МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. В. Сенченко
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Управление информационной безопасностью

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **38.05.01 Экономическая безопасность**
Направленность (профиль) / специализация: **Экономико-правовое обеспечение экономической безопасности**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **5**
Семестр: **9**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	9 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	18	18	часов
3	Лабораторные работы	12	12	часов
4	Всего аудиторных занятий	58	58	часов
5	Самостоятельная работа	86	86	часов
6	Всего (без экзамена)	144	144	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	180	180	часов
		5.0	5.0	З.Е.

Экзамен: 9 семестр

Томск

Согласована на портале № 51635

Рассмотрена и одобрена на заседании кафедры
протокол № 12 от «26» 11 2019 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 38.05.01 Экономическая безопасность, утвержденного 16.01.2017 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:

Старший преподаватель каф. КИБЭВС _____ Н. С. Егошин

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ А. А. Конев

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ А. Ю. Якимук

Согласована на портале № 51635

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью дисциплины является овладение основными принципами управления уровнем информационной безопасности защищаемых ресурсов организации.

1.2. Задачи дисциплины

– Получение студентами знаний о структуре и принципах построения политики информационной безопасности организации.

– Получение студентами умений и навыков по построению моделей угроз и нарушителей

– и по оценке рисков информационной безопасности в организации.

– Получение студентами знаний об основных методах контроля обеспечения информационной безопасности в организации.

2. Место дисциплины в структуре ОПОП

Дисциплина «Управление информационной безопасностью» (Б1.В.01.01) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Деловые коммуникации, Организационное и правовое обеспечение информационной безопасности.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-20 способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности ;

– ПСК-2 способностью выявлять условия, способствующие совершению правонарушений в отношении сведений, составляющих государственную, банковскую, коммерческую тайну, персональных данных, других сведений ограниченного доступа;

В результате изучения дисциплины обучающийся должен:

– **знать** основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основные методы управления информационной безопасностью; принципы формирования политики информационной безопасности в автоматизированных системах

– **уметь** оценивать информационные риски в автоматизированных системах; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; разрабатывать частные политики информационной безопасности автоматизированных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем

– **владеть** профессиональной терминологией в области информационной безопасности; навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами управления информационной безопасностью автоматизированных систем; методами оценки информационных рисков; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 5.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры

Согласована на портале № 51635

		9 семестр
Аудиторные занятия (всего)	58	58
Лекции	28	28
Практические занятия	18	18
Лабораторные работы	12	12
Самостоятельная работа (всего)	86	86
Оформление отчетов по лабораторным работам	12	12
Проработка лекционного материала	42	42
Подготовка к практическим занятиям, семинарам	32	32
Всего (без экзамена)	144	144
Подготовка и сдача экзамена	36	36
Общая трудоемкость, ч	180	180
Зачетные Единицы	5.0	5.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Прак. зан., ч	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
9 семестр						
1 Анализ объекта защиты	8	8	0	24	40	ПК-20, ПСК-2
2 Внутренние угрозы ИБ	4	10	0	20	34	ПК-20, ПСК-2
3 Подбор и увольнение сотрудников	2	0	0	4	6	ПК-20, ПСК-2
4 Текущая работа с персоналом	2	0	0	4	6	ПК-20, ПСК-2
5 Разграничение доступа и контроль работы сотрудников	2	0	0	4	6	ПК-20, ПСК-2
6 Управление инцидентами ИБ	4	0	12	20	36	ПК-20, ПСК-2
7 Системы менеджмента ИБ	2	0	0	4	6	ПК-20, ПСК-2
8 Свод правил по управлению ИБ	2	0	0	2	4	ПК-20, ПСК-2
9 Обеспечение защиты информации в экстренных ситуациях	2	0	0	4	6	ПК-20, ПСК-2
Итого за семестр	28	18	12	86	144	
Итого	28	18	12	86	144	

Согласована на портале № 51635

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины (по лекциям)	Трудоемкость, ч	Формируемые компетенции
9 семестр			
1 Анализ объекта защиты	Анализ объектов защиты часть 1	4	ПСК-2
	Анализ объектов защиты часть 2	4	
	Итого	8	
2 Внутренние угрозы ИБ	Внутренние угрозы ИБ	4	ПК-20, ПСК-2
	Итого	4	
3 Подбор и увольнение сотрудников	Подбор и увольнение сотрудников	2	ПК-20, ПСК-2
	Итого	2	
4 Текущая работа с персоналом	Текущая работа с персоналом	2	ПК-20, ПСК-2
	Итого	2	
5 Разграничение доступа и контроль работы сотрудников	Разграничение доступа и контроль работы сотрудников	2	ПК-20, ПСК-2
	Итого	2	
6 Управление инцидентами ИБ	Управление инцидентами ИБ	4	ПК-20, ПСК-2
	Итого	4	
7 Системы менеджмента ИБ	Системы менеджмента ИБ	2	ПК-20, ПСК-2
	Итого	2	
8 Свод правил по управлению ИБ	Свод правил по управлению ИБ	2	ПК-20, ПСК-2
	Итого	2	
9 Обеспечение защиты информации в экстренных ситуациях	Обеспечение защиты информации в экстренных ситуациях	2	ПК-20, ПСК-2
	Итого	2	
Итого за семестр		28	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин								
	1	2	3	4	5	6	7	8	9
Предшествующие дисциплины									
1 Деловые коммуникации			+	+					
2 Организационное и правовое обеспечение информационной безопасности			+	+	+				

Согласована на портале № 51635

Последующие дисциплины									
1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	+					+	+	+	+

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4.

Таблица 5.4 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий				Формы контроля
	Лек.	Прак. зан.	Лаб. раб.	Сам. раб.	
ПК-20	+	+	+	+	Экзамен, Отчет по лабораторной работе, Тест, Отчет по практическому занятию
ПСК-2	+	+	+	+	Экзамен, Отчет по лабораторной работе, Тест, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
9 семестр			
6 Управление инцидентами ИБ	Анализ и управление рисками информационной системы	4	ПК-20, ПСК-2
	Анализ рисков на основе модели угроз и уязвимостей	4	
	Анализ рисков на основе DigitalSecurity. Кондор	4	
	Итого	12	
Итого за семестр		12	

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8.1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
9 семестр			
1 Анализ объекта защиты	Анализ объекта защиты часть 1	4	ПК-20, ПСК-2
	Анализ объекта защиты часть 2	4	
	Итого	8	
2 Внутренние угрозы ИБ	Внутренние угрозы ИБ	10	ПК-20, ПСК-2
	Итого	10	

Согласована на портале № 51635

Итого за семестр		18	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
9 семестр				
1 Анализ объекта защиты	Подготовка к практическим занятиям, семинарам	16	ПК-20, ПСК-2	Отчет по практическому занятию, Тест, Экзамен
	Проработка лекционного материала	8		
	Итого	24		
2 Внутренние угрозы ИБ	Подготовка к практическим занятиям, семинарам	16	ПК-20, ПСК-2	Отчет по практическому занятию, Тест, Экзамен
	Проработка лекционного материала	4		
	Итого	20		
3 Подбор и увольнение сотрудников	Проработка лекционного материала	4	ПК-20, ПСК-2	Тест, Экзамен
	Итого	4		
4 Текущая работа с персоналом	Проработка лекционного материала	4	ПК-20, ПСК-2	Тест, Экзамен
	Итого	4		
5 Разграничение доступа и контроль работы сотрудников	Проработка лекционного материала	4	ПК-20, ПСК-2	Тест, Экзамен
	Итого	4		
6 Управление инцидентами ИБ	Проработка лекционного материала	8	ПК-20, ПСК-2	Отчет по лабораторной работе, Тест, Экзамен
	Оформление отчетов по лабораторным работам	12		
	Итого	20		
7 Системы менеджмента ИБ	Проработка лекционного материала	4	ПК-20, ПСК-2	Тест, Экзамен
	Итого	4		
8 Свод правил по управлению ИБ	Проработка лекционного материала	2	ПК-20, ПСК-2	Тест, Экзамен
	Итого	2		
9 Обеспечение защиты информации в экстренных	Проработка лекционного материала	4	ПК-20, ПСК-2	Тест, Экзамен
	Итого	4		

Согласована на портале № 51635

ситуациях				
Итого за семестр		86		
	Подготовка и сдача экзамена	36		Экзамен
Итого		122		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
9 семестр				
Отчет по лабораторной работе	10	10	10	30
Отчет по практическому занятию		10	10	20
Тест		10	10	20
Итого максимум за период	10	30	30	70
Экзамен				30
Нарастающим итогом	10	40	70	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11.2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)

Согласована на портале № 51635

3 (удовлетворительно) (зачтено)	65 - 69	
	60 - 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Курило, А.П. Основы управления информационной безопасностью. Серия «Вопросы управления информационной безопасностью». Выпуск 1 [Электронный ресурс] [Электронный ресурс] [Электронный ресурс]: учебное пособие / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов [и др.]. – Электрон. дан. – М.: Горячая линия- Телеком, 2012. – 244 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=5178 (дата обращения: 01.07.2021).

12.2. Дополнительная литература

1. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. М., 2009, 50 с [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=173886 (дата обращения: 01.07.2021).

2. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М., 2008, 31 с. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=129018 (дата обращения: 01.07.2021).

3. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. М., 2014, 106 с. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=183918 (дата обращения: 01.07.2021).

4. ГОСТ Р ИСО/МЭК 27003-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности. М., 2014, 58 с. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=183599 (дата обращения: 01.07.2021).

5. ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. М., 2012, 62 с. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=179060 (дата обращения: 01.07.2021).

6. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М., 2011, 51 с. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=177398 (дата обращения: 01.07.2021).

7. ГОСТ Р ИСО/МЭК 27006-2008. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=175608 (дата обращения: 01.07.2021).

8. ГОСТ Р ИСО/МЭК 27007-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=187871 (дата обращения: 01.07.2021).

9. ГОСТ Р ИСО/МЭК 27011-2012. Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=183954 (дата обращения: 01.07.2021).

10. ГОСТ Р ИСО/МЭК 27013-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?

Согласована на портале № 51635

control=7&id=187948 (дата обращения: 01.07.2021).

11. ГОСТ Р ИСО/МЭК 27031-2012. Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=184904 (дата обращения: 01.07.2021).

12. ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=179072 (дата обращения: 01.07.2021).

13. ГОСТ Р ИСО/МЭК 27033-3-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=187869 (дата обращения: 01.07.2021).

14. ГОСТ Р ИСО/МЭК 27034-1-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=187929 (дата обращения: 01.07.2021).

15. ГОСТ Р ИСО/МЭК 27037-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=187854 (дата обращения: 01.07.2021).

16. ГОСТ Р ИСО/МЭК 27038-2016. Информационные технологии. Методы обеспечения безопасности. Требования и методы электронного цензурирования. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document1.aspx?control=31&id=204467 (дата обращения: 01.07.2021).

17. Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 2 [Электронный ресурс]: учеб. пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 130 с — Режим доступа: https://e.lanbook.com/book/5179 (дата обращения: 01.07.2021).

18. Милославская, Н.Г. Серия «Вопросы управление информационной безопасностью". Выпуск 3 [Электронный ресурс] [Электронный ресурс] [Электронный ресурс]: учеб. пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — Москва : Горячая линия-Телеком, 2013. — 170 с. — Режим доступа: https://e.lanbook.com/book/5180 (дата обращения: 01.07.2021).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Голиков, А. М. Основы информационной безопасности [Электронный ресурс]: Учебное пособие для практических и семинарских занятий [Электронный ресурс] / А. М. Голиков. — Томск: ТУСУР, 2007. — 154 с. — Режим доступа: https://edu.tusur.ru/publications/1017 (дата обращения: 01.07.2021).

12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;

Согласована на портале № 51635

– в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. http://protect.gost.ru - Федеральное агенство по техническому регулированию и метрологии;
2. http://www.elibrary.ru - научная электронная библиотека;
3. http://www.edu.ru - веб-сайт системы федеральных образовательных порталов;
4. http://edu.fb.tusur.ru/ - образовательный портал факультета безопасности;
5. https://fstec.ru/ - Федеральная служба по техническому и экспортному контролю.

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для практических занятий

Лаборатория организации финансовых расследований
учебная аудитория для проведения занятий практического типа
634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 400 ауд.
Описание имеющегося оборудования:
- Следственный чемодан (портфель);
- Манекен;
- Лазерный тир ЭТ-110ПМ;
- Набор первой медицинской помощи;
- Компьютер: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
– Microsoft Windows 10

13.1.3. Материально-техническое и программное обеспечение для лабораторных работ

Аудитория Интернет-технологий и информационно-аналитической деятельности
учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа
634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 402 ауд.
Описание имеющегося оборудования:
- Экран раздвижной;
- Мультимедийный проектор View Sonic PJD5154 DLP;
- Компьютеры: AMD A8-5600K/ ASUS A88XM-A/ DDR3 4 Gb/ WD5000AAKX 500 Gb/ мышь/ клавиатура/ монитор (15шт.);
- Компьютеры: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор (6шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
– Kaspersky Endpoint Security 10 для Windows
– Microsoft Windows 10

Согласована на портале № 51635

– VirtualBox
– Visio

13.1.4. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:

- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

14.1.1. Тестовые задания

1. Какие ресурсы используют при построении модели информационных потоков в ГРИФ?

Группы пользователей и права доступа

Пользователи и группы

Сервер и рабочая станция

Риски и контрмеры

Согласована на портале № 51635

2. По каким угрозам в системе ГРИФ не оценивается ущерб?
Конфиденциальности
Целостности
Достоверность
Доступность
3. Какой категории угроз не представлено в системе ГРИФ?
Физические угрозы человека
Угрозы персонала
Системные ошибки
Физические угрозы
4. Какого типа экономического ущерба не существует?
Долговременный экономический ущерб
Кратковременный экономический ущерб
Отсроченный экономический ущерб
Немедленный экономический ущерб
5. Какой тип экономического ущерба должен быть присвоен при обнаружении критерия «нарушение бизнес-деятельности»?
Кратковременный экономический ущерб
Отсроченный экономический ущерб
Немедленный экономический ущерб
Долговременный экономический ущерб
6. Как повлияет на веса средств защиты ответ «Положения политики внедрены частично» на первый вопрос раздела о политике безопасности?
Не повлияет
Приравняет к нулю
Вызовет уменьшение
Вызовет рост
7. Какая из перечисленных выполняемых проверок не входит в перечень обязательных действий, входящих в руководство по реализации средств управления против злонамеренного кода?
Проверка любых файлов на электронном или оптическом носителе, а также файлов, полученных по сетям, на наличие злонамеренного кода перед использованием
Проверка web-страниц на наличие злонамеренного кода
Проверка обновлений средства управления против злонамеренного кода
Проверка приложений к электронным письмам и загрузок на наличие злонамеренного кода перед использованием
8. По какой причине для класса группы авторизованных интернет-пользователей в системе ГРИФ не предлагается никаких средств защиты рабочего места?
Для данной группы характерна минимальная вероятность реализации угрозы
Для группы по умолчанию выбран набор средств защиты рабочего места
Для группы неизвестно, откуда будет осуществляться доступ
Для группы неизвестна степень влияния на систему
9. Какие данные нельзя указать при задании контрмер в системе ГРИФ?
Стоимость внедрения
Возможное снижение затрат на ИБ
Срок внедрения контрмеры
Название для отчета
10. Какие параметры нельзя включить в состав отчета по проекту в системе КОНДОР?
Выполненные требования
Невыполненные требования
Риски
Контрмеры
11. Какой тип экономического ущерба должен быть присвоен при обнаружении критерия «подрыв репутации»?
Кратковременный экономический ущерб

Согласована на портале № 51635

Отсроченный экономический ущерб
Долговременный экономический ущерб
Немедленный экономический ущерб
12. Какой тип экономического ущерба должен быть присвоен при обнаружении критерия «снижение розничных продаж»?
Отсроченный экономический ущерб
Немедленный экономический ущерб
Кратковременный экономический ущерб
Долговременный экономический ущерб
13. Какой информации не содержится в отчете по периоду, формируемом системой КОНДОР?
Количество выполненных и невыполненных требований в целом по системе для выбранного периода аудита
Уровень риска невыполнения требований стандарта в целом по системе для выбранного периода аудита
Изменения затрат на контрмеры в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита
Затраты на контрмеры в целом по системе для выбранного периода аудита
14. Чему по умолчанию равны вероятность в течение года и критичность реализации для только что созданной угрозы?
25 %
15 %
10 %
0 %
15. Какой информации не содержится в отчете по проекту, формируемом системой КОНДОР?
Изменения количества выполненных требований в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита
Изменения уровня риска в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита
Текст выполненных требований по каждому разделу
Изменения затрат на контрмеры в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита
16. Какое количество мер защиты содержит в себе «Оценка уровня обеспечения ИБ организации БС РФ в соответствии с требованиями СТО БР ИББС-1.0»?
32
33
34
35
17. В каком формате выводятся результаты оценки объекта на предмет обеспечения требований из СТО БР ИББС-1.2?
Диаграмма Ганта
Гистограмма
Круговая диаграмма
Срез структуры
18. Что понимается под базовым временем простоя ресурсов?
Время необходимое на обработку информации после запроса
Время отклика системы на запрос
Время, в течение которого доступ к информации ресурса невозможен
Время, в течение которого система загружает необходимые для работы службы
19. Фактором, значимым для использования уязвимости не является?
Время, затрачиваемое на идентификацию уязвимости
Техническая компетентность специалиста
Программное средство, требуемое для анализа

Согласована на портале № 51635

Знание проекта и функционирования объекта

20. Что понимается под эффективностью средства защиты информации?

Показатель быстродействия системы в условиях использования средств защиты информации

Коэффициент снижения уровня риска по отношению к первоначальному уровню

Степень влияния на защищенность информации и рабочего места группы пользователей

Субъективная оценка экспертами корректности функционирования средства защиты информации

21. Что понимается под базовой вероятностью конфиденциальности?

Вероятность огласки информации минимального уровня конфиденциальности в системе

Минимальная вероятность реализации угрозы

Максимальная вероятность реализации угрозы

Вероятность огласки информации максимального уровня конфиденциальности в системе

22. Какой тип внутренних нарушителей наиболее подвержен социальной инженерии?

Подрабатывающий

Внедренный

Манипулируемый

Нелояльный

23. К внешним чрезвычайным ситуациям не относятся?

Стихийные бедствия

Преступные действия

Техногенные аварии и сбои

Диверсии

24. Что не входит перечень того, что для любой организации, серьезно относящейся к информационной безопасности, важно применять в структурном и плановом подходе ГОСТ Р ИСО/МЭК ТО 18044–2007?

Обнаружение, оповещение об инцидентах информационной безопасности и их оценка

Реагирование на инциденты информационной безопасности, включая активацию защитных мер для предотвращения, уменьшения последствий и (или) восстановление после негативных воздействий

Предотвращение инцидентов информационной безопасности

Извлечение уроков из инцидентов информационной безопасности, введение превентивных защитных мер и улучшение общего подхода к менеджменту инцидентов информационной безопасности

25. Что понимается под инцидентом информационной безопасности?

Процесс сравнения количественно оцененного риска с заданными критериями риска для определения его значимости

Идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности

Появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы информационной безопасности

Процесс обеспечения восстановления операции в случае возникновения какого-либо неожиданного или нежелательного инцидента, способного негативно воздействовать на непрерывность важных функций бизнеса и поддерживающих его элементов

26. К какому варианту неработоспособности относится болезнь сотрудника?

Полное прекращение выполнения сотрудником своих обязанностей

Опасность для жизни персонала

Прекращение выполнения сотрудником рутинных операций

Саботаж

27. К какой группе внешних чрезвычайных ситуаций относится скупка контрольного пакета акций?

Согласована на портале № 51635

Общественные
Правовые
Экономические
Стихийные бедствия

28. Какому из перечисленных типов внутренних нарушителей характерна постановка задачи извне?

Халатный
Манипулируемый
Подрабатывающий
Обиженный

29. Что понимается под характеристиками группы пользователей?

Состав группы пользователей
Название группы пользователей
Вид доступа группы пользователей
Описание группы пользователей

30. Какая статья расходов не входит в расходы на информационную безопасность?

Затраты на приобретение систем защиты информации
Затраты на управление системой защиты информации
Затраты на разработку политики безопасности
Затраты на обучение персонала

31. Что произойдет, если задать пороговое значение риска в 50% в системе КОНДОР?

Будут отображены все положения стандартов, риски для которых ниже 50%
Будут отображены все положения стандартов, риски для которых выше 50%
Будут отображены только критичные положения стандартов, которые не выполнены
Будут отображены только критичные положения стандартов, которые выполнены

14.1.2. Экзаменационные вопросы

1. Цель и этапы анализа объектов защиты.
2. Перечислите этапы оценки рисков информационной безопасности автоматизированных систем.
3. Идентификация и классификация объектов защиты.
4. Типизация информационных систем. Данные об информационной системе, необходимые для построения модели документооборота.
5. Подходы к разграничению доступа в рамках организации. Структура документов, регламентирующих разграничение доступа.
6. Подходы к построению модели нарушителя.
7. Классификация нарушителей (ФСТЭК).
8. Классификация угроз безопасности персональных данных (ФСТЭК).
9. Методика определения актуальных угроз (ФСТЭК).
10. Методика оценки ущерба, нанесённого при реализации угроз информационной безопасности.
11. Угрозы, источником которых является персонал организации.
12. Методы «социальной инженерии» и способы защиты от них.
13. Обязанности сотрудников Службы безопасности при приёме сотрудников на работу.
14. Нормативная документация, обязательная к ознакомлению и подписанию при приёме на работу.
15. Предоставление сотруднику доступа к конфиденциальной информации. Основные разделы Инструкции по внесению изменений в списки пользователей.
16. Обязанности сотрудников Службы безопасности при обучении и увольнении сотрудников.
17. Упрощённая модель классификации субъектов.
18. Основные положения инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы организации.
19. Основные положения регламента контроля использования технических средств обра-

Согласована на портале № 51635

ботки и передачи информации.

20. Основные положения инструкции по организации парольной защиты.

21. Основные положения документов, регламентирующих использование средств аутентификации и носителей ключевой информации.

22. Основные положения инструкции по организации антивирусной защиты.

23. Основные положения инструкции по работе с электронной почтой.

24. Типы чрезвычайных ситуаций. Структура аварийного плана. Причины изменения аварийного плана.

25. Классификация объектов при составлении аварийного плана.

26. Требования к различным классам объектов и их резервированию.

27. Основные положения плана обеспечения непрерывной работы и восстановления работоспособности.

28. Приведите примеры источников информации об инцидентах информационной безопасности.

29. Перечислите аспекты анализа инцидентов информационной безопасности, направленные на совершенствование системы управления информационной безопасностью.

30. Приведите требования к формированию политики информационной безопасности организации и учитываемые в ней категории безопасности.

14.1.3. Вопросы для подготовки к практическим занятиям, семинарам

Анализ объекта защиты часть 1

Анализ объекта защиты часть 2

Внутренние угрозы ИБ

14.1.4. Темы лабораторных работ

Анализ и управление рисками информационной системы

Анализ рисков на основе модели угроз и уязвимостей

Анализ рисков на основе DigitalSecurity. Кондор

14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами исходя из состояния обучающегося на момент проверки

14.3. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

– в печатной форме;

Согласована на портале № 51635

– в печатной форме с увеличенным шрифтом;
– в форме электронного документа;
– методом чтения ассистентом задания вслух;
– предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

– письменно на бумаге;
– набор ответов на компьютере;
– набор ответов с использованием услуг ассистента;
– представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в форме электронного документа;
– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;
– в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 51635