МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета _____ Гусев П.Ю.

«31» августа 2021 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Планирование и управление информационной безопасностью»

Специальность 10.05.02 Информационная безопасность телекоммуникационных систем

Специализация специализация № 9 "Управление безопасностью телекоммуникационных систем и сетей"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2021

Автор программы _____ /Белоножкин В.И./

Заведующий кафедрой
Систем информационной
безопасности _____ /Остапенко А.Г./

Руководитель ОПОП _____ /Остапенко А.Г./

Воронеж 2021

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 «Планирование и управление информационной безопасностью» относится к дисциплинам обязательной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Планирование и управление информационной безопасностью» направлен на формирование следующих компетенций:

ОПК-9.1 - Способен формировать, внедрять и обеспечивать функционирование системы менеджмента информационной безопасности телекоммуникационных систем и сетей

ОПК-9.2 - Способен реализовывать комплекс организационных мероприятий по обеспечению информационной безопасности и устойчивости телекоммуникационных систем и сетей

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-9.1	знать процессы и методы планирования системы управления информационной безопасностью телекоммуникационных систем;
	уметь определять и обосновывать активы, ресурсы, роли для процессов системы управления информационной безопасностью телекоммуникационных систем; определять возможность применения соответствующего математического аппарата при использовании количественных и качественных методов оценки рисков

	владеть навыками формирования и описания процессов системы управления информационной безопасностью телекоммуникационных систем
ОПК-9.2	знать процессы и методы проверки функционирования и совершенствования системы организационного управления информационной безопасностью телекоммуникационных систем;
	уметь определять и обосновывать активы, ресурсы, роли для процессов системы управления информационной безопасностью телекоммуникационных систем

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Планирование и управление информационной безопасностью» составляет 8 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		9	10
Аудиторные занятия (всего)	126	54	72
В том числе:			
Лекции	72	36	36
Практические занятия (ПЗ)	54	18	36
Самостоятельная работа	162	18	144
Виды промежуточной аттестации - зачет, зачет с оценкой	+	+	+
Общая трудоемкость: академические часы зач.ед.	 288 8	 72 2	 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	Прак зан.	СРС	Всего, час
1	Общая модель управления информационной безопасностью объекта	Термины и определения: информационная безопасность телекоммуникационной системы, управление (менеджмент) информационной безопасностью телекоммуникационной системы, система управления (менеджмента) информационной безопасностью, риск информа-	12	8	26	46

		ционной безопасности, мониторинг информационной безопасности телекоммуникационной системы. Области обеспечения информационной безопасности (ИБ) объекта. Различные подходы по управлению ИБ в зависимости от категории защищаемых информационных информационных активов. Процессный подход к управлению телекоммуникационной системой. Иерархия управления (управление основными процессами телекоммуникационной системы, управление ИБ). Система управления ИБ телекоммуникационной системы – часть системы управления ИБ организации. Общая модель системы управления (менеджмента) ИБ телекоммуникационной системы. Принципы корпоративного управления ИБ: установление безопасности в масштабах организации; принятие подхода, основанного на риске; соответствие внутренним и внешним требованиям; поддержка безопасности среды; проверка эффективности ИБ по отношению к результатам бизнеса (деятельности). Обязательства руководства в отношении ИБ. Распределение ролей и обязанностей по обеспечению ИБ.				
2	Планирование системы управления ИБ телекоммуникационной системы	Определение контекста телекоммуникационной системы. Определение области действия системы управления (менеджмента) ИБ телекоммуникационной системы. Политика ИБ объекта, частью информационной сферы которого является телекоммуникационная система. Принципы формирования политики ИБ объекта: соответствие целям объекта; определение целей ИБ объекта и телекоммуникационных систем; установление структуры, поддерживающей цели ИБ; постоянное совершенствование системы управления ИБ. Стратегии оценки рисков ИБ (базовая, детальная, комбинированная). Определение критериев оценки рисков ИБ и критериев принятия рисков ИБ. Идентификация рисков ИБ: определение и оценка активов, анализ и оценка угроз ИБ, анализ и оценка уязвимостей ИБ. Анализ рисков ИБ: оценка потенциаль-	12	8	26	46

		ных последствий реализации идентифицированных рисков ИБ; оценка вероятности появления идентифицированных рисков ИБ, определение уровня идентифицированных рисков ИБ в соответствии с критериями оценки рисков ИБ. Оценивание рисков ИБ в соответствии с критериями принятия рисков ИБ. Выбор вариантов обработки рисков ИБ и определение защитных мер, необходимых для реализации выбранных вариантов обработки рисков ИБ. Формирование политики ИБ телекоммуникационной системы. Формирование плана реализации защитных мер телекоммуникационной системы, определяющего необходимые ресурсы и сроки. Принятие остаточных рисков ИБ.				
3	Поддержка и функционирование системы управления ИБ телекоммуникационной системы	Реализация защитных мер. Техническое обслуживание, сопровождение защитных мер. Требования к эксплуатационной документации. Осведомление об ИБ. Обучение персонала ИБ. Способы реализации программ обучения ИБ и осведомления об ИБ. Управление изменениями телекоммуникационной системы, влияющими на ИБ. Управление инцидентами ИБ. Подготовка к управлению инцидентами ИБ. Обнаружение и анализ инцидентов ИБ. Сдерживание и устранение инцидента ИБ. Извлечение уроков из инцидентов ИБ. Обеспечение непрерывности функционирования телекоммуникационных систем и восстановление систем после прерываний. Периодическая оценка и обработка рисков ИБ. Управление (менеджмент) безопасностью сетей. Управление ИБ сетевых ресурсов и сетевых сервисов. Сетевой мониторинг. Роли и обязанности, связанные с обеспечением сетевой безопасности.	12	8	26	46
4	Проверка функционирования системы управления ИБ телекоммуникационной системы	Мониторинг и контроль системы управления ИБ телекоммуникационной системы. События и процессы, регистрируемые при мониторинге ИБ. Способы реализации системы мониторинга ИБ (системы мониторинга со сбором данных в сегментах телекоммуникационной системы, системы мониторинга ИБ с первичным анализом данных в	12	10	28	50

		сегментах телекоммуникационной системы, системы мониторинга с анализом данных в сегментах). Проверка соответствия системы управления ИБ телекоммуникационной системы требованиям в отношении системы управления ИБ. Проверка соответствия системы управления ИБ телекоммуникационной системы с помощью аудита ИБ. Виды аудита ИБ. Принципы аудита ИБ. Источники и методы получения свидетельств аудита ИБ. Управление программой аудита ИБ. Виды оценки ИБ телекоммуникационных систем (процессноориентированная, рискориентированная). Анализ системы управления ИБ телекоммуникационной системы со стороны руководства. Входные и выходные данные анализа системы управления ИБ телекоммуникационной системы со стороны руководства. Формирование корректирующих мер в отношении системы управления ИБ телекоммуникационной системы				
5	Совершенствование системы управления ИБ телекоммуникационной системы	Реализация улучшений и изменений (корректирующих и превентивных действий) в отношении ИБ телекоммуникационной системы. Информирование об изменениях и их согласование с заинтересованными сторонами. Оценка достижения поставленных целей системы управления ИБ телекоммуникационной системы	12	10	28	50
6			12	10	28	50
		Итого	**72**	**54**	**162**	**288**

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-9.1	знать процессы и методы планирования системы управления информационной безопасностью телекоммуникационных систем;	знание процессов и методик планирования системы управления информационной безопасностью телекоммуникационных систем;	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь определять и обосновывать активы, ресурсы, роли для процессов системы управления информационной безопасностью телекоммуникационных систем; определять возможность применения соответствующего математического аппарата при использовании количественных и качественных методов оценки рисков	умение определять и обосновывать активы, ресурсы, роли для процессов системы управления информационной безопасностью телекоммуникационных систем; определять возможность применения соответствующего математического аппарата при использовании количественных и качественных методов оценки рисков	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками формирования и описания процессов системы управления информационной безопасностью телекоммуникационных систем	владение навыками формирования и описания процессов системы управления информационной безопасностью телекоммуникационных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-9.2	знать процессы и методы проверки функционирования и совершенствования системы организационного управления информационной безопасностью телекоммуникационных систем;	знание процессы и методы проверки функционирования и совершенствования системы организационного управления информационной безопасностью телекоммуникационных систем;	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь определять и обосновывать активы, ресурсы, роли для процессов системы управления информационной безопасностью телекоммуникационных систем	умение определять и обосновывать активы, ресурсы, роли для процессов системы управления информационной безопасностью телекоммуникационных систем	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 9, 10 семестре для очной формы обучения по двух/четырехбалльной системе:

«зачтено»

«не зачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено

ОПК-9.1	знать процессы и методы планирования системы управления информационной безопасностью телекоммуникационных систем;	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь определять и обосновывать активы, ресурсы, роли для процессов системы управления информационной безопасностью телекоммуникационных систем; определять возможность применения соответствующего математического аппарата при использовании количественных и качественных методов оценки рисков	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеть навыками формирования и описания процессов системы управления информационной безопасностью телекоммуникационных систем	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
ОПК-9.2	знать процессы и методы проверки функционирования и совершенствования системы организационного управления информационной безопасностью телекоммуникационных систем;	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь определять и обосновывать активы, ресурсы, роли для процессов системы управления информационной безопасностью телекоммуникационных систем	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

или
«отлично»;
«хорошо»;
«удовлетворительно»;
«неудовлетворительно».

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл.**	**Неудовл.**
ОПК-9.1	знать процессы и методы планирования системы управления информационной безопасностью телекоммуникационных	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов

	систем;					
	уметь определять и обосновывать активы, ресурсы, роли для процессов системы управления информационной безопасностью телекоммуникационных систем; определять возможность применения соответствующего математического аппарата при использовании количественных и качественных методов оценки рисков	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
	владеть навыками формирования и описания процессов системы управления информационной безопасностью телекоммуникационных систем	Решение прикладных задач в конкретной предметной области	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-9.2	знать процессы и методы проверки функционирования и совершенствования системы организационного управления информационной безопасностью телекоммуникационных систем;	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь определять и обосновывать активы, ресурсы, роли для процессов системы управления информационной безопасностью телекоммуникационных систем	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 (управ-

ления). 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 тех-

нической 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 защиты 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

1. Дайте определение понятия «система»?
2. Каковы основные свойства системы?
3. В чем заключается системный подход к исследованию объектов?

4. Каковы особенности рассмотрения системного подхода применительно к управлению?

5. Какие элементы процесса могут быть исключены из определения: входные данные процесса, выходные данные процесса, управляющее воздействие, ресурсы?

6. Какие виды деятельности в организации можно назвать процессом (или бизнес-процессом)?

7. Какую роль играют процессы в терминах системного подхода к организации?

8. Кто в организации может и должен определить цели бизнес-процессов?

9. Что понимается под ресурсами в рамках определения понятия процесса?

10. Что понимается под управляющим воздействие в рамках определения понятии процесса?

11. В чем заключайся процессный подход?

12. Дайте определение понятия «управление» с позиций системного подхода.

13. Дайте определение понятия «менеджмент».

14. В чем отличия понятий «управление» и «менеджмент»?

15. Каковы основные функции управления?

16. Что такое метод управления?

17. Что такое система управления?

18. Что такое система управления, основанная на процессном подходе?

19. Каковы особенности рассмотрения процессного подхода применительно к управлению?

20. К каким процессам организации может быть применена циклическая модель PDCA?

7.2.5 Примерный перечень заданий для решения прикладных задач

1. В чем состоят основные преимущества использования циклической модели PDCA?

2. В чем отличие терминов «защита информации» и «информационная безопасность»?

3. Какие свойства ИБ в современных условиях должны приниматься во внимание? Расшифруйте что понимается под каждым из свойств.

4. Какой стандарт (серия стандартов) счал основоположником стандартизации систем управления ИБ?

5. Для организации какой сферы применимы стандарты серии ISO/IEC 27000?

6. Каковы отличительные черты серии стандартов ISO/IEC 27000?

7. Какой из стандартов серии ISO/IEC 27000 содержится руководство к внедрению, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ?

8. В чем состоит основные различия и сходства стандартов ISO/IEC 27001 и ITU-T X.1051?

9. Какой из стандартов серии ISO/IEC 27000 признан каталогом «лучших» практик по ИБ?

10.В каком стандарте серии 1SO/IEC 27000 содержится руководство но внедрению СУИБ?

11.На основании чего может проводиться оценка эффективности СУИБ?

12.Можно ли проводить, аудит (или сертификацию) на соответствие стандарту ISO/IEC 27002 (бывший ISO/IKC 17799)?

13.Каковы основные идеи руководства по аудиту СУИБ и средств управления ИБ, реализованных в СУИБ?

14.Почему подход к приведению аудитов систем менеджмента качества и окружающей среды, изложенный в стандарте ISO/IEC 19011. может быть применен для проведения внутренних аудитов СУИБ?

15.В каком стандарте серии ISO/IEC 27000 описана инфраструктура руководства ИБ?

16.Какой стандарт серии ISO/IEC 27000 рассматривает вопросы управления безопасностью сетей?

17.В чем состоят преимущества использования (учета) требований российских и меж-

дународных стандартов по управлению ИБ при построении СУИБ или отдельных процессов управления ИБ?

18.Каковы преимущества одновременного учета требований стандартов. предъявляемых как к СУИБ в целом, так и стандартов, предъявляющих требования к отдельным процессам, разрабатываемым в рамках СУИБ?

19.В чем состоят основные сходства и различия между стандартами па СУИБ и на отдельные процессы управления ИБ?

20.Какие методы и средства ОИБ для ИГ рассматриваются в стандартах ISO/IEC 13335 и идентичных им ГОСТ Р ИСО/МЭК 13335?

21.Как оценивается ИБ ИГ согласно стандартам ISO/IEC 15408 и 18045 и идентичных им ГОСТ Г ИСО/МЭК?

22.Какие из рассмотренных стандартов затрагивают аспекты анализа рисков ИБ?

23.Каковы основные цели построения системы УНБ, соответствующей требованиям стандартов BS 25999 и 25777?

24.В чем может заключаться различие между требованиями *к* системам управления непрерывностью бизнеса и к процессу управления непрерывностью бизнеса?

25.Каковы основные цели следования модели PDCA при построении процесса управления инцидентами ИБ в соответствии с требованиями ГОСТ Р ИСО/МЭК ТО 18044?

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

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 набрал 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	Общая модель управления информационной безопасностью объекта	ОПК-9.1, ОПК-9.2	Тест, защита практических работ
2	Планирование системы управления ИБ телекоммуникационной системы	ОПК-9.1, ОПК-9.2	Тест, защита практических работ
3	Поддержка и функционирование системы управления ИБ телекоммуникационной системы	ОПК-9.1, ОПК-9.2	Тест, защита практических работ
4	Проверка функционирования	ОПК-9.1, ОПК-9.2	Тест, защита практических работ

	системы управления ИБ телекоммуникационной Системы		
5	Совершенствование системы управления ИБ телекоммуникационной системы	ОПК-9.1, ОПК-9.2	Тест, защита практических работ
6	Общая модель управления информационной безопасностью объекта	ОПК-9.1, ОПК-9.2	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.

2. Проверка и оценка деятельности по управлению информационной безопасностью: Учебное пособие / Милославская Н. Г. - Москва: Горячая линия - Телеком, 2012. - 166 с.

Дополнительная литература

1.Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие / Милославская Н. Г. - Москва: Горячая линия - Телеком, 2012. - 214 с.

2. Управление инцидентами информационной безопасности и непрерывностью бизнеса : Учебное пособие / Милославская Н. Г. - Москва: Горячая

линия - Телеком, 2012. - 170 с.

3. Управление рисками информационной безопасности: Учебное пособие / Милославская Н. Г. - Москва : Горячая линия - Телеком, 2012. - 130 с.

4. 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

5. 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

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://www.eios.vorstu.ru (электронная информационно-обучающая система ВГТУ)
http://e.lanbook.com/ (ЭБС Лань)
http://znanium.com/ (ЭБС Знаниум)
http://IPRbookshop.ru/ (ЭБС IPRbooks (Айбукс))

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума

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

По дисциплине «Планирование и 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 по следующим направлениям:

1.Модель решётки

2.Дискреционное управлением доступом

(модели Харрисона-Руззо-Ульмана и типизированная матрицы доступов)

3.Управление распространением прав доступа на основе классической модели Take-Grant

4.Управление распространением прав доступа на основе расширенной модели Take-Grant

5.Модель Белла-ЛаПадулы. Мандатное управление доступом

6. Ролевое и мандатное ролевое управление доступом

7. Изучение средств управления безопасностью на уровне операционной системы на примере Windows Server 2008.

8. Управления учетными записями пользователей

9. Изучение средств управления безопасностью на уровне операционной системы на примере Windows Server 2008.

10. 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, зачетом с оценкой три дня эффективнее всего использовать для повторения и систематизации материала.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП
1	2	3	4