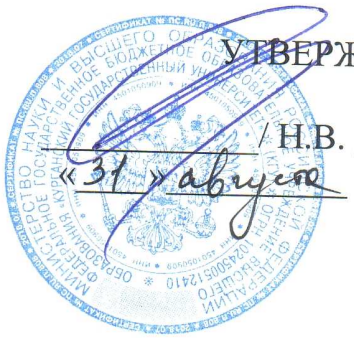
Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»



УТВЕРЖДАЮ:
Ректор
/ Н.В. Дубив/
«31» августа 2020 г.

Рабочая программа учебной дисциплины

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

образовательной программы высшего образования –
программы специалитета
10.05.03 Информационная безопасность автоматизированных систем
Направленность: (специализация №7) обеспечение информационной безопасности распределенных информационных систем
Форма обучения: очная

Курган 2020

Рабочая программа дисциплины «Аудит информационной безопасности» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» (Обеспечение информационной безопасности распределенных информационных систем), утвержденным для очной формы обучения «28» августа 2020 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 31 августа 2020 года, протокол № 1.

Рабочую программу составил:
ст. преподаватель  В.В. Москвин

Согласовано:

Заведующий кафедрой «БИАС»
канд. пед. наук, доцент  Е.Н. Полякова

Начальник Управления
образовательной деятельности  С.Н. Синицын

Специалист по учебно-методической
работе Учебно-методического
отдела  Г.В. Казанкова

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 4 зачетных единицы трудоемкости (144 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр
		8
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**48**	**48**
Лекции	16	16
Лабораторные работы	16	16
Практические занятия	16	16
Самостоятельная работа, всего часов в том числе:	**96**	**96**
Подготовка к зачету	18	18
Другие виды самостоятельной работы (подготовка к практическим занятиям, лабораторным работам и рубежному контролю)	60	60
Контрольная работа	18	18
Вид промежуточной аттестации	**зачет с оценкой**	**зачет с оценкой**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**144**	**144**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Аудит информационной безопасности» относится к дисциплинам по выбору вариативных дисциплин Блока 1.

Изучение дисциплины базируется на результатах обучения, сформированных при изучении следующих дисциплин:

- Основы информационной безопасности.
- Криптографические методы защиты информации.
- Безопасность сетей ЭВМ.
- Безопасность операционных систем.
- Стандарты информационной безопасности.

Результаты обучения по дисциплине необходимы для выполнения разделов курсового проекта по дисциплине «Разработка и эксплуатация защищенных автоматизированных систем», разделов курсовой работы по дисциплине «Управление информационной безопасностью», а также выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью изучения дисциплины является: приобретение обучаемыми необходимого объема знаний и практических навыков, для проведения анализа состояния безопасности на организационном и техническом уровнях, оценке соответствия политики безопасности компании и организационно-распорядительной документации требованиям нормативных документов и существующим рискам

Задачи дисциплины:

- наиболее полно и объективно научить студентов проводить оценку защищенности информационных ресурсов компании;
- наиболее эффективно разрабатывать политику ИБ;
- идентифицировать, оценивать и ликвидировать уязвимости ИС;
- обеспечивать соответствие ИС требованиям действующего законодательства РФ и международным стандартам.

Компетенции, формируемые в результате освоения дисциплины:

- способность к самоорганизации и самообразованию (ОК-8);
- способность проводить анализ защищенности автоматизированных систем (ПК-3);
- способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);
- способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);
- способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);

- способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы (ПК-19);

- способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

- способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК 7.3).

В результате изучения дисциплины обучающийся должен:

знать:

- основные положения правовой и нормативно-методической базы, регулирующей процессы аудита информационной безопасности организаций различных форм собственности (ПК-3, ПК-16, ПК-17);

- основные виды, способы, принципы и критерии проведения аудитов ИБ (ОК-8, ПК-19, ПК-22);

- порядок, содержание и правила разработки документов, оформляемых на этапе подготовки, в ходе проведения и по результатам аудита ИБ организаций различных форм собственности (для ОК-8, ПК-7, ПК16, ПК-17, ПК- 19);

уметь:

- правильно строить отношения с представителями организаций (структурных подразделений компании), задействованных в проведении аудита ИБ (ПК-7, ПК-16, ПК-17, ПК-19);

- эффективно использовать все виды средств для проведения аудита защищённости информационных систем (ПК-17, ПК-19, ПК-22, ПСК-7.3).

иметь навыки:

- разработки нормативно-методических материалов по регламентации аудита ИБ организаций (ОК-8, ПК-7, ПК-16, ПК-17);

- применения различных способов и методов проведения аудита ИБ организаций (ПК-16, ПК-17, ПК-19, ПСК-7.3).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

Рубеж	Номер раздела, темы	Наименование раздела, темы	Количество часов контактной работы с преподавателем		
			Лекции	Практич. занятия	Лаборатор. работы
Семестр 9					
Рубеж 1	*Введение*	Аудит информационной безопасности (ИБ) – необходимый инструмент обеспечения информационной безопасности в современных условиях.	1	-	-
	1	Процессы и системы.	3	2	-
	2	Аудит информационной безопасности организации и систем.	4	2	2
	3	Исследования полученных оценок ИБ.	2	3	6

Рубеж 2	4	Практика аудита ИБ организаций и систем.	4	4	-
	5	Аудит и доверие ИБ.	2	5	8
		Всего:	**16**	**16**	**16**

4.2. Содержание лекционных занятий

Введение. Аудит информационной безопасности (ИБ) – необходимый инструмент обеспечения информационной безопасности в современных условиях.

Понятия аудита, аттестации, консалтинга и аутсорсинга в области информационной безопасности. ИТ-аудит и аудит информационной безопасности. Цели и задачи проведения аудита. Классификация видов аудита. Нормативная база, используемая при проведении аудита ИБ. Особенности аудита информационной безопасности в России. Этические правила аудитора.

Раздел I. Процессы и системы.

Структура и свойства процессов и систем. Понятие процесса. Методы формализации процессов. Цели и задачи формализации процессов. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ). Основные процессы СУИБ и требования, предъявляемые к ним каждым из стандартов.

Линейная модель управления качеством процессов и систем. Замкнутая циклическая модель менеджмента качества процессов и систем. Обзор моделей безопасности бизнеса. Вводная информация о моделях безопасности.

Способы и цели контроля и проверки процессов и систем. Цели контроля и проверки процессов и систем. Оценка процессов – основа контроля и проверки процессов и систем. Определение входных данных оценки. Роли и обязанности по проведению оценивания. Модель оценки процесса. Мероприятия процесса оценивания и выходные данные оценивания. Факторы успешной оценки процесса. Внутренний и внешний аудит.

Раздел II. Аудит информационной безопасности организации и систем.

Правовые и методологические основы аудита ИБ. Международные правовые аспекты, стандарты и руководства по основам аудита информационной безопасности. Международные организации, курирующие вопросы разработки стандартов и методик аудита, подготовки аудиторов в области ИБ. Национальные стандарты и руководства по основам аудита ИБ. Отечественные законы и стандарты по основам аудита. Обзор программ профессиональной сертификации аудиторов ИБ.

Организация проведения аудита. Планирование аудита информационной безопасности организации. Управление процессом аудита. Практические этапы аудита. Информационное обследование. Анализ соответствия требованиям. Инструментальное обследование защищенности. Анализ рисков. Разработка первоочередных рекомендаций или плана защиты. Виды отчетных документов по результатам проведения аудита. Методы и инструментальные средства анализа защищенности элементов.

Осознание и менеджмент аудита ИБ. Система обеспечения информационной безопасности – совокупность процессов осознания и менеджмента информационной безопасности. Осознание аудита информационной безопасности. Планирование и реализация программы аудита ИБ. Контроль и совершенствование программы аудита ИБ.

Методы оценивания ИБ. Задачи анализа информационных рисков. Основные методики анализа информационных рисков. Базовый и полный анализ рисков. Оценка затрат на информационную безопасность организации. Оценивание ИБ на основе показателей ИБ. Модели зрелости компаний с точки зрения ИБ. Оценивание ИБ на основе моделей зрелости процессов обеспечения ИБ. Затраты на проведение аудита и анализа рисков. Обзор инструментальных средств анализа рисков.

Раздел III. Исследования полученных оценок ИБ.

Оценивание результатов аудита и самооценки информационной безопасности. Оценивание процессов проведения аудита. Риск-ориентированная интерпретация полученных оценок ИБ.

Пассивные и активные методы анализа защищенности. Сканирование и зондирование. Классификация и архитектуры систем анализа защищенности. Средства анализа параметров защиты. Сетевые сканеры безопасности. Сканеры прикладных сервисов. Средства контроля защищенности системного уровня. Сравнительный анализ возможностей современных средств анализа защищенности.

Раздел IV. Практика аудита ИБ организаций и систем.

Особенности аудита ИБ банковской системы. Особенности развития средств и систем автоматизации. Направления обеспечения и оценки информационной безопасности. Размерность и значимость объектов оценки при проведении аудита ИБ. Работы по созданию системы оценки ИБ организаций банковской системы РФ.

Аудит управления непрерывностью бизнеса и восстановления после сбоев. Предпосылки. Основные термины. Методологии, стандарты и нормативные требования в области управления непрерывностью бизнеса. Основные цели аудита. Основные вопросы, рассматриваемые при аудите. Реализация аудита. Заключительные процедуры аудита.

Особенности аудита ИБ, использующих аутсорсинг. Использование аутсорсинга. Перечень услуг и функций, переданных в аутсорсинг. Требования по обеспечению требуемого уровня услуг. Требования по обеспечению физической и логической безопасности. Требования к поставщику услуг. Процедуры взаимодействия компании с поставщиком услуг. Юридические аспекты (содержание и полнота контракта).

Раздел V. Аудит и доверие ИБ.

Аспекты, программы аудита ИБ. Методы доверия. Обеспечение доверия к информационной безопасности. Объект доверия. Критерии доверия. Стадия доверия. Свидетельство доверия.

4.3 Практические занятия

Номер раздела	Наименование раздела, темы	Наименование тем практических занятий	Норматив времени, час.
1	Процессы и системы	Процессы и системы.	2
2	Аудит информационной безопасности организации и систем.	Аудит информационной безопасности организации и систем. Правовые и методологические основы аудита ИБ.	2
3	Исследования полученных оценок ИБ	Исследования оценок ИБ.	2
	1-ый рубежный контроль	***Тестирование***	***1***
4	Практика аудита ИБ организаций и систем	Практика аудита ИБ организаций и систем	4
5	Аудит и доверие ИБ	Аудит и доверие ИБ	4
	2-ой рубежный контроль	***Тестирование***	***1***
	Итого		**16**

4.4. Лабораторные работы

Номер темы	Наименование раздела, темы	Наименование лабораторных работ	Норматив времени, час.
2	Аудит информационной безопасности организации и систем.	Аудит информационной безопасности автоматизированных систем на соответствие требованием стандартов	2
3	Исследования полученных оценок ИБ	Внешний активный аудит информационных систем	3
		Внутренний активный аудит информационных систем	3
5	Аудит и доверие ИБ	Разработка программного комплекса для проведения аудита на соответствие требованиям стандартов ИБ	8
	Итого		**16**

4.5 Контрольная работа

Целью контрольной работы является формирование навыков проведения аудита безопасности информационных систем (ИС).

Задачами проведения аудита информационной безопасности является обучить студентов проводить:

- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов ИС;
- оценка текущего уровня защищенности ИС;
- локализация узких мест в системе защиты ИС;
- оценка соответствия ИС существующим стандартам в области информационной безопасности;
- выработка рекомендаций по внедрению новых и повышению эффектив-

ности существующих механизмов безопасности ИС;
- подготовка отчетных документов.

Каждому студенту выдается индивидуальное задание на контрольную работу. Объем контрольной работы 10-15 страниц.

Примерные темы контрольных работ.

- Внешний аудит ИБ конкретного предприятия (конкретной информационной системы).
- Внутренний аудит ИБ конкретного предприятия (конкретной информационной системы).

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной или практической работы.

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения лабораторных работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале лабораторной работы.

Преподавателем запланировано применение на практических и лабораторных занятиях технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

Для текущего контроля успеваемости по очной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на практических и лабораторных занятиях в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным и практическим занятиям, к рубежным контролям, выполнение контрольной работы и подготовку к зачету с оценкой.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. Час.
Самостоятельное изучение тем раздела	38
Подготовка к практическим занятиям (по 2часа на каждое занятие)	10
Подготовка к лабораторным работам (по 2часа на каждое занятие)	8
Подготовка к рубежным контролям (по 2 часа на каждый рубежный контроль)	4
Контрольная работа	18
Подготовка к зачету	18
Всего:	**96**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ.
2. Отчеты студентов по лабораторным работам.
3. Отчеты студентов по практическим занятиям.
4. Банк тестовых заданий к рубежным контролям № 1, № 2.
5. Контрольная работа.
6. Вопросы к зачету с оценкой

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

№	Наименование	Содержание							
1	Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения студентов на первом учебном занятии)*	Распределение баллов							
		Вид учебной работы:	Посещение лекций	Выполнение и защита отчетов по лабораторным работам	Выполнение практической работы	Защита контрольной работы	Рубежный контроль №1	Рубежный контроль №2	Зачет с оценкой
		Балльная оценка:	$1_б$ x 8=$8_б$	$5_б$ x 4 = $20_б$	$5_б$ x 5 =$25_б$	5	6	6	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета	60 и менее баллов – неудовлетворительно; не зачтено; 61…73 – удовлетворительно; зачтено; 74… 90 – хорошо; 91…100 – отлично							

3	Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов	Для допуска к промежуточной аттестации (зачету с оценкой) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все лабораторные и практические работы, а также контрольную работу. Для получения экзаменационной оценки «автоматически» студенту необходимо набрать следующее минимальное количество баллов: - 68 для получения «автоматически» зачета с оценкой «удовлетворительно». По согласованию с преподавателем студенту, набравшему минимум 68 балл, могут быть добавлены дополнительные (бонусные) баллы за активность на практических занятиях, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения практических и лабораторных работ, за участие в значимых учебных и внеучебных мероприятиях кафедры и выставлена автоматически оценка «хорошо» или «отлично».
4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (зачету с оценкой) набрана сумма менее 50 баллов, студенту необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных лабораторных и практических работ. Формы дополнительных заданий (назначаются преподавателем): - выполнение и защита пропущенной лабораторной или практической работы (при невозможности дополнительного проведения лабораторной или практической работы преподаватель устанавливает форму дополнительного задания по тематике пропущенной работы самостоятельно) – до 5 баллов. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования.

Перед проведением каждого рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. Варианты тестовых заданий состоят для 1 и 2 рубежного контроля из 18 вопросов. На каждое тестирование при рубежном контроле студенту отводится 2 академических часа.

Баллы студенту выставляются в зависимости от числа правильно выбранных ответов. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании. Помножив полученное значение на 100%, можно привести итоговую оценку к традиционной следующим образом:

«неудовлетворительно» – менее 50%

«удовлетворительно» – 50% - 70%

«хорошо» – 70% - 90%

«отлично» – 90% - 100% .

Преподаватель оценивает в баллах результаты тестирования каждого студента по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

Зачет состоит из 2 вопросов. Вопросы к зачету доводятся до студентов на последней лекции в семестре. Каждый вопрос оценивается в 15 баллов. На подготовку ответа студенту отводится 1 астрономический час.

Результаты текущего контроля успеваемости и зачета заносятся преподавателем в зачетную ведомость, которая сдается в организационный отдел института в день зачета, а также выставляются в зачетную книжку студента.

6.4. Примеры оценочных средств для рубежных контролей и зачета

1-ый рубежный контроль

1. *Аудит информационной безопасности – это…*

a. оценка текущего состояния системы информационной безопасности
b. проверка используемых компанией информационных систем, систем безопасности
c. это проверка способности успешно противостоять угрозам
d. специальная проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам

2. *Анализ рисков включает в себя …*

a. набор адекватных контрмер осуществляется в ходе управления рисками
b. анализ причинения ущерба и величины ущерба, наносимого ресурсам ИС, в случае осуществления угрозы безопасности
c. выявление существующих рисков и оценку их величины
d. мероприятия по обследованию безопасности ИС, с целью определения того какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите

3. *Активный аудит – это…*

a. исследование средств для определения соответствия их решениям задач информационной безопасности
b. исследование состояние системы сетевой защиты, использование которой помогает хакеру проникнуть в сети и нанести урон компании
c. исследование состояния защищенности информационной системы с точки зрения хакера (или некоего злоумышленника, обладающего высокой квалификацией в области информационных технологий).

2-ой рубежный контроль

1. *Право доступа к информации – это …*

a. совокупность правил доступа к информации, установленных правовыми документами или собственником либо владельцем информации
b. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям

c. возможность доступа к информации, не нарушающая установленные правила разграничения доступа
d. нарушение установленных правил разграничения доступа
e. лицо или процесс, осуществляющие несанкционированного доступа к информации

2. Идентификация субъекта – это ...

a. процедура распознавания субъекта по его идентификатору
b. проверка подлинности субъекта с данным идентификатором
c. установление того, является ли субъект именно тем, кем он себя объявил
d. процедура предоставления законному субъекту соответствующих полномочий и доступных ресурсов системы
e. установление лиц или процессов, осуществляющих несанкционированного доступа к информации

3. Сертификат продукта, обеспечивающий информационную безопасность, ...

a. подтверждает его соответствие стандарту РФ
b. подтверждает отсутствие в продукте не задекларированных возможностей
c. подтверждает его качество
d. просто является документом, необходимым для реализации продукции

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. ИТ-аудит и аудит информационной безопасности.
2. Классификация видов аудита.
3. Нормативная база, используемая при проведении аудита ИБ.
4. Понятие процесса. Методы формализации процессов.
5. Цели и задачи формализации процессов. Понятие процессного подхода.
6. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ).
7. Основные процессы СУИБ и требования, предъявляемые к ним каждым из стандартов.
8. Оценка процессов – основа контроля и проверки процессов и систем.
9. Определение входных данных оценки. Роли и обязанности по проведению оценивания.
10. Модель оценки процесса.
11. Факторы успешной оценки процесса.
12. Внутренний и внешний аудит.
13. Международные правовые аспекты, стандарты и руководства по основам аудита информационной безопасности.
14. Международные организации, курирующие вопросы разработки стандартов и методик аудита, подготовки аудиторов в области ИБ.
15. Национальные стандарты и руководства по основам аудита ИБ.
16. Отечественные законы и стандарты по основам аудита.
17. Планирование аудита информационной безопасности организации.
18. Управление процессом аудита. Практические этапы аудита.

19. Информационное обследование. Анализ соответствия требованиям.
20. Инструментальное обследование защищенности. Анализ рисков.
21. Разработка первоочередных рекомендаций или плана защиты.
22. Виды отчетных документов по результатам проведения аудита.
23. Методы и инструментальные средства анализа защищенности элементов.
24. Система обеспечения информационной безопасности – совокупность процессов осознания и менеджмента информационной безопасности.
25. Осознание аудита информационной безопасности.
26. Планирование и реализация программы аудита ИБ.
27. Контроль и совершенствование программы аудита ИБ.
28. Задачи анализа информационных рисков. Основные методики анализа информационных рисков.
29. Базовый и полный анализ рисков.
30. Оценка затрат на информационную безопасность организации.
31. Оценивание ИБ на основе показателей ИБ.
32. Модели зрелости компаний с точки зрения ИБ.
33. Оценивание ИБ на основе моделей зрелости процессов обеспечения ИБ.
34. Затраты на проведение аудита и анализа рисков.
35. Оценивание результатов аудита и самооценки информационной безопасности. Оценивание процессов проведения аудита.
36. Риск-ориентированная интерпретация полученных оценок ИБ.
37. Пассивные и активные методы анализа защищенности.
38. Сканирование и зондирование.
39. Классификация и архитектуры систем анализа защищенности.
40. Средства анализа параметров защиты.
41. Сетевые сканеры безопасности.
42. Сканеры прикладных сервисов.
43. Средства контроля защищенности системного уровня.
44. Сравнительный анализ возможностей современных средств анализа защищенности.
45. Размерность и значимость объектов оценки при проведении аудита ИБ.
46. Методологии, стандарты и нормативные требования в области управления непрерывностью бизнеса.
47. Основные цели аудита. Основные вопросы, рассматриваемые при аудите. Реализация аудита. Заключительные процедуры аудита.
48. Использование аутсорсинга. Перечень услуг и функций, переданных в аутсорсинг.
49. Требования по обеспечению требуемого уровня услуг.
50. Требования по обеспечению физической и логической безопасности.
51. Процедуры взаимодействия компании с поставщиком услуг.
52. Методы доверия. Обеспечение доверия к информационной безопасности.
53. Объект доверия. Критерии доверия. Стадия доверия. Свидетельство доверия.

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

Основная учебная литература:

1. С.А. Петренко, А.А. Петренко. Аудит безопасности Intranet. [Электронный ресурс] М.: ДМК Пресс, 2010. – 416 с. – Доступ ЭБС «Консультант студента».

2. Аверченков В. И. Аудит информационной безопасности: учебное пособие для вузов. 3-е изд., стер. [Электронный ресурс] - М.: Флинта, 2013. – 269 с. Доступ ЭБС «Консультант студента».

Дополнительная учебная литература:

1. Авдошин С.М., Савельева А.А., Сердюк В.А. Технологии и продукты Microsoft в обеспечении информационной безопасности. [Электронный ресурс] – М.: Национальный Открытый Университет "ИНТУИТ", 2016.

2. Аудит информационной безопасности органов исполнительной власти : учеб. пособие [Электронный ресурс] / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский. - 4-е изд., стереотип. - М.: ФЛИНТА, 2016. - 100 с. - ISBN 978-5-9765-1277-1. Доступ ЭБС «Консультант студента».

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Международная организация по стандартизации -https://www.iso.org/;
2. Электронный фонд правовой и нормативно-технической документации - http://docs.cntd.ru;
3. ЭБС «Лань» - https://e.lanbook.com/;
4. ЭБС «Znanium» - https://znanium.com/;
5. ЭБС «Консультант студента» - https://www.studentlibrary.ru;
6. Национальный Открытый Университет «ИНТУИТ» - https://intuit.ru;
7. Вебинары компании «Код безопасности» - https://www.securitycode.ru/company/events/
8. - Аудит информационной безопасности: Читальный зал / Информационный онлайн портал ISO27000.ru - http://www.iso27000.ru/chitalnyi-zai/audit-informacionnoi-bezopasnosti.

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

Система KESS поддержки образовательного процесса КГУ http://dist.kgsu.ru/.

Информационно-справочная система «КонсультантПлюс».

При чтении лекций используются слайдовые презентации.

Минимальные требования к операционной системе и программному обеспечению компьютера, используемого при показе слайдовых презентаций: Windows XP, Libre Office.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Переносной проектор BENQ PB6110 с экраном, локальная сеть компьютеров на базе Intel Core i3-2120 - 16 шт. с выходом в Internet, коммутатор 2-го уровня D-LINK DGS-101D/E1A.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины

«Аудит информационной безопасности»

образовательной программы высшего образования –
программы специалитета

10.05.03 – Информационная безопасность автоматизированных систем

Направленность:
(специализация №7)

Обеспечение информационной безопасности распределенных информационных систем

Трудоемкость дисциплины: 4 з.е. (144 академических часа)
Семестр: 8 (очная форма обучения)
Форма промежуточной аттестации: зачет с оценкой
Содержание дисциплины. Основные разделы

Аудит информационной безопасности организации и систем. Исследования полученных оценок ИБ. Практика аудита ИБ организаций и систем.