МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета _____ С.М. Пасмурнов
«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Управление рисками в распределённых информационных системах»

Специальность 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет

Форма обучения очная

Год начала подготовки 2016

Автор программы _____ /Д. Т. Пономарев /

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

Руководитель ОПОП _____ / А. Т. Остапенко /

Воронеж 2017

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины является подготовка специалистов, обладающих теоретическими знаниями и практическими навыками в области управления рисками, а также формирование профессиональных и профессиональных специальных компетенций которые позволят им принимать эффективные управленческие решения в области обеспечения информационной безопасности распределенных информационных систем.

1.2. Задачи освоения дисциплины

- сформировать у студентов представления об основных методах развития риск-менеджмента в современных условиях; теоретическим основам управления рисками, позволяющим им овладеть современными инструментами и технологиями управления рисками, комплексным подходом к рассмотрению проблем стратегического управления организацией с точки зрения обеспечения информационной безопасности и принятию эффективных управленческих решений;
- организовать учебный процесс в части формирования способности студента разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы;
- реализовать полный объём работ направленных на приобретение студентами способностей, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлением мониторинга и аудита безопасности автоматизированной системы;
- формирование навыков удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах;

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Управление рисками в распределённых информационных системах» относится к дисциплинам вариативной части (дисциплина по выбору) блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Управление рисками в распределённых информационных системах» направлен на формирование следующих компетенций:

ПК-4 - способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы;

ПК-28 - способностью управлять информационной безопасностью автоматизированной системы;

ПСК-7.4 - способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных

информационных системах;

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-4	знать основные элементы, источники и параметры среды распространения информативного сигнала с целью выявления количественных и качественных параметров оценки силы (опасности) и вероятности проявления угроз нарушения ИБ АС
	уметь разрабатывать модели угроз и модели нарушителя объекта информатизации
ПК-28	знать современные подходы к управлению ИБ и направления их развития, а также основные стандарты, регламентирующие управление ИБ
	уметь, используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность
	владеть навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ;
ПСК-7.4	знать функции операционных систем, позволяющие получить удалённый доступ к компьютеру через Интернет или ЛВС и производить управление и администрирование удалённого компьютера в реальном времени.
	владеть навыками удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Управление рисками в распределённых информационных системах» составляет 13 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры		
		7	8	9
Аудиторные занятия (всего)	186	54	72	60
В том числе:				
Лекции	112	36	36	40
Практические занятия (ПЗ)	74	18	36	20
Самостоятельная работа	246	108	54	84
Курсовой проект	+	+		
Часы на контроль	36	-	-	36

Виды промежуточной аттестации - экзамен, зачет	+	+	+	+
Общая трудоемкость: академические часы зач.ед.	 468 13	 162 4.5	 126 3.5	 180 5

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	Понятие распределённых систем и методы оценки информационных рисков	Понятие распределенной системы. Преимущества и недостатки распределенных систем. Масштабируемость. Прозрачность. Аппаратные и программные средства построения распределенных систем. Синхронизация времени в распределенных системах. Необходимость. Алгоритм Кристиана. Алгоритм Беркли. Децентрализованный алгоритм. Логическое время. Распределенная обработка данных в современных СУБД Методы оценки рисков информационной безопасности: CORAS, OCTAVE, RiskWatch, матричный метод.	20	12	40	72
2	Модель угроз и нарушителя безопасности в РКС	Характеристики безопасности данных, обрабатываемых в типовых информационных системах. Способы и характеристика источника угроз нарушения целостности, доступности и конфиденциальности данных. Описание каналов атак. Тип нарушителя при использовании криптографических средств защиты информации.	20	12	40	72
3	Реализация частных политик информационной безопасности автоматизированной системы	Назначение, цели создания и эксплуатации АС как объекта информатизации. Категории пользователей АС, режимы использования и уровни доступа к информации. Уязвимость основных компонентов АС. Угрозы информационной безопасности и их источники. Неформальная модель возможных нарушителей. Защита	18	12	40	70

		информации от утечки по техническим каналам. Управление системой обеспечения информационной безопасности				
4	Методы принятия решений при управлении ИБ в РКС в условиях риска	Методы выбора решений, основанные на использовании отношения функций правдоподобия. Непараметрические методы выбора решений Упорядочение и отбор признаков для выбора решений. Выбор решения в задаче стохастического управления Марковской динамической системы.	18	12	42	72
5	Методы принятия решений при управлении ИБ в РКС в условиях конфликта	Методы обобщённого градиента в безусловной негладкой локально-выпуклой задаче выбора решений. Конечно-разностный метод минимизации критериальных функций. Метод наискорейшего спуска. Минимаксная задача как задача математического программирования.	18	12	42	72
6	Инструменты управления удаленными серверами и приложениями с позиций ИБ в ОС Windows и Linux	*ОС Windows:* Инструменты для сертификатов Active Directory (AD CS), Инструменты DHCP сервера, Инструменты DNS сервера, Инструменты файловых услуг, Инструменты управления групповой политикой, Инструменты Hyper-V, Инструменты управления IP-адресами (IPAM), Инструменты сервера SMTP, Инструменты управления ресурсами системы Windows *ОС Linux:*SElinux. Методы разграничения доступа. Архитектура. Политики.	18	14	42	74
		Итого	**112**	**74**	**246**	**432**

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 предусматривает выполнение курсового проекта в 7 семестре для очной формы обучения.

Примерная тематика курсового проекта:

«Оптимизация защищённости РИС организации на основе анализа рисков»

Организации выбираются индивидуально для каждого студента.

Задачи, решаемые при выполнении курсового проекта:

• Сформировать знания по теоретическим и методологическим положениям теории информационных рисков.

• Изучить отечественную и зарубежную нормативную правовую базу по оценке рисков нарушения информационной безопасности.

• Приобрести практический опыт использования программ и программных комплексов, реализующих методы анализа информационных рисков.

Курсовой проект включат в себя графическую часть и расчетно-пояснительную записку.

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».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-4	знать основные элементы, источники и параметры среды распространения информативного сигнала с целью выявления количественных и качественных параметров оценки силы (опасности) и вероятности проявления угроз нарушения ИБ АС	знание актуальных угроз связанных с НСД к информации, осуществляемых при непосредственном физическом доступе к средствам АС	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	уметь разрабатывать модели угроз и модели нарушителя объекта информатизации	умение разрабатывать модели защиты информации, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты предусмотренных для соответствующего класса данных	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-28	знать современные подходы к управлению ИБ и направления их развития, а также основные стандарты, регламентирующие управление ИБ	знание современных подходов к управлению ИБ и направления их развития, а также основные стандарты, регламентирующие управление ИБ	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь, используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность	умение разрабатывать процессы управления ИБ, учитывающих особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ	владение навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ;	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПСК-7.4	знать функции операционных систем, позволяющие получить удалённый доступ к компьютеру через Интернет или ЛВС и производить управление и администрирование удалённого компьютера в реальном времени.	знание функций операционных систем, позволяющие получить удалённый доступ к компьютеру через Интернет или ЛВС и производить управление и администрирование удалённого компьютера	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	владеть навыками удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах.	владение навыками удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах.	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 7, 8, 9 семестре для очной формы обучения по двух/четырехбалльной системе:

«зачтено»

«не зачтено»

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ПК-4	знать основные элементы, источники и параметры среды распространения информативного сигнала с целью выявления количественных и качественных параметров оценки силы (опасности) и вероятности проявления угроз нарушения ИБ АС	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь разрабатывать модели угроз и модели нарушителя объекта информатизации	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-28	знать современные подходы к управлению ИБ и направления их развития, а также основные стандарты, регламентирующие управление ИБ	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь, используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

	оценивать их эффективность			
	владеть навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ;	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПСК-7.4	знать функции операционных систем, позволяющие получить удалённый доступ к компьютеру через Интернет или ЛВС и производить управление и администрирование удалённого компьютера в реальном времени.	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	владеть навыками удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах.	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

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

Компе-тенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл.**	**Неудовл.**
ПК-4	знать основные элементы, источники и параметры среды распространения информативного сигнала с целью выявления количественных и качественных параметров оценки силы (опасности) и вероятности проявления угроз нарушения ИБ АС	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь разрабатывать модели угроз и	Решение стандартных практических задач	Задачи решены в полном объеме и	Продемонстрирован верный ход решения всех,	Продемонстрирован верный ход решения в	Задачи не решены

	модели нарушителя объекта информатизации		получены верные ответы	но не получен верный ответ во всех задачах	большинстве задач	
ПК-28	знать современные подходы к управлению ИБ и направления их развития, а также основные стандарты, регламентирующие управление ИБ	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь, используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность	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 анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ;	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
ПСК-7.4	знать функции операционных систем, позволяющие получить удалённый доступ к компьютеру через Интернет или ЛВС и производить управление и администрирование удалённого компьютера в реальном времени.	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	владеть навыками удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах.	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

(минимум 10 вопросов для тестирования с вариантами ответов)

1. Что такое риск?

а) разновидность ситуации, объективно содержащая высокую вероятность невозможности осуществления цели

б)наличие факторов, при которых результаты действий не являются детерминированными, а степень возможного влияния этих факторов на результаты неизвестна

в) следствие действия либо бездействия, в результате которого существует реальная возможность получения неопределенных результатов различного характера+

2. Какие потери можно обозначить как трудовые?

а) потери рабочего времени+

б) уменьшение выручки вследствие снижения цен на реализуемую продукцию

в) уплата дополнительных налогов

г) невыполнение сроков сдачи объекта

д) потери материалов

е) ущерб здоровью

ж) потери сырья

з) ущерб репутации

и) выплата штрафа

3. Какие компании называют кэптивными?

а) универсальные страховые;

б) специализированные страховые;

в) ведомственные страховые.+

4.Какие потери можно считать финансовыми?

а) потери ценных бумаг+

б) потери сырья

в) невыполнение сроков сдачи объекта

г) выплата штрафа+

д) уплата дополнительных налогов+

е) уменьшение выручки вследствие снижения цен на реализуемую продукцию+

5.Факторы, которые влияют на уровень финансовых рисков подразделяются на:

а) объектные и субъектные;+

б) позитивные и негативные;

в) простые и сложные.

6. Какие потери можно отнести к потерям времени

а) невыполнение сроков сдачи объекта+

б) потери ценных бумаг

в) выплата штрафа

г) уменьшение выручки вследствие снижения цен на реализуемую продукцию
д) уплата дополнительных налогов

7. Как называется процесс использования механизмов уменьшения рисков?
а) диверсификация;
б) лимитирование;
в) хеджирование.+

8.Что такое анализ риска?
а) систематизация множества рисков на основании каких-либо признаков и критериев, позволяющих объединить подмножества рисков в более общие понятия
б) систематическое научное исследование степени риска, которому подвержены конкретные объекты, виды деятельности и проекты+
в) начальный этап системы мероприятий по управлению рисками, состоящий в систематическом выявлении рисков, характерных для определенного вида деятельности, и определении их характеристик

9. Что является принципом действия механизма диверсификации?
а) избежание рисков;
б) разделение рисков;+
в) снижение рисков.

10. Что такое идентификация риска?
а) систематизация множества рисков на основании каких-либо признаков и критериев, позволяющих объединить подмножества рисков в более общие понятия
б) начальный этап системы мероприятий по управлению рисками, состоящий в систематическом выявлении рисков, характерных для определенного вида деятельности, и определении их характеристик+
в) систематическое научное исследование степени риска, которому подвержены конкретные объекты, виды деятельности и проекты

11. Под максимальным объемом страховой защиты предприятия по конкретным видам страхуемых финансовых рисков понимается:
а) страховой тариф;
б) страховая сумма;+
в) страховая премия.

12. Как называются риски, которые могут нести в себе как потери, так и дополнительную прибыль?
а) чистыми
б) критическими
в) спекулятивными+

13. На какие виды подразделяются риски по уровню финансовых потерь?
а) допустимый, критический и катастрофический;+
б) недопустимый, допустимый и критический;
в) критический, катастрофический и недопустимый.

14. Что такое последствия риска?

а) скорее положительными
б) как положительными, так и отрицательными+
в) только отрицательными

15. Как называются риски, которые практически всегда несут в себе потери?
а) критическими
б) спекулятивными
в) чистыми+

16. В основе какой из ниже предложенных операции лежит обмен финансовыми активами или обязательствами для улучшения их структуры и снижения возможных потерь:
а) своп;+
б) хеджирование;
в) репо.

17. Как называются риски, которые обусловлены деятельностью самого предприятия и его контактной аудиторией?
а) внешними
б) внутренними+
в) чистыми

18. Как называются риски, в результате реализации которых предприятию грозит потеря прибыли?
а) катастрофическими
б) критическими
в) допустимыми+

19.Чем измеряется величина или степень риска?
а) средним ожидаемым значение
б) изменчивостью возможного результата
в) оба варианта верны+

20. В чем состоит социально-экономическая функция риска?
а) в том, что в процессе рыночной деятельности риск и конкуренция позволяет выделить социальные группы эффективных собственников в общественных классах, а в экономике – отрасли деятельности, в которых риск приемлем+
б) в том, что реализация риска может обеспечить дополнительную по сравнению с плановой прибыль в случае благоприятного исхода
в) оба варианта верны

7.2.2 Примерный перечень заданий для решения стандартных задач

(минимум 10 вопросов для тестирования с вариантами ответов)

1. Управление риском - это:

а) отказ от рискованного проекта;

б) комплекс мер, направленных на снижение вероятности реализации риска;

в) комплекс мер, направленных на компенсацию, снижение, перенесение, уход или принятие риска;+

г) комплекс мероприятий, направленных на подготовку к реализации риска.

2. Содержательная сторона управления рисками включает в себя:

а) планирование деятельности по реализации рискованного проекта;

б) сравнение вероятностей и характеристик риска, полученных в результате оценки и анализа риска;+

3. Что из перечисленного не является элементом системы управления рисками?

а) выявление расхождений в альтернативах риска;

б) разработка планов, позволяющих действовать оптимальным образом в ситуации риска;

в) разработка конкретных мероприятий, направленных на минимизацию или устранение негативных последствий;

г) учет психологического восприятия рискованных проектов;

д) ни один из вариантов не являются элементом системы риск-менеджмента;

е) все перечисленные варианты является элементами системы риск-менеджмента.+

4. Что представляет собой стандарт ISO/IEC 27799?

а) Стандарт по защите персональных данных о здоровье;+

б) Новая версия BS 17799;

в) Определения для новой серии ISO 27000;

г) Новая версия NIST 800-60

5. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?

а) NIST и OCTAVE являются корпоративными;

б) NIST и OCTAVE ориентирован на ИТ;+

в) AS/NZS ориентирован на ИТ;

г) NIST и AS/NZS являются корпоративными;

6. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?

а) Анализ связующего дерева;

б) AS/NZS;

в) NIST;

г) Анализ сбоев и дефектов;+

7. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

а). Список стандартов, процедур и политик для разработки программы безопасности

б). Текущая версия ISO 17799

в). Структура, которая была разработана для снижения внутреннего мошенничества в компаниях

г). Открытый стандарт, определяющий цели контроля +

8. Из каких четырех доменов состоит CobiT?

а).Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка +

б). Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

в). Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка

г). Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

9. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?

а). COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам

б). COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень+

в).COSO учитывает корпоративную культуру и разработку политик
г). COSO – это система отказоустойчивости

10. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

а). Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
б). Когда риски не могут быть приняты во внимание по политическим соображениям
в). Когда необходимые защитные меры слишком сложны
г). Когда стоимость контрмер превышает ценность актива и потенциальные потери +

7.2.3 Примерный перечень заданий для решения прикладных задач

(минимум 10 вопросов для тестирования с вариантами ответов)

1. Виды информационной безопасности:

1. Персональная, корпоративная, государственная+
2. Клиентская, серверная, сетевая
3. Локальная, глобальная, смешанная

2. Цели информационной безопасности – своевременное обнаружение, предупреждение:

1. несанкционированного доступа, воздействия в сети+
2. инсайдерства в организации
3. чрезвычайных ситуаций

3. Основные объекты информационной безопасности:

1. Компьютерные сети, базы данных+
2. Информационные системы, психологическое состояние пользователей
3. Бизнес-ориентированные, коммерческие системы

4. Основными рисками информационной безопасности являются:

1. Искажение, уменьшение объема, перекодировка информации
2. Техническое вмешательство, выведение из строя оборудования сети
3. Потеря, искажение, утечка информации+

5. К основным принципам обеспечения информационной безопасности относится:

1. Экономической эффективности системы безопасности+
2. Многоплатформенной реализации системы
3. Усиления защищенности всех звеньев системы

6. Почему количественный анализ рисков в чистом виде не достижим?

1. Он достижим и используется
2. Он присваивает уровни критичности. Их сложно перевести в денежный вид.
3. Это связано с точностью количественных элементов
4. Количественные измерения должны применяться к качественным элементам +

7. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

1. Много информации нужно собрать и ввести в программу +
2. Руководство должно одобрить создание группы
3. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
4. Множество людей должно одобрить данные

8. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

1. Список стандартов, процедур и политик для разработки программы безопасности
2. Текущая версия ISO 17799

3. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
4. Открытый стандарт, определяющий цели контроля+

9. Из каких четырех доменов состоит CobiT?

1. Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка +
2. Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
3. Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
4. Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

10. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?

1. COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам
2. COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень+
3.COSO учитывает корпоративную культуру и разработку политик
4. COSO – это система отказоустойчивости

7.2.4 Примерный перечень вопросов для подготовки к зачету

Укажите вопросы для зачета

1. Привести примеры задач принятия решений.

2. Классифицировать задачи принятия решений. Чем один тип задач отличается от другого?

3.Охарактеризовать роль лица, принимающего решения, экспертов, консультантов в задачах принятия решений.

4. Привести примеры задач оценивания.

5. Привести общую схему алгоритма экспертизы.

6. Описать основные этапы экспертизы.

7. Какие основные предположения должны выполняться при проведении групповой экспертизы?

8. Охарактеризовать основные шкалы измерения.

9. Описать основные форы опроса экспертов, взаимодействия экспертов при опросе.

10. Каким образом подбирают экспертов? По каким критериям оценивают экспертов?

11. Построить структурную схему метода Дельфи.

12. Описать способы оценивания компетентности экспертов.

13. Как оценить связь между достижением двух различных целей при проведении одной совокупности мероприятий?

14. Как оценить взаимосвязь между ранжировками?

15. Составить алгоритм оценивания согласованности мнений экспертов.

16. Описать методы формирования исходного множества альтернатив.

17. Семь сравниваемых альтернатив эксперт расположил в порядке уменьшения их важности: представить данную ранжировку с помощью стандартизованных рангов.

18. Что такое область компромиссов, область согласия, множество Парето, множество эффективных решений? Как выделяют область компромиссов? Предложить алгоритмы построения паретовского множества для выпуклого и невыпуклого случаев, используя модели их описания.

19. Описать признаки и свойства методов решения многокритериальных задач принятия решений. Провести классификацию методов многокритериальной оценки альтернатив и методов решения многокритериальных задач принятия решений.

20. Охарактеризовать аксиоматические методы многокритериальной оценки альтернатив. Какие аксиомы применяются в этих методах? Указать способы проверки аксиом.

21. Какие принципы оптимальности используются в прямых методах многокритериальной оценки альтернатив?

22. Определить нормализованную задачу без приоритета.

23. Каковы основные приемы нормализации критериев?

24. Как определяется важность критериев?

253

25. Как корректируются принципы оптимальности при различной важности критериев?

26. Выделить роль ЛПР при реализации различных принципов оптимальности и предложить диалоговые варианты реализации принципов оптимальности.

27. Какие принципы оптимальности инвариантны к единицам измерения критериев?

28. Какие принципы оптимальности используют минимальную информацию о взаимной важности критериев?

29. Предложить различные постановки задач оптимизации на основе комбинирования принципов оптимальности.

30. Построить структурные схемы методов порогов несравнимости. К каким решениям могут приводить данные методы?

31. Предложить модификацию метода простых ограничений.

32. Построить структурную схему метода аналитической иерархии.

33. Модифицировать метод аналитической иерархии, предложив иные способы оценки весового вектора.

34. Привести содержательные примеры задач, решаемых с помощью принципов оптимальности, метода аналитической иерархии, метода ограничений

35. Чем различаются задачи принятия решений при риске и при определенности? В чем состоит неопределенность задачи принятия решений при риске?

36. Описать основные особенности однокритериальной модели принятия решений при риске. Привести постановку задачи принятия решений. Построить обобщенную структурную схему однокритериальной задачи принятия решений при риске.

37. Описать основные особенности многокритериальной модели

принятия решений при риске. Привести постановку задачи принятия решений. Построить обобщенную структурную схему двухуровневой многокритериальной задачи принятия решений при риске.

38. Какова роль ЛПР в задачах принятия решений при риске?

39. В чем заключается неопределенность задачи принятия решений при риске? Как преодолевается эта неопределенность?

40. Каковы виды априорной информированности ЛПР в задачах принятия решений при риске?

41. С помощью каких критериев преодолевается неопределенность задач принятия решений при риске? Каковы преимущества и недостатки этих критериев?

42. В чем состоит преимущество комбинированного критерия?

43. Как используются принципы оптимальности в задачах принятия решений при риске?

44 . Как можно использовать методы принятия решений при определенности в задачах принятия решений при риске?

45. Дайте классификацию задачам оптимизации с точки зрения вида целевой функции и ограничений.

46. Приведите формальную постановку задачи оптимизации.

7.2.5 Примерный перечень заданий для решения прикладных задач

Понятие распределённых систем и методы оценки информационных рисков Понятие распределенной системы. Преимущества и недостатки распределенных систем. Масштабируемость. Прозрачность. Аппаратные и программные средства построения распределенных систем. Синхронизация времени в распределенных системах. Необходимость. Алгоритм Кристиана. Алгоритм Беркли. Децентрализованный алгоритм. Логическое время. Распределенная обработка данных в современных СУБД Методы оценки рисков информационной безопасности: CORAS, OCTAVE, RiskWatch, матричный метод.

Модель угроз и нарушителя безопасности в РКС Характеристики безопасности данных, обрабатываемых в типовых информационных системах. Способы и характеристика источника угроз нарушения целостности, доступности и конфиденциальности данных. Описание каналов атак. Тип нарушителя при использовании криптографических средств защиты информации.

Реализация частных политик информационной безопасности автоматизированной системы Назначение, цели создания и эксплуатации АС как объекта информатизации. Категории пользователей АС, режимы использования и уровни доступа к информации. Уязвимость основных компонентов АС. Угрозы информационной безопасности и их источники. Неформальная модель возможных нарушителей. Защита информации от утечки по техническим каналам. Управление системой обеспечения информационной безопасности

Методы принятия решений при управлении ИБ в РКС в условиях риска

Методы выбора решений, основанные на использовании отношения функций правдоподобия. Непараметрические методы выбора решений Упорядочение и отбор признаков для выбора решений. Выбор решения в задаче стохастического управления Марковской динамической системы.

Методы принятия решений при управлении ИБ в РКС в условиях конфликта Методы обобщённого градиента в безусловной негладкой локально-выпуклой задаче выбора решений. Конечно-разностный метод минимизации критериальных функций. Метод наискорейшего спуска. Минимаксная задача как задача математического программирования.

Инструменты управления удаленными серверами и приложениями с позиций ИБ в ОС Windows и Linux ОС Windows: Инструменты для сертификатов Active Directory (AD CS), Инструменты DHCP сервера, Инструменты DNS сервера, Инструменты файловых услуг, Инструменты управления групповой политикой, Инструменты Hyper-V, Инструменты управления IP-адресами (IPAM), Инструменты сервера SMTP, Инструменты управления ресурсами системы Windows. ОС Linux:SElinux. Методы разграничения доступа. Архитектура. Политики.

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 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	Понятие распределённых систем и методы оценки информационных рисков	ПК-4, ПК-27, ПК-28, ПСК-7.4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
2	Модель угроз и нарушителя безопасности в РКС	ПК-4, ПК-27, ПК-28, ПСК-7.4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

3	Реализация частных политик информационной безопасности автоматизированной системы	ПК-4, ПК-27, ПК-28, ПСК-7.4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
4	Методы принятия решений при управлении ИБ в РКС в условиях риска	ПК-4, ПК-27, ПК-28, ПСК-7.4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
5	Методы принятия решений при управлении ИБ в РКС в условиях конфликта	ПК-4, ПК-27, ПК-28, ПСК-7.4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….
6	Инструменты управления удаленными серверами и приложениями с позиций ИБ в ОС Windows и Linux	ПК-4, ПК-27, ПК-28, ПСК-7.4	Тест, контрольная работа, защита лабораторных работ, защита реферата, требования к курсовому проекту….

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.

Защита курсовой работы, курсового проекта или отчета по всем видам практик осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература

1.Остапенко А.Г. Методология риск-анализа и моделирования кибернетических систем, атакуемых вредоносным программным обеспечением [Электронный ресурс] : Учеб. пособие. - Электрон. текстовые, граф. дан. (112 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 1 файл. - 30-00.

2. Остапенко А.Г. Теория управления рисками информационных систем [Электронный ресурс] : Учеб. пособия. - Электрон. текстовые, граф. дан. (190 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.

Дополнительная литература

1. Методические указания к самостоятельным работам по дисциплинам «Теория управления информационной безопасностью распределенных компьютерных систем», «Управление информационной безопасностью» для студентов специальностей 090301 «Компьютерная безопасность», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: К. А. Разинкин, А. А. Голозубов. - Электрон. текстовые, граф. дан. (925 Кб). - Воронеж : ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

2. Савинков, А.Ю. Управление процессами в современных операционных системах : учеб. пособие. - Воронеж : ВГТУ, 2002. - 141 с. - 25.00.

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://att.nica.ru
http://www.edu.ru/
http://window.edu.ru/window/library
http://www.intuit.ru/catalog/
https://marsohod.org/howtostart/marsohod2
http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp
https://cchgeu.ru/education/cafedras/kafsib/?docs
http://www.eios.vorstu.ru
http://e.lanbook.com/ (ЭБС Лань)
http://IPRbookshop.ru/ (ЭБС IPRbooks)

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 практикума.

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

По дисциплине «Управление рисками в распределённых информационных системах» 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 следующих практических навыков:

1. Проектирование распределенной базы данных.
2. Аутентификация и управление пользователями в СУБД Oracle.
3. Методики и программные продукты для оценки рисков
4. Построение модели угроз безопасности защищаемого объекта информатизации.
5. Исследование методов и моделей оценки уязвимости информации.
6. Реализация политики безопасности в MS Windows
7. Реализация политики безопасности в Linux
8. Решение практических задач в рамках методов принятия решений при управлении ИБ в РКС в условиях риска.
9. Решение практических задач в рамках методов принятия решений при управлении ИБ в РКС в условиях конфликта.
10. Адресация и маршрутизация в IP-сетях
11. DHCP-сервер: установка и управление
12. DNS-сервер: установка и управление
13. Создание и администрирование учетных записей пользователей и
14. Мандатное разграничение прав в Linux

Занятия проводятся путем решения конкретных задач в аудитории.

Методика выполнения курсового проекта изложена в учебно-методическом пособии. Выполнять этапы курсового проекта должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсового проекта, защитой курсового проекта.

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, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала.