МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ФИТКБ

_____/Гусев П.Ю./

28.02.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Управление информационной безопасностью»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация специализация N 7 "Анализ безопасности информационных систем"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2023

Автор программы _____К.А. Разинкнн

Заведующий кафедрой Систем информационной безопасности _____А.Г. Остапенко

Руководитель ОПОП _____А.Г. Остапенко

Воронеж 2023

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины является приобретение студентами знаний о системе управления информационной безопасностью, о процессах планирования, реализации, проверки и совершенствовании системы управления информационной безопасностью телекоммуникационных систем и умений по оценке и обработке рисков информационной безопасности, формированию политик информационной безопасности телекоммуникационной системы, оценке информационной безопасности телекоммуникационной системы.

1.2. Задачи освоения дисциплины

- сформировать у будущего специалиста в области безопасности телекоммуникационных систем знания, умения и навыки в области формирования, внедрения и обеспечения функционирования системы менеджмента информационной безопасности телекоммуникационных систем и сетей;
- предоставить возможность изучения особенностей реализации комплекса организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Управление информационной безопасностью» относится к дисциплинам обязательной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Управление информационной безопасностью» направлен на формирование следующих компетенций:

ОПК-5 - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите и нформации;

ОПК-13 - Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем;

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-5	знать основные документы по стандартизации в сфере управления ИБ, принципы формирования политики информационной безопасности в автоматизированных системах
	уметь формировать политики информационной безопасности организации
ОПК-13	знать требования информационной безопасности при эксплуатации автоматизированной системы, программные средства, позволяющие вести автоматизированный аудит
	осуществлять выбор и обоснование критериев эффективности функционирования защищенных

	автоматизированных информационных систем; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Управление информационной безопасностью» составляет 6 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		10
Аудиторные занятия (всего)	126	126
В том числе:		
Лекции	54	54
Практические занятия (ПЗ)	72	72
Самостоятельная работа	90	90
Виды промежуточной аттестации - зачет с оценкой	+	+
Общая трудоемкость: академические часы зач.ед.	 216 6	 216 6

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Практ зан.	СРС	Всего, час
1	Основные понятия и подходы к управлению информационной безопасностью	Заполните содержание разде Базовая терминология. Системный и процессный подходы к управлению ИБ. Управление логическим доступом к активам организации. Управление защищенной передачей данных и организационной деятельностью. Управление конфигурациями, изменениями и обновлениями.	10	12	14	36
2	Стандартизация систем и процессов управления информационной безопасностью	Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности». Стандарты на отдельные процессы управления ИБ и оценку безопасности ИТ. Отраслевые стандарты в области управления ИБ.	10	12	14	36
3	Политика информационной безопасности	Понятие политики обеспечения ИБ и политики ИБ организации. Причины разработки политики. Основные требования и принципы, учитываемые при разработке и внедрения политики ИБ.	10	12	14	36

		Содержание политики ИБ. Жизненный цикл политики ИБ. Ответственность за исполнение политики				
4	Модели управления доступом и информационными потоками	Модели дискреционного управления доступом. Модели изолированной программной среды. Модели с мандатным управлением доступом. Модели безопасности информационных потоков. Модели с ролевым управлением доступом_	8	12	16	36
5	Управление и система управления информационной безопасностью	Необходимость управления обеспечением ИБ организации. Деятельность по обеспечению ИБ организации как процесс. Определение управления ИБ организации. Управление ИБ информационно-телекоммуникационных технологий организации. Система управления ИБ организации. Область действия СУИБ. Документальное обеспечение СУИБ. Документальное обеспечение СУИБ. Процессный подход в рамках управления ИБ. Работа с процессами СУИБ организации. Стратегии построения и внедрения СУИБ.	8	12	16	36
6	Организационные и кадровые вопросы управления информационной безопасностью	Модели организационного управления ИБ. Организационная инфраструктура ИБ. Служба ИБ организации. Компетентностные уровни профессионалов в области ИБ	8	12	16	36
		Итого	**54**	**72**	**90**	**216**

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-5	знать основные документы по стандартизации в сфере управления ИБ, принципы формирования политики информационной безопасности в автоматизированных системах	знает основные документы по стандартизации в сфере управления ИБ, принципы формирования политики информационной безопасности в автоматизированных системах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь формировать политики информационной безопасности организации	умеет формировать политики информационной безопасности организации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-13	знать требования информационной безопасности при эксплуатации автоматизированной системы, программные средства, позволяющие вести автоматизированный аудит	знать требования информационной безопасности при эксплуатации автоматизированной системы, программные средства, позволяющие вести автоматизированный аудит	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь осуществлять выбор и обоснование критериев эффективности функционирования защищенных автоматизированных информационных систем; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	умеет осуществлять выбор и обоснование критериев эффективности функционирования защищенных автоматизированных информационных систем; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 10 семестре для очной формы обучения по четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-5	знать основные документы по стандартизации в сфере управления ИБ, принципы формирования политики информационной безопасности в автоматизированных системах	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь формировать политики информационной безопасности организации	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ОПК-13	знать требования информационной безопасности при эксплуатации автоматизированной системы, программные средства, позволяющие вести автоматизированный аудит	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь осуществлять выбор и обоснование критериев эффективности функционирования защищенных автоматизированных информационных систем; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Как называется информация, которую следует защищать (по нормативам, правилам сети, системы)?
   а) Регламентированной
   б) Правовой
   в) Защищаемой+
2. Разновидностями угроз безопасности (сети, системы) являются:
   а) Программные, технические, организационные, технологические+
   б) Серверные, клиентские, спутниковые, наземные
   в) Личные, корпоративные, социальные, национальные
3. Относятся к правовым методам, обеспечивающим информационную безопасность:
   а) Разработка аппаратных средств обеспечения правовых данных
   б) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
   в) Разработка и конкретизация правовых нормативных актов обеспечения безопасности+
4. Основные источники угроз информационной безопасности:
   а) Хищение жестких дисков, подключение к сети, инсайдерство
   б) Перехват данных, хищение данных, изменение архитектуры системы+
   в) Хищение данных, подкуп системных администраторов, нарушение регламента работы
5. Выберите виды информационной безопасности:
   а) Персональная, корпоративная, государственная+
   б) Клиентская, серверная, сетевая
   в) Локальная, глобальная, смешанная
6. Цели информационной безопасности – своевременное обнаружение, предупреждение:
   а) несанкционированного доступа, воздействия в сети+
   б) инсайдерства в организации
   в) чрезвычайных ситуаций
7. Основными объектами информационной безопасности являются:
   а) Компьютерные сети, базы данных+
   б) Информационные системы, психологическое состояние пользователей
   в) Бизнес-ориентированные, коммерческие системы
8. Утечка информации в системе:
   а) это ситуация, которая характеризуется потерей данных в системе+
   б) это ситуация, которая характеризуется изменением формы информации
   в) это ситуация, которая характеризуется изменением содержания информации
9. Выберите наиболее важный момент при реализации защитных мер политики безопасности а) Аудит, анализ затрат на проведение защитных мер
   б) Аудит, анализ безопасности
   в) Аудит, анализ уязвимостей, риск-ситуаций+
10. Определите, какой подход к обеспечению безопасности имеет место:
    а) теоретический
    б) комплексный +
    в) логический

7.2.2 Примерный перечень заданий для решения стандартных задач

1.К моделям КС с дискреционным управлением доступом относятся:
- **модель матрицы доступов Харрисона-Рузо-Ульмана**
- модель Белла-ЛаПадулы
- автоматная модель безопасности информационных потоков
- вероятностная модель контроля информационных потоков

2.Математические понятия, относящиеся к моделям безопасности:
(несколько вариантов ответов)

- граф;

- автомат;

- решётка;

- дифференциальное уравнения

- уравнение в конечных разностях.

3. Дайте правильное определение основной аксиомы компьютерной безопасности:

-в рамках субъект сущностного подхода все вопросы безопасности информации в КС описываются доступами субъектов к сущностям;

- информационным потоком от сущности к источнику к сущности-приемнику называется преобразование данных в сущности-приемнике;

- все действия в КС, в том числе выполнение операций над сущностями, могут быть инициированы только субъектами КС с использованием доступов к сущностям КС.

4. Правилами (де-юре) классической модели Take-Grant являются: (несколько вариантов ответов)

- **take**
- **grant**
- **crteate**
- **remove**
- delete
- post
- pass
- spy

5. Стоимость правила в модели Take-Grant может:

- являться константой

- не зависеть от специфики правила

- зависеть от степени требуемого взаимодействия и не зависеть от числа и состава участников при применении правила.

6. Процессный подход это:

- систематическая идентификация и менеджмент применяемых организацией бизнес-процессов и особенно взаимодействия таких процессов;

- менеджмент применяемых организацией бизнес-процессов и особенно взаимодействия таких процессов;

- внесистемная организация бизнес-процессов, в части идентификации и особенно взаимодействия таких процессов

7. Определение инцидента (выберите правильное, согласно стандарта ISO/IEC 27000:201):

- событие или серия нежелательных или непредвиденных событий ИБ, которые могут с большой долей вероятности привести к компрометации бизнес-операций или созданию угрозы ИБ;

- последовательность событий;

- единичное событие;

- событие, обусловленное действиями субъекта-нарушителя;

- событие, приводящее к компрометации бизнес-операций или созданию угрозы ИБ

8. Основные признаки инцидента (выбирайте несколько вариантов ответов):

− вероятностный характер события;

− неблагоприятные последствия;

− изменение профилей защиты СЗИ**;**

− маппинг физических смещений на виртуальные адреса**;**

− изменение имён открытых файлов для каждого процесса.

9. Целью какого процесса является определение и контроль компонентов услуг и

конфигурационных единиц, а также предоставление достоверной информации о состоянии услуг и инфраструктур?

планирование и поддержка внедрения

управление изменениями

управление активами и конфигурациями

управление релизами и развертыванием

10. В рамках какого элемента Управления информационной безопасностью происходит выбор метрик информационной безопасности?

планирование

реализация

оценка

контроль

поддержка

11. Как называется процесс, отвечающий за допуск пользователей к использованию услуг, данных или других активов?

управление конфигурациями

управление доступом

управление информационной безопасностью

управление инцидентами

12. Какую аббревиатуру носит система политик, процессов, стандартов, руководящих документов и средств, которые обеспечивают организации достижение целей управления информационной безопасностью?

SKWIT

ISMS

SMIS

CMS

7.2.3 Примерный перечень заданий для решения прикладных задач

1. *Дайте правильное определение СУИБ*

   А. Часть общей системы управления организации, основанной на подходе оценки и анализа бизнес-рисков, предназначенную для разработки, внедрения, эксплуатации, постоянного контроля, анализа, поддержания и улучшения ИБ, и включающую организационную структуру, политику, планирование действий, обязанности, установившийся порядок, процедуры, процессы и ресурсы в области ИБ.

   Б. Часть общей системы управления организации, учитывающий необходимость анализа бизнес-процессов, для контроля, анализа, и улучшения ИБ, интегрированную в организационную структуру, с учётом политики и планирования действий и обязанностей сотрудников.

   В. Часть общей системы управления организации, ориентированной на оптимизацию процессов разработки, внедрения, эксплуатации, постоянного контроля, анализа, поддержания и улучшения ИБ, и включающую организационную структуру, политику, планирование действий, обязанности, установившийся порядок, процедуры, процессы и ресурсы в области ИБ.

2. *Системный подход - это ….*

   А. методологическое направление исследование их объекта как системы с разных сторон, комплексно, в совокупности отношений и связей между его элементами, в отличие от ранее применявшихся (физических, структурных и т. д.).

   Б. организационно- методическое всестороннее направление исследования системы в совокупности отношений и связей между его элементами, в отличие от ранее

применявшихся (физических, структурных и т. д.).
В. комплексное исследование объекта как системы с учётом совокупности связей между элементами.

3. *Процесс – это: ...*
А. совокупность взаимосвязанных или взаимодействующих видов деятельности, преобразующая входы в выходы и требующая для этого определенных ресурсов и управляющих воздействий (управления). Входами к процессу обычно являются выходы
Б. интеграция различных видов деятельности, преобразующая входы в выходы и требующая для этого определенных ресурсов и управляющих воздействий (управления). Входами к процессу обычно являются выходы
В. перечень совокупности связанных и/или взаимодействующих видов деятельности, преобразующая входы в выходы и требующая для этого определенных ресурсов и управляющих воздействий (управления). Выходы к процессу обычно являются входы.
4. *Процессный подход — это..*
А. систематическая идентификация и менеджмент применяемых организацией бизнес-процессов и особенно взаимодействия таких процессов.
Б. периодическое оценивание и управление бизнес-процессами, в том числе особенно взаимодействия таких процессов.
В. способ организации управленческой деятельности, который предполагает полное описание бизнес-процессов организации.

5. *Управление с позиции системного подхода определяется как ....*
А. осуществление совокупности непрерывных взаимосвязанных воздействий на объект (управляемую систему), выбранных из множества возможных воздействий ни основан на информации о поведении объекта и состоянии внешней среды для достижения заданной цели.
Б. реализация перечня инструкций по воздействию на объект (управляемую систему), выбранных из множества возможных реализаций информации о поведении объекта и состоянии внешней среды для достижения заданной цели.
В. рациональный выбор совокупности непрерывных взаимосвязанных воздействий на объект (управляемую систему), выбранных из множества возможных воздействий ни основан на информации о поведении объекта и состоянии внешней среды для достижения заданной цели.

6. *Системный подход к управлению организацией – это ...*
А. выявление, понимание и административное управление системой взаимосвязанных процессов с целью достижения заданной стратегической цели.
Б. формирование управленческих воздействий на систему с целью понимания взаимосвязанных процессов для достижения заданной стратегической цели.
В. выявление, объяснение и формирование на их основе политики безопасности на основе анализа взаимосвязанных процессов с целью достижения заданной стратегической цели.

7. *В ISO/IEC 27000:2009 СУИБ определяется как .....*
А. часть общей системы управления, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, сопровождения (поддержания) и совершенствования (улучшения) ИБ.
Б. часть общей системы управления, призванная на основе методов математического

моделирования разрабатывать, внедрять, производить мониторинг и анализировать и в целом повышать эффективность ИБ организации.

В. часть общей системы управления, основанная на использовании методов оценки бизнес-рисков создания архитектуры, проекта и реализации технической безопасности для сетей, которые будут обеспечивать эффективную, соответствующую бизнсс-требованиям защиту, опирающуюся на базовые модели и понятную для всех сотрудников организации, вовлеченных в планирование, проектирование и внедрение архитектурных аспектов безопасности сетей.

8. ISO/IEC 27033-2 «Руководство по проектированию и внедрению системы обеспечения безопасности сетей», определяет…

А. как организация должна создавать архитектуру, проект и реализацию технической безопасности для сетей, которые будут обеспечивать эффективную, соответствующую бизнес-требованиям защиту, опирающуюся на базовые модели и понятную для всех сотрудников организации, вовлеченных в планирование, проектирование и внедрение архитектурных аспектов безопасности сетей.

Б. как организация должна создавать архитектуру, проект и реализацию технической безопасности для сетей системы управления, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, сопровождения (поддержания) и совершенствования (улучшения) ИБ.

В. как организация должна создавать архитектуру, проект и реализацию управления специфическими рисками, методики проектирования и средства управления для защиты соединений, устанавливаемых посредством использования виртуальных частных сетей.

9. ISO/IEC 27033-5 «Обеспечение безопасности виртуальных частных сетей - угрозы, методы проектирования и средства управления», определяет…

А. специфические риски, методики проектирования и средства управления для защиты соединений, устанавливаемых посредством использования виртуальных частных сетей. Предназначен для всех сотрудников организации, вовлеченных в планирование, проектирование и внедрение ВЧС.

Б. специфические риски, методики проектирования и средства управления для защиты беспроводных и радиосетей специфические риски, методики проектирования и средства управления для защиты беспроводных и радиосетей. Предназначен для всех сотрудников организации, вовлеченных в планирование, проектирование и внедрение ВЧС.

В. специфические риски, методики проектирования и средства управления для понимания как организация должна создавать архитектуру, проект и реализацию технической безопасности для сетей системы управления, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, сопровождения (поддержания) и совершенствования (улучшения) ИБ

10. ISO/IEC 27033-7 «Руководство по обеспечению безопасности беспроводных сетей - риски, методы проектирования и средства управления», определяет

А. специфические риски, методики проектирования и средства управления для защиты беспроводных и радиосетей. Предназначен для всех сотрудников организации, вовлеченных в планирование, проектирование и внедрение таких сетей.

Б. специфические риски, методики проектирования и средства управления для за-

щиты беспроводных и радиосетей специфические риски, методики проектирования и средства управления для защиты беспроводных и радиосетей.

В. специфические риски, методики проектирования и средства управления для защиты беспроводных и радио - и виртуальных частных сетей. Предназначен для всех сотрудников организации, вовлеченных в планирование, проектирование и внедрение таких сетей.

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень заданий для решения прикладных задач

1. Какие определения ПолИБ даются и различных международных стандартах?
2. В чем различие политик, стандартов, правил и процедур ОИБ?
3. Что такое трастовые модели?
4. С каких точек зрении и как можно описать виды ПолИБ?
5. Что понимают под ПолИБ и широким и узком смыслах?
6. Для чего разрабатываются организационные (административные) и технические ПолИБ?
7. Перечислите основные требования, предъявляемые в различных источниках к ПолИБ?
8. Каковы основные принципы позволяющие разработать эффективную ПолИБ?
9. Каково содержание документа, описывающего корпоративную ПолИБ? Что излагается в каждом из разделов этой политики?
10. Назовите типовые цели корпоративной ПолИБ.
11. 11.Каковы отличительные особенности содержания частной ПолИБ для отдельной области, требующей ОИБ, и для отдельной системы, используемой в организации? Что общего между ними подтипами? Что излагается в каждом из разделов этих политик?
12. 12.Назовите основные стадии жизненного цикла ПолИБ? Из каких шагов они состоят? Какие из этик шагов выполняются итерационно и почему?
13. 13.Отдельно сформулируйте цель к основным мероприятия, осуществляемые на каждом шаге жизненною цикла ПолИБ.
14. Как происходит процесс информирования в отношении ПолИБ?
15. Для чего и кем осуществляются ревизия, мониторинг и аудит ПолИБ? В чем отличия этих шагов жизненного цикла ПолИБ?
16. Что понимаемся под исключениями в ПолИБ?
17. Зачем необходим пересмотр ПолИБ?
18. В каких случаях ПолИБ может быть аннулирована?
19. Что такое «роль»? Какие роли связаны с использованием ПолИБ?
20. Какие виды ответственности связаны со всеми стадиями жизненного цикла ПолИБ?
21. Какими принципами необходимо руководствоваться при установлении ответственности в отношении соблюдения ПолИБ?
22. Дайте определения «ОИБ», «управления ИБ» и «СУИБ» организации.
23. Опишите деятельность по ОИБ организации как процесс. Каковы его входные и выходные данные, ресурсы и управляющие воздействия?
24. Как процесс ОИБ организации связан с процессами основной деятельности организации?
25. Каковы основные этапы процесса управления ИБ ИТТ
26. Что является хорошей практикой при выборе области действия СУИБ? Какие стратегии выбора области действии СУИБ существуют?
27. Какие факторы необходимо учитывать при выборе области действия СУИБ?
28. Какие параметры процессов являются наиболее значимыми при выборе области

действия проектируемой СУИБ?

29. Что входит в документальное обеспечение СУИБ? Каковы этапы его жизненного цикла?

30. Какие уровни документов включает в себя иерархия документов СУИБ? Какие виды конкретных документа создаются на каждом из уровней?

31. И чем состоит основное отличие между понятиями документ и запись?

32. В чем заключается процесс управления документами и записями?

33. Какова взаимосвязь между понятиями ПолИБ и политика СУИБ?

34. Что должна включать в себя политика СУИБ?

35. На каких панах руководство организации должно продемонстрировать свою приверженность к разработке, реализации, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ?

36. В чем состоит основная необходимость участия высшего руководства в жизненном цикле СУИБ?

37. Каким образом при использовании циклической модели PDCA применительно к СУИБ требования и ожидания к результатам ОИБ преобразуются я управляемую ИБ?

38. Дате определение «процесс управления ИБ» организации.

39. Какие действия и процессы выполняются на стадии планировании СУИБ? Каковы задачи данного этапа?

40. Специалистов каких подразделении необходимо включать в рабочую группу по построению СУИБ и почему?

41. Какие действия и процессы выполняются на стадии реализации и внедрения СУИБ? Каковы задачи данного этапа?

42. Какие действия и процессы выполняются на стадии проверки СУИБ? Каковы задачи данною этапа?

43. Какие действия и процессы выполняются на стадии совершенствования СУИБ. Каковы задачи данного этана?

44. В чем разница и сходство между понятиями корректирующего и предупреждающего действия?

45. Почему в рамках процесса подхода к управлению ИБ следует особое внимание уделять мониторингу и анализу результативности и эффективности СУИБ?

46. В чем состоят различия между основными свойствами процессов: эффективность и результативностъ?

47. Что входит в понятие «задание процесса у правления ИБ»?

48. Какие этапы включает в себя идентификация процессов управления ИБ в организации и какие действия необходимо предпринять в рамках этих этапов?

49. Каковы основные преимущества документировании процессов управления ИБ в организации и наличия подробных карт процессов организации?

50. Каковы основные элементы процесса мониторинга процессов управления ИБ организации?

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

(Например: Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент на-

брал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Основные понятия и подходы к управлению информационной безопасностью	ОПК-5, ОПК-13	Тест, защита практических работ
2	Стандартизация систем и процессов управления информационной безопасностью	ОПК-5, ОПК-13	Тест, защита практических работ
3	Политика информационной безопасности	ОПК-5, ОПК-13	Тест, защита практических работ
4	Модели управления доступом и информационными потоками	ОПК-5, ОПК-13	Тест, защита практических работ
5	Управление и система управления информационной безопасностью	ОПК-5, ОПК-13	Тест, защита практических работ
6	Организационные и кадровые вопросы управления информационной безопасностью	ОПК-5, ОПК-13	Тест, защита практических работ

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература

1.Основы управления информационной безопасностью : Учебное пособие / Курило А. П. - Москва : Горячая линия - Телеком, 2012. - 244 с. - ISBN

978-5-9912-0271-8. URL: http://www.iprbookshop.ru/12021.html

2.Методические указания к практическим занятиям № 1–4 по дисциплине «Управление информационной безопасностью» для студентов специальности 090303 «Информационная безопасность автоматизированных систем» очной формы обучения» / ФГБОУ ВПО «Воронежский государственный технический университет»; сост. К. А. Разинкин. Воронеж, 2014. 57 с. https://cchgeu.ru/upload/iblock/e3f/razinkin_pz_uib_1_4.pdf

3.Методические указания к практическим занятиям № 5–6 по дисциплине «Управление информационной безопасностью» для студентов специальности 090303 «Информационная безопасность автоматизированных систем» очной формы обучения» / ФГБОУ ВПО «Воронежский государственный технический университет»; сост. К. А. Разинкин. – Воронеж, 2014. 50 с.

https://cchgeu.ru/upload/iblock/815/razinkin_pz_uib_5_6.pdf

Дополнительная литература

1.Комплексное обеспечение информационной безопасности автоматизированных систем: учебное пособие / составители М. А. Лапина [и др.]. — Ставрополь: СКФУ, 2016. — 242 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/155111

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

http://eios.vorstu.ru/ http://www.studentlibrary.ru/ http://znanium.com/ http://ibooks.ru/ http://e.lanbook.com/; http://www.iprbookshop.ru/

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специфического материально-технического обеспечения не требуется

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Управление информационной безопасностью» читаются лекции, проводятся практические занятия.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Практические занятия направлены на приобретение практических навыков

1. Модель решётки
2. Дискреционное управлением доступом
3. (модели Харрисона-Руззо-Ульмана и типизированная
4. матрицы доступов)
5. Управление распространением прав доступа на основе классической

модели Take-Grant

6. Управление распространением прав доступа на основе расширенной модели Take-Grant
7. Модель Белла-ЛаПадулы. Мандатное
8. управление доступом
9. Ролевое и мандатное ролевое управление доступом
10. Изучение средств управления безопасностью на уровне операционной системы на примере Windows Server 2003.
11. Управления учетными записями пользователей
12. Изучение средств управления безопасностью на уровне операционной системы на примере Windows Server 2003.
13. Настройка политик безопасности

Занятия проводятся путем решения конкретных задач в аудитории.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом с оценкой три дня эффективнее всего использовать для повторения и систематизации материала.