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

Документ подписан электронной подписью
Сертификат: a1119608-cdff-4455-b54e-5235117c185c
Владелец: Сенченко Павел Васильевич
Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Разработка и эксплуатация защищенных автоматизированных систем

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль) / специализация: **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4, 5**
Семестр: **8, 9**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	8 семестр	9 семестр	Всего	Единицы
1	Лекции	20	30	50	часов
2	Практические занятия	30	30	60	часов
3	Контроль самостоятельной работы (курсовой проект / курсовая работа)	0	36	36	часов
4	Всего аудиторных занятий	50	96	146	часов
5	Самостоятельная работа	58	120	178	часов
6	Всего (без экзамена)	108	216	324	часов
7	Подготовка и сдача экзамена	0	36	36	часов
8	Общая трудоемкость	108	252	360	часов
		3.0	7.0	10.0	З.Е.

Зачёт: 8 семестр
Экзамен: 9 семестр
Курсовой проект / курсовая работа: 9 семестр

Томск

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) 10.05.03 Информационная безопасность автоматизированных систем, утвержденного 01.12.2016 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

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью преподавания дисциплины является: освоение основных методов, 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 «Разработка и эксплуатация защищенных автоматизированных систем» (Б1.Б.05.05) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Разработка и эксплуатация защищенных автоматизированных систем.

Последующими дисциплинами являются: Разработка и эксплуатация защищенных автоматизированных систем.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-1 способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранных языках;
– ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы;
– ПК-8 способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем;
– ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности;
– ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы;
– ПК-13 способностью участвовать в проектировании средств защиты информации автоматизированной системы;
– ПК-20 способностью организовывать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности;
– ПК-25 способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций;
– ПК-28 способностью управлять информационной безопасностью автоматизированной системы;

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 дея-

тельности 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; − 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 10.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры	
		8 семестр	9 семестр
Аудиторные занятия (всего)	146	50	96
Лекции	50	20	30
Практические занятия	60	30	30
Контроль самостоятельной работы (курсовой проект / курсовая работа)	36	0	36
Самостоятельная работа (всего)	178	58	120
Выполнение курсового проекта / курсовой работы	36	0	36
Проработка лекционного материала	96	42	54
Подготовка к практическим занятиям, семинарам	46	16	30
Всего (без экзамена)	324	108	216
Подготовка и сдача экзамена	36	0	36
Общая трудоемкость, ч	360	108	252
Зачетные Единицы	10.0	3.0	7.0

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
8 семестр						
1 Поиск, изучение, обобщение и систематизация научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности.	2	0	0	4	6	ПК-5
2 Составление технического задания на автоматизированные информационные системы	2	0	0	4	6	ПК-5
3 Проектирование автоматизированных информационных систем	2	10	0	12	24	ПК-5
4 Основные стадии создания автоматизированных информационных систем	4	10	0	14	28	ПК-5
5 Содержание работ на этапах создания автоматизированных информационных систем	4	10	0	16	30	ПК-5
6 Средства автоматизации проектирования автоматизированных информационных систем	6	0	0	8	14	ПК-5
14 Составление технического задания на разработку автоматизированной системы	0	0	0	0	0	
15 Проведение предпроектного исследования. Защита результатов научно-исследовательской работы	0	0	0	0	0	
16 Реализация модуля безопасности системы	0	0	0	0	0	
Итого за семестр	20	30	0	58	108	
9 семестр						
7 Средства построения пользовательского интерфейса	4	10	36	27	41	ПК-12, ПК-25, ПК-28, ПК-5, ПК-9
8 Средства разработки программноинформационного ядра информационных систем	4	10		27	41	ПК-25, ПК-28, ПК-5, ПК-9
9 Тестирование автоматизированных информационных систем	4	0		8	12	ПК-5
10 Подготовка приложения к распро-	4	10		18	32	ПК-5

странению						
11 Ввод в эксплуатацию автоматизированных информационных систем	4	0		8	12	ПК-5
12 Эксплуатация автоматизированных информационных систем	4	0		8	12	ПК-5
13 Анализ рисков информационной безопасности Автоматизированной системы	6	0		24	30	ПК-13, ПК-20, ПК-25, ПК-28, ПК-5, ПК-9
Итого за семестр	30	30	36	120	216	
Итого	50	60	36	178	324	

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
8 семестр			
1 Поиск, изучение, обобщение и систематизация научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности.	Поиск, накопление и обработканаучнотехнической информации.Использованиеклассификаций.Электронные формы информационныхресурсов документов. Обработканаучно-технической информации,еёфиксация и хранение. Информационнопоисковые системы для поискадокументов.Патентный закон РоссийскойФедерации от 23 сентября 1992 г. №3517-1 с изменениями идополнениями,внесеннымиФедеральным законом от 07 февраля2003г. // Доступ из справ.-правовойсистемы-Консультант-Плюс	2	ПК-5
	Итого	2	
2 Составление технического задания на автоматизированные информационные системы	Предмет и задачи курса. Краткий обзоризучаемого материала на семестр.Изучениегосударственных стандартов, содержащихтребования к составлению техническойдокументации на этапе планирования работ - ГОСТ 21552-84«Средства вычислительной техники.Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование ихранение», ГОСТ19.201-78 «ЕСКД Техническое здание.Требование к содержанию оформлению» и ГОСТ 34.602-89«Информационная технология.Комплекс стандартов на автоматизированные системы.Техническое задание на создание автоматизированной системы»	2	ПК-5
	Итого	2	

3 Проектирование автоматизированных информационных систем	Изучение государственных стандартов, содержащих требования, устанавливаемыероссийскимзаконодательством к построениюавтоматизированных систем-ГОСТ24.104-85 «Автоматизированные системы управления. Общие требования.Единая системастандартов» и ГОСТ34.003-90«Информационная технология.-Комплекс стандартов на автоматизированные системы.Термины и определения».Изучение специфики научно-исследовательской работы.	2	ПК-5
	Итого	2	
4 Основные стадии создания автоматизированных информационных систем	Изучение государственных стандартов,содержащих требования, устанавливаемые российским законодательством к стадиям создания автоматизированных систем - ГОСТ 19.102-77 «ЕСПД Стадииразработки», ГОСТ 24.601-86 «Автоматизированные системы. Стадии создания»,ГОСТ 24.602-86 «Автоматизированныесистемы управления. Со-став и содержание работ по стадиям создания» и ГОСТ34.601-90 «Информационная технология.Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания». Рассмотрение вопроса разбиения проекта на этапы и определения ключевых параметров каждого изних. Рассмотрение методики построенияIDEF.	4	ПК-5
	Итого	4	
5 Содержание работ на этапах создания автоматизированных информационных систем	Изучение государственных стандартов,содержащих требования, устанавливаемыероссийским законодательством к оформлению документации по этапам разработки –ГОСТ 19.101-77 (СТ СЭВ 1626-79)«ЕСПДВиды программ и программных документов» и ГОСТ34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированныхсистем». Ознакомление с ГОСТ РИСО/МЭК15408-1-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценкибезопасности информационных технологий. Часть 1. Введение и общая модель».Рассмотрение типового комплекта документации.	4	ПК-5
	Итого	4	
6 Средства	Изучение государственного стандарта, со-	6	ПК-5

автоматизации проектирования автоматизированных информационных систем	держащего требования, устанавливаемыероссийским законодательством к оформлению алгоритмов - ГОСТ 19.701-90(ИСО 5807-85) «ЕСПД Схемы алгоритмов, программ данных и систем. Рассмотрение вопросов, связанных с построениеми реализацией алгоритмов. Ознакомлениес 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 оценочныхуровней доверия и классификации автоматизированных систем.		
	Итого	6	
Итого за семестр		20	
9 семестр			
7 Средства построения пользовательского интерфейса	Изучение государственных стандартов,содержащих требования, устанавливаемыероссийским законодательством к параметрам пользовательского интерфейса – ГОСТР ИСО 9241-11-2010 «Эргономические требования к проведению офисных работ с использованием видеодисплейных терминалов (VDT).Руководство по обеспечению пригодности использования» иГОСТ РИСО 9241-210-2012 «Эргономика взаимодействия человек-система. Человеко-ориентированное проектирование интерактивных систем». Определение ключевых параметров для построения пользовательского интерфейса.Рассмотрениепримеров документации.	4	ПК-5
	Итого	4	
8 Средства разработки программноинформационного ядра информационных систем	Изучение государственных стандартов,содержащих требования, устанавливаемые российским законодательством к построению модуля безопасности - ГОСТ Р50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования», ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации» иГОСТ Р ИСО/МЭК 15408-2-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критериоценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности».Ознакомлениес содержанием ГОСТ	4	ПК-5

	Р ИСО/МЭК I54O8-3-2OO8 «Информационная технология. Методы и средства обеспечения Безопасности. Критерии оценки Безопасности информационных технологий. Часть 3. Требования доверия к безопасности Условные обозначения». Изучение технологии заботы ядра безопасности, мониторов обращений и прочих компонентов, позволяющих обеспечить безопасность создаваемого программного комплекса. Рассмотрение примеров документации. Рассмотрение типовых профилей защиты автоматизированных систем.		
	Итого	4	
9 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.	4	ПК-5
	Итого	4	
10 Подготовка приложения к распространению	Изучение государственных стандартов, содержащих требования, устанавливаемые российским законодательством к документации на создаваемую программную продукцию - ГОСТ 19.106-78 (СТ СЭВ 2088-80) «ЕСКД Требования к программным документам, выполненным печатным способом», РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов» и ГОСТ 19.501-78 «ЕСПД Формуляр. Требования к содержанию и оформлению». Рассмотрение примеров документации. Изучение принципов документального процесса сопровождения автоматизированной системы.	4	ПК-5
	Итого	4	
11 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 иоформлению» и ГОСТ 19.505-79 «Руководство оператора. Требования к содержанию и оформлению». Определение ключевых различий между руководствами программиста и администратора.	4	ПК-5

	Рассмотрение примеров документации.		
	Итого	4	
12 Эксплуатация автоматизированных информационных систем	Обобщение результатов изучения предыдущих этапов. Рассмотрение автоматизированной системы на этапе эксплуатации, условий вывода из эксплуатации. Изучение требований к управлению информационной безопасностью и восстановлению систем после сбоя.	4	ПК-5
	Итого	4	
13 Анализ рисков информационной безопасности Автоматизированной системы	Оценка эффективности системы защиты-информации, сравнительная характеристика своей системы защиты информации возможностей нарушителя по ее-преодолению. Модель и критерии 'эффективности системы эащиты. Методымногокритериальной эценки 'эффективности: метод Последовательных уступок иметод Анализа иерархий.	6	ПК-5
	Итого	6	
Итого за семестр		30	
Итого		50	

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	10	11	12	13	14	15	16
Предшествующие дисциплины																
1 Разработка и эксплуатация защищенных автоматизированных систем	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Последующие дисциплины																
1 Разработка и эксплуатация защищенных автоматизированных систем	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

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.	
ПК-1			+		Защита курсовых проектов / курсовых работ
ПК-5	+	+	+	+	Экзамен, Защита курсовых проектов / курсовых работ, Тест, Отчет по курсовому проекту / курсовой работе, Отчет по практическому занятию
ПК-8			+		Отчет по курсовому проекту / курсовой работе
ПК-9			+	+	Защита курсовых проектов / курсовых работ, Отчет по курсовому проекту / курсовой работе, Тест
ПК-12			+	+	Защита курсовых проектов / курсовых работ, Отчет по курсовому проекту / курсовой работе, Тест
ПК-13			+	+	Защита курсовых проектов / курсовых работ, Отчет по курсовому проекту / курсовой работе, Тест
ПК-20			+	+	Защита курсовых проектов / курсовых работ, Отчет по курсовому проекту / курсовой работе, Тест
ПК-25			+	+	Защита курсовых проектов / курсовых работ, Тест, Отчет по курсовому проекту / курсовой работе
ПК-28			+	+	Защита курсовых проектов / курсовых работ, Отчет по курсовому проекту / курсовой работе, 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
8 семестр			

3 Проектирование автоматизированных информационных систем	Анализ сертифицированного СЗИ на предмет его функциональных возможностей-.Построение модели типа «черный ящик»для исследуемой системы с последующейдетализацией по технологии IDEF0.	10	ПК-5
	Итого	10	
4 Основные стадии создания автоматизированных информационных систем	Оценка общих критериев и определение класса защищенности автоматизированнойсистемы.	10	ПК-5
	Итого	10	
5 Содержание работ на этапах создания автоматизированных информационных систем	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.	10	ПК-5
	Итого	10	
Итого за семестр		30	
9 семестр			
7 Средства построения пользовательского интерфейса	Проектирование планируемой автоматизированной системы с учетом государственных стандартов.	10	ПК-5
	Итого	10	
8 Средства разработки программноинформационного ядра информационных систем	Анализ реализации модулей автоматизированных систем	10	ПК-5
	Итого	10	
10 Подготовка приложения к распространению	Анализ полноты проектнойдокументации	10	ПК-5
	Итого	10	
Итого за семестр		30	
Итого		60	

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
8 семестр				
1 Поиск, изучение, обобщение и	Проработка лекционного материала	4	ПК-5	Тест, Экзамен

систематизация научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности.	Итого	4		
2 Составление технического задания на автоматизированные информационные системы	Проработка лекционного материала	4	ПК-5	Тест, Экзамен
	Итого	4		
3 Проектирование автоматизированных информационных систем	Подготовка к практическим занятиям, семинарам	4	ПК-5	Отчет по практическому занятию, Тест, Экзамен
	Проработка лекционного материала	8		
	Итого	12		
4 Основные стадии создания автоматизированных информационных систем	Подготовка к практическим занятиям, семинарам	4	ПК-5	Отчет по практическому занятию, Тест, Экзамен
	Проработка лекционного материала	10		
	Итого	14		
5 Содержание работ на этапах создания автоматизированных информационных систем	Подготовка к практическим занятиям, семинарам	8	ПК-5	Отчет по практическому занятию, Тест, Экзамен
	Проработка лекционного материала	8		
	Итого	16		
6 Средства автоматизации проектирования автоматизированных информационных систем	Проработка лекционного материала	8	ПК-5	Тест, Экзамен
	Итого	8		
Итого за семестр		58		
9 семестр				
7 Средства построения пользовательского интерфейса	Подготовка к практическим занятиям, семинарам	10	ПК-5, ПК-12, ПК-25, ПК-28, ПК-9	Отчет по курсовому проекту / курсовой работе, Отчет по практическому
	Проработка лекционно-	7		

	го материала			занятию, Тест, Экзамен
	Выполнение курсового проекта / курсовой работы	10		
	Итого	27		
8 Средства разработки программноинформационного ядра информационных систем	Подготовка к практическим занятиям, семинарам	10	ПК-5, ПК-25, ПК-28, ПК-9	Защита курсовых проектов / курсовых работ, Отчет по практическому занятию, Тест, Экзамен
	Проработка лекционного материала	7		
	Выполнение курсового проекта / курсовой работы	10		
	Итого	27		
9 Тестирование автоматизированных информационных систем	Проработка лекционного материала	8	ПК-5	Тест, Экзамен
	Итого	8		
10 Подготовка приложения к распространению	Подготовка к практическим занятиям, семинарам	10	ПК-5	Отчет по практическому занятию, Тест, Экзамен
	Проработка лекционного материала	8		
	Итого	18		
11 Ввод в эксплуатацию автоматизированных информационных систем	Проработка лекционного материала	8	ПК-5	Тест, Экзамен
	Итого	8		
12 Эксплуатация автоматизированных информационных систем	Проработка лекционного материала	8	ПК-5	Тест, Экзамен
	Итого	8		
13 Анализ рисков информационной безопасности Автоматизированной системы	Проработка лекционного материала	8	ПК-5, ПК-13, ПК-20, ПК-25, ПК-28, ПК-9	Защита курсовых проектов / курсовых работ, Тест, Экзамен
	Выполнение курсового проекта / курсовой работы	16		
	Итого	24		
Итого за семестр		120		
	Подготовка и сдача экзамена	36		Экзамен
Итого		214		

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
9 семестр		
Формирование заданий на курсовую работу. Составление технического задания на разработку автоматизированной системы.	8	ПК-1, ПК-13, ПК-25, ПК-5, ПК-9
Проведение предпроектного исследования. Защита результатов курсовой работы.	8	
Реализация модуля безопасности системы	12	
Анализ результатов выполнения этапов написания курсовойработы	8	
Итого за семестр	36	

10.1. Темы курсовых проектов / курсовых работ

Примерная тематика курсовых проектов / курсовых работ:

- Курсовая работа по дисциплине служит для закрепления практических умений и проверки эффективности владения приобретенными навыками. Курсовая работа включает в себя написание программного комплекса, содержащего N модулей из следующего перечня:
- – модуль идентификации/аутентификации;
- – модуль разграничения доступа;
- – модуль журналирования;
- – модуль управления;
- – модуль шифрования.
- Помимо этого, в рамках курсовой работы от студента потребуется составить комплект документации к разработанному программному комплексу с учетом имеющихся ГОСТов по их оформлению.

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
8 семестр				
Отчет по практическому занятию	20	20	30	70
Тест	10	10	10	30
Итого максимум за период	30	30	40	100
Нарастающим итогом	30	60	100	100
9 семестр				
Отчет по практическому	10	10	20	40

занятию				
Тест	10	10	10	30
Итого максимум за период	20	20	30	70
Экзамен				30
Нарастающим итогом	20	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)
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. Технология разработки программных систем [Электронный ресурс]: Учебное пособие / И. Г. Боровской - 2012. 260 с — Режим доступа: https://edu.tusur.ru/publications/2436 (дата обращения: 05.07.2021).

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: 05.07.2021).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Основы проектирования защищенных телекоммуникационных систем [Электронный ресурс]: Методические указания по курсовому проектированию, практическим занятиям и самостоятельной работе студентов / А. М. Голиков - 2015. 27 с. — Режим доступа: https://edu.tusur.ru/publications/6297 (дата обращения: 05.07.2021).

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;
- в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. https://edu.tusur.ru; – образовательный портал университета;
2. http://www.lib.tusur.ru – библиотека университета;
3. http://protect.gost.ru; – база государственных стандартов.
4. Дополнительно к профессиональным базам данных рекомендуется использовать информационные, справочные и нормативные базы данных https://lib.tusur.ru/ru/resursy/bazy-dannyh

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 Windows 10
- VirtualBox

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

1. 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 научноинформаци-

онной

деятельности (НИД).

2. Документ - это

о Материальный носитель с закрепленной на ней социальной (функционирующей в обществе) информацией, в том числе научной, учебной, производственной.

о Систематизированные сведения об опубликованных или еще неопубликованных, а также

непубликуемых материалах, либо результат анализа и обобщения сведений, представленных в первоисточниках.

о Монографии, сборники статей, статьи из научных, научно-технических, производственных журналов, препринты, авторефераты диссертации, патенты и др.

о Отчеты о научно-исследовательских работах (НИР) и опытно-конструкторских разработок

(ОКР), диссертации, научные переводы из зарубежных журналов, конструкторскую документацию

на нестандартное оборудование, решения ученых советов, технические задания, проекты и др.

3. Составление библиографического описания, аннотирование, реферирование и составление обзоров – это

о Анализ первичных документов.

о Анализ вторичных документов.

о Процедуры каталогизации.

о Процессы библиографического анализа.

4. Самая лаконичная и обязательная разновидность вторичного документа, создаваемая с

целью идентификации и выявления совокупности внешних признаков без ознакомления с содержанием текста первичного документа – это

о Обзор.

о Аннотация.

о Реферат.

о Библиографическая запись.

5. Подробное отображение текста первичного документа с целью идентификации новизны,

полноты, полезности содержания, выявления основных наиболее важных фактов, гипотез, концепций, теорий, методик и методов – это

о Аннотация.

о Библиографическая запись .

о Реферат.

о Обзор.

6. Краткая характеристика первичного документа с точки зрения содержания, особенностей

назначения, формы, тематики и других особенностей – это

о Аннотация.

о Обзор.

о Библиографическая запись .

о Реферат

7. Результат глубокого анализа множества первичных документов, сходных по тематике разработок, характеру деятельности, выполняемым этапам, задачам, исполнителям с целью обобщения, установления разницы и сходства, оценки, путей развития проблемы, степени их разработанности и возможного прогноза – это

о Библиографическая запись .

о Обзор.

о Аннотация.

о Реферат.

8. - федеральные органы НТИ и научно-технические библиотеки (НТБ);

- отраслевые органы НТИ и НТБ;

- региональные центры НТИ (республиканские институты, межотраслевые центры и отраслевые республиканские службы НТИ) и НТБ;

- информационные отделы (бюро) в научно-исследовательских институтах, проектных,

конструкторских и других организациях – это

o Органы ЦНТИ.

o Органы НТИ.

o Органы НТИ и НТБ.

o Органы ГСНТИ.

9. Релевантность – это

o получение той научно-технической информации, которая будет способствовать получению нового знания.

o соотношение объема полезной информации к общему объему полученной информации.

o степень соответствия запроса и найденного, уместность результата.

o соответствие найденных информационно-поисковой системой документов информационным потребностям пользователя.

10. Проранжируйте по времени Порядок выполнения патентных исследований по ГОСТ Р 15.011-96.

o 1.

- определение задач, видов и методов проведения исследовании, разработка задания на проведение исследований;
- определение требований к поиску документации, разработка регламента поиска;
- поиск и отбор документации в соответствии с утвержденным регламентом и оформление отчета о поиске;
- систематизация и анализ отобранной документации.

o 2.

- поиск и отбор документации в соответствии с утвержденным регламентом и оформление отчета о поиске;
- систематизация и анализ отобранной документации.
- определение задач, видов и методов проведения исследовании, разработка задания на проведение исследований;
- определение требований к поиску документации, разработка регламента поиска;

o 3.

- определение требований к поиску документации, разработка регламента поиска;
- определение задач, видов и методов проведения исследовании, разработка задания на проведение исследований;
- поиск и отбор документации в соответствии с утвержденным регламентом и оформление отчета о поиске;
- систематизация и анализ отобранной документации.

o 4.

- определение задач, видов и методов проведения исследовании, разработка задания на проведение исследований;
- определение требований к поиску документации, разработка регламента поиска;
- систематизация и анализ отобранной документации.
- поиск и отбор документации в соответствии с утвержденным регламентом и оформление отчета о поиске.

11. Дайте определение :

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

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

o Риск - это стоимостное выражение вероятностного события, ведущего к потерям.

o Риск - это процесс получения количественной или качественной оценки ущерба, который может произойти в случае реализации угрозы безопасности ИС

12. Проранжируйте компоненты ИС по возрастанию риска информационной безопасности

o 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.;

- 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.;

13. 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;

14. 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.

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

o Обнаружение Несанкционированного доступа к данным;

o Обнаружение Руткита;

o Обнаружение Эксплойта.

o Обнаружение ошибки Сетевого программного обеспечения.

16. В чем суть требований семейства ИСО/МЭК-15408 FTP_ITC «Доверенный канал»?

o Реализация ПФБ управления доступом;

o Реализация связывания пользователь – субъект.

o Реализация ПФБ управления информационными потоками;

o Реализация связывания субъект – объект;

17. 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.

18. Проранжируйте по времени основные этапы, проводимые при анализе риска безопасности ИС

o 1.

Определение уязвимых мест ИС.

Оценка ожидаемых размеров потерь.

Оценка выгоды от применения предполагаемых мер.

Описание компонентов ИС.

Оценка вероятностей проявления угроз безопасности ИС.

Обзор возможных методов защиты и оценка их стоимости.

o 2.

Описание компонентов ИС.

Оценка вероятностей проявления угроз безопасности ИС.

Обзор возможных методов защиты и оценка их стоимости.

Определение уязвимых мест ИС.

Оценка ожидаемых размеров потерь.

Оценка выгоды от применения предполагаемых мер.

o 3.

Описание компонентов ИС.

Определение уязвимых мест ИС.

Оценка вероятностей проявления угроз безопасности ИС.

Оценка ожидаемых размеров потерь.

Обзор возможных методов защиты и оценка их стоимости.

Оценка выгоды от применения предполагаемых мер.

o 4.

Описание компонентов ИС.

Определение уязвимых мест ИС.

Оценка вероятностей проявления угроз безопасности ИС.

Обзор возможных методов защиты и оценка их стоимости.

Оценка ожидаемых размеров потерь.

Оценка выгоды от применения предполагаемых мер.

19. Проранжируйте по возрастанию значимости примеры опасных воздействий, которые могут привести к нарушению конфиденциальности, целостности и доступности компонентов и ресурсов ИС

o 1.

Стихийные бедствия.

Преднамеренные нарушения. Действия обиженных служащих, взяточников, любопытных посетителей, конкурентов и т.д.

Внешние воздействия. Подключение к сети, интерактивная работа, воздействие хакеров.

Неумышленные ошибки. Ввод ошибочной команды, данных, использование неисправных устройств, носителей, а также пренебрежение некоторыми правилами безопасности.

о 2.

Стихийные бедствия.

Неумышленные ошибки. Ввод ошибочной команды, данных, использование неисправных устройств, носителей, а также пренебрежение некоторыми правилами безопасности.

Преднамеренные нарушения. Действия обиженных служащих, взяточников, любопытных посетителей, конкурентов и т.д.

Внешние воздействия. Подключение к сети, интерактивная работа, воздействие хакеров.

о 3.

Стихийные бедствия.

Неумышленные ошибки. Ввод ошибочной команды, данных, использование неисправных устройств, носителей, а также пренебрежение некоторыми правилами безопасности.

Внешние воздействия. Подключение к сети, интерактивная работа, воздействие хакеров.

Преднамеренные нарушения. Действия обиженных служащих, взяточников, любопытных посетителей, конкурентов и т.д.

о 4.

Стихийные бедствия.

Внешние воздействия. Подключение к сети, интерактивная работа, воздействие хакеров.

Преднамеренные нарушения. Действия обиженных служащих, взяточников, любопытных посетителей, конкурентов и т.д.

Неумышленные ошибки. Ввод ошибочной команды, данных, использование неисправных устройств, носителей, а также пренебрежение некоторыми правилами безопасности.

20. Проранжируйте по степени эффективности методы оценки вероятностей проявления угроз

о 1.

Эмпирическая оценка количества проявлений угрозы за некоторый период времени. Как правило, этот метод применяется для оценки вероятности стихийных бедствий.

Непосредственная регистрация событий. Обычно этот метод применяется для оценки вероятности часто проявляющихся событий (попытки входа в систему, доступ к определенному объекту и т.д.).

Оценка частоты проявления угрозы по таблице. Некоторые методы анализа риска позволяют оценить вероятность появления каких либо событий по специальной таблице, выбирая один из коэффициентов.

Метод «Дельфийский оракул». С помощью этого метода каждый конкретный коэффициент выводится из частоты появления определенного события. Эти частоты накапливаются и преобразуются в коэффициенты модели угроз.

о 2.

Эмпирическая оценка количества проявлений угрозы за некоторый период времени. Как правило, этот метод применяется для оценки вероятности стихийных бедствий.

Метод «Дельфийский оракул». С помощью этого метода каждый конкретный коэффициент выводится из частоты появления определенного события. Эти частоты накапливаются и преобразуются в коэффициенты модели угроз.

Оценка частоты проявления угрозы по таблице. Некоторые методы анализа риска позволяют оценить вероятность появления каких либо событий по специальной таблице, выбирая один из коэффициентов.

Непосредственная регистрация событий. Обычно этот метод применяется для оценки вероятности часто проявляющихся событий (попытки входа в систему, доступ к определенному объекту и т.д.).

о 3.

Эмпирическая оценка количества проявлений угрозы за некоторый период времени. Как правило, этот метод применяется для оценки вероятности стихийных бедствий.

Оценка частоты проявления угрозы по таблице. Некоторые методы анализа риска позволяют оценить вероятность появления каких либо событий по специальной таблице, выбирая один из коэффициентов.

Непосредственная регистрация событий. Обычно этот метод применяется для оценки вероятности часто проявляющихся событий (попытки входа в систему, доступ к определенному объекту и т.д.).

Метод «Дельфийский оракул». С помощью этого метода каждый конкретный коэффициент выводится из частоты появления определенного события. Эти частоты накапливаются и преобразуются в коэффициенты модели угроз.

о 4.

Эмпирическая оценка количества проявлений угрозы за некоторый период времени. Как правило, этот метод применяется для оценки вероятности стихийных бедствий.

Метод «Дельфийский оракул». С помощью этого метода каждый конкретный коэффициент выводится из частоты появления определенного события. Эти частоты накапливаются и преобразуются в коэффициенты модели угроз.

Непосредственная регистрация событий. Обычно этот метод применяется для оценки вероятности часто проявляющихся событий (попытки входа в систему, доступ к определенному объекту и т.д.).

Оценка частоты проявления угрозы по таблице. Некоторые методы анализа риска позволяют оценить вероятность появления каких либо событий по специальной таблице, выбирая один из коэффициентов.

21. Назовите основные угрозы информационной безопасности ИС:

о Нарушение конфиденциальности информации. Информация, хранимая и обрабатываемая в ИС, может иметь большую ценность для ее владельца. Ее использование другими лицами наносит значительный ущерб интересам владельца.

о Нарушение целостности информации. Потеря целостности информации (полная или частичная, компрометация, дезинформация) -угроза близкая к ее раскрытию.

о Нарушение (частичное или полное) работоспособности ИС (нарушение доступности).

о Несанкционированный доступ (НСД). Он заключается в получении пользователем доступа к объекту, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности.

22. Назовите уровни обеспечения информационной безопасности ИС:

о Инициация. Закупка. Установка. Эксплуатация.

о Законодательный, административный, процедурный, программно-технический.

о Организационный; Технологический; Процедурный; Технический.

о Техническое задание, Рабочий проект, Внедрение, Эксплуатация.

23. На каком этапе проектирования ИС внедряется Блок информационной безопасности ИС?

о На каждом из перечисленных этапов соответствующим образом, сообразно данному этапу;

о На этапе рабочего проекта;

о На этапе технического задания;

о На этапе эскизного проекта;

24. На каком уровне внедряется Принцип минимизации привилегий?

о Административный;

о Процедурный;

о Технический.

о Программный;

25. Принцип минимизации привилегий – это реализация Теоремы

о Диффи-Хеллмана симметричного шифрования;

о Харрисона-Ульмана распределения прав доступа;

о Белла-Лападулы основная теорема безопасности;

o Шамира-Алдемана асимметричного шифрования
26. Сформулируйте условия синтеза полностью безопасной ИС:
o Интерфейсы ИС полностью безопасны, машина реальная;
o Ядро и все интерфейсы ИС полностью безопасны, машина виртуальная;
o Ядро и все интерфейсы ИС полностью безопасны, машина реальная.
o Ядро ИС является полностью безопасным, машина реальная;
27. Какие нормативные документы регламентируют создание ТЗ на защиту информации в ИС?
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»;
o Приказ ФСТЭК России от 14.03.2014 г. №31;
28. На основании каких нормативных документов строится проектная документация на систему защиты ИС?
o ГОСТ 34.603;
o ГОСТ Р 51624;
o ГОСТ 34.601;
o ГОСТ Р 51583;
29. На основании каких нормативных документов строится эксплуатационная документация на систему защиты ИС?
o ГОСТ 34.601;
o ГОСТ 34.201.
o ГОСТ Р 51583;
o ГОСТ 34.603;
30. Какой нормативный документ определяет классы защищенности ИС?
o Постановление Правительства РФ № 1119;
o Постановление Правительства РФ № 676;
o Приказ ФСТЭК РФ №17 от 11.02.2013;
o Постановление Правительства РФ № 675.
31. Выполним следующий запрос на языке Transact-SQL:

```
declare @time_1 int, @time_2 int, @time_3 int
set @time_1=@@IDLE
SELECT @time_ms AS 'время 1'
set @time_2=@@IDLE / 360000
SELECT @time_2 AS 'время 2'
set @time_3=(@@IDLE % 360000)/6000
SELECT @time_3 AS 'время 3'
```

Сколько Msek проработал сервер?
o @time_1;
o @@IDLE / 360000;
o @time_2;
o @time_3;
32. Выполним следующий запрос на языке Transact-SQL:

```
declare @year int
set @year=Year(GetDate ())
SELECT @year AS 'год'
if @year%4 = 0 print 'no'
else print ' yes '
```

В случае печати 'no' что можно сказать о текущем годе?
o Сумма цифр года не делится на 4;
o Год не является високосным;
o Сумма цифр года делится на 4;
o Год является високосным;
33. Выполним следующий запрос на языке Transact-SQL:

```
declare @v bigint, @t int, @r int, @s varchar(100)
select @v=23, @t=1, @r=0, @s=convert(varchar(100),@v)
while @t<=len(@s)
begin
set @r=@r+substring(@s,@t,1)
set @t=@t+1
end
```

Что будет в ячейке @r ?

- Число букв слова;
- Сумма цифр в заданной строке символов;
- Цифра в символьном формате;
- Число цифр числа;

34. Выполним следующий запрос на языке Transact-SQL:

```
declare @tlm char(100), @tlm1 varchar(100), @countW int, @lenT int, @npos int, @pos int
set @countW=0
set @tlm='I will arrivel today. Отделение почты.'
set @tlm1 = Ltrim(Rtrim(SubString(@tlm,1,CharIndex ('.',@tlm, 1))))
select @tlm1
set @lenT=Len(@tlm1)
select @lenT as 'len'
```

Что будет в ячейке @tlm1 ?

- исходный текст;
- длина исходного текста в символах;
- исходный текст очищенный от пробелов слева и справа;
- исходный текст очищенный от пробелов слева.

35. Выполним следующий запрос на языке Transact-SQL:

```
declare @tlm char(100), @tlm1 varchar(100), @countW int, @lenT int, @npos int, @pos int
while @pos<@lenT
begin
set @npos=CharIndex (' ',@tlm1,@pos)+1
if @npos=1 break
else
begin
set @countW=@countW+1
set @pos=@npos
end
end
```

Что будет в ячейке @countW ?

- число слов исходного текста;
- номер первого пробела в тексте;
- число букв исходного текста;
- число пробелов исходного текста;

36. Выполним следующий запрос на языке Transact-SQL:

```
declare @tlm char(100), @tlm1 varchar(100), @countW int, @lenT int, @npos int, @pos int
select @countW as 'words'
select 'cost: ' + convert(char(3),(@countW*33)/100) + 'cost1' + convert(char(2),
(@countW*33)%100) + 'cost2'
print 'cost: ' + convert(char(3),(@countW*33)/100) + 'cost1' + convert(char(2),
(@countW*33)%100) + 'cost2'
```

Что будет в ячейке char(2) ?

- рубли и копейки;
- копейки;
- копейки и рубли;
- рубли;

37. Выполним следующий запрос на языке Transact-SQL:
```
declare @alf char(27), @k int, @stroka varchar(40), @len int, @nposalf int, @npos int, @bukva char, @zamena char ,@stroka2 varchar(40), @stroka3 varchar(40)
set @stroka='Victor'
set @alf='ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'
set @len=Len(@stroka)
print 'len= '+ convert(char,@len)
set @k=2
print 'before= '+@stroka
```
Что будет напечатано?
o Перевернутый исходный текст;
o Длина строки и строка;
o Строка до конвертации;
o Исходный текст;
38. Определите запрограммированный шифр:
```
declare @alf char(27), @k int, @stroka varchar(40), @len int, @nposalf int, @npos int, @bukva char, @zamena char ,@stroka2 varchar(40), @stroka3 varchar(40)
set @stroka2=''
set @npos=0
while @len>0
begin
set @npos=@npos+1
set @bukva=SubString(@stroka,@npos,1)
set @nposalf=CharIndex (@bukva,@alf,1)
set @zamena=SubString(@alf,@nposalf+@k,1)
set @stroka2=@stroka2+@zamena
set @len=@len-1
End
```
o Шифр сложной замены;
o Шифр простой замены;
o Шифр Цезаря;
o Шифр Гронсфельда;
39. Определите вид кодировки шифра и ключ:
```
declare @alf char(27), @k int, @stroka varchar(40), @len int, @nposalf int, @npos int, @bukva char, @zamena char ,@stroka2 varchar(40), @stroka3 varchar(40)
set @len=Len(@stroka2)
set @stroka3=''
set @npos=0
while @len>0
begin
set @npos=@npos+1
set @bukva=SubString(@stroka2,@npos,1)
set @nposalf=CharIndex(@bukva,@alf,1)
set @zamena=SubString(@alf,@nposalf-@k,1)
set @stroka3=@stroka3+@zamena
set @len=@len-1
End
```
o Прямая кодировка,@k ;
o Обратная кодировка,-@k ;
o Гибридная кодировка,-@k .
o Обратная кодировка,@k ;
40. Выполним следующий запрос на языке Transact-SQL:
```
USE AdventureWorks2008
SELECT BusinessEntityID as [Номер сотрудника], BirthDate as [дата рождения],
```

DateDiff (yy, BirthDate, GetDate ()) as [лет], (DateDiff (mm, BirthDate,
GetDate ())%12) as [мес], Day(GetDate ()) - Day(BirthDate) as [дней]
FROM HumanResources.Employee
Where ((Day(GetDate ()) - Day(BirthDate)) = -1) and (Month(BirthDate)=Month(GetDate()))
ORDER BY [Номер сотрудника]

Что будет распечатано по данному запросу:

o Список сотрудников, у которых в этом месяце День рождения;

o Список сотрудников, у которых в следующем месяце День рождения;

o Список сотрудников, у которых завтра День рождения;

o Список сотрудников, у которых вчера был день рождения.

41. Что такое Уровень гарантированности?

o Полная функциональная спецификация функций безопасности объекта.

o Мера доверия, которая может быть оказана архитектуре и реализации информационной системы;

o Описание архитектуры безопасности.

o Представление реализации функций безопасности объекта.

42. Что такое Механизмы безопасности, согласно Оранжевой книге?

o Произвольное управление доступом; безопасность повторного использования объектов; метки безопасности; принудительное управление доступом.

o Аутентификационные данные и секреты;

o Политики функций безопасности управления доступом и информационными потоками.

o Атрибуты пользователей, ресурсов, субъектов, объектов, сеансов, данных состояния функций безопасности объекта и операций в пределах области действия

43. Назовите классы безопасности, согласно Оранжевой книге.

o (A1, A2, A3, B1, B2, C1, D1) с постепенным возрастанием степени доверия. Наивысший класс – D1.

o (C1, C2, B1, B2, B3, A1) с постепенным возрастанием степени доверия. Наивысший класс – A1.

o (C1, C2, C3, B1, B2,A1) с постепенным возрастанием степени доверия. Наивысший класс – A1;

o (A1, A2, B1, B2, B3, C1, D1) с постепенным возрастанием степени доверия. Наивысший класс – D1.

44. Что лежит в основе проектирования системы управления ИБ предприятия?

o Функции безопасности объекта (предприятия), чьи механизмы осуществляют правила, определенные в функциональных требованиях безопасности и предоставпяют необходимые возможности.

o Функциональные компоненты безопасности, направленные на противодействие угрозам в предполагаемой среде функционирования.

o Политика безопасности организации.

o Зависимое от реализации изложение потребностей в безопасности для конкретного идентифицированного предприятия.

45. Что такое цель безопасности (security objective)?

o Совокупность функциональных возможностей всего аппаратного, программного и программно-аппаратного обеспечения ОО, которые необходимо использовать для корректной реализации ФТБ.

o Требование безопасности (security requirement), то есть требование, изложенное на стандартизованном языке и направленное на достижение безопасности для объекта оценивания.

o Изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и/или предположениям.

o Совокупность правил, описывающих

46. Что отражает политика безопасности организации в контексте ИСО/МЭК – 15408?

o Требование безопасности (security requirement), то есть требование, изложенное на стандартизованном языке и направленное на достижение целей безопасности для организации.

o Совокупность правил, процедур или руководящих принципов в области безопасности для

некоторой организации.

о Цель безопасности (security objective), то есть изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и/или предположениям.

о Безопасное состояние (secure state), то есть состояние, при котором данные функций безопасности организации являются непротиворечивыми и продолжают корректно реализовывать функциональные требования безопасности.

47. Что такое Проблема безопасности (security problem)?

о Изложение, которое в формализованном виде определяет характер и масштабы безопасности, которую должен обеспечивать объект оценки (ОО).

о Изложение угроз продукту ИТ, отличному от ОО, для которого имеются свои функциональные требования, организационно скоординированные с ОО, и который, как предполагается, реализует свои функциональные требования корректно.

о Описание субъектов, пользователей (включая внешние продукты ИТ), объектов, информации, сеансов и/или ресурсов, которые используются при определении ФТБ, и значения которых используются при осуществлении ФТБ.

о Описание угроз, которым должно быть обеспечено противостояние со стороны объекта оценки; политики безопасности организации, осуществляемых ОО, и - предположений, которые определены для ОО и его среды функционирования.

48. Что такое Функциональные возможности безопасности ОО (TOE security functionality)?

о Функциональные возможности всех аппаратных и программных средств объекта оценки(ОО) по обеспечению безопасности ОО.

о Все политики функций безопасности (ПФБ), реализуемые функциями безопасности объекта (ФБО), чьи механизмы осуществляют правила, определенные в функциональных требованиях безопасности (ФТБ).

о Различные политики функций безопасности (ПФБ), определяемые ФТБ. Каждая такая ПФБ специфицирует свою область действия, определяющую субъекты, объекты, ресурсы или информацию и операции, по отношению к которым она применяется.

о Совокупность функциональных возможностей всего аппаратного, программного и программно-аппаратного обеспечения объекта оценки (ОО), которые необходимо использовать для корректной реализации ФТБ.

49. Что такое Функциональные компоненты безопасности?

о Те части ОО, которые направлены на корректную реализацию ФТБ и определяются как Функциональные компоненты безопасности объекта оценки (ФКБ). ФКБ объединяют функциональные возможности всех аппаратных, программных и программно-аппаратных средств ОО, на которые как непосредственно, так и косвенно возложено обеспечение безопасности.

о В случае распределенного ОО, состоящего из нескольких разделенных частей, это части ОО, обеспечивающие реализацию ФТБ и выполнение конкретного сервиса для ОО и взаимодействующие с другими частями ОО через внутренний канал связи.

о Совокупность функциональных компонентов, предназначенных для использования в качестве стандартных шаблонов, на основе которых следует устанавливать функциональные требования к ОО. ИСО/МЭК 15408-2 содержит каталог функциональных компонентов, систематизированных по семействам и классам.

о Если ОО состоит из нескольких частей, то каждая часть может иметь собственное подмножество ФБО, которое обменивается данными ФБО и пользователей через внутренние каналы связи с другими подмножествами ФБО. В этом случае части ФБО формируют объединенные ФБО, которые называются функциональными компонентами безопасности для этого ОО.

50. Что такое Компоненты доверия к безопасности?

о Элементы действий разработчика, определяющие действия, которые должны выполняться разработчиком. Этот набор действий далее уточняется доказательным материалом, упоминаемым в

последующем наборе элементов.

о Элементы содержания и представления свидетельств, определяющие требуемые свидетельства и отражаемую в них информацию. Требования к содержанию и представлению свидетельств обозначены буквой "С" после номера элемента.

о Набор действий, непосредственно включающий в себя подтверждение того, что требования, предписанные элементами содержания и представления свидетельств, выполнены, а также явные действия и анализ, которые должны выполняться в дополнение к уже проведенным разработчиком.

о Совокупность компонентов доверия, предназначенных для использования в качестве стандартных шаблонов, на основе которых следует устанавливать требования доверия к ОО.

ИСО/МЭК 15408-3 содержит каталог компонентов доверия, систематизированных по семействам и

классам.

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

о Приказ ФСТЭК России от 14.03.2014 г. №31;

о (ГОСТ 34.601, ГОСТ Р 51583);

о Приказ ФСТЭК России от 11.02.2013 №17;

о 149-ФЗ «Об информации, ИТ и о ЗИ»;

52. На основании каких нормативных документов строится проектная документация на систему защиты ИС?

о ГОСТ 34.601;

о ГОСТ Р 51583;

о ГОСТ 34.603;

о ГОСТ Р 51624;

53. На основании каких нормативных документов производятся аттестационные испытания системы защиты ИС?

о ГОСТ РО 0043-003-2012;

о ГОСТ Р 51624;

о ГОСТ 34.603;

о ГОСТ Р 51583;

54. На основании каких нормативных документов строится эксплуатационная документация на систему защиты ИС?

о ГОСТ 34.603;

о ГОСТ 34.201;

о ГОСТ 34.601;

о ГОСТ Р 51583;

55. Какой нормативный документ определяет классы защищенности ИС?

о Постановление Правительства РФ № 1119;

о Постановление Правительства РФ № 676;

о Приказ ФСТЭК РФ №17 от 11.02.2013;

о Постановление Правительства РФ № 675.

56. На основании каких нормативных документов производится внедрение системы защиты ИС?

о ГОСТ 34.601;

о ГОСТ Р 51583;

о ГОСТ Р 51624;

о ГОСТ 34.603;

57. На основании каких нормативных документов производятся приемочные испытания системы защиты ИС?

о ГОСТ 34.601;

о ГОСТ Р 51624;

о ГОСТ Р 51583;

о ГОСТ 34.603;

58. На основании каких нормативных документов производятся предварительные испытания системы защиты ИС?

o ГОСТ Р 51583;

o ГОСТ 34.603;

o ГОСТ 34.201;

o ГОСТ 34.601;

59. На основании каких нормативных документов производится опытная эксплуатация системы защиты ИС?

o ГОСТ 34.603;

o ГОСТ 34.201;

o ГОСТ 34.601;

o ГОСТ Р 51583;

60. Назовите документы ФСТЭК, регулирующие вопросы ЗИ в ИС.

o Требования мер защиты информации в ИС;

o Приказ ФСТЭК России от 11.02.2013 №17;

o Требования о ЗИ, не составляющей ГТ, содержащейся в ИС;

o Меры защиты информации в государственных информационных системах;

61. Назовите показатели защищенности, которые должны поддерживаться СВТ:

o мандатный принцип контроля доступа;

o санкционированное изменение списка защищаемых объектов;

o санкционированное изменение правил разграничения доступа;

o санкционированное изменение списка пользователей СВТ;

62. Для реализации дискретизационного принципа контроля доступа

o При санкционированном внесении в список пользователей нового субъекта ему должны быть назначены классификационные метки.

o КСЗ при вводе новых данных в систему должен запрашивать и получать от санкционированного пользователя классификаци¬онные метки этих данных.

o Каждому пользователю непосредственно прописываются права на чтение, запись и выполнение.

o Внешние классификационные метки (субъектов, объектов) должны точно соответствовать внутренним меткам (внутри КСЗ).

63. Для реализации мандатного принципа контроля доступа

o Для каждой пары (субъект — объект) в СВТ должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (например, читать, писать), т.е. тех типов доступа,

которые являются санкционированными для данного субъекта (индивида или группы индивидов) к

данному ресурсу СВТ (объекту).

o Используется мандатная модель безопасности Белла–ЛаПадулы. Эта модель основывается на правилах секретного документооборота применяемых во многих странах.

o Субъект может писать в объект, если уровень иерархической классификации в классификационном уровне субъекта не меньше, см уровень иерархической классификации в классификационном ровне субъекта, и неиерархические категории в классификационном уровне субъекта

включают в себя все неиерархические категории в классификационном уровне объекта.

o Субъект осуществляет чтение объекта, если классификационный уровень субъекта в

иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все неиерархические категории в классификационном уровне субъекта

включены в неиерархические категории классификационном уровне объекта.

64. Назовите основные свойства хэш-функции (hash-function) для реализации КЗИ:

o Функция может служить для создания аутентификатора в качестве шифрованного сообщения, когда в качестве аутентификатора используется сам шифрованный текст всего сообщения.

o Функция может служить для создания аутентификатора в качестве кода аутентичности сообщения (Message Authentication Code – MAC), когда в качестве аутентификатора выступает значение фиксированной длины, создаваемое некоторой открытой функцией сообщения и секретным

ключом.

о Функция не может служить для создания аутентификатора, когда в качестве аутентификатора используется значение фиксированной длины, создаваемое некоторой открытой функцией от сообщения произвольной длины.

о Невозможно найти другое сообщение, чьё значение хэш-функции совпадало бы со значением хэш-функции данного сообщения.

65. Назовите основные свойства электронно-цифровой подписи (ЭЦП):

о Для заданного подписанного сообщения вычислительно трудно подобрать другое (фальсифицированное) сообщение, имеющее ту же ЭЦП.

о Хэш-функция не обеспечивает ЭЦП, так как и отправитель, и получатель используют один и тот же общий ключ.

о ЭЦП не должна быть проверяема третьей стороной в случае возникновения спора.

о Создавать цифровую подпись должно быть вычислительно трудно.

66. Дайте определение Пользовательского интерфейса:

о Описание аппаратных средств, программных средств и материалов, связанных с видеодисплейным терминалом.

о Все компоненты интерактивной системы (программное обеспечение или аппаратное обеспечение), которые предоставляют пользователю информацию и являются инструментами управления для выполнения определенных задач.

о Требования и рекомендации, относящиеся к характеристикам аппаратных средств, программных средств и способствующие обеспечению пригодности использования видеодисплейного терминала, а также эргономические принципы, лежащие в основе этих требований.

о Совокупность команд, доступных пользователю, при помощи которых он отдает приказание системе на выполнение действий.

67. Программный документ выполняют одним из следующих печатных способов:

о машинным - на обеих сторонах листа, с расстоянием между основаниями строк, обеспечивающим пригодность к микрофильмированию;

о допускается через один или два интервала, если обеспечивается пригодность к микрофильмированию по ГОСТ 13.1.002-2003;

о машинным - на одной стороне листа, с расстоянием между основаниями строк, обеспечивающим пригодность к микрофильмированию;

о машинописным - на одной стороне листа, через два интервала; допускается через один или два интервала, если обеспечивается пригодность к микрофильмированию по ГОСТ 13.1.002-2003.

68. Программные документы оформляют:

о не допускается оформление на листах формата А3;

о на листах форматов А4 и А3, предусматриваемых выходными характеристиками устройств вывода данных, - при изготовлении документа рукописным способом.

о на листах формата А4 (ГОСТ 2.301-68) - при изготовлении документа машинописным или рукописным способом (форма 1);

о не допускаются отклонения размеров листов, соответствующих форматам А4 и А3, определяемые возможностями применяемых технических средств.

69. Руководство программиста должно содержать следующие разделы:

о характеристики программы;

о требования к составу и параметрам периферийных устройств.

о назначение и функции, выполняемые программой;

о условия, необходимые для выполнения программы;

70. Руководство оператора должно содержать следующие разделы:

о последовательность действий оператора, обеспечивающих загрузку, запуск, выполнение и завершение программы;

о описание функций, формата и возможных вариантов команд оператора;

о минимальный и (или) максимальный состав аппаратурных и программных средств, необходимых для запуска программы;

o назначение программы;
71. Чем Руткит отличается от Эксплойта?
o Эксплойт может быть полезным, а руткит – нет;
o Руткит может быть полезным, а эксплойт – нет;
o Эксплойт есть просто набор утилит, а руткит – это лазейка в ядро;
o Руткит есть подвид вредоносных программ, а эксплойт – нет;
72. Как защититься от Эксплойта?
o Оставаться скрытным;
o Провести расследование;
o Установить фильтры защиты;
o «Почистить» за собой систему.
73. Что такое Shell-код?
o Полезная оболочка эксплойта;
o Средство борьбы против руткитов;
o Полезная оболочка руткита;
o Система обнаружения вторжений;
74. Что такое Полиморфные техники?
o Изменение сигнатуры для данного образца вредоносной программы;
o Изменение расшифровывающего кода;
o Изменение расшифровываемого кода;
o Расшифровка вредоносного кода;
75. Что делает Руткит для режима ядра?
o Обнаруживает атаку;
o Вызывает систему обнаружения вторжений;
o Организует атаку;
o Организует удаленное управление и прослушивание программ;
76. Что такое HIPS?
o Средство борьбы против эксплойтов;
o Средство борьбы против руткитов;
o Разновидность эксплойтов;
o Хорошо спроектированный руткит;
77. Что такое NIDS?
o Разновидность эксплойтов;
o Сетевые системы обнаружения вторжений;
o Разновидность руткитов;
o Хорошо спроектированный руткит;
78. Что такое HIDS?
o Локальные системы обнаружения вторжений;
o Разновидность руткитов;
o Хорошо спроектированный руткит;
o Разновидность эксплойтов;
79. Назовите меры борьбы с руткитом:
o Шифровать данные до того, как они будут сохранены в файловой системе;
o Использовать Активные методы Обхода IDS- и IPS-программ;
o Использовать Пассивные методы Обхода IDS- и IPS-программ;
o Использовать сканер вирусов;
80. Назовите средства борьбы с фишингом:
o Активные методы Обхода IDS- и IPS-программ;
o Полиморфные техники;
o Мониторинг фишинговых сайтов;
o Пассивные методы Обхода IDS- и IPS-программ.
81. Назовите показатели защищенности, которые должны поддерживаться СВТ:
o санкционированное изменение правил разграничения доступа;
o санкционированное изменение списка пользователей СВТ;

o санкционированное изменение списка защищаемых объектов;

o мандатный принцип контроля доступа;

82. Для реализации дискретизационного принципа контроля доступа

o При санкционированном внесении в список пользователей нового субъекта ему должны быть назначены классификационные метки.

o Каждому пользователю непосредственно прописываются права на чтение, запись и выполнение.

o Внешние классификационные метки (субъектов, объектов) должны точно соответствовать внутренним меткам (внутри КСЗ).

o КСЗ (комплекс средств защиты) при вводе новых данных в систему должен запрашивать и получать от санкционированного пользователя классификационные метки этих данных.

83. Для реализации мандатного принципа контроля доступа

o Используется мандатная модель безопасности Белла–ЛаПадулы. Эта модель основывается на правилах секретного документооборота применяемых во многих странах.

o Субъект может писать в объект, если уровень иерархической классификации в классификационном уровне субъекта не меньше, см уровень иерархической классификации в классификационном ровне субъекта, и неиерархические категории в классификационном уровне субъекта включают в себя все неиерархические категории в классификационном уровне объекта.

o Субъект осуществляет чтение объекта, если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все неиерархические категории в классификационном уровне субъекта включены в неиерархические категории классификационном уровне объекта.

o Для каждой пары (субъект — объект) в СВТ должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (например, читать, писать), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту).

84. Назовите основные свойства хэш-функции (hash-function) для реализации КЗИ

o Функция может служить для создания аутентификатора в качестве шифрованного сообщения, когда в качестве аутентификатора используется сам шифрованный текст всего сообщения.

o Функция может служить для создания аутентификатора в качестве кода аутентичности сообщения (Message Authentication Code – MAC), когда в качестве аутентификатора выступает значение фиксированной длины, создаваемое некоторой открытой функцией сообщения и секретным ключом.

o Невозможно найти другое сообщение, чьё значение хэш-функции совпадало бы со значением хэш-функции данного сообщения.

o Функция не может служить для создания аутентификатора, когда в качестве аутентификатора используется значение фиксированной длины, создаваемое некоторой открытой функцией от сообщения произвольной длины.

85. Назовите основные свойства электронно-цифровой подписи (ЭЦП)

o Хэш-функция не обеспечивает ЭЦП, так как и отправитель, и получатель используют один и тот же общий ключ.

o Для заданного подписанного сообщения вычислительно трудно подобрать другое (фальсифицированное) сообщение, имеющее ту же ЭЦП.

o ЭЦП не должна быть проверяема третьей стороной в случае возникновения спора.

o Создавать цифровую подпись должно быть вычислительно трудно.

86. Чем объяснима необходимость криптографии информации, курсирующей в вычислительной сети?

o Сложность управления и контроля доступа к системе.

o Разделение совместно используемых ресурсов.

o Данные IP, и TCP-протокола полностью прозрачны для злоумышленника.

o Множество точек атаки.

87. Дайте определение показателя эффективности системы защиты информации

o Сравнительная характеристика системы защиты информации и возможностей нарушителя

по ее преодолению.

о Совокупность свойств, определяющих степень ее приспособленности к выполнению поставленных перед нею задач. В некоторых работах указанная совокупность свойств названа термином "качество".

о Ее влияние на достижение (при прочих равных условиях) конечных целей функционирования системы обработки информации или на степень использования потенциальных боевых возможностей группировки войск в данной конкретной обстановке.

о Численная мера, количественно характеризующая степень выполнения системой защиты целей своего функционирования.

88. Кто формирует политику безопасности организации?

о Организация – разрабочик;

о Отдел Защиты информации;

о Руководство организации;

о Сторонняя специализированная организация;

89. Проранжируйте по степени эффективности меры обеспечения информационной безопасности ИС:

о Организация учета, хранения, использования и уничтожения документов и носителей с конфиденциальной информацией; распределение реквизитов разграничения доступа (паролей, профилей полномочий и т.п.); организация скрытого контроля за работой пользователей и персонала ИС;

о Административные меры защиты, Процедурные меры защиты, Физические меры защиты, Программно-технические меры защиты;

о Идентификация и аутентификация субъектов (пользователей, процессов и т.д.) ИС; контроль доступа к ресурсам ИС; регистрация и анализ событий, происходящих в ИС; контроль целостности объектов ИС; шифрование данных; резервирование ресурсов и компонентов ИС;

о Разработка правил обработки информации в ИС; мероприятия, осуществляемые при подборе и подготовке персонала; организация надежного пропускного режима; организация учета, хранения, использования и уничтожения документов и носителей с конфиденциальной информацией;

90. Выявление критически важных функций организации; идентификация ресурсов, необходимых для выполнения критически важных функций; определение перечня возможных аварий; разработка стратегии; подготовка к реализации выбранной стратегии – это

о Активный аудит (оперативный анализ регистрационной информации и некоторые аспекты реагирования на нарушения), служит для обнаружения и отражения атак.

о Процесс планирования восстановительных работ.

о Пассивный аудит.

о Предупреждение или обнаружение атак.

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 операто-

ра. Руководство по техническому обслуживанию. Требования к содержанию и оформлению

– Виды программ и программных документов. Описание языка. Требования к содержанию и оформлению

14.1.3. Вопросы для подготовки к практическим занятиям, семинарам

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.

Проектирование планируемой автоматизированной системы с учетом государственных стандартов.

Анализ реализации модулей автоматизированных систем

Анализ полноты проектнойдокументации

14.1.4. Зачёт

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.

Проектирование планируемой автоматизированной системы с учетом государственных стандартов.

Анализ реализации модулей автоматизированных систем

Анализ полноты проектной документации

14.1.5. Темы курсовых проектов / курсовых работ

– Создание автоматизированной системы по продаже авиа-билетов
– Создание автоматизированной системы по продаже ж/д билетов
– Создание автоматизированной системы в сфере здравоохранения
– Создание автоматизированной системы в банковской организации
– Создание автоматизированной системы в сфере образования

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	Собеседование по вопросам к зачету,	Преимущественно устная проверка

зрения	опрос по терминам	(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.