ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
(ФГБОУ ВО ИрГУПС)

УТВЕРЖДЕНА
приказом ректора
от «08» мая 2020 г. № 266-1

Б1.В.04 Теоретические основы компьютерной безопасности

рабочая программа дисциплины

Специальность – 10.05.03 Информационная безопасность автоматизированных систем
Специализация – Безопасность открытых информационных систем
Квалификация выпускника – специалист по защите информации
Форма обучения – очная
Нормативный срок обучения – 5 лет
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 6
Часов по учебному плану – 216

Формы промежуточной аттестации в семестрах:
зачет (5), экзамен (6), курсовая работа (6)

Распределение часов дисциплины по семестрам

Семестр	8	9	**Итого**
Число недель в семестре	18	18	
Вид занятий	Часов по учебному плану	Часов по учебному плану	**Часов по учебному плану**
Аудиторная контактная работа по видам учебных занятий	**54**	**36**	**90**
– лекции	18	18	36
– практические (семинарские)	18	18	36
– лабораторные	18		18
Самостоятельная работа	**54**	**36**	**90**
Экзамен		**36**	**36**
Итого	**108**	**108**	**216**

ИРКУТСК

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1 Цель освоения дисциплины	
1	обучение студентов базовым принципам и методикам в области защиты информации (ЗИ), основам комплексного проектирования, построения, эксплуатации защищенных автоматизированных систем (АС)
1.2 Задачи освоения дисциплины	
1	изучение - методологии проектирования и построения защищенных АС;
2	- критериев и методов оценки защищенности АС;
3	- методологии формирования политики информационной безопасности (ПИБ) АС организации;
4	- базовых характеристик механизмов/сервисов современных средств ЗИ.
1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины	
Профессионально-трудовое воспитание обучающихся	
Цель профессионально-трудового воспитания – формирование у обучающихся осознанной профессиональной ориентации, понимания общественного смысла труда и значимости его для себя лично, ответственного, сознательного и творческого отношения к будущей деятельности, профессиональной этики, способности предвидеть изменения, которые могут возникнуть в профессиональной деятельности, и умению работать в изменённых, вновь созданных условиях труда. Цель достигается по мере решения в единстве следующих задач: – формирование сознательного отношения к выбранной профессии; – воспитание чести, гордости, любви к профессии, сознательного отношения к профессиональному долгу, понимаемому как личная ответственность и обязанность; – формирование психологии профессионала; – формирование профессиональной культуры, этики профессионального общения; – формирование социальной компетентности и другие задачи, связанные с имиджем профессии и авторитетом транспортной отрасли	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП	
2.1 Требования к предварительной подготовке обучающегося	
1	Б1.Б.1.12 «Теория информации»
2	Б1.Б.1.13 Информатика
3	Б1.Б.1.22 Основы информационной безопасности
4	Б1.В.03 «Информационные технологии»
5	Б1.В.ДВ.05.01 «Введение в специальность»
6	Б1.В.ДВ.02.01 «Основы системного анализа»
2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее	
1	Б1.Б.1.23 Криптографические методы защиты информации
2	Б1.Б.1.ДС.03 Информационная безопасность открытых систем
3	Б1.Б.1.ДС.05 Аудит информационных технологий и систем обеспечения информационной безопасности
4	Б1.Б.1.29 Разработка и зксплуатация защищенных автоматизированных систем
5	Б1.В.06 Комплексная защита в информационных системах персональных данных
6	Б2.Б.03(П) Производственная – эксплуатационная
7	Б2.Б.04(Н) Производственная - научно-исследовательская работа
8	Б2.Б.05(П) Производственная - технологическая
9	Б2.Б.06(Пд) Производственная - преддипломная

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕС ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
ПК-11: способность разрабатывать политику информационной безопасности автоматизированной системы	
Минимальный уровень освоения компетенции	
Знать	методики формирования ПИБ верхнего уровня (цели, концепции, доктрины);
Уметь	разрабатывать ПИБ верхнего уровня (цели, концепции, доктрины);
Владеть	навыками разработки общих положений ПИБ;

Базовый уровень освоения компетенции	
Знать	методики формирования ПИБ среднего уровня (стандарты);
Уметь	формировать ПИБ среднего уровня (стандарты);
Владеть	навыками разработки положений ПИБ среднего уровня детализации;
Высокий уровень освоения компетенции	
Знать	способы формирования ПИБ нижнего уровня (методики, процедуры, инструкции).
Уметь	разрабатывать ПИБ нижнего уровня (методики, процедуры, инструкции);
Владеть	навыками разработки детализированных положений ПИБ.

ПК-22: способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	
Минимальный уровень освоения компетенции	
Знать	этапы создания комплексной системы защиты информации (КСЗИ);
Уметь	принимать участие в формировании ПИБ;
Владеть	навыками организации работ по оценке защищенности АС.
Базовый уровень освоения компетенции	
Знать	базовый набор рисков информационной безопасности (ИБ) для организации;
Уметь	идентифицировать риски ИБ АС;
Владеть	способами оценки рисков ИБ АС;
Высокий уровень освоения компетенции	
Знать	критерии защищенности АС организации;
Уметь	провести анализ рисков ИБ АС и предложить меры по их нейтрализации.
Владеть	навыками аудита ИБ АС организации.

В результате освоения дисциплины обучающийся должен

Знать	
1	основные понятия теории компьютерной безопасности;
2	причины, виды и каналы утечки информации;
3	основные принципы обеспечения ИБ;
4	базовые математические модели обеспечения ИБ;
5	критерии защищенности АС;
6	этапы создания КСЗИ.
Уметь	
1	проводить научные исследования при разработке КСЗИ;
2	применять основные критерии защищенности АС;
3	оценивать эффективность функционирования КСЗИ.
Владеть	
1	навыками анализа информационных рисков;
2	методологией разработки и реализации ПИБ.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часы	Код компетенции	Учебная литература, ресурсы сети «Интернет»
	Раздел 1. Архитектура электронных систем обработки данных				
1.1	Краткие сведения о компонентах электронных систем обработки данных. Функциональные назначения компонентов /Лек/	5	2	ПК-11, ПК-22	Л1.1 Л1.4 Л2.3 Э8 Э9
1.2	Три аспекта рассмотрения архитектурных решений /Ср/	5	3	ПК-11, ПК-22	Л1.1 Л1.4 Л2.3 Э8 Э9
	Раздел 2. Формальные модели; модели безопасности; политика информационной безопасности (ПИБ)				
2.1	Модель АС и модели безопасности. Основные понятия. Описание типовых ПИБ: модели разграни-	5	2	ПК-11, ПК-22	Л1.2 Л1.6 Л2.1 Л2.2 Э1 Э2 Э9

	чения доступа, построенные по принципу предоставления прав. Описание типовых ПИБ: модели разграничения доступа - информационные модели. Описание типовых ПИБ: модели разграничения доступа - вероятностные модели. Описание типовых ПИБ: механизм защиты от отказа в обслуживании (DoS). Понятия доступа, монитора безопасности. Изолированная программная среда /Лек/				
2.2	Стандарт оценки безопасности компьютерных систем TCSEC. Концепция защиты АС и средств вычислительной техники (СВТ) по руководящим документам (РД) Гостехкомиссии (ГТК) РФ /Пр/	5	2	ПК-11, ПК-22	Л1.6 Э1 Э4 Э5 Э9
2.3	Средства борьбы с вредоносным программным обеспечением /Лаб/	5	2	ПК-11, ПК-22	Л4.1
2.4	Структуризация методов обеспечения ИБ. /Ср/	5	6	ПК-11, ПК-22	Л4.1
	Раздел 3. Критерии и классы защищенности СВТ и АС в соответствии с РД ГТК РФ. Стандарты по оценке защищенных систем				
3.1	Требования к защите конфиденциальной информации. Требования к защите секретной информации. Зарубежные критерии безопасности АС (ITSEC, «Единые критерии»). Стратегия защиты информации /Лек/	5	2	ПК-11, ПК-22	Л1.1 Л1.4 Л2.2 Л2.3 Э3 Э9
3.2	РД ГТК РФ: Защита от несанкционированного доступа к информации (НСДИ). Термины и определения /Пр/	5	2	ПК-11, ПК-22	Э1 Э4 Э5
3.3	РД ГТК РФ: СВТ. Защита от НСДИ. Показатели защищенности от НСДИ /Пр/	5	2	ПК-11, ПК-22	Э1 Э4 Э5
3.4	РД ГТК РФ: АС. Защита от НСДИ. Классификация АС и требования по защите информации /Пр/	5	2	ПК-11, ПК-22	Э1 Э4 Э5
3.5	Проработка лекционного материала , подготовка к семинарским занятиям /Ср/	5	6	ПК-11, ПК-22	Л4.1 Э1 Э4 Э5
	Раздел 4. Примеры практической реализации; построение парольных систем				
4.1	Общие подходы к построению парольных систем защиты от НСДИ. Требования к выбору паролей. Проблемы передачи паролей по сети. Задача удаленной аутентификации /Лек/	5	4	ПК-11, ПК-22	Л1.1 Л1.4 Л1.6 Л2.1 Л2.2 Л2.3 Э6 Э9
4.2	Парольные системы. Технология выбора пароля в ОС Windows и проверка его стойкости /Лаб/	5	3	ПК-11, ПК-22	Л1.1 Л1.4 Л2.3 Э6
4.3	Назначение и порядок работы сканеров безопасности /Лаб/	5	3	ПК-11, ПК-22	Л1.1 Л1.4 Л2.3 Э7
4.4	Примеры механизмов и сервисов безопасности (аудит, обнаружение вторжений) /Ср/	5	9	ПК-11, ПК-22	Л1.1 Л1.4 Л1.6 Л2.1 Л2.2 Л2.3 Л4.1 Э6 Э7 Э9
	Раздел 5. Особенности применения криптографических методов; способы реализации криптографической подсистемы; особенности реализации систем с симметричными и асимметричными ключами				

5.1	Средства криптографической защиты информации (СКЗИ). Требования к СКЗИ Предварительное и динамическое шифрование. Методы шифрования с симметричным ключом. Системы шифрования с открытым ключом и электронной цифровой подписи /Лек/	5	4	ПК-11, ПК-22	Л1.1 Л1.4 Л1.5 Л1.6 Л2.1 Л2.3 Э2 Э8 Э9
5.2	РД ГТК РФ: Положение о государственном лицензировании деятельности в области защиты информации /Пр/	5	2	ПК-11, ПК-22	Л1.5 Э1 Э4 Э5 Э9
5.3	Криптоанализ шифра простой замены (на основе криптопакета PrZamena) /Лаб/	5	6	ПК-11, ПК-22	Л1.1 Л1.4 Э8
5.4	Криптоанализ шифра простой замены (на основе программной реализации метода частотного анализа) /Лаб/	5	4	ПК-11, ПК-22	Л1.1 Л1.4 Э8
5.5	Криптографическая защита на транспортном и прикладном уровнях распределенных АС. Особенности сертификации и стандартизации криптографических средств. Перспективы использования криптозащиты информации в АС. Стеганографические методы защиты информации /Ср/	5	12	ПК-11, ПК-22	Л1.1 Л1.4 - Л1.6 Л2.1 Л2.3 Л4.1 Э1 Э4 Э5 Э8 Э9
	Раздел 6. Методология обследования и проектирования систем защиты				
6.1	Этапы создания комплексной системы защиты информации. Научно-исследовательская разработка КСЗИ. Создание организационной структуры КСЗИ /Лек/	5	2	ПК-11, ПК-22	Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Э8 Э9
6.2	Проработка лекционного материала , подготовка к семинарским занятиям /Ср/	5	12	ПК-11, ПК-22	Л1.4 - Л1.6 Л2.1 - Л2.3 Л4.1 Э8 Э9
	Раздел 7. Методы построения защищенных АС; исследование корректности КСЗИ				
7.1	Концепция создания защищенных АС. Построение систем защиты от угроз нарушения конфиденциальности, целостности, доступности информации и угрозы раскрытия параметров АС. Подходы к оценке эффективности КСЗИ: классический подход; официальный подход; экспериментальный подход /Лек/	5	2	ПК-11, ПК-22	Л1.2 Л1.3 Л1.7 Л2.1 Л2.2 Л2.3 Э8 Э9
7.2	РД ГТК РД ГТК РФ: Положение по аттестации объектов информатизации по требованиям безопасности информации /Пр/	5	2	ПК-11, ПК-22	Л1.5 Э1 Э4 Э5
7.3	РД ГТК РД ГТК РФ: Положение по сертификации средств защиты информации по требованиям безопасности информации /Пр/	5	2	ПК-11, ПК-22	Л1.5 Э1 Э4 Э5
7.4	РД ГТК РФ: СВТ. Межсетевые экраны. Защита от НСДИ. Показатели защищенности от НСДИ /Пр/	5	2	ПК-11, ПК-22	Э1 Э4 Э5
7.5	РД ГТК РФ: Защита информации. Специальные защитные знаки. Классификация и общие требования /Пр/	5	2	ПК-11, ПК-22	Э1 Э4 Э5
7.6	Выбор показателей эффективности и критериев оптимальности КСЗИ. Практические средства и методы оценки корректности КСЗИ /Ср/	5	6	ПК-11, ПК-22	Л1.1 - Л1.7 Л2.1 - Л2.3 Л4.1 Э1 Э4 Э5
	Раздел 8. Основные понятия и определения, используемые при описании математических моделей безопасности АС				
8.1	Математические основы моделей безопасности. Элементы теории автоматов и гра-	6	4	ПК-11, ПК-22	Л1.2 Л1.3 Л1.7 Л2.3

	фов. Модель «решетки». Основные виды моделей безопасности /Лек/				Э8 Э9
8.2	Модель «Решетки». Решение задач /Пр/	6	4	ПК-11, ПК-22	Л1.2 Э9
8.3	Классификация угроз безопасности информации. Алгоритмически разрешимые и алгоритмически неразрешимые проблемы /Ср/	6	12	ПК-11, ПК-22	Л1.2 Л2.3 Э8 Э9
	Раздел 9. Модели систем дискреционного и мандатного разграничения доступа				
9.1	Модель Харрисона -Руззо-Ульмана (ХРУ). Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant /Лек/	6	6	ПК-11, ПК-22	Л1.2 Л2.3 Э9
9.2	Классическая модель Белла-ЛаПадула. Политика low-watermark в модели Белла-ЛаПадула /Лек/	6	4	ПК-11, ПК-22	Л1.2 Э9
9.3	Модель Take-Grant. Решение задач /Пр/	6	7	ПК-11, ПК-22	Л1.2 Э9
9.4	Модель Белла-ЛаПадула Решение задач /Пр/	6	7	ПК-11, ПК-22	Л1.2 Э9
9.5	Анализ безопасности систем ХРУ /Ср/	6	12	ПК-11, ПК-22	Л1.2 Л2.3
	Раздел 10.Субъектно-ориентированная модель изолированной программной среды				
10.1	Монитор безопасности объектов. Монитор безопасности субъектов. Изолированная программная среда /Лек/	6	4	ПК-11, ПК-22	Л1.2 Э9
10.2	Проработка лекционного материала , подготовка к семинарским занятиям /Ср/	6	12	ПК-11, ПК-22	Л1.2 Л4.1 Э9
	Раздел 11. Аттестация				
11.1	Подготовка к экзамену /Экзамен/	6	36	ПК-11, ПК-22	Л1.1 - Л1.7 Л2.1 - Л2.3 Л4.1 Э1 - Э9

5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине разрабатывается в соответствии с Положением о формировании фондов оценочных средств для проведения текущего контроля успеваемости, промежуточной и государственной итоговой аттестации № П.312000.06.7.188-2017.

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по данной дисциплине оформляется в виде приложения № 1 к рабочей программе дисциплиныи размещаются в электронной информационно-образовательной среде Университета, доступной обучающемуся через его личный кабинет.

6 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1 Основная литература

	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/100% онлайн
Л1.1	Афанасьев А.А., Веденьев Л.Т., Воронцов А.А.	Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам; http://e.lanbook.com/books/element.php?pl1_id=5114: для ВПО	Горячая линия-Телеком, 2012	100 % онлайн
Л1.2	Девянин П.Н.	Модели безопасности компьютерных систем. Управление доступом и информационными потоками: Учебное пособие	Горячая линия-Телеком, 2013	100% онлайн

		http://e.lanbook.com/books/element.php?pl1_id=63235		
Л1.3	Никитин И. А. , Цулая М. Т.	Процессы анализа и управления рисками в области ИТ: Учебная литература для ВУЗов; http://biblioclub.ru/index.php?page=book_red&id=429089:	М.: Национальный Открытый Университет «ИНТУИТ», 2016	100% онлайн
Л1.4	Ададуров С.Е., Глухов А.П., Корниенко А.А., Диасамидзе С.В., Корниенко А.А.	Информационная безопасность и защита информации на железнодорожном транспорте: Учебное пособие для ВО	М.: УМЦ по образованию на ж.-д. трансп., 2014	30
Л1.5	Коваленко Ю.И.	Правовой режим лицензирования и сертификации в сфере информационной безопасности: Для ВПО и курсов переподготовки http://e.lanbook.com/books/element.php?pl1_id=5163	М.: Горячая линия-Телеком, 2012	100% онлайн
Л1.6	Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.	Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1: Для ВПО http://e.lanbook.com/books/element.php?pl1_id=5178	М.: Горячая линия-Телеком, 2012	100% онлайн
Л1.7	Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.	Управление рисками информационной безопасности. Серия «Вопросы управление информационной безопасностью". Выпуск 2: Для ВПО http://e.lanbook.com/books/element.php?pl1_id=5179	М.: Горячая линия-Телеком, 2012	100% онлайн
6.1.2 Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год издания	Кол-во экз. в библиотеке/100% онлайн
Л2.1	Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А.	Основы информационной безопасности: Для ВПО http://e.lanbook.com/books/element.php?pl1_id=5121	М:. Горячая линия-Телеком, 2006	100% онлайн
Л2.2	Яковлев В.В., Корниенко А.А.	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта: Учеб. для вузов ж.-д. трансп.	М.: УМК МПС России, 2002	153
Л2.3	Шелупанов А.А. и др.	Основы защиты информации : Учебное пособие в трех частях	Томск: В-Спектр, 2010	25
6.1.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/100% онлайн
Л4.1	Завгородний В.И.	«Комплексная защита информации в компьютерных системах»; http://www.proklondike.com/books/defence/zavgorodniy_complex_defence.html; http://bezopasnik.org/article/book/zavgorodniy_-_Complex_Defend.pdf		100% онлайн

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»		
Э1	Сайт ФСТЭК РФ	http://fstec.ru/
Э2	Сайт ФСБ РФ	http://www.fsb.ru/
Э3	Материалы "Единые критерии"	http://oplib.ru/random/view/273781
Э4	РД ГТК	http://www.studmed.ru/docs/document16873?view=50&page=5
Э5	РД ГТК	http://oplib.ru/random/view/441942
Э6	Материалы "Парольные системы"	http://infoprotect.net/category/note
Э7	Материалы "Сканеры безопасности, сетевые угрозы"	http://www.securitylab.ru/analytics/365241.p

		hp
Э8	Материалы "Комплексная защита информации в компьютерных системах"	http://mexalib.com/view/2248
Э9	Материалы "Теоретические основы компьютерной безопасности"	http://elar.urfu.ru/bitstream/10995/1778/5/1335332_schoolbook.pdf
6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)		
6.3.1 Перечень базового программного обеспечения		
6.3.1.1	ОС Microsoft Windows XP Professional with Service Pack 2, лицензия Open License; количество – 427;	
6.3.1.2	ОС Microsoft Windows 7;	
6.3.1.3	Офисный пакет Microsoft Office 2010, OpenLicense; количество – 155;	
6.3.1.4	BorlandDelphi 7.	
6.3.2 Перечень специализированных средств и программного обеспечения		
6.3.2.1	средство антивирусной защиты Dr. Web cureit! (свободное программное обеспечение (ПО));	
6.3.2.2	учебная программа PrZamena (свободное ПО);	
6.3.2.3	учебная программа «Генератор безопасных паролей spass.exe» (свободное ПО);	
6.3.2.4	учебная программа «Генератор безопасных паролей PassGen.exe» (свободное ПО);	
6.3.2.5	учебная программа «lcp4.exe» (свободное ПО);	
6.3.2.6	учебная программа «lc4setup.exe» (свободное ПО);	
6.3.2.7	учебная программа «lc3setup02.exe» (свободное ПО);	
6.3.2.8	сканер «XSpider.exe 7.x» (demo);	
6.3.2.9	сканер Nessus-3.x (версия: свободное ПО);	
6.3.2.10	сканер SSS v5.27 (demo).	
6.3.3 Перечень информационных справочных систем		
6.3.3.1	Информационно-справочная система КонсультантПлюс http://www.consultant.ru	

7 ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

1	Учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран), служащими для представления учебной информации большой аудитории.
2	Учебная лаборатория «Средства и методы защиты информации», Д-523. Оснащена компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечена доступом в электронную информационно-образовательную среду ИрГУПС. Перечень установленных программных средств: MicrosoftOffice 2010, OpenOffice 3.0.1, 7-zip, BorlandDelphi 7, AbodeReaderXI, MicrosoftSecurityEssentials, а также специализированное ПО.
3	Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно-образовательную среду ИрГУПС. Помещения для самостоятельной работы обучающихся: – читальные залы; – учебные залы вычислительной техники А-401, А-509, А-513, А-516, Д-501, Д-503, Д-505, Д-507.

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, то необходимо сформулировать вопрос и задать преподавателю на консультации, на лабораторной работе.
Практические (семинарские)	Обобщение, расширение и углубление пройденного материала на лекции. Выступление с докладами по заданной теме, формирование навыков самостоятельной работы,

занятия	анализа литературных источников, публичного выступления и аргументации собственного мнения. Обсуждение вопросов, вызвавших затруднение, с преподавателем. Участие в дискуссиях. Контроль качества усвоения пройденного материала.
Лабораторная работа	Один из видов практической работы, проводимой с целью углубления и закрепления теоретических знаний, развития навыков самостоятельной деятельности. Включает подготовку необходимых программно-аппаратных средств, составление плана работы, ее проведение и написание отчета.
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины, размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.	

Приложение № 1 к рабочей программе по дисциплине
Б1.В.04 Теоретические основы компьютерной безопасности

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине
Б1.В.04 «Теоретические основы компьютерной безопасности»

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Дисциплина «**Теоретические основы компьютерной безопасности**» участвует в формировании компетенций:

ПК-11: способность разрабатывать политику информационной безопасности автоматизированной системы;
ПК-22: способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации.

Таблица траекторий формирования у обучающихся компетенций ПК-11, ПК-22 при освоении образовательной программы

Код компетенции	Наименование компетенции	Индекс и наименование дисциплин/ практик, участвующих в формировании компетенции	Семестр изучения дисциплины	Этапы формирования компетенции
ПК-11	способность разрабатывать политику информационной безопасности автоматизированной системы	Б1.Б.1.22 Основы информационной безопасности	3	1
		Б1.В.04 Теоретические основы компьютерной безопасности	5, 6	2
		Б1.В.ДВ.04.01 Защита электронного документооборота	9	3
		Б1.В.ДВ.04.02 Защита и обработка конфиденциальных документов	9	3
		Б2.Б.06(Пд) Производственная - преддипломная	А	4
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	А	4
ПК-22	способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Б1.В.04 Теоретические основы компьютерной безопасности	5, 6	1
		Б1.В.06 Комплексная защита в информационных системах персональных данных	9	2
		Б2.Б.06(Пд) Производственная - преддипломная	А	3
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	А	3

Таблица соответствия уровней освоения компетенций ПК-11, ПК-22

планируемым результатам обучения

Код компетенции	Наименование компетенции	Наименования разделов дисциплины	Уровни освоения компетенций	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции)
ПК-11	способность разрабатывать политику информационной безопасности автоматизированной системы	Раздел 1. Архитектура электронных систем обработки данных. Раздел 2. Формальные модели; модели безопасности; политика ин-	Минимальный уровень	Знать методики формирования политики информационной безопасности (ПИБ) верхнего уровня (цели, концепции, доктрины);
				Уметь разрабатывать ПИБ верхнего уровня (цели, концепции, доктрины);
				Владеть навыками разработки

		формационной безопасности (ПИБ). **Р**аздел 3. Критерии и классы защищенности СВТ и АС в соответствии с РД ГТК РФ. Стандарты по оценке защищенных систем. Раздел 4. Примеры практической реализации; построение парольных систем. Раздел 5. Особенности применения криптографических методов; способы реализации криптографической подсистемы; особенности реализации систем с симметричными и асимметричными ключами. Раздел 6. Методология обследования и проектирования систем защиты. Раздел 7. Методы построения защищенных АС; исследование корректности комплексной системы защиты информации (КСЗИ). Раздел 8. Основные понятия и определения, используемые при описании математических моделей безопасности АС. Раздел 9. Модели систем дискреционного и мандатного разграничения доступа. Раздел 10. Субъектно-ориентированная модель изолированной программной среды.		общих положений ПИБ.
			Базовый уровень	Знать методики формирования ПИБ среднего уровня (стандарты);
				Уметь формировать ПИБ среднего уровня (стандарты);
				Владеть навыками разработки положений ПИБ среднего уровня детализации.
			Высокий уровень	Знать способы формирования ПИБ нижнего уровня (методики, процедуры, инструкции).
				Уметь разрабатывать ПИБ нижнего уровня (методики, процедуры, инструкции);
				Владеть навыками разработки детализированных положений ПИБ.
ПК-22	способность участвовать в формировании политики	Раздел 1. Архитектура электронных систем обработки	Минимальный уровень	Знать этапы создания комплексной системы защиты информации (КСЗИ);
				Уметь принимать участие в

	информационной безопасности организации и контролировать эффективность ее реализации	данных. Раздел 2. Формальные модели; модели безопасности; политика информационной безопасности (ПИБ). Раздел 3. Критерии и классы защищенности СВТ и АС в соответствии с РД ГТК РФ. Стандарты по оценке защищенных систем. Раздел 4. Примеры практической реализации; построение парольных систем. Раздел 5. Особенности применения криптографических методов; способы реализации криптографической подсистемы; особенности реализации систем с симметричными и асимметричными ключами. Раздел 6. Методология обследования и проектирования систем защиты. Раздел 7. Методы построения защищенных АС; исследование корректности комплексной системы защиты информации (КСЗИ). Раздел 8. Основные понятия и определения, используемые при описании математических моделей безопасности АС. Раздел 9. Модели систем дискреционного и мандатного разграничения доступа. Раздел 10. Субъектно-ориентированная модель изолированной программной сре-		формировании ПИБ;
				Владеть навыками организации работ по оценке защищенности АС.
			Базовый уровень	Знать базовый набор рисков информационной безопасности (ИБ) для организации;
				Уметь идентифицировать риски ИБ АС;
				Владеть способами оценки рисков ИБ АС.
			Высокий уровень	Знать критерии защищенности АС организации;
				Уметь провести анализ рисков ИБ АС и предложить меры по их нейтрализации;
				Владеть навыками аудита ИБ АС организации.

		ды.		

Программа контрольно-оценочных мероприятий
за период изучения дисциплины

№	Неделя	Наименование контрольно-оценочного мероприятия	Объект контроля (понятия, тема / раздел дисциплины, компетенция, и т.д.)		Наименование оценочного средства (форма проведения)
5 семестр					
1	2	Текущий контроль	Средства борьбы с вредоносным программным обеспечением	ПК-11, ПК-22	Защита лабораторной работы
2	4	Текущий контроль	Парольные системы. Технология выбора пароля в ОС Windows и проверка его стойкости	ПК-11, ПК-22	Защита лабораторной работы
3	6	Текущий контроль	Назначение и порядок работы сканеров безопасности	ПК-11, ПК-22	Защита лабораторной работы
4	8	Текущий контроль	Назначение и порядок работы сканеров безопасности	ПК-11, ПК-22	Защита лабораторной работы
5	10	Текущий контроль	Криптоанализ шифра простой замены (на основе криптопакета PrZamena)	ПК-11, ПК-22	Защита лабораторной работы
6	12	Текущий контроль	Криптоанализ шифра простой замены (на основе криптопакета PrZamena)	ПК-11, ПК-22	Защита лабораторной работы
7	14	Текущий контроль	Криптоанализ шифра простой замены (на основе криптопакета PrZamena)	ПК-11, ПК-22	Защита лабораторной работы
8	16	Текущий контроль	Криптоанализ шифра простой замены (на основе программной реализации метода частотного анализа)	ПК-11, ПК-22	Защита лабораторной работы
9	18	Текущий контроль	Криптоанализ шифра простой замены (на основе программной реализации метода частотного анализа)	ПК-11, ПК-22	Защита лабораторной работы
10	1-18	Текущий контроль	Индивидуальное выступление с докладом на семинарском занятии по теме в соответствии с РПД по данной дисциплине	ПК-11, ПК-22	Сообщение, доклад (устно); наличие презентации
11	18	Промежуточная аттестация – зачет	Разделы 1 – 7 РПД	ПК-11, ПК-22	Собеседование (устно)
6 семестр					
1	1-18	Текущий контроль	Индивидуальное выступление с докладом на семинарском занятии по теме в соответствии с РПД по данной дисциплине	ПК-11, ПК-22	Сообщение, доклад (устно); наличие презентации
2	18	Тест	Разделы 1 – 10 РПД	ПК-11, ПК-22	Перечень тестовых заданий
3	18	Промежуточная аттестация – экзамен	Разделы 1 – 10 РПД	ПК-11, ПК-22	Собеседование (устно)

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная

аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

Текущий контроль успеваемости – основной вид систематической проверки знаний, умений, навыков обучающихся. Задача текущего контроля – оперативное и регулярное управление учебной деятельностью обучающихся на основе обратной связи и корректировки. Результаты оценивания учитываются в виде средней оценки при проведении промежуточной аттестации.

Для оценивания результатов обучения используется четырехбалльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и/или двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций на различных этапах их формирования, а так же краткая характеристика этих средств приведены в таблице

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Защита лабораторной работы	Средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной задачи, самостоятельно применять стандартные методы решения поставленной задачи с использованием имеющейся лабораторной базы, проводить анализ полученного результата работы. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся	Темы лабораторных работ и требования к их защите
2	Сообщение, доклад	Продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы докладов, сообщений
3	Курсовая работа	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся. Может быть использовано для оценки умений, навыков и (или) опыта деятельности обучающихся в предметной или межпредметной областях	Темы типовых групповых и / или индивидуальных проектов и типовое задание на курсовой проект (работу)
4	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий
5	Зачет	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (билетов) к зачету
6	Экзамен	Средство, позволяющее оценить знания, умения, навыков и (или) опыта деятельности обучающегося по дисциплине. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Перечень теоретических вопросов и практических заданий (билетов) к экзамену

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета и экзамена, а также шкала для оценивания уровня освоения компетенций

Шкалы оценивания	Критерии оценивания	Уровень освоения компетенций
«зачтено»	Обучающийся правильно ответил на теоретические вопросы. Показал отличные знания в рамках учебного материала. Правильно выполнил практические задания. Показал отличные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на все дополнительные вопросы	Высокий
	Обучающийся с небольшими неточностями ответил на теоретические вопросы. Показал хорошие знания в рамках учебного материала. С небольшими неточностями выполнил практические задания. Показал хорошие умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Ответил на большинство дополнительных вопросов	Базовый
	Обучающийся с существенными неточностями ответил на теоретические вопросы. Показал удовлетворительные знания в рамках учебного материала. С существенными неточностями выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала. Допустил много неточностей при ответе на дополнительные вопросы	Минимальный
«не зачтено»	Обучающийся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов	Компетенции не сформированы

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Доклад, сообщение

Шкала оценивания	Критерии оценивания
«отлично»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint,Flash–презентация, видео-презентация и др.) Использованы дополнительные источники информации. Содержание заданной темы раскрыто в полном объеме. Отражена структура доклада (вступление, основная часть, заключение, присутствуют выводы и примеры). Оформление работы. Оригинальность выполнения (работа сделана самостоятельно, представлена впервые)
«хорошо»	Доклад создан с использованием компьютерных технологий (презентация PowerPoint,Flash–презентация, видео-презентация и др.) Содержание доклада включает в себя информацию из основных источников (методическое пособие), дополнительные источники информации не использовались. Содержание заданной темы раскрыто не в полном объеме. Структура доклада сохранена (вступление, основная часть, заключение, присутствуют выводы и примеры)
«удовлетворительно»	Доклад сделан устно, без использования компьютерных технологий. Содержание доклада ограничено информацией только из методического пособия. Содержание заданной темы раскрыто не в полном объеме. Отсутствуют выводы и примеры. Оригиналь-

	ность выполнения низкая
«неудовлетворительно»	Доклад сделан устно, без использования компьютерных технологий и других наглядных материалов. Содержание ограничено информацией только из методического пособия. Заданная тема доклада не раскрыта, основная мысль сообщения не передана

Курсоваяработа

Шкала оценивания	Критерии оценивания
«отлично»	Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Все выводы и предложения убедительно аргументированы. Оформление курсовой работы и полученные результаты полностью отвечают требованиям, изложенным в методических указаниях. При защите курсовой работы обучающийся правильно и уверенно отвечает на вопросы преподавателя, демонстрирует глубокое знание теоретического материала, способен аргументировать собственные утверждения и выводы
«хорошо»	Содержание курсовой работы полностью соответствует заданию. Представлены результаты обзора литературных и иных источников. Структура курсовой работы логически и методически выдержана. Большинство выводов и предложений аргументировано. Оформление курсовой работы и полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две несущественные ошибки в использовании терминов, в построенных диаграммах и схемах. Наличествует незначительное количество грамматических и/или стилистических ошибок. Программа демонстрирует устойчивую работу на тестовых наборах исходных данных, подготовленных обучающимся, но обрабатывает не все исключительные ситуации. При защите курсового проекта (работы) обучающийся правильно и уверенно отвечает на большинство вопросов преподавателя, демонстрирует хорошее знание теоретического материала, но не всегда способен аргументировать собственные утверждения и выводы. При наводящих вопросах преподавателя исправляет ошибки в ответе
«удовлетворительно»	Содержание курсовой работы частично не соответствует заданию. Результаты обзора литературных и иных источников представлены недостаточно полно. Есть нарушения в логике изложения материала. Аргументация выводов и предложений слабая или отсутствует. Имеются одно-два существенных отклонений от требований в оформлении курсовой работы. Полученные результаты в целом отвечают требованиям, изложенным в методических указаниях. Имеются одна-две существенных ошибки в использовании терминов, в построенных диаграммах и схемах. Много грамматических и/или стилистических ошибок. Программа работает неустойчиво, не обрабатывает исключительные ситуации, тестовые наборы исходных данных не подготовлены. При защите курсовой работы обучающийся допускает грубые ошибки при ответах на вопросы преподавателя и /или не дал ответ более чем на 30% вопросов, демонстрирует слабое знание теоретического материала, в большинстве случаев не способен уверенно аргументировать собственные утверждения и выводы
«неудовлетворительно»	Содержание курсовой работы в целом не соответствует заданию. Имеются более двух существенных отклонений от требований в оформлении курсовой работы. Большое количество существенных ошибок по сути работы, много грамматических и стилистических ошибок и др. Полученные результаты не отвечают требованиям, изложенным в методических указаниях. Программа не разработана и/или находится в нерабочем состоянии. При защите курсовой работыобучающийся демонстрирует слабое понимание программного материала. Курсовой работы не представлена преподавателю. Обучающийся не явился на защиту курсовой работы.

Тест (структура теста по компетенциям)

Проверяемый уровень освоения компетенции компетенций (части компетенций, элементов компетенций)	Минимальное количество тестовых заданий на один раздел программы	Рекомендуемые формы тестовых заданий	Количество баллов за одно тестовое задание

Минимальный уровень освоения компетенции	19	Тестовые задания с выбором одного правильного ответа из нескольких	1
		Тестовые задания с выбором нескольких правильных ответов из множества ответов	
		Тестовые задания на установление соответствия	
		Тестовые задания на установление правильной последовательности	
Базовый уровень освоения компетенции	8	Тестовые задания с закрытым конструируемым ответом (ввод одного или нескольких слов, цифры)	4
Высокий уровень освоения компетенции	6	Тестовые задания со свободно конструируемым ответом (интервью, эссе) Структурированный тест Кейсы	7

Тест (шкала и критерии оценивания, уровни освоения)

Шкалы оценивания		Критерии оценивания	Уровень освоения компетенции
«отлично»	«зачтено»	Обучающийся при тестировании набрал 86-93 баллов	Высокий
«хорошо»		Обучающийся при тестировании набрал 69-85 баллов	Базовый
«удовлетворительно»		Обучающийся при тестировании набрал 53-68 баллов	Минимальный
«неудовлетворительно»	«не зачтено»	Обучающийся при тестировании набрал 0-52 баллов	Компетенция не сформирована

Защита лабораторной работы

Шкала оценивания	Критерии оценивания
«отлично»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет без замечаний. Лабораторная работа выполнена обучающимся в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; показал необходимые для проведения работы теоретические знания, практические умения и навыки. Работа (отчет) оформлена аккуратно, в наиболее оптимальной для фиксации результатов форме
«хорошо»	Лабораторная работа выполнена в обозначенный преподавателем срок, письменный отчет с небольшими недочетами. Лабораторная работа выполнена обучающимся в полном объеме и самостоятельно. Допущены отклонения от необходимой последовательности выполнения, не влияющие на правильность конечного результата. Работа показывает знание обучающимся основного теоретического материала и овладение умениями, необходимыми для самостоятельного выполнения работы. Допущены неточности и небрежность в оформлении результатов работы (отчета)
«удовлетворительно»	Лабораторная работа выполнена с задержкой, письменный отчет с недочетами. Лабораторная работа выполняется и оформляется обучающимся при посторонней помощи. На выполнение работы затрачивается много времени. Обучающийся показывает знания теоретического материала, но испытывает затруднение при самостоятельной работе с источниками знаний или приборами
«неудовлетворительно»	Лабораторная работа не выполнена, письменный отчет не представлен. Результаты, полученные обучающимся не позволяют сделать правильных выводов и полностью расходятся с поставленной целью. Показывается плохое знание

	теоретического материала и отсутствие необходимых умений. Лабораторная работа не выполнена, у учащегося отсутствуют необходимые для проведения работы теоретические знания, практические умения и навыки

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

3.1 Перечень типовых тем докладов, сообщений

1. Стандарт оценки безопасности компьютерных систем TCSEC. Концепция защиты АС и средств вычислительной техники (СВТ) по руководящим документам (РД) Гостехкомиссии (ГТК) РФ.
2. РД ГТК РФ: Защита от несанкционированного доступа к информации (НСДИ). Термины и определения.
3. РД ГТК РФ: СВТ. Защита от НСДИ. Показатели защищенности от НСДИ
4. РД ГТК РФ: АС. Защита от НСДИ. Классификация АС и требования по защите информации.
5. РД ГТК РФ: Положение о государственном лицензировании деятельности в области защиты информации.
6. РД ГТК РФ: Положение по аттестации объектов информатизации по требованиям безопасности информации.
7. РД ГТК РФ: Положение по сертификации средств защиты информации по требованиям безопасности информации
8. РД ГТК РФ: СВТ. Межсетевые экраны. Защита от НСДИ. Показатели защищенности от НСДИ.
9. РД ГТК РФ: Защита информации. Специальные защитные знаки. Классификация и общие требования.

3.2. Перечень типовых тем курсовых работ

1. Методы и средства обеспечения конфиденциальности информации;
2. Методы и средства обеспечения целостности информации;
3. Методы и средства обеспечения доступности информации;
4. Защита от угрозы раскрытия параметров АС;
5. Исследование корректности функционирования системы защиты информации в АС;
6. Средства и методы анализа защищенности информации в АС;
7. Подходы к формированию множества угроз ИБ. Системная классификация угроз ИБ;
8 Система и содержание показателей уязвимости информации;
9. Оценка требуемого уровня защиты информации;
10. Состав и правила функционирования службы ИБ;
11. Виды и категории информации огра¬ниченного доступа;
12. Порядок определения потенциальных каналов и способов несанкционированного доступа к информации в АС;
13. Методики оценки качества комплексной системы информационной безопасности;
14. Понятие, состав и процесс формирования политики информационной безопасности предприятия;
15. Формирование модели потенциального нарушителя ИБ на предприятии;
16. Архитектура электронных систем обработки информации;

17. Сравнение российских и зарубежных нормативных требований защищенности ин формации в АС;
18. Роль аудита в структуре комплексной системы информационной безопасности;
19. Биометрические средства аутентификации;
20. Компьютерная стеганография;
21. Экономические аспекты построения КСЗИ;
22. Практические методы и средства защиты информации от вредоносного программного обеспечения.

3.3. Тест

1. «Несанкционированный доступ к информации» - это:
   - доступ, реализующий возможности совокупности физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;
   - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств;
   - доступ с использованием совокупности средств технической разведки и прочих средств, которыми добывается защищаемая информация;
   - доступ к информации, реализуемый путём уничтожения технических средств информационной системы.

2. «Угроза информационной безопасности (ИБ)» - это
   - некоторая уязвимость АС;
   - потенциально возможное событие/действие, которое может нанести ущерб информации.

3. При реализации системой защиты мандатного принципа контроля доступа субъект может читать объект, только если иерархическая классификация субъекта _____, чем иерархическая классификация объекта:
   - больше;
   - меньше;
   - не больше;
   - не меньше.

4. Начиная с класса _____ требований ГТК РФ по защите информации в многопользовательских АС с различным уровнем доступа, необходимо управление потоками информации:
   - 1Г
   - 2Б
   - 1В
   - 3А
   - 1Б
   - 2А
   - 3Б

5. «Сборка мусора» - это
   - поиск удаленной информации на носителях;
   - вскрытие шифров криптозащиты информации;
   - внедрение программных/аппаратных закладок.

6. Политика информационной безопасности – это
   - общий документ, где перечисляются правила доступа в хранилище информации;
   - набор документов, регламентирующих порядок хранения, обработки и передачи информации.

7. Модели разграничения доступа могут быть классифицированы следующим образом (выделить все верные варианты):

○ модели разграничения доступа, построенные по принципу предоставления прав;
○ модели разграничения доступа, использующие принципы математической статистики.
○ модели разграничения доступа, построенные на основе принципов теории информации.

8. Основными типами моделей, построенных на предоставлении прав, являются модели (выделить все верные варианты
○ дискреционного доступа;
○ дискретного доступа;
○ мандатного доступа;
○ непрерывного доступа.

9. Модель Белла- ЛаПадула относится к классу моделей
○ дискреционного доступа;
○ дискретного доступа;
○ мандатного доступа.

10. Модель Биба контроля целостности имеет следующее количество вариаций;
○ 2;
○ 3;
○ 4.

11. Парольные системы аутентификации имеют следующий уровень стойкости:
○ низкий;
○ средний;
○ высокий.

12. Основная аксиома безопасности формулируется так:
○ все вопросы безопасности информации определяются доступами субъектов к объектам;
○ все вопросы безопасности информации определяются матрицей предоставления прав доступа субъектов к объектам;
○ все вопросы безопасности информации определяются правилами аутентификации и авторизации субъектов.

13. Определите последовательность следующих процедур (1-2-3):
○ авторизация субъекта (3);
○ аутентификация субъекта (2);
○ идентификация субъекта (1).

14. «Информационная система» - это:
○ совокупность информации, информационных технологий и технических средств;
○ совокупность информации, информационных технологий, технических средств и персонала, обслуживающего систему;
○ совокупность информационных технологий и технических средств;
○ совокупность информации, технических средств и персонала, обслуживающего информационную систему
○ совокупность информации, технических средств и персонала, обслуживающего и эксплуатирующего информационную систему.

15. Документ РД ГТК «Средства вычислительной техники (СВТ). Защита от НСД к информации. Показатели защищенности от НСД к информации» определяет _____ классов защищенности СВТ:
○ 4
○ 5
○ 6
○ 7

16. Третья группа СВТ (РД ГТК «(СВТ). Защита от НСД к информации. Показатели защищенности от НСД к информации») характеризуется _____ защитой и содержит четвертый, третий и второй классы:

- ○ дискреционной:
- ○ ролевой;
- ○ мандатной;
- ○ непрерывной.

17. Дискреционный принцип контроля доступа для СВТ требуется для следующих показателей защищенности СВТ от НСД к информации (обозначить все варианты):

- ○ 1;
- ○ 2;
- ○ 4;
- ○ 5.

18. «Специальные исследования (специсследования)» - это:

- ○ выявление с помощью контрольно - измерительной аппаратуры возможных каналов утечки информации;
- ○ определение соответствия условий эксплуатации объектов информатизации требованиям аттестатов соответствия, и других руководящих документов по спецзащите без применения контрольно - измерительной аппаратуры;
- ○ проверки технических средств иностранного и совместного производства на наличие внедренных электронных устройств перехвата информации.

19. Пассивными способами защиты информации являются:

- ○ создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях технических средств.
- ○ ослабление наводок ПЭМИ в посторонних проводниках и соединительных линиях технических средств, выходящих за пределы контролируемой зоны.

20. Модель Харрисона -Руззо-Ульмана относится к классу моделей _____ (дискреционного) разграничения доступа.

21. Угроза ИБ всегда направлена на определенную _____ (уязвимость)АС.

22. _____ (Подстановки) могут быть полиалфавитными и моноалфавитными.

23. Средство, осуществляющее перехват всех обращений субъектов к объектам и разграничивающее доступ в соответствии с заданным принципом разграничения доступа, называется _____ (диспетчером) доступа.

24. Выделяют 4 классических вида угроз безопасности информации: угрозы конфиденциальности, целостности, доступности и _____ (раскрытия) параметров АС.

25. Алгоритм RSA опирается на следующий тип необратимых преобразований: разложения больших чисел на простые _____ (множители).

26. Алгоритм _____ (Диффи-Хэллмана) представляет собой метод получения секретного ключа для участников сессии обмена конфиденциальной информацией.

27. Одним из способов аутентификации является предъявление _____ (ключевого) носителя.

28. Существует ли абсолютно невскрываемый шифр? Если да, опишите его свойства.

29. Приведите правило Кергхоффа.

30. В чем заключаются основные проблемы симметричных криптосистем?

31. Что такое гаммирование?

32. Нарисуйте схему асимметричного шифрования.

33. Приведите требования к системам с открытым ключом.

3.4. Перечень теоретических вопросов к зачету

1. Краткие сведения о компонентах электронных систем обработки данных.
2. Функциональные назначения компонентов.

3. Модель АС и модели безопасности. Основные понятия.
4. Описание типовых ПИБ: модели разграничения доступа, построенные по принципу предоставления прав.
5. Описание типовых ПИБ: модели разграничения доступа - информационные модели.
6. Описание типовых ПИБ: модели разграничения доступа - вероятностные модели.
7. Описание типовых ПИБ: механизм защиты от отказа в обслуживании (DoS).
8. Понятия доступа, монитора безопасности.
9. Изолированная программная среда.
10. Требования к защите конфиденциальной информации.
11. Требования к защите секретной информации.
12. Зарубежные критерии безопасности АС (ITSEC, «Единые критерии»). Общие подходы к построению парольных систем защиты от НСДИ.
13. Требования к выбору паролей.
14. Средства криптографической защиты информации (СКЗИ). Требования к СКЗИ
15. Предварительное и динамическое шифрование.
16. Методы шифрования с симметричным ключом.
17. Системы шифрования с открытым ключом и электронной цифровой подписи
18. Этапы создания комплексной системы защиты информации.

3.5. Перечень типовых простых практических заданий к зачету

Формируется на основании требований к выполнению лабораторных работ и результатов их защиты.

3.6. Перечень типовых практических заданий к зачету

Формируется на основании требований к выполнению лабораторных работ и результатов их защиты.

3.7. Перечень теоретических вопросов к экзамену

1. Краткие сведения о компонентах электронных систем обработки данных.
2. Функциональные назначения компонентов.
3. Модель АС и модели безопасности. Основные понятия.
4. Описание типовых ПИБ: модели разграничения доступа, построенные по принципу предоставления прав.
5. Описание типовых ПИБ: модели разграничения доступа - информационные модели.
6. Описание типовых ПИБ: модели разграничения доступа - вероятностные модели.
7. Описание типовых ПИБ: механизм защиты от отказа в обслуживании (DoS).
8. Понятия доступа, монитора безопасности.
9. Изолированная программная среда.
10. Требования к защите конфиденциальной информации.
11. Требования к защите секретной информации.
12. Зарубежные критерии безопасности АС (ITSEC, «Единые критерии»). Общие подходы к построению парольных систем защиты от НСДИ.
13. Требования к выбору паролей.
14. Средства криптографической защиты информации (СКЗИ). Требования к СКЗИ
15. Предварительное и динамическое шифрование.
16. Методы шифрования с симметричным ключом.
17. Системы шифрования с открытым ключом и электронной цифровой подписи
18. Этапы создания комплексной системы защиты информации.
19. Математические основы моделей безопасности.

20. Элементы теории автоматов и графов. Модель «решетки». Основные виды моделей безопасности.
21. Модель Харрисона -Руззо-Ульмана.
22. Модель распространения прав доступа Take-Grant.
23. Расширенная модель Take-Grant.
24. Классическая модель Белла-ЛаПадула.
25. Монитор безопасности объектов. Монитор безопасности субъектов.
26. Изолированная программная среда.

3.8. Перечень типовых простых практических заданий к экзамену

Формируется на основании требований к выполнению лабораторных работ и результатов их защиты.

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

В таблице приведены описания процедур проведения контрольно-оценочных мероприятий и процедур оценивания результатов обучения с помощью оценочных средств в соответствии с рабочей программой дисциплины.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Сообщение, доклад	Обучаемый получает тему от преподавателя изучает литературу (не менее 3-4 источников, включая самостоятельный поиск в интернете), готовит доклад (сообщение), объемом до 10 стр. текста размером 12 пунктов, интервал 1,2; предоставляет доклад (сообщение) преподавателю, отвечает на его вопросы. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Тест	Обучаемый самостоятельно отвечает на вопросы теста в письменной форме. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.
Защита лабораторной работы	Обучаемый самостоятельно, под руководством преподавателя выполняет лабораторную работу на заданную тему. Тема (задание) предлагается в конкретном виде. Методы и инструменты для ее разработки предлагаются преподавателем. После выполнения задания обучаемый готовит пояснительную записку, предоставляет ее преподавателю, отвечает на его вопросы в ходе собеседования (защиты). Оценка ставится по представленным результатам и результатам собеседования. Преподаватель информирует обучающихся о результатах проверки работы в конце занятия или на следующем занятии после проведения контрольно-оценочного мероприятия; оцененные/проверенные работы преподаватель возвращает обучающимся.

Для организации и проведения промежуточной аттестации (в форме зачета/экзамена) составляются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы:

– перечень теоретических вопросов к зачету/экзамену для оценки знаний;

– перечень типовых простых практических заданий к зачету/экзамену для оценки умений;

– перечень типовых практических заданий к зачету/экзамену для оценки навыков и (или) опыта деятельности.

Перечень теоретических вопросов и перечни типовых практических заданий разного уровня сложности к зачету/экзамену обучающиеся получают в начале семестра через электронную информационно-образовательную среду ИрГУПС (личный кабинет обучающегося).

Описание процедур проведения промежуточной аттестации в форме зачета и оценивания результатов обучения

При проведении промежуточной аттестации в форме зачета преподаватель может воспользоваться результатами текущего контроля успеваемости в течение семестра. Оценочные средства и типовые контрольные задания, используемые при текущем контроле, позволяют оценить знания, умения и владения навыками/опытом деятельности обучающихся при освоении дисциплины. С целью использования результатов текущего контроля успеваемости, преподаватель подсчитывает среднюю оценку уровня сформированности компетенций обучающегося (сумма оценок, полученных обучающимся, делится на число оценок).

Шкала и критерии оценивания уровня сформированности компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета по результатам текущего контроля (без дополнительного аттестационного испытания)

Средняя оценка уровня сформированности компетенций по результатам текущего контроля	Оценка
Оценка не менее 3,0 и нет ни одной неудовлетворительной оценки по текущему контролю	«зачтено»
Оценка менее 3,0 или получена хотя бы одна неудовлетворительная оценка по текущему контролю	«не зачтено»

Описание процедур проведения промежуточной аттестации в форме экзамена и оценивания результатов обучения

Промежуточная аттестация в форме экзамена проводится путем устного собеседования по билетам. Билеты составлены таким образом, что в каждый из них включал в себя теоретические вопросы и практические задания.

Билет содержит: два теоретических вопроса для оценки знаний. Теоретические вопросы выбираются из перечня вопросов к экзамену; три практических задания: два из них для оценки умений (выбираются из перечня типовых простых практических заданий к экзамену); третье практическое задание для оценки навыков и (или) опыта деятельности (выбираются из перечня типовых практических заданий к экзамену).

Распределение теоретических вопросов и практических заданий по экзаменационным билетам находится в закрытом для обучающихся доступе. Разработанный комплект билетов (25-30 билетов) не выставляется в электронную информационно-образовательную среду ИрГУПС, а хранится на кафедре-разработчике ФОС на бумажном носителе в составе ФОС по дисциплине.

На экзамене обучающийся берет билет, для подготовки ответа на экзаменационный билет обучающемуся отводится время в пределах 45 минут. В процессе ответа обучающегося на вопросы и задания билета, преподаватель может задавать дополнительные вопросы.

Каждый вопрос/задание билета оценивается по четырехбалльной системе, а далее вычисляется среднее арифметическое оценок, полученных за каждый вопрос/задание. Среднее арифметическое оценок округляется до целого по правилам округления.

Образец экзаменационного билета

ИРГУПС 2016-2017 учебный год	**Экзаменационный билет № 1** **по дисциплине «_____»** **__ ____ семестр**	Утверждаю: Заведующий кафедрой «_____» ИрГУПС _____
1. ……. 2. ……. 3. …….. 4. …….. 5 ……..……. Варианты размеров билета: Билет формата А5 – 148*210мм Билет формата А4 – 210*297мм		

В разделе «Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы» приведены типовые контрольные задания, для оценки результатов освоения образовательной программы. Задания, по которым проводятся контрольно-оценочные мероприятия, оформляются в соответствии с формами оформления оценочных средств, приведенными ниже, и не выставляются в электронную информационно-образовательную среду ИрГУПС, а хранятся на кафедре-разработчике ФОС на бумажном носителе в составе ФОС по дисциплине.