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

Технологии обеспечения информационной безопасности

Уровень образования: **высшее образование - магистратура**
Направление подготовки / специальность: **10.04.01 Информационная безопасность**
Направленность (профиль) / специализация: **Информационная безопасность объектов критической информационной инфраструктуры**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **1**
Семестр: **1**
Учебный план набора 2021 года

Распределение рабочего времени

№	Виды учебной деятельности	1 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Практические занятия	36	36	часов
3	Всего аудиторных занятий	54	54	часов
4	Самостоятельная работа	90	90	часов
5	Всего (без экзамена)	144	144	часов
6	Подготовка и сдача экзамена	36	36	часов
7	Общая трудоемкость	180	180	часов
		5.0	5.0	З.Е.

Экзамен: 1 семестр

Томск

Согласована на портале № 48766

Рассмотрена и одобрена на заседании кафедры
протокол № 13 от «24» 12 2019 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.04.01 Информационная безопасность, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчики:

ст.преподаватель каф. КИБЭВС	_____	А. Ю. Якимук
доцент каф. КИБЭВС	_____	А. А. Конев
Заведующий обеспечивающей каф. КИБЭВС	_____	А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ	_____	Д. В. Кручинин
Заведующий выпускающей каф. КИБЭВС	_____	А. А. Шелупанов

Эксперты:

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)	_____	К. С. Сарин
Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)	_____	Е. Ю. Костюченко

Согласована на портале № 48766

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью преподавания дисциплины является: освоение основных технологий, использующихся при работе с защищенными автоматизированными системами на этапах их разработки,реализации и эксплуатации.

1.2. Задачи дисциплины

– Задачами изучения дисциплины являются: дать студентам знания о способах проектирования и документального оформления процесса разработки защищенных автоматизированных систем на основе специализированных международных стандартов, развить в них умения и навыки применения специализированных международных стандартов при разработке средств защиты информации, умения и навыки в области разработки защищенных автоматизированных систем в соответствии с требованиями профиля защиты, а также дать знания о методах организации и регламентации процесса эксплуатации защищенных автоматизированных систем.

2. Место дисциплины в структуре ОПОП

Дисциплина «Технологии обеспечения информационной безопасности» (Б1.Б.1) относится к блоку 1 (базовая часть).

Последующими дисциплинами являются: Разработка компонентов средств защиты информации, Управление информационной безопасностью, Управление компьютерными инцидентами.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОК-2 способностью самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения;

– ОПК-2 способностью к самостоятельному обучению и применению новых методов исследования профессиональной деятельности;

– ПК-5 способностью анализировать фундаментальные и прикладные проблемы информационной безопасности в условиях становления современного информационного общества;

В результате изучения дисциплины обучающийся должен:

– **знать** основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; − автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; − методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем; − содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем; − методы, способы и средства обеспечения отказоустойчивости автоматизированных систем; − основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); − основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах; − основные информационные технологии, используемые в автоматизированных системах.

– **уметь** разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; - администрировать подсистемы информационной безопасности автоматизированных систем; - восстанавливать работоспособность подсистемы информационной безопасности автоматизированных систем в нештатных ситуациях; - исследовать эффективность создаваемых средств автоматизации, проводить технико-экономическое обоснование проектных решений; - разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов; - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; - выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем.

– **владеть** профессиональной терминологией в области информационной безопасности; −

Согласована на портале № 48766

навыками поддержания работоспособности, обнаружения и устранения неисправностей в работе электронных аппаратных средств автоматизированных систем; − методами и технологиями проектирования, моделирования, исследования автоматизированных систем и подсистем безопасности автоматизированных систем; − навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; − навыками использования программно-аппаратных средств обеспечения информационной безопасности автоматизированных 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
		1 семестр
Аудиторные занятия (всего)	54	54
Лекции	18	18
Практические занятия	36	36
Самостоятельная работа (всего)	90	90
Проработка лекционного материала	14	14
Написание рефератов	16	16
Подготовка к практическим занятиям, семинарам	50	50
Подготовка к тесту	10	10
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	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
1 семестр					
1 Поиск, изучение, обобщение и систематизация научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности.	2	0	2	4	ОК-2, ОПК-2, ПК-5
2 Проектирование автоматизированных информационных систем.	2	0	2	4	ОК-2, ОПК-2, ПК-5
3 Основные стадии создания автоматизированных информационных систем.	2	0	2	4	ОК-2, ОПК-2, ПК-5
4 Средства автоматизации проектирования автоматизированных информационных си-	4	12	22	38	ОК-2, ОПК-2, ПК-5

Согласована на портале № 48766

стем.					
5 Тестирование автоматизированных информационных систем.	2	6	14	22	ОК-2, ОПК-2, ПК-5
6 Ввод в эксплуатацию автоматизированных информационных систем.	2	0	2	4	ОК-2, ОПК-2, ПК-5
7 Анализ рисков информационной безопасности автоматизированной системы.	4	18	46	68	ОК-2, ОПК-2, ПК-5
Итого за семестр	18	36	90	144	
Итого	18	36	90	144	

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
1 семестр			
1 Поиск, изучение, обобщение и систематизация научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности.	Поиск, накопление и обработка научно-технической информации. Использование классификаций. Электронные формы информационных ресурсов документов. Обработка научно-технической информации, её фиксация и хранение. Информационно-поисковые системы для поиска документов. Патентный закон Российской Федерации от 23 сентября 1992 г. №3517-1 с изменениями и дополнениями,внесенными Федеральным законом от 07 февраля 2003 г.	2	ОК-2, ОПК-2, ПК-5
	Итого	2	
2 Проектирование автоматизированных информационных систем.	Изучение государственных стандартов, содержащих требования, устанавливаемые российским законодательством к построению автоматизированных систем ГОСТ 24.104-85 «Автоматизированные системы управления. Общие требования. Единая система стандартов» и ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения». Изучение специфики научно-исследовательской работы.	2	ОК-2, ОПК-2, ПК-5
	Итого	2	
3 Основные стадии создания автоматизированных информационных систем.	Изучение государственных стандартов, содержащих требования, устанавливаемые российским законодательством к стадиям создания автоматизированных систем – ГОСТ 19.102-77 «ЕСПД Стадии разработки», ГОСТ 24.601-86 «Автоматизированные системы. Стадии создания», ГОСТ 24.602-86 «Автоматизированные	2	ОК-2, ОПК-2, ПК-5

Согласована на портале № 48766

	системы управления. Со-став и содержание работ по стадиям создания» и ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания». Рассмотрение вопроса разбиения проекта на этапы и определения ключевых параметров каждого из них. Рассмотрение методики построения IDEF.		
	Итого	2	
4 Средства автоматизации проектирования автоматизированных информационных систем.	Изучение государственного стандарта, содержащего требования, устанавливаемые российским законодательством к оформлению алгоритмов – ГОСТ 19.701-90 (ИСО 5807-85) «ЕСПД Схемы алгоритмов, программ данных и систем. Рассмотрение вопросов, связанных с построением и реализацией алгоритмов. Ознакомление с содержанием ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности Условные обозначения». Изучение оценочных уровней доверия и классификации автоматизированных систем.	4	ОК-2, ОПК-2, ПК-5
	Итого	4	
5 Тестирование автоматизированных информационных систем.	Изучение государственного стандарта, содержащего требования, устанавливаемые российским законодательством к тестированию автоматизированных систем – ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем». Изучение видов испытаний и технологию их применения на практике. Рассмотрение примеров документации.	2	ОК-2, ОПК-2, ПК-5
	Итого	2	
6 Ввод в эксплуатацию автоматизированных информационных систем.	Изучение государственных стандартов, содержащих требования, устанавливаемые российским законодательством к рабочей документации на продукцию – ГОСТ 19.504-79 «Руководство программиста. Требования к содержанию и оформлению» и ГОСТ 19.505-79 «Руководство оператора. Требования к содержанию и оформлению». Определение ключевых различий между руководствами программиста и администратора. Рассмотрение примеров документации.	2	ОК-2, ОПК-2, ПК-5

Согласована на портале № 48766

	Итого	2	
7 Анализ рисков информационной безопасности автоматизированной системы.	Оценка эффективности системы защиты информации, сравнительная характеристика своей системы защиты информации и возможностей нарушителя по ее преодолению. Модель и критерии эффективности системы защиты. Методы многокритериальной оценки эффективности: метод последовательных уступок и метод анализа иерархий.	4	ОК-2, ОПК-2, ПК-5
	Итого	4	
Итого за семестр		18	

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
Последующие дисциплины							
1 Разработка компонентов средств защиты информации							
2 Управление информационной безопасностью							
3 Управление компьютерными инцидентами							

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.	Сам. раб.	
ОК-2	+	+	+	Экзамен, Опрос на занятиях, Выступление (доклад) на занятии, Тест, Отчет по практическому занятию
ОПК-2	+	+	+	Экзамен, Опрос на занятиях, Выступление (доклад) на занятии, Тест, Отчет по практическому занятию
ПК-5	+	+	+	Экзамен, Опрос на занятиях, Выступление (доклад) на занятии, Тест, Отчет по практическому занятию

Согласована на портале № 48766

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Не предусмотрено РУП.

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
1 семестр			
4 Средства автоматизации проектирования автоматизированных информационных систем.	Система управления проектами	6	ОПК-2, ПК-5
	Использование системы контроля версий исходного кода программ	6	
	Итого	12	
5 Тестирование автоматизированных информационных систем.	Использование средства автоматизации тестирования программного обеспечения	6	ОК-2, ОПК-2, ПК-5
	Итого	6	
7 Анализ рисков информационной безопасности автоматизированной системы.	Анализ сертифицированного СЗИ на предмет его функциональных возможностей. Построение модели типа «черный ящик» для исследуемой системы с последующей детализацией по технологии IDEF0.	6	ОК-2, ОПК-2, ПК-5
	Оценка общих критериев и определение класса защищенности автоматизированной системы.	6	
	Анализ СЗИ с использованием ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности Условные обозначения» на предмет оценочных уровней доверия.	6	
	Итого	18	
Итого за семестр		36	

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
1 семестр				
1 Поиск, изучение, обобщение и систематизация	Проработка лекционного материала	2	ОК-2, ОПК-2, ПК-5	Тест, Экзамен
	Итого	2		

Согласована на портале № 48766

научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности.				
2 Проектирование автоматизированных информационных систем.	Проработка лекционного материала	2	ОК-2, ОПК-2, ПК-5	Тест, Экзамен
	Итого	2		
3 Основные стадии создания автоматизированных информационных систем.	Проработка лекционного материала	2	ОК-2, ОПК-2, ПК-5	Тест, Экзамен
	Итого	2		
4 Средства автоматизации проектирования автоматизированных информационных систем.	Подготовка к практическим занятиям, семинарам	20	ОК-2, ОПК-2, ПК-5	Отчет по практическому занятию, Тест, Экзамен
	Проработка лекционного материала	2		
	Итого	22		
5 Тестирование автоматизированных информационных систем.	Подготовка к практическим занятиям, семинарам	12	ОК-2, ОПК-2, ПК-5	Отчет по практическому занятию, Тест, Экзамен
	Проработка лекционного материала	2		
	Итого	14		
6 Ввод в эксплуатацию автоматизированных информационных систем.	Проработка лекционного материала	2	ОК-2, ОПК-2, ПК-5	Тест, Экзамен
	Итого	2		
7 Анализ рисков информационной безопасности автоматизированной системы.	Подготовка к тесту	10	ОК-2, ОПК-2, ПК-5	Выступление (доклад) на занятии, Отчет по практическому занятию, Тест, Экзамен
	Подготовка к практическим занятиям, семинарам	18		
	Написание рефератов	16		
	Проработка лекционного материала	2		
	Итого	46		
Итого за семестр		90		

Согласована на портале № 48766

	Подготовка и сдача экзамена	36		Экзамен
Итого		126		

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
1 семестр				
Выступление (доклад) на занятии			15	15
Опрос на занятиях	5	5	5	15
Отчет по практическому занятию		15	15	30
Тест			10	10
Итого максимум за период	5	20	45	70
Экзамен				30
Нарастающим итогом	5	25	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)
3 (удовлетворительно) (зачтено)	65 - 69	

Согласована на портале № 48766

	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. Технология разработки программных систем [Электронный ресурс]: Учебное пособие / И. Г. Боровской - 2012. 260 с. — Режим доступа: https://edu.tusur.ru/publications/2436 (дата обращения: 24.03.2020).
2. Основы информационной безопасности : Учебное пособие для вузов. - М. : Горячая линия-Телеком , 2006. - 544 с. (наличие в библиотеке ТУСУР - 81 экз.)

12.2. Дополнительная литература

1. Основы информационной безопасности [Электронный ресурс]: Учебное пособие / А. М. Голиков - 2007. 201 с. — Режим доступа: https://edu.tusur.ru/publications/1024 (дата обращения: 24.03.2020).
2. Петин, Виктор Александрович. Создание умного дома на базе Arduino [Электронный ресурс] / В. А. Петин ; ред. Д. А. Мовчан. - Электрон. текстовые дан. - М. [Электронный ресурс]: ДМК Пресс, 2018. - on-line : цв. ил., схемы. - ISBN 978-5-97060-620-9 : Б. ц. — Режим доступа: https://e.lanbook.com/reader/book/107890 (дата обращения: 24.03.2020).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Конев А.А., Якимук А.Ю. Технологии обеспечения информационной безопасности [Электронный ресурс]: практические работы [Электронный ресурс]: методические указания по выполнению практических работ. – Томск: В-Спектр, 2019. — Режим доступа: http://keva.tusur.ru/sites/default/files/upload/work_progs/yay/TOIB.pdf (дата обращения: 24.03.2020).

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;
- в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

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

12.5. Периодические издания

1. Информация и безопасность [Электронный ресурс]: научный журнал. - Воронеж : ВГТУ . - Журнал выходит с 1998 г. — Режим доступа: https://elibrary.ru/title_about.asp?id=8748 (дата обращения: 24.03.2020).

Согласована на портале № 48766

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

Аудитория информатики, технологий и методов программирования

учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, помещение для курсового проектирования (выполнения курсовых работ), помещение для самостоятельной работы

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 408 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard 78" с ПО ActivInspire;
- Проектор ViewSonic PJD5154 DLP;
- Компьютеры: DEPO Neos 235/ A8-7650K/ DDR3 4G/ 1Tb / мышь/ клавиатура/ монитор (10 шт.);
- 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
- VirtualBox
- Visio
- Обучающее ПО: Git-bash

13.1.3. 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.

Согласована на портале № 48766

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

Научно-техническая информация (НТИ) - это

о Вся негуманитарная информация по точным, естественным и техническим наукам, технике, медицине и сельскому хозяйству.

о Научно-техническая информация (НТИ) - «документированная информация, возникающая в результате научного и технического развития», т. е. в процессе научного познания, «получаемая и (или) используемая в области науки и (или) техники».

о Информационные издания, как правило, содержащие либо систематизированные сведения об опубликованных или еще неопубликованных, а также непубликуемых документах, либо результат анализа и обобщения сведений, представленных в первоисточниках.

о Информация, полученная в процессе научно-исследовательской, опытно-конструкторской, технологической, проектной, иной научной и производственной, а также научноинформационной деятельности (НИД).

Дайте определение :

о Риск – это способ определения сильных и слабых сторон существующих и предлагаемых мер защиты.

о Риск – это определение мероприятий по оценке угроз и разработке новых, более эффективных методов и средств защиты от них.

о Риск - это стоимостное выражение вероятностного события, ведущего к потерям. о Риск - это процесс получения количественной или качественной оценки ущерба, который может произойти в случае реализации угрозы безопасности ИС.

Проранжируйте компоненты ИС по возрастанию риска информационной безопасности

о 1.

- сотрудники — пользователи и обслуживающий персонал.
- данные — временные, хранимые постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;
- оборудование — ЭВМ и их составные части (процессоры, мониторы, терминалы, рабочие станции), периферийные устройства (дисководы, устройства back-up, порты ввода-вывода, принтеры, кабели, контроллеры, линии связи) и т.д.;

Согласована на портале № 48766

- программное обеспечение — исходные, объектные, загрузочные модули, приобретенные программы, «домашние» разработки, утилиты, операционные системы и системные программы (компиляторы, компоновщики и др.), диагностические программы и т.д.;

о 2.

- оборудование — ЭВМ и их составные части (процессоры, мониторы, терминалы, рабочие станции), периферийные устройства (дисководы, устройства back-up, порты ввода-вывода, принтеры, кабели, контроллеры, линии связи) и т.д.;
- программное обеспечение — исходные, объектные, загрузочные модули, приобретенные программы, «домашние» разработки, утилиты, операционные системы и системные программы (компиляторы, компоновщики и др.), диагностические программы и т.д.;
- данные — временные, хранимые постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;
- сотрудники — пользователи и обслуживающий персонал.

о 3.

- сотрудники — пользователи и обслуживающий персонал;
- данные — временные, хранимые постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;
- программное обеспечение — исходные, объектные, загрузочные модули, приобретенные программы, «домашние» разработки, утилиты, операционные системы и системные программы (компиляторы, компоновщики и др.), диагностические программы и т.д.;
- оборудование — ЭВМ и их составные части (процессоры, мониторы, терминалы, рабочие станции), периферийные устройства (дисководы, устройства back-up, порты ввода-вывода, принтеры, кабели, контроллеры, линии связи) и т.д.

о 4.

- данные — временные, хранимые постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;
- сотрудники — пользователи и обслуживающий персонал.
- оборудование — ЭВМ и их составные части (процессоры, мониторы, терминалы, рабочие станции), периферийные устройства (дисководы, устройства back-up, порты ввода-вывода, принтеры, кабели, контроллеры, линии связи) и т.д.;
- программное обеспечение — исходные, объектные, загрузочные модули, приобретенные программы, «домашние» разработки, утилиты, операционные системы и системные программы (компиляторы, компоновщики и др.), диагностические программы и т.д.;

Дайте определение :

о Ролевой метод доступа является разновидностью модели Дискреционного метода доступа;

о Ролевой метод доступа является разновидностью модели Обязательного метода доступа;

о Ролевой метод доступа является самостоятельной моделью метода доступа к данным, основанной на градации ролей.

о Ролевой метод доступа является разновидностью модели Мандатного метода доступа;

В чем суть требований компонента ИСО/МЭК-15408 FAU_SAA.2 «Выявление аномалии, основанное на профиле»?

о Обнаружение Эксплойта;

о Обнаружение Несанкционированного доступа к данным;

о Обнаружение Руткита;

о Обнаружение ошибки Сетевого программного обеспечения.

В чем суть требований семейства ИСО/МЭК-15408 FPT_SSP «Протокол синхронизации состояний»?

о Обнаружение Несанкционированного доступа к данным;

о Обнаружение Руткита;

о Обнаружение Эксплойта.

Согласована на портале № 48766

o Обнаружение ошибки Сетевого программного обеспечения.

Проранжируйте роли по возрастанию риска информационной безопасности

o - пользователь сети, - менеджер программного обеспечения, - оператор системы, администратор баз данных, - администратор безопасности.

o - пользователь сети, - администратор баз данных, - менеджер программного обеспечения,- оператор системы, - администратор безопасности.

o - администратор безопасности, - оператор системы, - менеджер программного обеспечения, - администратор баз данных, - пользователь сети.

o - оператор системы, - менеджер программного обеспечения, - администратор безопасности, - пользователь сети, администратор баз данных.

Принцип минимизации привилегий – это реализация Теоремы

o Диффи-Хеллмана симметричного шифрования;

o Харрисона-Ульмана распределения прав доступа;

o Белла-Лападулы основная теорема безопасности;

o Шамира-Алдемана асимметричного шифрования.

Какие нормативные документы регламентируют создание ТЗ на защиту информации в ИС?

o Приказ ФСТЭК России от 14.03.2014 г. №31;

o (ГОСТ 34.601, ГОСТ Р 51583);

o Приказ ФСТЭК России от 11.02.2013 №17;

o 149-ФЗ «Об информации, ИТ и о ЗИ»;

14.1.2. Экзаменационные вопросы

– Назначение ЕСПД. Классификация и обозначение стандартов ЕСПД – Виды программ и программных документов. Стадии разработки.

– Виды программ и программных документов. Обозначения программ и программных документов.

– Виды программ и программных документов. Основные надписи. Общие требования к программной документации. Требования по оформлению и содержанию технического задания.

– Виды программ и программных документов. Программа и методика испытаний.

– Общие требования к программной документации. Текст и описание программы. Требования к содержанию и оформлению.

– Виды программ и программных документов. Общие требования к программной документации. Пояснительная записка. Требования к содержанию и оформлению.

– Руководство системного программиста. Руководство программиста. Руководство оператора. Руководство по техническому обслуживанию. Требования к содержанию и оформлению. – Виды программ и программных документов. Описание языка. Требования к содержанию и оформлению.

14.1.3. Темы докладов

Оценка общих критериев и определение класса защищенности автоматизированной системы.

Анализ средства защиты информации на предмет оценочных уровней доверия.

14.1.4. Темы опросов на занятиях

Изучение государственных стандартов, содержащих требования, устанавливаемые российским законодательством к стадиям создания автоматизированных систем – ГОСТ 19.102-77 «ЕСПД Стадии разработки», ГОСТ 24.601-86 «Автоматизированные системы. Стадии создания», ГОСТ 24.602-86 «Автоматизированные системы управления. Со-став и содержание работ по стадиям создания» и ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания». Рассмотрение вопроса разбиения проекта на этапы и определения ключевых параметров каждого из них. Рассмотрение методики построения IDEF.

Оценка эффективности системы защиты информации, сравнительная характеристика своей системы защиты информации и возможностей нарушителя по ее преодолению. Модель и критерии эффективности системы защиты. Методы многокритериальной оценки эффективности: метод последовательных уступок и метод анализа иерархий.

Согласована на портале № 48766

14.1.5. Вопросы для подготовки к практическим занятиям, семинарам

Система управления проектами

Использование системы контроля версий исходного кода программ

Использование средства автоматизации тестирования программного обеспечения

Анализ сертифицированного СЗИ на предмет его функциональных возможностей. Построение модели типа «черный ящик» для исследуемой системы с последующей детализацией по технологии IDEF0.

Оценка общих критериев и определение класса защищенности автоматизированной системы.

Анализ СЗИ с использованием ГОСТ Р ИСО/МЭК 15408-3-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности Условные обозначения» на предмет оценочных уровней доверия.

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;
- 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, адапти-

Согласована на портале № 48766

рованных 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 № 48766