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

Защищенные информационные системы

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: **2**
Семестр: **3**
Учебный план набора 2021 года

Распределение рабочего времени

№	Виды учебной деятельности	3 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Практические занятия	18	18	часов
3	Контроль самостоятельной работы (курсовой проект / курсовая работа)	18	18	часов
4	Всего аудиторных занятий	54	54	часов
5	Самостоятельная работа	126	126	часов
6	Всего (без экзамена)	180	180	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	216	216	часов
		6.0	6.0	З.Е.

Экзамен: 3 семестр
Курсовой проект / курсовая работа: 3 семестр

Томск

Согласована на портале № 48789

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 №_____.

Разработчик:

доцент каф. БИС _____ С. С. Харченко

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 № 48789

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Освоение дисциплинарных компетенций, связанных с созданием и изучением современной защищенных информационных систем различного применения и степени сложности. Обучение принципам и методам защиты информации, комплексного проектирования, построения, обслуживания и анализа защищенных информационных систем, а также содействовать формированию научного мировоззрения и развитию системного мышления.

1.2. Задачи дисциплины

– системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности;

– обоснование выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

– разработка систем, комплексов, средств и технологий обеспечения информационной безопасности;

– разработка программ и методик испытаний средств и систем обеспечения информационной безопасност

2. Место дисциплины в структуре ОПОП

Дисциплина «Защищенные информационные системы» (Б1.Б.3) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Разработка компонентов средств защиты информации, Технологии обеспечения информационной безопасности.

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

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-2 способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

– ПК-3 способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

– ПК-16 способностью разрабатывать проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности;

В результате изучения дисциплины обучающийся должен:

– **знать** современную классификацию средств защиты информации в вычислительных сетях и системах; современные программные и аппаратные средства защиты информации; типовые угрозы информации в информационных системах и сетях; технологии построения защищенных информационных систем; этапы и технологии проектирования и создания защищенных информационных систем;

– **уметь** анализировать и оценивать угрозы информационной без-опасности; делать выбор функциональной структуры системы обеспечения информационной безопасности; анализировать и оценивать угрозы информационной без-опасности.

– **владеть** навыками работы современными программными и аппаратными комплексными средствами защиты информации; навыками разработки комплексной инфраструктуры защищенных информационных систем;

Согласована на портале № 48789

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 6.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		3 семестр
Аудиторные занятия (всего)	54	54
Лекции	18	18
Практические занятия	18	18
Контроль самостоятельной работы (курсовой проект / курсовая работа)	18	18
Самостоятельная работа (всего)	126	126
Проработка лекционного материала	90	90
Подготовка к практическим занятиям, семинарам	36	36
Всего (без экзамена)	180	180
Подготовка и сдача экзамена	36	36
Общая трудоемкость, ч	216	216
Зачетные Единицы	6.0	6.0

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	КП/КР, ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
3 семестр						
1 Теоретические вопросы защиты информации и построения информационных систем	8	9	18	45	62	ОК-2, ОПК-2, ПК-16, ПК-2, ПК-3
2 Способы и методы защиты информации в информационных системах.	10	9		81	100	ОК-2, ОПК-2, ПК-16, ПК-2, ПК-3
Итого за семестр	18	18	18	126	180	
Итого	18	18	18	126	180	

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
3 семестр			
1 Теоретические вопросы защиты	Автоматизированная информационная система. Классификации задач, решаемых с	4	ОК-2, ОПК-2, ПК-2

Согласована на портале № 48789

информации и построения информационных систем	использованием информационных систем. Свойства систем. Классификации систем. Ранги систем. Закон необходимости разнообразия (закон Эшби).		
	Основы теории надежности. Связь с основными задачами информационной безопасности. Надежность программно-аппаратных реализаций информационных систем.	2	
	Подходы к проектированию и реализации информационных систем. Жизненный цикл информационной системы. Вопросы информационной безопасности и аспекты построения защищенных систем. Место процесса кодирования и языка программирования в проблемах информационной безопасности.	2	
	Итого	8	
2 Способы и методы защиты информации в информационных системах.	Типология распределенных информационных систем. Процессы в информационных системах. Тенденции и подходы к защите информации в информационных системах.	4	ОК-2, ОПК-2, ПК-2, ПК-3
	Методы и способы обеспечения идентификации, аутентификации и авторизации в информационных системах. Криптографическая защита информации. Понятие несанкционированного доступа и принципы защиты от несанкционированного доступа. Мониторинг и аудит в информационных системах.	2	
	Стандарты и нормативные документы в области информационной безопасности. Построение защищенной информационной системы в соответствии с нормативами и требованиями. Защита информационных систем, обрабатывающих персональные данные. Государственные информационные системы. Системы управления технологическими процессами.Подходы к аудиту и оценке защищенности информационных систем.	4	
	Итого	10	
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.

Согласована на портале № 48789

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин	
	1	2
Предшествующие дисциплины		
1 Разработка компонентов средств защиты информации	+	+
2 Технологии обеспечения информационной безопасности	+	+
Последующие дисциплины		
1 Защита выпускной квалификационной работы, включая подготовку к защите 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.	КСР (КП/КР)	Сам. раб.	
ОК-2	+	+	+	+	Опрос на занятиях, Защита курсовых проектов / курсовых работ, Тест
ОПК-2	+	+	+	+	Опрос на занятиях, Защита курсовых проектов / курсовых работ, Тест
ПК-2	+	+	+	+	Опрос на занятиях, Защита курсовых проектов / курсовых работ, Тест
ПК-3	+	+	+	+	Опрос на занятиях, Защита курсовых проектов / курсовых работ, Тест
ПК-16		+	+	+	Опрос на занятиях, Защита курсовых проектов / курсовых работ, Тест

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
3 семестр			
1 Теоретические	Разработка и проектирование информаци-	9	ОК-2, ОПК-2,

Согласована на портале № 48789

вопросы защиты информации и построения информационных систем	онных систем.		ПК-16, ПК-2, ПК-3
	Итого	9	
2 Способы и методы защиты информации в информационных системах.	Обеспечение информационной безопасности в информационных системах.	9	ОК-2, ОПК-2, ПК-16, ПК-2, ПК-3
	Итого	9	
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
3 семестр				
1 Теоретические вопросы защиты информации и построения информационных систем	Проработка лекционного материала	15	ОК-2, ОПК-2, ПК-2	Тест
	Проработка лекционного материала	15		
	Проработка лекционного материала	15		
	Итого	45		
2 Способы и методы защиты информации в информационных системах.	Подготовка к практическим занятиям, семинарам	36	ОК-2, ОПК-2, ПК-16, ПК-2, ПК-3	Опрос на занятиях, Тест
	Проработка лекционного материала	15		
	Проработка лекционного материала	15		
	Проработка лекционного материала	15		
	Итого	81		
Итого за семестр		126		
	Подготовка и сдача экзамена	36		Экзамен
Итого		162		

10. Курсовой проект / курсовая работа

Трудоемкость аудиторных занятий и формируемые компетенции в рамках выполнения курсового проекта / курсовой работы представлены таблице 10.1.

Таблица 10.1 – Трудоемкость аудиторных занятий и формируемые компетенции в рамках выполнения курсового проекта / курсовой работы

Наименование аудиторных занятий	Трудоемкость, ч	Формируемые компетенции

Согласована на портале № 48789

3 семестр		
Проектирование, разработка и обеспечение информационной безопасности информационной системы.	18	ОК-2, ОПК-2, ПК-16, ПК-2, ПК-3
Итого за семестр	18	

10.1. Темы курсовых проектов / курсовых работ

Примерная тематика курсовых проектов / курсовых работ:

- web-ориентированная информационная система
- информационная система персональных данных
- персональная информационная система
- корпоративная информационная система
- медицинская информационная система

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
3 семестр				
Защита курсовых проектов / курсовых работ			30	30
Опрос на занятиях	5	5	10	20
Тест		10	10	20
Итого максимум за период	5	15	50	70
Экзамен				30
Нарастающим итогом	5	20	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)

Согласована на портале № 48789

4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
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. Информационная безопасность и защита информации [Текст] : учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А. Клейменов. - 4-е изд., стер. - М. : Академия, 2009. - 336 с. (наличие в библиотеке ТУСУР - 21 экз.)

2. Основы информационной безопасности [Электронный ресурс]: учебное пособие / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — Москва : Горячая линия-Телеком, 2011. — 558 с. — Режим доступа: https://e.lanbook.com/book/111016 (дата обращения: 24.03.2020).

12.2. Дополнительная литература

1. 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://docs.cntd.ru/document/1200076805 (дата обращения: 24.03.2020).

2. 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://docs.cntd.ru/document/1200113359 (дата обращения: 24.03.2020).

3. 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://docs.cntd.ru/document/1200113374 (дата обращения: 24.03.2020).

4. 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://docs.cntd.ru/document/1200112883 (дата обращения: 24.03.2020).

5. ГОСТ Р ИСО/МЭК 27038-2016. Информационные технологии. Методы обеспечения безопасности. Требования и методы электронного цензурирования. [Электронный ресурс]: — Режим доступа: http://docs.cntd.ru/document/1200136904 (дата обращения: 24.03.2020).

6. ГОСТ Р ИСО/МЭК 52863-2007 Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования. 38 с. [Электронный ресурс]: — Режим доступа: http://docs.cntd.ru/document/1200065692 (дата обращения: 24.03.2020).

7. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения, 12 с. [Электронный ресурс]: — Режим доступа: http://docs.cntd.ru/document/1200058320 (дата обращения: 24.03.2020).

8. ГОСТ Р 58412-2019 Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения, 28 с. [Электронный ресурс]: — Режим доступа: http://docs.cntd.ru/document/1200164529 (дата обращения: 24.03.2020).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Основы информационной безопасности [Электронный ресурс]: Учебное пособие для практических и семинарских занятий / А. М. Голиков - 2007. 154 с. — Режим доступа:

Согласована на портале № 48789

https://edu.tusur.ru/publications/1017 (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://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

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:

- Microsoft SQL Server 2014
- Microsoft Windows 10
- VirtualBox

Согласована на портале № 48789

– Visio
– Visual Studio

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.

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

К правовым методам, обеспечивающим информационную безопасность, относятся:

1. Разработка аппаратных средств обеспечения правовых данных
2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий
3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности

Основными источниками угроз информационной безопасности являются все указанное в

Согласована на портале № 48789

списке:

1. Хищение жестких дисков, подключение к сети, инсайдерство
2. Перехват данных, хищение данных, изменение архитектуры системы
3. Хищение данных, подкуп системных администраторов, нарушение регламента работы

Угроза информационной системе (компьютерной сети) – это:

1. Вероятное событие
2. Детерминированное (всегда определенное) событие
3. Событие, происходящее периодически

Для чего предназначены информационные системы автоматизированного проектирования?

1. для автоматизации функций управленческого персонала.
2. для автоматизации любых функций компании и охватывают весь цикл работ от проектирования до сбыта продукции
3. для автоматизации функций производственного персонала.
4. для автоматизации работы при создании новой техники или технологии.

Информационная система (ИС) - это:

1. это совокупность условий, средств и методов на базе компьютерных систем, предназначенных для создания и использования информационных ресурсов.
2. это совокупность программных продуктов, установленных на компьютере, технология работы в которых позволяет достичь поставленную пользователем цель.
3. это взаимосвязанная совокупность средств, методов и персонала, используемых для обработки данных.
4. это совокупность данных, сформированная производителем для ее распространения в материальной или в нематериальной форме.
5. это процесс, определяемый совокупностью средств и методов обработки, изготовления, изменения состояния, свойств, формы сырья или материала.
6. это процесс, использующий совокупность средств и методов обработки и передачи данных и первичной информации для получения информации нового качества о состоянии объекта, процесса или явления.

Методика тестирования на проникновение называется:

1. Аудит
2. Пентест
3. Honeypot
4. Metasploit

Что из перечисленного не является целью проведения аудита безопасности?

1. Анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов системы
2. Выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности системы
3. Оценка будущего уровня защищенности системы
4. Оценка соответствия системы существующим стандартам в области информационной безопасности.

К какой категории охраняемой информации относится врачебная тайна?

1. государственная тайна
2. служебная тайна
3. профессиональная тайна
4. объекты авторского права

Какой институт в США занимается вопросами информационной безопасности, разрабатывая стандарты и технологии в этой области?

1. PIST
2. NIST
3. DAST
4. ANB

Как называется разновидность DDOS атаки при которой атакующий шлёт маленький по объёму HTTP-пакет, но такой, чтобы сервер ответил на него пакетом, размер которого в сотни раз

Согласована на портале № 48789

больше?

1. HTTP-флуд
2. Ping-флуд
3. Smurf-атака
4. Атака Fraggle
5. SYN-флуд

Как называется разновидность DDOS атаки при которой атакующий шлёт ICMP-сообщения через усиливающую сеть?

1. HTTP-флуд
2. Ping-флуд
3. Smurf-атака
4. Атака Fraggle
5. SYN-флуд

Как называется разновидность DDOS атаки при которой атакующий шлёт UDP пакеты через усиливающую сеть?

1. HTTP-флуд
2. Ping-флуд
3. Smurf-атака
4. Атака Fraggle
5. SYN-флуд

Как называется разновидность DDOS атаки при которой атакующий подменяет свой IP адрес на несуществующий при установки соединения?

1. HTTP-флуд
2. Ping-флуд
3. Smurf-атака
4. Атака Fraggle
5. SYN-флуд

Как называется атака. которая осуществляется путём размещения на веб-странице ссылки или скрипта, пытающегося получить доступ к сайту, на котором атакуемый пользователь заведомо (или предположительно) уже аутентифицирован.

1. DDOS
2. CSRF
3. XSS
4. CORS

Как называется механизм безопасности, который позволяет веб-странице из одного домена обращаться к ресурсу с другим доменом (кросс-доменным запросом)?

1. XSS
2. JSONP
3. OWASP
4. CORS

14.1.2. Экзаменационные вопросы

Общие определения и характеристики систем. Понятие сложности, критерии и свойства.

Критерии и свойства для системы. Вероятностная модель системы и пример пограничных состояний.

Информационные системы. Автоматизированные системы. Определения. Структура и классификация систем.

Базовые информационные процессы в системах.

Закон необходимого разнообразия Эшби. Энтропийная форма закона. Следствия из закона Эшби.

Основные принципы обеспечения информационной безопасности для информационных систем.

Методическая и нормативная база для построения защищенных систем.

Виды защищенных автоматизированных систем в соответствии с требованиями ГОСТ.

Принципы защиты информации в автоматизированных системах в соответствии с требова-

Согласована на портале № 48789

ниями ГОСТ.

Принципы защиты информации в ИСПДН.

Аспекты построения доверенной вычислительной среды (ТСВ).

Способы реализации механизмов парольной защиты. Хранение и передача паролей.

Принципы распределения и реализации системы полномочий и доступов.

Пример построения защищенной системы на основе микроядерной ОС.

Программные аспекты построения защищенных систем. Работа с памятью.

Общие принципы обеспечения резервирования и защиты от сбоев.

Протоколы резервирования сетевой инфраструктуры.

Аспекты резервирования и надежности виртуальных систем.

Иерархическая модель данных.

Сетевая модель данных.

Реляционная модель данных.

Модель данных «Сущность-Связь».

Модель системы защиты. Комплексный подход.

Международные стандарты оценки защищённости.

Руководящие документы Гостехкомиссии России.

14.1.3. Темы опросов на занятиях

Анализ организационно-методического обеспечения защиты информационной системы ПДн на предприятии

Системы контроля и учета доступа (СКУД) предприятия

Менеджмент информационной безопасности на уровне предприятия посредством метода CVSS

Разграничение доступа в Web-приложениях

Разработка системы защиты государственной информационной системы

Построение модели угроз информационной безопасности медицинской информационной системы учреждений здравоохранения

Тестирование на проникновение Linux-подобных систем

Создание и расследование инцидента информационной безопасности

Нейросетевые технологии анализа защищенности информационных систем

Моделирование атаки и защита веб-приложения с уязвимостями XSS и CSRF

Внедрение системы двухфакторной аутентификации на предприятии

Применение бесконтактных смарт-карт и NFS модулей для решения вопросов информационной безопасности

Определение DDOS атаки на магистральные каналы связи клиента посредством отраженных DNS-запросов оператора связи

Метод PROBABILISTIC MODEL CHECKING для протоколов безопасности

Архитектура высокоэффективных систем биометрического контроля доступа на основе радужной оболочки глаза

Оценка защищенности предприятия от каналов утечки акустической информации

14.1.4. Темы курсовых проектов / курсовых работ

web-ориентированная информационная система

web-ориентированная информационная система

персональная информационная система

корпоративная информационная система

медицинская информационная система

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	Виды дополнительных оценочных	Формы контроля и оценки

Согласована на портале № 48789

обучающихся	материалов	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, 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 № 48789