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 КГУ

_____ / Н.В. Дубив/

«_31_» августа 2020 г.

Рабочая программа учебной дисциплины

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

образовательной программы высшего образования –
программы специалитета
10.05.03 ─ Информационная безопасность автоматизированных систем

Направленность: (специализация №7) обеспечение информационной
безопасности распределенных информационных систем
Формы обучения: очная

Курган 2020

Рабочая программа дисциплины «Управление информационной безопасностью» составлена в соответствии с учебными планами 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:
канд. пед. наук, доцент Е.Н. Полякова

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: 5 зачетных единицы трудоемкости (180 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	семестр
		9
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**48**	**48**
Лекции	32	32
Лабораторные работы	-	-
Практические занятия	16	16
Самостоятельная работа, всего часов в том числе:	132	132
Подготовка к зачету	18	18
Курсовая работа	36	36
Другие виды самостоятельной работы (подготовка к практическим занятиям и рубежному контролю)	78	78
Вид промежуточной аттестации	**Зачет с оценкой**	**Зачет с оценкой**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**180**	**180**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Управление информационной безопасностью» относится к базовой части Блока 1.

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

- Правоведение,
- Гуманитарные основы информационной безопасности,
- Основы управленческой деятельности,
- Организационное и правовое обеспечение информационной безопасности,
- Техническая защита информации
- Стандарты информационной безопасности,
- Программно-аппаратные средства защиты информации,
- Разработка и эксплуатация защищенных автоматизированных систем".

Результаты обучения по дисциплине необходимы для выполнения курсового работы, а также выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью изучения дисциплины является: приобретение обучаемыми необходимого объема знаний и практических навыков по управлению технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии.

Задачами дисциплины являются:

- изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии;
- приобретение необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, оценки рисков информационных ресурсов предприятия и аудита информационной безопасности;
- организация работы и разграничения полномочий персонала, ответственного за информационную безопасность;
- формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности (ИБ) автоматизированных систем (АС).

Компетенции, формируемые в результате освоения дисциплины:

- способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);
- способность к самоорганизации и самообразованию (ОК-8);
- способность использовать нормативные правовые акты в своей профессиональной деятельности (ОПК- 6);

- способность. разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);

- способность разрабатывать политики информационной безопасности автоматизированных систем (ПК-11);

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

- способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);

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

- способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);

- способность управлять информационной безопасностью автоматизированной системы (ПК-28);

- способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах (ПСК-7.2);

- способность. координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении (ПСК-7.5).

В результате изучения дисциплины обучающийся должен:

- знать основные методы управления информационной безопасностью (для ОК-5, ОК-8, ОПК-6, ПК-21, ПСК-7.5);

- знать методы, способы, средства, последовательность и содержание этапов проектирования и моделирования АС и подсистем безопасности АС (для ПК-4, ПК-11, ПК-19, ПК-22, ПК-23, ПК-28, ПСК-7.2);

- уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем (для ОК-5, ОК-8, ОПК-6, ПК-21, ПСК-7.5);

- уметь разрабатывать частные политики безопасности автоматизированных систем (для ПК-4, ПК-11, ПК-19, ПК-22, ПК-23, ПК-28, ПСК-7.2);

- владеть методами оценки информационных рисков (для ПК-19, ПК-23, ПСК-7.2);

- владеть методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем (для ОК-5, ОК-8, ОПК-6, ПК-4, ПК-11, ПК-21, ПК-22, ПК-23, ПК-28, ПСК-7.5).

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	Лабораторные работы
Рубеж 1	*Тема 1.*	Введение	2	-	-
	Тема 2	Базовые вопросы управления ИБ	2	7	-
	Тема 3	Процессный подход	2	-	-
	Тема 4	Область деятельности СУИБ	2	-	-
	Тема 5	Ролевая структура СУИБ	2	-	-
	Тема 6	Политика СУИБ	2	5	-
	Тема 7	Рискология ИБ	2	4	-
Рубеж 2	*Тема 8*	Основные процессы СУИБ. Обязательная документация СУИБ	2	-	-
	Тема 9	Внедрение разработанных процессов. Документ «Положение о применимости».	2	-	-
	Тема 10	Процесс «Управление инцидентами ИБ»	4	-	-
	Тема 11	Процесс «Обеспечение непрерывности ведения бизнеса»	4	-	-
	Тема 12	Обеспечение соответствия требованиям законодательства РФ	2	-	-
	Тема 13	Эксплуатация и независимый аудит СУИБ	4	-	-
		Всего:	**32**	**16**	-

4.2. Содержание лекционных занятий

Тема 1. Введение.

Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности. Цели и задачи курса. Основные понятия и определения. Содержание процесса управления информационной безопасностью АС и предприятия в целом. Рекомендуемая литература. Виды контроля знаний.

Тема 2. Базовые вопросы управления ИБ.

Сущность и функции управления. Наука управления. Принципы, подходы и виды управления. Цели и задачи управления ИБ. Понятие системы управления. Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием.

Стандартизация в области построения систем управления. История развития. Существующие стандарты и методологии по управлению ИБ: их отличия, сильные и слабые стороны (на примере семейства стандартов ISO/IEC 2700x, СТО БР ИББС-1.0, ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 27001, ISO/IEC 18044, ISO/IEC 25999 и др.).

Тема 3. Процессный подход.

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

Тема 4. Область деятельности СУИБ .

Понятие области деятельности СУИБ. Механизм выбора области деятельности. Состав области деятельности (процессы, структурные подразделения организации, кадры). Описание области деятельности (структура и содержание документа).

Тема 5. Ролевая структура СУИБ.

Понятие роли. Использование ролевого принципа в рамках СУИБ. Преимущества использования ролевого принципа. Ролевая структура СУИБ (основные и дополнительные роли).

Роль высшего руководства организации в СУИБ. Этапы разработки и функционирования СУИБ, на которых важно участие руководства организации. Суть участия руководства организации на этих этапах (утверждение документов, результатов анализа рисков и т.д.).

Тема 6. Политика СУИБ.

Понятие Политики СУИБ. Цели Политики СУИБ. Структура и содержание Политики СУИБ. Источники информации для разработки Политики СУИБ.

Тема 7. Рискология ИБ.

Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Разработка Методики анализа рисков ИБ.

Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации.

Выбор угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ.

Тема 8. Основные процессы СУИБ. Обязательная документация СУИБ.

Процессы «Управление документами» и «Управление записями» (цели и задачи процессов, входные/выходные данные, роли участников, обязательные этапы процессов, связи с другими процессами СУИБ).

Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»).

Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса».

Процесс «Анализ со стороны высшего руководства».

Процесс «Обучение и обеспечение осведомленности».

Тема 9. Внедрение разработанных процессов. Документ «Положение о применимости».

Этапы внедрения процессов и их последовательность. Обучение сотрудников, как один из этапов внедрения. Сложности, возникающие при внедрении

процессов управления ИБ, и способы их решения. Контроль над внедрением процессов.

Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа.

Тема 10. Процесс «Управление инцидентами ИБ».

Цели и задачи процесса «Управления инцидентами ИБ, важность процесса с точки зрения управления ИБ Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.

Тема 11. **Процесс «Обеспечение непрерывности ведения бизнеса».**

Цели и задачи процесса «Обеспечение непрерывности ведения бизнеса». Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.

Тема 12. Обеспечение соответствия требованиям законодательства РФ.

Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ (авторское право, защита персональных данных и т.д.).

Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).

Тема 13. Эксплуатация и независимый аудит СУИБ

Ввод системы в эксплуатацию. Возможные проблемы и способы их решения.

Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация.

Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации.

4.3 Практические занятия

Номер темы	Наименование раздела, темы	Наименование тем практических занятий	Норматив времени, час.
2	Базовые вопросы управления ИБ	Методика описания ролей.	2
		Методика описания активов организации, подлежащих защите.	2
		Методика оценки рисков ИБ.	2
	1-ый рубежный контроль	Тестирование	1
6	Политика СУИБ	Методика подготовки политики безопасности организации.	2
		Разработка и управление политикой ИБ информационной систе-	2

		мы	
	2-ой рубежный контроль	Тестирование	1
7	Рискология ИБ	Анализ модели угроз ИБ и уязвимостей	2
		Анализ модели информационных потоков	2
	Итого		**16**

4.4 КУРСОВАЯ РАБОТА

Целью курсовой работы является реализация полученных знаний по управлению информационной безопасностью.

Курсовая работа включает: оглавление; введение; теоретический раздел; подбор и анализ ситуации по теме; выводы и рекомендации; список литературы. Во введении необходимо раскрыть актуальность выбранной темы, перечислить ее основные проблемы, назвать ученых и практиков, занимающихся ими. В конце введения следует привести мотивировку выбранной темы, обосновать цель и задачи курсовой работы.

В теоретической части работы излагаются основные понятия по изучаемой теме, раскрываются ее главные проблемы. При этом данная часть должна иметь название, отвечающее теме работы, а также выводы, обобщающие теоретический материал.

В практической части курсовой работы приводится описание и анализ конкретной ситуации по выбранной теме. Ситуация также должна иметь соответствующее название и выводы, увязывающие практический материал с теоретическим.

В выводах и рекомендациях по работе в целом студент должен подвести итоги своего исследования, четко сформулировать основные выводы и предложения, направленные на повышение эффективности рассматриваемых явлений и процессов.

При использовании в тексте цитат и цифровых данных, заимствованных из каких-либо литературных источников, обязательно следует делать сноску.

Курсовая работа должна иметь иллюстрированный материал: схемы, диаграммы, графики, рисунки, таблицы и др., которые помещаются по ходу текста для большей наглядности, при этом заголовки должны отражать содержание иллюстраций.

Объем курсовой работы 30-40 страниц печатного текста на одной стороне листа (А4) через 1,5 интервала между строками шрифтом размера 14.

ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ РАБОТ ПО ДИСЦИПЛИНЕ «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

1 Анализ подходов к ролевому управлению доступом.
2 Современные проблемы авторизации субъекта доступа.
3 Исследование проблем безопасности при синхронизации данных и управлении средой виртуализации в комплексе территориально разнесенных ЦОДов.

4 Исследование проблем информационной безопасности мобильного доступа для государственных информационных систем.
5 Обеспечение режима информационной безопасности при использовании облачных сервисов.
6 Место DLP-систем в современной структуре обеспечения ИБ АИС.
7 Правовые инструменты обеспечения информационной безопасности в странах Евросоюза.
8 Характеристика механизмов технического регулирования информационной безопасности в России и за рубежом.
9 Обеспечение информационной безопасности при заключении договоров IT-аутсорсинга.
10 Характеристика направлений обеспечения информационной безопасности на предприятиях малого и среднего бизнеса.
11 Характеристика организационно-технических мероприятий по обеспечению информационной безопасности.
12 Построение системы информационной безопасности компьютерных программ для предприятия-разработчика.
13 Защита конфиденциальной информации на предприятиях государственного и частного сектора.
14 Построение системы информационной безопасности в организации.
15 Структурирование массива событий и инцидентов информационной безопасности с использованием специализированного ПО.
16 Разработка рекомендаций по повышению эффективности защиты информации в корпоративной сети передачи данных.
17 Минимизация рисков информационной безопасности при обеспечении доступа в Интернет.
18 Управление инцидентами информационной безопасности в крупной телекоммуникационной компании.

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 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 практических работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Преподавателем запланировано применение на практических занятиях разбор конкретных ситуаций.

Для текущего контроля успеваемости по очной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки акаде-

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 занятиях в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к практическим занятиям, к рубежным контролям, выполнение курсовой работы, подготовку к зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем раздела	42
Введение	2
Базовые вопросы управления ИБ	4
Процессный подход	2
Область деятельности СУИБ	2
Ролевая структура СУИБ	2
Политика СУИБ	2
Риск-ология ИБ	4
Основные процессы СУИБ. Обязательная документация СУИБ	4
Внедрение разработанных процессов. Документ «Положение о применимости»	4
Процесс «Управление инцидентами ИБ»	4
Процесс «Обеспечение непрерывности ведения бизнеса»	4
Обеспечение соответствия требованиям законодательства РФ	4
Эксплуатация и независимый аудит СУИБ	
Подготовка к практическим занятиям (по 4 часа)	28
Подготовка к рубежным контролям (по 4 часа на каждый рубежный контроль)	8
Подготовка к зачету	18
Подготовка курсовой работы	36
Всего:	132

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ (для очной формы обучения)
2. Отчеты студентов по практическим занятиям.
3. Курсовая работа.
3. Банк тестовых заданий к рубежным контролям № 1, № 2.
4. Вопросы к зачету.

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

<table>
<tr><td>№</td><td>Наименование</td><td colspan="6">Содержание</td></tr>
<tr><td rowspan="5">1</td><td rowspan="5">Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы (доводятся до сведения студентов на первом учебном занятии)</td><td colspan="6">Распределение баллов</td></tr>
<tr><td>Вид учебной работы:</td><td>Посещение лекций</td><td>Выполнение и защита практической работы</td><td>Рубежный контроль №1</td><td>Рубеж-ный кон-троль №2</td><td>Зачет</td></tr>
<tr><td>Балльная оценка:</td><td>1б х 16=16б</td><td>4б х 8=32б</td><td>11</td><td>11</td><td>30</td></tr>
<tr><td colspan="6">Курсовая работа</td></tr>
<tr><td>Качество пояснительной записки</td><td colspan="2">Ритмичность выполнения</td><td>Ритмичность выполнения</td><td>Качество защиты</td><td>Всего</td></tr>
<tr><td>до 40</td><td colspan="2">до 20</td><td>до 10</td><td>до 30</td><td>100</td></tr>
<tr><td>2</td><td>Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета</td><td colspan="6">60 и менее баллов – неудовлетворительно; незачет;
61…73 – удовлетворительно; зачет;
74… 90 – хорошо;
91…100 – отлично</td></tr>
<tr><td>3</td><td>Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов</td><td colspan="6">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 практические работы и курсовая работа.
Для получения экзаменационной оценки «автоматически» студенту необходимо набрать следующее минимальное количество баллов:
- 68 для получения «автоматически» оценки удовлетворительно».
По согласованию с преподавателем студенту, набравшему минимум 68 баллов, 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 работ, за участие в значимых учебных и внеучебных мероприятиях кафедры и выставлена за зачет «автоматически» оценка «хорошо» или «отлично».</td></tr>
<tr><td>4</td><td>Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра</td><td colspan="6">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 практических работ.
Формы дополнительных заданий (назначаются преподавателем):
- выполнение и защита пропущенной практической работы – до 4 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.</td></tr>
</table>

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования.

Зачет – в форме устного ответа на 2 вопроса. Перечень вопросов преподаватель выдает заранее. Время, отводимое студенту на подготовку вопросов, составляет 1 академический час. Каждый вопрос оценивается в 15 баллов.

Перед проведением каждого рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии.

Варианты тестовых заданий для рубежных контролей № 1 – состоит из 11 вопросов, а № 2 состоит из 11 вопросов.

На каждое тестирование при рубежном контроле студенту отводится 45 минут (1 академический час).

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

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

Примерные тестовые задания для рубежного контроля №1

1. Кто является основным ответственным за определение уровня классификации информации?
    1. Руководитель среднего звена
    2. Высшее руководство
    3. Владелец
    4. Пользователь
2. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководителю?
    1. Снизить уровень безопасности этой информации для обеспечения её доступности и удобства использования
    2. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
    3. Улучшить контроль за безопасностью этой информации
    4. Снизить уровень классификации этой информации

Примерные тестовые задания для рубежного контроля №2

1. На каком уровне утверждается политика информационной безопасности предприятия?
    1. Это не имеет значения
    2. На уровне начальника службы ИБ
    3. На уровне технического директора

4. На уровне высшего руководства предприятия

5. На уровне высшестоящего или надзирающего органа

2. Какой из пунктов содержит наиболее точное определение? Инцидент информационной безопасности – это…

1. …любое нарушение политики ИБ

2. …существенное или грубое нарушение политики ИБ

3. …угроза или существенное снижение защищенности

4. … событие, реализующее угрозу или существенно снижающее защищенность

5. …действия злоумышленника, существенно снижающие защищенность

6. …действия злоумышленника, наносящие вред информационной системе.

Примерный перечень вопросов к зачету

1. Сущность и функции управления. Наука управления. Принципы, подходы и виды управления.
2. Цели и задачи управления ИБ. Понятие системы управления. Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием.
3. Стандартизация в области построения систем управления.
4. Существующие стандарты и методологии по управлению ИБ: их отличия, сильные и слабые стороны.
5. Понятие и методы формализации процессов. Цели и задачи формализации процессов.
6. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИБ).
7. Основные процессы СУИБ и требования, предъявляемые к ним каждым из стандартов.
8. Понятие области деятельности СУИБ.
9. Механизм выбора области деятельности.
10. Состав области деятельности (процессы, структурные подразделения организации, кадры).
11. Использование ролевого принципа в рамках СУИБ. Преимущества использования ролевого принципа.
12. Ролевая структура СУИБ (основные и дополнительные роли).
13. Роль высшего руководства организации в СУИБ.
14. Этапы разработки и функционирования СУИБ, на которых важно участие руководства организации.
15. Понятие Политики СУИБ. Цели Политики СУИБ.
16. Структура и содержание Политики СУИБ.
17. Источники информации для разработки Политики СУИБ.
18. Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ.
19. Разработка Методики анализа рисков ИБ.

20. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации.
21. Выбор угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов.
22. Оценка рисков ИБ. Планирование мер по обработке рисков ИБ.
23. Использование результатов анализа рисков ИБ.
24. Процессы «Управление документами» и «Управление записями».
25. Процессы улучшения СУИБ.
26. Процесс «Мониторинг эффективности».
27. Понятие «Зрелость процесса».
28. Процесс «Анализ со стороны высшего руководства».
29. Процесс «Обучение и обеспечение осведомленности».
30. Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа.
31. Процесс разработки документа, решение спорных ситуаций при разработке документа.
32. Цели и задачи процесса «Управления инцидентами ИБ, важность процесса с точки зрения управления ИБ Входные/выходные данные процесса.
33. Цели и задачи процесса «Обеспечение непрерывности ведения бизнеса». Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса.
34. Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ (авторское право, защита персональных данных и т.д.).
35. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация.
36. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации СУИБ перед сертификацией.
37. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации.

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

1. Ярочкин В.И. Информационная безопасность. М.: Академический проект, 2008. 544 с.

2. Корнеев И.К., Степанов И.А. Защита информации в офисе. М.: Изд во "Проспект", 2008. 336 с.

3. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности. – М.: Академия, 2008 г. – 192 стр.

4. Гришина Н.В. Организация комплексной системы защиты информации. М.: Гелиос АРВ, 2007. 256 с.

5. Галатенко В.А. Стандарты информационной безопасности. – М.: Интернет-университет информационных технологий, 2006 г. – 264 с.

6. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

7. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью

8. BS ISO/IEC 27002:2005 RU Информационные технологии - Методы обеспечения безопасности.

9. Защита информации. Уч.пособие/ Ю.М. Краковский – Ростов н/Д: Феникс, 2016 – 347с(1)с: ил.-(Высшее образование) Доступ из ЭБС ISBN 978-5-222-26911-4 http//www studentlibrary.ru/book/ISBN 9785222269114 html

7.2. Дополнительная учебная литература

1. Защита компьютерной информации. Эффективные методы и средства/ Шаньгин В.Ф. – М.: ДМК Пресс, 2010 – 544с:ил- Доступ из ЭБС ISBN 978-5-91074-518-1 http//www studentlibrary.ru/book/ISBN 9785910745181 html.

2. Фисун А.П., Касилов А.Н., Глоба Ю.А. Право и информационная безопасность. — М., 2005.— 272 с.

3. Казанцев С. Правовое обеспечение информационной безопасности. – М.: Академия, 2007 г. – 240 с.

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

1. Информационно-справочная система «КонсультантПлюс».
2. Электронно-библиотечная система научно-издательского центра «ИНФРА-М». – Режим доступа: http://znanium.com/. – загл. с экрана.
3. Электронно-библиотечная система издательства «Лань». – Режим доступа: http://e.lanbook.com/. – загл. с экрана.
4. ЭБС htt://www.iprbookshop.ru/
5. ЭБС htt://www.studentlibrary.ru
6. http://nio.kgsu.ru/ Сайт КГУ. Научно-исследовательский отдел
7. http://window.edu.ru/. Единое окно доступа к образовательным ресурсам
8. http://elibrary.ru/. Научная электронная библиотека
9. http://dspace.kgsu.ru/xmlui/ Электронная библиотека КГУ

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1. Операционные системы семейств Microsoft Windows 200x, Linux;
2. Пакет программ VMWare Workstation.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Компьютерный класс с установленным программным обеспечением: VMWare Workstation 5.0, MS Windows 200x, Linux., мультимедийное оборудование (ноутбук, мультимедийный проектор, экран).

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины
«Управление информационной безопасностью»

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

Трудоемкость дисциплины: 5 з.е. (180 академических часа)
Семестр: 9 (очная форма обучения)
Форма промежуточной аттестации: зачет с оценкой

Содержание дисциплины

Система управления информационной безопасностью АС. Политика безопасности АС. Организация обеспечения информационной безопасности АС. Аудит информационной безопасности АС. Средства поддержки процессов управления информационной безопасностью АС.