворительн</b>            основных проектных решения по обеспечению безопасности автоматизированных систем.            Частично сформированное умение применять проектные решения, комбинировать их, а также анализировать эффективность различных решений и обосновывать их выбор.            Фрагментарное применение навыков практической реализации проектных решений по обеспечению безопасности автоматизированных систем.</p> <p><b>Хорошо</b>            Сформированное, но содержащее отдельные пробелы знание основные проектные решения по обеспечению безопасности автоматизированных систем.            В целом успешное, но содержащее отдельные пробелы умение применять проектные решения, комбинировать их, а также анализировать эффективность различных решений и обосновывать их выбор.            В целом успешное, но содержащее отдельные пробелы применения навыков практической реализации проектных решений по обеспечению безопасности автоматизированных систем.</p> <p><b>Отлично</b>            Сформированные и систематические знания основных проектных решений по обеспечению безопасности автоматизированных систем.            Сформированное умение применять проектные решения, комбинировать их, а также анализировать эффективность различных решений и обосновывать их выбор.            Успешное и систематическое применение навыков практической реализации проектных решений по обеспечению безопасности автоматизированных систем.</p>
<p><b>ПК.4</b>            способность проводить</p>	<p>Знать основные средства обеспечения защиты</p>	<p><b>Неудовлетворител</b>            Отсутствие знаний</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности</p>	<p>информации. Уметь применять средства защиты информации исходя из требований предъявляемых к конкретной автоматизированной системе. Владеть практическими навыками по применению способов и средств защиты информации.</p>	<p><b>Неудовлетворител</b> Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков</p> <p><b>Удовлетворительн</b> Общие, но не структурированные знания основных средств обеспечения защиты информации. Частично сформированное умение применять средства защиты информации исходя из требований предъявляемых к конкретной автоматизированной системе Фрагментарное применение навыков работы со средствами защиты информации.</p> <p><b>Хорошо</b> Сформированные, но содержащие отдельные пробелы знания основных средства обеспечения защиты информации. В целом успешные, но содержащие отдельные пробелы умения применять средства защиты информации исходя из требований предъявляемых к конкретной автоматизированной системе. В целом успешные, но содержащие отдельные пробелы владения практическими навыками по применению способов и средств защиты информации.</p> <p><b>Отлично</b> Сформированные систематические знания основных средства обеспечения защиты информации. Сформированное умение применять средства защиты информации исходя из требований предъявляемых к конкретной автоматизированной системе. Успешное владение практическими навыками по применению способов и средств защиты информации.</p>
<p><b>ПК.17</b> Способность разрабатывать планы работы первичных подразделений</p>	<p>уметь планировать работу по регламентному обслуживанию компьютерных систем</p>	<p><b>Неудовлетворител</b> не умеет планировать работу по регламентному обслуживанию компьютерных систем</p> <p><b>Удовлетворительн</b> Частично сформированное умение</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p align="center"><b>Удовлетворительн</b></p> планировать работу по регламентному обслуживанию компьютерных систем <p align="center"><b>Хорошо</b></p> Сформированное, но содержащее пробелы умение планировать работу по регламентному обслуживанию компьютерных систем <p align="center"><b>Отлично</b></p> Сформированное умение планировать работу по регламентному обслуживанию компьютерных систем
<p><b>ПК.18</b>            способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы</p>	уметь проводить анализ защищенности автоматизированных систем и предлагать решения по их совершенствованию	<p align="center"><b>Неудовлетворител</b></p> Отсутствие умений проводить анализ защищенности автоматизированных систем и предлагать решения по их совершенствованию <p align="center"><b>Удовлетворительн</b></p> Частично сформированное умение проводить анализ защищенности автоматизированных систем <p align="center"><b>Хорошо</b></p> Сформированное умение проводить анализ защищенности автоматизированных систем, но ошибочные решения по их совершенствованию <p align="center"><b>Отлично</b></p> Полностью сформированное умение проводить анализ защищенности автоматизированных систем и предлагать решения по их совершенствованию
<p><b>ПК.10</b>            Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления</p>	Знать требования предъявляемые к политике информационной безопасности автоматизированной системы. Уметь разрабатывать частную политику информационной безопасности автоматизированной системы. Владеть навыками мониторинга безопасности автоматизированной системы.	<p align="center"><b>Неудовлетворител</b></p> Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков <p align="center"><b>Удовлетворительн</b></p> Общие, но не структурированные, знания требований, предъявляемых к политике информационной безопасности автоматизированной системы. Частично сформированное умение разрабатывать частную политику информационной безопасности

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>доступом и информационными потоками в компьютерных системах</p>		<p><b>Удовлетворительн</b> автоматизированной системы. Фрагментарное применение навыков мониторинга безопасности автоматизированной системы.</p> <p><b>Хорошо</b> формированное, но содержащее отдельные пробелы, знание требований, предъявляемых к политике информационной безопасности автоматизированной системы. В целом успешное, но содержащее отдельные пробелы, умение разрабатывать частную политику информационной безопасности автоматизированной системы. В целом успешное, но содержащее отдельные пробелы, применение навыков мониторинга безопасности автоматизированной системы.</p> <p><b>Отлично</b> Сформированные и систематические знания требований предъявляемых к политике информационной безопасности автоматизированной системы. Сформированное умение разрабатывать частную политику информационной безопасности автоматизированной системы. Успешное и систематическое применение навыков мониторинга безопасности автоматизированной системы.</p>

## 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 44 до 60

«неудовлетворительно» / «незачтено» менее 44 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<b>Входной контроль</b>	Введение. Основные понятия в области теории управления <b>Входное тестирование</b>	Проверяются остаточные знания ранее пройденных дисциплин: «Правовое и организационное обеспечение информационной безопасности автоматизированных систем», «Технические средства защиты информации»
<b>ПК.14</b> способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения <b>ПК.15</b> Способность оценивать эффективность системы защиты информации в компьютерных системах	Система управления информационной безопасностью. <b>Защищаемое контрольное мероприятие</b>	Понимание базовых вопросов системы управления ИБ.

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p><b>ПК.4</b>  способность проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности</p> <p><b>ПК.5</b>  Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций</p> <p><b>ПК.10</b>  Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p> <p><b>ПК.11</b>  способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи</p> <p><b>ПК.19</b>  Способность принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем</p>	<p>Частные политики информационной безопасности</p> <p><b>Защищаемое контрольное мероприятие</b></p>	<p>понимание политики информационной безопасности. Риски ИБ. Система управления рисками ИБ.</p>

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p><b>ПК.2</b> способность осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем</p> <p><b>ПК.9</b> Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем</p> <p><b>ПК.17</b> Способность разрабатывать планы работы первичных подразделений</p> <p><b>ПК.18</b> способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы</p>	<p>Управление системой защиты персональных данных (СЗИПДн) в информационных системах обработки персональных данных (ИСПДн)</p> <p><b>Защищаемое контрольное мероприятие</b></p>	<p>Знание требований к средствам криптографической защиты в организации. Порядок создания СЗИПДн.</p>

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p><b>ПК.2</b> способность осуществлять подбор, изучение и обобщение научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности компьютерных систем</p> <p><b>ПК.4</b> способность проводить анализ безопасности компьютерных систем с использованием отечественных и зарубежных стандартов в области компьютерной безопасности</p> <p><b>ПК.5</b> Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций</p> <p><b>ПК.9</b> Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем</p> <p><b>ПК.10</b> Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p> <p><b>ПК.11</b> способность оценивать степень</p>	<p>Итоговое контрольное мероприятие. Экзамен.</p> <p><b>Итоговое контрольное мероприятие</b></p>	<p>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</p>

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи</p> <p><b>ПК.14</b> способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения</p> <p><b>ПК.15</b> Способность оценивать эффективность системы защиты информации в компьютерных системах</p> <p><b>ПК.17</b> Способность разрабатывать планы работы первичных подразделений</p> <p><b>ПК.18</b> способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью компьютерной системы</p> <p><b>ПК.19</b> Способность принимать участие в эксплуатации системы обеспечения информационной безопасности компьютерных систем</p>		

### Спецификация мероприятий текущего контроля

#### Введение. Основные понятия в области теории управления

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

Условия проведения мероприятия: **в часы самостоятельной 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

### **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**

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

### **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**

<b>Показатели оценивания</b>	<b>Баллы</b>
Знание политики информационной безопасности, требования к Политике ИБ. Создание Политики ИБ. Реализация Политики ИБ Частные Политики ИБ.	10
Показатель БаллЗнание основных задач , этапов управление рисками ИБ.	10

### **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**

<b>Показатели оценивания</b>	<b>Баллы</b>
Умение управлять системой защиты персональных данных, создание организационной документации по ИСПДн с помощью средств автоматизации. Управление изменениями системы защиты ПДн в ИСПДн.	10
Знание требований к средствам криптографической защиты в организации. Эксплуатация системы криптографии. Управление ключевой информацией.	10

### **Итоговое контрольное мероприятие. Экзамен.**

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

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

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

Проходной балл: **17**

<b>Показатели оценивания</b>	<b>Баллы</b>
Ответ на дополнительный вопрос	10
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