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.02 Теоретические основы компьютерной безопасности

рабочая программа дисциплины

Направление подготовки – 10.03.01 Информационная безопасность
Профиль – "Безопасность автоматизированных систем"
Квалификация выпускника – бакалавр
Форма обучения – очная
Нормативный срок обучения – 4 года
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 2
Часов по учебному плану – 72

Формы промежуточной аттестации в семестрах:
зачет (3)

Распределение часов дисциплины по семестрам

Семестр	3	**Итого**
Число недель в семестре	18	
Вид занятий	Часов по учебному плану	**Часов по учебному плану**
Аудиторная контактная работа по видам учебных занятий	**36**	**36**
– лекции	18	18
– практические (семинарские)	18	18
Самостоятельная работа	**36**	**36**
Итого	**72**	**72**

ИРКУТСК

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цели освоения дисциплины

1	обучение студентов основным принципам и базовым методикам в области защиты информации (ЗИ), комплексного проектирования, построения, эксплуатации защищенных автоматизированных систем (АС);

1.2 Задачи освоения дисциплины

1	изучение • возможностей механизмов/сервисов ЗИ; • методических аспектов проектирования и построения защищенных АС; • критериев и методов оценки защищенности АС; • основ формирования политики информационной безопасности (ПИБ) АС предприятия.

1.3 Цель воспитания и задачи воспитательной работы в рамках дисциплины

Научно-образовательное воспитание обучающихся

Цель научно-образовательного воспитания – создание условий для реализации научно-образовательного потенциала обучающихся в форме наставничества, тьюторства, научного творчества.

Цель достигается по мере решения в единстве следующих задач:
– формирование системного и критического мышления, мотивации к обучению, развитие интереса к творческой научной деятельности;
– создание в студенческой среде атмосферы взаимной требовательности к овладению знаниями, умениями и навыками;
– популяризация научных знаний среди обучающихся;
– содействие повышению привлекательности науки, поддержка научно-технического творчества;
– создание условий для получения обучающимися достоверной информации о передовых достижениях и открытиях мировой и отечественной науки, повышения заинтересованности в научных познаниях об устройстве мира и общества;
– совершенствование организации и планирования самостоятельной работы обучающихся как образовательной технологии формирования будущего специалиста путем индивидуальной познавательной и исследовательской деятельности

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 психологи 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.07 Информатика
2	Б1.Б.05 Математика
3	Б1.Б.11 Основы информационной безопасности
4	Б1.Б.25 Информационные технологии

2.2 Дисциплины и практики, для которых изучение данной дисциплины необходимо как предшествующее

1	Б1.Б.13 Программно-аппаратные средства защиты информации
2	Б1.В.01 Комплексное обеспечение информационной безопасности автоматизированных систем
3	Б1.В.04 Безопасность операционных систем
4	Б1.В.03 Безопасность вычислительных сетей
5	Б1.В.05 Комплексная защита в информационных системах персональных данных
6	Б1.В.06 Безопасность систем баз данных
7	Б1.В.08 Методология построения защищенных автоматизированных систем

8	Б1.В.09 Теория и практика защиты информации в автоматизированных системах железнодорожного транспорта
9	Б1.В.ДВ.06.01 Информационная безопасность открытых систем
10	Б2.В.03(П) Производственная практика - эксплуатационная
11	Б2.В.02(У) Учебная практика - по получению первичных профессиональных умений и навыков

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕС ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

Минимальный уровень освоения компетенции	
Знать	порядок выделения информации, подверженной угрозам информационной безопасности (ИБ);
Уметь	выделять виды и формы информации, подверженной угрозам ИБ;
Владеть	навыками выделения видов и форм информации, подверженной угрозам ИБ;
Базовый уровень освоения компетенции	
Знать	порядок проведения аудита ИБ предприятия;
Уметь	проводить аудит ИБ АС;
Владеть	навыками проведения аудита ИБ АС;
Высокий уровень освоения компетенции	
Знать	методы и способы реализации атак на информационные ресурсы АС;
Уметь	анализировать методы и способы реализации атак на информационные ресурсы АС;
Владеть	навыками применения методов и способов реализации атак на информационные ресурсы АС.

ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

Минимальный уровень освоения компетенции	
Знать	минимальный набор стандартов ИБ;
Уметь	применять минимальный набор стандартов для оценки защищенности объектов и систем;
Владеть	методиками анализа ИБ;
Базовый уровень освоения компетенции	
Знать	основные нормативно-правовые документы ФСТЭК в области ИБ;
Уметь	применять основные нормативно-правовые документы ФСТЭК в области ИБ для анализа уровня защищенности объекта;
Владеть	навыками аудита защищенности объектов информатизации;
Высокий уровень освоения компетенции	
Знать	базовые положения нормативно-правовых документов ФСТЭК и зарубежных стандартов;
Уметь	применять основные нормативно-правовые документы ФСТЭК в области информационной безопасности;
Владеть	навыками применения базового набора нормативно-правовых документов ФСТЭК и зарубежных стандартов в области ЗИ.

В результате освоения дисциплины обучающийся должен

Знать	
1	основные понятия теории компьютерной безопасности;
2	причины, виды и каналы утечки информации;
3	основные принципы обеспечения информационной безопасности (ИБ);
4	критерии защищенности АС;
5	этапы создания комплексной системы защиты информации (КСЗИ).
Уметь	
1	применять основные критерии защищенности АС;
2	оценивать эффективность 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. Модели безопасности; понятие и структура ПИБ				
1.1	Модель автоматизированной системы (АС) и модели безопасности. Основные понятия. Описание типовых ПБ: модели разграничения доступа, построенные по принципу предоставления прав. Описание типовых ПБ: модели разграничения доступа - информационные модели. Описание типовых ПБ: модели разграничения доступа - вероятностные модели. Описание типовых ПБ: механизм защиты от отказа в обслуживании (DoS) /Лек/	3	2	ОПК-7 ПК-10	Л1.2 Л1.6 Л2.1 Л2.2 Э1 Э2 Э9
1.2	Стандарт оценки безопасности компьютерных систем TCSEC. Концепция защиты АС и средств вычислительной техники (СВТ) по руководящим документам (РД) Гостехкомиссии (ГТК) РФ /Пр/	3	2	ОПК-7 ПК-10	Л1.6 Э1 Э4 Э5 Э9
1.3	РД ГТК РФ: Защита от несанкционированного доступа к информации (НСДИ). Термины и определения /Пр/	3	2	ОПК-7 ПК-10	Л1.1 Э1 Э4 Э5
1.4	Структуризация методов обеспечения информационной безопасности (ИБ). Понятия доступа, монитора безопасности. Изолированная программная среда. Проработка лекционного материала, подготовка к семинарскому занятию /Ср/	3	6	ОПК-7 ПК-10	Л1.1 Л1.2 Л1.6 Л2.1 Л2.2 Э1 Э4 Э5 Э9
	Раздел 2. Критерии и классы защищенности средств вычислительной техники и АС в соответствии с руководящими документами Гостехкомиссии РФ. Стандарты по оценке защищенных систем				
2.1	Критерии и классы защищенности СВТ и АС. РД ГТК РФ. Требования к защите конфиденциальной информации. Требования к защите секретной информации /Лек/	3	2	ОПК-7 ПК-10	Л1.1 Л1.4 Л2.2 Л2.3 Э3 Э9
2.2	РД ГТК РФ: СВТ. Защита от НСДИ. Показатели защищенности от НСДИ /Пр/	3	2	ОПК-7 ПК-10	Э1 Э4 Э5
2.3	РД ГТК РФ: АС. Защита от НСДИ. Классификация АС и требования по защите информации /Пр/	3	2	ОПК-7 ПК-10	Э1 Э4 Э5
2.4	Зарубежные критерии безопасности АС (TCSEC, ITSEC, «Единые критерии») /Пр/	3	2	ОПК-7 ПК-10	Э1 Э4 Э5
2.5	Проработка лекционного материала, подготовка к семинарскому занятию /Ср/	3	6	ОПК-7 ПК-10	Л1.1 Л1.4 Л2.2 Л2.3 Э1 Э3 Э4 Э5
	Раздел 3. Примеры практической реализации; построение парольных систем				
3.1	Общие подходы к построению парольных систем защиты от НСДИ. Требования к выбору паролей. Проблемы передачи паролей по сети. Задача удаленной аутентификации.	3	4	ОПК-7 ПК-10	Л1.1 Л1.4 Л1.6 Л2.1 Л2.2 Л2.3 Э6 Э9

	Примеры механизмов и сервисов безопасности (аудит, обнаружение вторжений) /Лек/				
3.2	РД ГТК РФ: СВТ. Межсетевые экраны. Защита от НСДИ. Показатели защищенности от НСДИ /Пр/	3	2	ОПК-7 ПК-10	Э1 Э4 Э5
3.3	Проработка лекционного материала, подготовка к семинарскому занятию /Ср/	3	6	ОПК-7 ПК-10	Л1.1 Л1.4 Л1.6 - Л2.3 Э1 Э4 Э5 Э6 Э7 Э9
	Раздел 4. Особенности применения криптографических методов защиты информации; способы реализации криптографической подсистемы				
4.1	Средства криптографической защиты информации (СКЗИ). Требования к СКЗИ. Предварительное и динамическое шифрование. Методы шифрования с симметричным ключом. Системы шифрования с открытым ключом и электронной подписи /Лек/	3	4	ОПК-7 ПК-10	Л1.1 Л1.4 Л1.5 Л1.6 Л2.1 Л2.3 Э2 Э8 Э9
4.2	РД ГТК РФ: Положение о государственном лицензировании деятельности в области защиты информации /Пр/	3	2	ОПК-7 ПК-10	Л1.5 Э1 Э4 Э5
4.3	РД ГТК РД ГТК РФ: Положение по сертификации средств защиты информации по требованиям безопасности информации /Пр/	3	2	ОПК-7 ПК-10	Л1.5 Э1 Э4 Э5
4.4	Криптографическая защита на транспортном и прикладном уровнях распределенных АС. Особенности сертификации и стандартизации криптографических средств. Перспективы использования криптозащиты информации в АС. Проработка лекционного материала, подготовка к семинарскому занятию /Ср/	3	6	ОПК-7 ПК-10	Л1.1 Л4 - Л1.6 Л2.1 Л2.3 Л.4.1 Э1 Э4 Э5 Э8
	Раздел 5. Методология обследования объекта и проектирования систем защиты				
5.1	Этапы создания комплексной системы защиты информации. Научно-исследовательская разработка КСЗИ /Лек/	3	4	ОПК-7 ПК-10	Л1.4 Л1.5 Л1.6 Л2.1 - Л2.3, Л3.1 Э8 Э9
5.2	Создание организационной структуры КСЗИ. Проработка лекционного материала, подготовка к семинарскому занятию /Ср/	3	6	ОПК-7 ПК-10	Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Э8 Э9
	Раздел 6. Методы построения защищенных АС; исследование корректности КСЗИ				
6.1	Концепция создания защищенных АС. Выбор показателей эффективности и критериев оптимальности КСЗИ. Подходы к оценке эффективности КСЗИ: классический подход; официальный подход; экспериментальный подход /Лек/	3	2	ОПК-7 ПК-10	Л1.2 Л1.3 Л1.7 Л2.1 Л2.2 Л2.3 Э8 Э9
6.2	РД ГТК: Положение по аттестации объектов информатизации по требованиям безопасности информации /Пр/	3	2	ОПК-7 ПК-10	Л1.5 Э1 Э4 Э5
6.3	Построение систем защиты от угроз нарушения конфиденциальности, целостности, доступности информации и угрозы раскрытия параметров АС. Практические средства и методы оценки	3	6	ОПК-7 ПК-10	Л1.1 Л1.2 Л1.3 Л1.5 Л1.7 Л2.1 - Л2.3, Л4.1

	корректности КСЗИ. Проработка лекционного материала, подготовка к семинарскому занятию /Ср/				

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 дисциплины и 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 http://e.lanbook.com/books/element.php?pl1_id=63235	Горячая линия-Телеком, 2013	100% онлайн
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 библио-

				теке/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
6.1.3 Методические разработки				
	Авторы, составители	Заглавие	Издательство, год издания/ Личный кабинет обучающегося	Кол-во экз. в библиотеке/100% онлайн
Л3.1	Глухов Н.И.	Оценка информационных рисков предприятия, учебное пособие.	Иркутск: ИрГУПС, 2013.	67
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	Личный кабинет	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.php
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
6.3.2 Перечень специализированных средств и программного обеспечения	
	Не предусмотрены учебным планом
6.3.3 Перечень информационных справочных систем	
6.3.3.1	Информационно-справочная система КонсультантПлюсhttp://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	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) занятия	Обобщение, расширение и углубление пройденного материала на лекции. Выступление с докладами по заданной теме, формирование навыков самостоятельной работы, анализа литературных источников, публичного выступления и аргументации собственного мнения. Обсуждение вопросов с преподавателем, вызвавших затруднение,. Участие в дискуссиях. Контроль качества усвоения пройденного материала.
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.02 Теоретические основы компьютерной безопасности

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине Б1.В.02 «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:

ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;
ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

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
ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Б1.Б.11 Основы информационной безопасности	2	1
		Б1.В.02 Теоретические основы компьютерной безопасности	3	2
		Б2.В.02(У) Учебная практика - по получению первичных профессиональных умений и навыков	4	2
		Б1.В.ДВ.07.02 Методология определения ценности информации	6	3
		Б1.В.ДВ.08.01 Методология анализа информационных рисков	6	3
		Б1.В.ДВ.08.02 Инстументарий анализа информационных рисков	6	3
		Б2.В.03(П) Производственная практика - эксплуатационная	6	3
		Б2.В.04(Пд) Производственная практика - преддипломная	8	4
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	4
ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Б1.В.02 Теоретические основы компьютерной безопасности	3	1
		Б1.В.07 Аудит информационной безопасности	6	2
		Б1.В.01 Комплексное обеспечение информационной безопасности автоматизированных систем	8	3
		Б2.В.04 (Пд) Производственная практика – преддипломная	8	3
		Б3.Б.01 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	8	3

Таблица соответствия уровней освоения компетенций ОПК-7, ПК-10

планируемым результатам обучения

Код компетенции		Наименования разделов дисциплины	Уровни освоения компетенций	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции)
ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Раздел 1. Модели безопасности; понятие и структура ПИБ. Раздел 2. Критерии и классы защищенности средств вычислительной техники и АС в соответствии с руководящими документами Гостехкомиссии РФ. Стандарты по оценке защищенных систем. Раздел 3. Примеры практической реализации; построение парольных систем. Раздел 4. Особенности применения криптографических методов защиты информации; способы реализации криптографической подсистемы. Раздел 5. Методология обследования объекта и проектирования систем защиты. Раздел 6. Методы построения защищенных АС; исследование корректности КСЗИ.	Минимальный уровень	Знать порядок выделения информации, подверженной угрозам информационной безопасности (ИБ);
				Уметь выделять виды и формы информации, подверженной угрозам ИБ;
				Владетьнавыками выделения видов и форм информации, подверженной угрозам ИБ;
			Базовый уровень	Знать порядок проведения аудита ИБ предприятия;
				Уметь проводить аудит ИБ АС;
				Владетьнавыками проведения аудита ИБ АС;
			Высокий уровень	Знать методы и способы реализации атак на информационные ресурсы АС;
				Уметь анализировать методы и способы реализации атак на информационные ресурсы АС;
				Владеть навыками применения методов и способов реализации атак на информационные ресурсы АС.
ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Раздел 1. Модели безопасности; понятие и структура ПИБ. Раздел 2. Критерии и классы защищенности средств вычислительной техники и АС в соответствии с руководящими документами Гостехкомиссии РФ. Стандарты по оценке защищенных систем.	Минимальный уровень	Знать минимальный набор стандартов ИБ;
				Уметь применять минимальный набор стандартов для оценки защищенности объектов и систем;
				Владеть методиками анализа ИБ;
			Базовый уровень	Знать основные нормативно-правовые документы ФСТЭК в области ИБ;
				Уметь применять основные нормативно-правовые документы ФСТЭК в области ИБ для анализа уровня защищенности объекта;
				Владеть навыками аудита защищенности объектов информатизации;
			Высокий уро-	Знать базовые положения нор-

		Раздел 3. Примеры практической реализации; построение парольных систем. Раздел 4. Особенности применения криптографических методов защиты информации; способы реализации криптографической подсистемы. Раздел 5. Методология обследования объекта и проектирования систем защиты. Раздел 6. Методы построения защищенных АС; исследование корректности КСЗИ.	вень	мативно-правовых документов ФСТЭК и зарубежных стандартов; Уметь применять основные нормативно-правовые документы ФСТЭК в области информационной безопасности; Владеть навыками применения базового набора нормативно-правовых документов ФСТЭК и зарубежных стандартов в области ЗИ.

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)
3 семестр					
1	1-18	Текущий контроль	Индивидуальное выступление с докладом на семинарском занятии по теме в соответствии с РПД по данной дисциплине	ОПК-7, ПК-10	Сообщение, доклад (устно); наличие презентации
2	18	Тест	Разделы 1 – 6 РПД	ОПК-7, ПК-10	Перечень тестовых заданий
3	18	Промежуточная аттестация – зачет	Разделы 1 – 6 РПД	ОПК-7, ПК-10	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 корректи-

ровки. 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	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
2	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
3	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

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. По-	Минимальный

	казал 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	
«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. Оригинальность 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

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)	7

		Структурированный тест Кейсы	

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

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. Зарубежные критерии безопасности АС (TCSEC, ITSEC, «Единые критерии»).
6. РД ГТК РФ: СВТ. Межсетевые экраны. Защита от НСДИ. Показатели защищенности от НСДИ.
7. РД ГТК РФ: Положение о государственном лицензировании деятельности в области защиты информации.
8. РД ГТК РФ: Положение по сертификации средств защиты информации по требованиям безопасности информации.
9. РД ГТК РФ: Положение по аттестации объектов информатизации по требованиям безопасности информации.

3.2. 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. Использование парольной системы обеспечивает выполнение требования _____ (аутентификации) при входе субъекта в АС.

10. Алгоритмы шифрования группы асимметричных криптосистем требуют более _____ ключей по сравнению с симметричными криптосистемами:

○ длинных;

○ коротких;

○ средних.

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. Вставить одно слово на место пропущенных:
    «Идентификация» (Identification) – это присвоение субъектам и объектам доступа _____ (идентификатора) и/или сравнение предъявляемого _____ (идентификатора) с перечнем присвоенных _____ (идентификаторов).
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.

3.3. 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. Требования к защите конфиденциальной информации.
9.. Требования к защите секретной информации.
10. Зарубежные критерии безопасности АС (ITSEC, «Единые критерии»).
11. Общие подходы к построению парольных систем защиты от НСДИ.
12. Требования к выбору паролей.
13. Средства криптографической защиты информации (СКЗИ). Требования к СКЗИ
14. Предварительное и динамическое шифрование.
15. Методы шифрования с симметричным ключом.
16. Системы шифрования с открытым ключом и электронной цифровой подписи
17. Этапы создания комплексной системы защиты информации.

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.

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»

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.