ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказом и.о. ректора
от «07» июня 2021 г. № 79

Б1.В.ДВ.08.01 Методология анализа информационных рисков

рабочая программа дисциплины

Специальность/направление подготовки – 10.03.01 Информационная безопасность
Специализация/профиль – Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)
Квалификация выпускника – Бакалавр
Форма и срок обучения – очная форма 4 года
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 2
Часов по учебному плану (УП) – 72
В том числе в форме практической подготовки (ПП) – 10
(очная)

Формы промежуточной аттестации
очная форма обучения:
зачет 7 семестр

Очная форма обучения **Распределение часов дисциплины по семестрам**

Семестр	7	**Итого**
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	42/10	**42/10**
– лекции	28	**28**
– практические (семинарские)	14/10	**14/10**
– лабораторные		
Самостоятельная работа	30	**30**
Итого	72/10	**72/10**

* В форме ПП – в форме практической подготовки.

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденным Приказом Министерства науки и высшего образования Российской Федерации от 17.11.2020 № 1427.

Программу составил(и):
к.э.н., доцент, С.П. Серёдкин

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «4» июня 2021 г. № 11-2

Зав. кафедрой, к.э.н., доцент Т.К. Кириллова

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1 Цели дисциплины

1	раскрытие сущности и значения методологии анализа информационных рисков реализации угроз, как основы информационной безопасности и защиты информации;
2	определение теоретических, концептуальных, методических и организационных основ информационной безопасности и защиты ценной для предприятия информации

1.2 Задачи дисциплины

1	изучить понятие «информационных активов» как основной характеристики системы оценки информационных рисков хозяйствующего субъекта;
2	определить место, роль, специфику системы оценки информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия;
3	оценить существующие методические подходы к оценке информационных рисков для выявления возможностей совершенствования данной деятельности;
4	изучить особенности организационного направления в деятельности по защите информационных активов и определение их влияния на создание и развитие системы защиты информационных активов хозяйствующего субъекта;
5	освоить методические положения по совершенствованию деятельности в сфере оценки информационных рисков хозяйствующих субъектов;
6	освоить методические подходы к оценке эффективности деятельности по защите информационных активов 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 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

Блок/часть ОПОП	Блок 1. Дисциплины / Часть, формируемая участниками образовательных отношений

2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины

1	Б1.В.ДВ.03.01 Основы программирования

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

1	Б2.В.02(Пд) Производственная - преддипломная практика
2	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
3	Б3.02(Д) Защита выпускной квалификационной работы

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ		
Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения**
ПК-1 Способен организовать работу по выявлению недостатков в функционировании системы защиты и инструментальных средствах программирования	ПК-1.2 Применяет методы анализа информационных рисков в автоматизированных системах	Знать: роль информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия; основные виды информационных активов (ресурсов) хозяйствующего субъекта; основные виды угроз информационной безопасности хозяйствующего субъекта и уязвимости ресурсов, через которые они могут быть реализованы; особенности и проблемы организационного направления в деятельности по защите информационных активов; методический подход к оценке защищенности информационных активов хозяйствующего субъекта на основе учета информационных рисков; основные направления по применению защитных мероприятий с целью увеличения рискозащищенности информационных активов предприятия; способы технико-экономического обоснования мероприятий по обеспечению информационной безопасности
		Уметь: определять состав, важность и ценность конфиденциальной информации применительно к видам тайны; выявлять информационные риски реализации угроз информационным активам предприятия и иным объектам защиты; разрабатывать модели угроз и нарушителя информационной безопасности предприятия; определять направления и виды защиты информации с учетом характера рисков реализации угроз информационным активам предприятия; выявлять недостатки (уязвимости) в функционировании системы защиты информации автоматизированной системы
		Владеть: основными методами выявления информационных рисков реализации угроз конфиденциальной информации; методами определения уровня информационных рисков; методами оценки возврата инвестиций от реализации контрмер по защите информации, и их эффективности; навыками работы со специальными программными комплексами управления информационными рисками предприятия; терминологией и системным подходом к выявлению недостатков (уязвимостей) информационных систем (АС); навыками анализа угроз ИБ и уязвимостей в АС; организационными, организационно-техническими, техническими и компьютерными средствами по контролю защиты информации в АС

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	**Наименование разделов, тем и видов работ**	**Очная форма**					***Код индикатора достижения компетенции**
		Семестр	**Часы**				
			Лек	**Пр**	**Лаб**	**СР**	
1.0	**Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия.**						
1.1	Тема 1. Риски, породившие мировой финансовый кризис. Информационные риски киберпространства (кибертерроризм, риски промышленных систем, риски утечки информации, риски электронных отчетов). Государственное регулирование. Оценка рисков как основа корпоративного управления.	7	2				ПК-1.2
1.2	Тема 2. Идентификация активов (описание бизнес-процессов).	7		2/1			ПК-1.2

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ							
Код	**Наименование разделов, тем и видов работ**	**Очная форма**					***Код индикатора достижения компетенции**
		Семестр	**Часы**				
			Лек	**Пр**	**Лаб**	**СР**	
1.3	Тема 3. Термины и определения в области управления информационными рисками.	7				2	ПК-1.2
1.4	Тема 4. Антология кибератак. Наихудшие сценарии кибератак.	7				2	ПК-1.2
2.0	**Раздел 2. Основные этапы и элементы управления рисками и их оценки.**						
2.1	Тема 5. Основные элементы управления рисками информационной безопасности. Понятие риска. Количественное и качественное определение величины риска. Активы организации как ключевые факторы риска. Подходы к управлению рисками.	7	4				ПК-1.2
2.2	Тема 6. Определение ценности активов (критерии оценки ущерба, таблица ценности активов).	7		1/1			ПК-1.2
2.3	Тема 7. Типовые угрозы информационной безопасности. Типовые уязвимости информационной безопасности.	7	4				ПК-1.2
2.4	Тема 8. Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей. Профиль и жизненный цикл угрозы.	7		2/1			ПК-1.2
2.5	Тема 9. Базовый опросник для определения степени критичности систем по методу CRAMM. Опросный лист для оценки угроз по методу CRAMM. Опросный лист для оценки уязвимостей по методу CRAMM.	7				4	ПК-1.2
2.6	Тема 10. Оценка угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки риска. Подготовка отчета об оценке рисков.	7		1/1			ПК-1.2
2.7	Тема 11. Обработка рисков информационной безопасности. Процесс обработки рисков. Способы обработки риска (принятие, уменьшение, передача, избежание риска). Оценка возврата инвестиций в информационную безопасность. План обработки рисков.	7	4				ПК-1.2
2.8	Тема 12. Задание контрмер. Расчет риска реализации по всем угрозам для информационной системы после задания контрмер. Эффективность контрмеры. Эффективность комплекса контрмер. Расчет совокупной стоимости владения. Расчет возврата инвестиций.	7		1/1		4	ПК-1.2
2.9	Тема 13. Декларация о применимости механизмов контроля.	7				4	ПК-1.2
3.0	**Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов.**						
3.1	Тема 14. Инструментальные средства для управления рисками. Выбор инструментария для оценки рисков. Обзор методов и инструментальных средств управления рисками.	7	4				ПК-1.2
3.2	Тема 15. Расчет риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса; риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы; риска реализации по всем угрозам для информационной системы.	7		2/1			ПК-1.2
3.3	Тема 16. Программные продукты для управления рисками информационной безопасности.	7				2	ПК-1.2
3.4	Тема 17. Анализ современных методических подходов к обеспечению защищенности информационных активов предприятия.	7	2				ПК-1.2
3.5	Тема 18. Исследование организационной защиты информационных активов предприятия. Оценка процессов СУИБ на соответствие ISO 27001.	7		2/1			ПК-1.2
3.6	Тема 19. Законодательные и нормативные акты Российской Федерациив области защиты информации.	7				2	ПК-1.2

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
3.7	Тема 20. Изучение документов ГТК (защита от несанкционированного доступа к информации).	7		1/1		2	ПК-1.2
3.8	Тема 21. BS ISO/IEC27001:2005 (BS 7799-2:2005). Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования. Взаимосвязь между стандартами ISO/IEC 27001:2005, BS 779993:2006 ИISO/IEC 27005:2008	7				4	ПК-1.2
4.0	**Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта.**						
4.1	Тема 22. Практические советы по внедрению системы управления рисками. Комплект типовых документов для управления рисками информационной безопасности.	7	4				ПК-1.2
4.2	Тема 23. Многофакторная модель оценки информационных рисков хозяйствующего субъекта. Укрупненная схема оценки защищенности информационных активов предприятия с учетом информационных рисков: подготовительный этап; оценка рисков информационной безопасности предприятия; управление информационными рисками; создание комплексной системы защиты информационных активов хозяйствующего субъекта; реализация программы обеспечения информационной безопасности компании; анализ эффективности вложений в информационную безопасность.	7		2/2			ПК-1.2
4.3	Тема 24. Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта.	7	4				ПК-1.2
4.4	Тема 25. Проработка лекционного материала. Подготовка к промежуточному тестированию.	7				4	ПК-1.2
	Форма промежуточной аттестации – зачет	7					
	Итого часов (без учёта часов на промежуточную аттестацию)		28	14/10		30	

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 оформлен в виде приложения № 1 к рабочей программе дисциплины и размещен 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

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.1.1	Никитин, И. А. Процессы анализа и управления рисками в области ИТ :- 2-е изд., испр. / И. А. Никитин, М. Т. Цулая. Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 167с. - Текст: электронный. - URL: https://biblioclub.ru/index.php?page=book&id=429089 (дата обращения: 14.09.2022)	Онлайн

6.1.2 Дополнительная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	Аверченков, В. И. Аудит информационной безопасности : учебное пособие - 4-е изд., стер. / В. И. Аверченков. Москва : ФЛИНТА, 2021. - 269с. - Текст:	Онлайн

	электронный. - URL: https://biblioclub.ru/index.php?page=book&id=93245 (дата обращения: 14.09.2022)	
6.1.2.2	Анисимов, А. А. Менеджмент в сфере информационной безопасности: курс лекций : курс лекций / А. А. Анисимов. Москва : Интернет-Университет Информационных Технологий (ИНТУИТ)|Бином. Лаборатория знаний, 2009. - 176с. - Текст: электронный. - URL: https://biblioclub.ru/index.php?page=book&id=232981 (дата обращения: 14.09.2022)	Онлайн
6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)		
	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.3.1	Серёдкин, С. П. Методические указания по изучению дисциплины Б1.В.ДВ.08.01 Методология анализа информационных рисков, по направлению подготовки 10.03.01 Информационная безопасность, профиль Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности) / С.П. Серёдкин, Т. К. Кириллова; ИрГУПС. – Иркутск : ИрГУПС, 2023. – 13 с. - Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_8966_1480_2021_1_signed.pdf	Онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	Научная электронная библиотека «КиберЛенинка» — https://cyberleninka.ru/	
6.2.2	Научная электронная библиотека eLIBRARY.RU — https://elibrary.ru/	
6.2.3	Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/	
6.3 Программное обеспечение и информационные справочные системы		
6.3.1 Базовое программное обеспечение		
6.3.1.1	Microsoft Windows Professional 10, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.2	Microsoft Office Russian 2010, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.3	FoxitReader, свободно распространяемое программное обеспечение http://free-software.com.ua/pdf-viewer/foxit-reader/	
6.3.1.4	Adobe Acrobat Reader DC свободно распространяемое программное обеспечение https://get.adobe.com/ru/reader/enterprise/	
6.3.1.5	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License	
6.3.2 Специализированное программное обеспечение		
6.3.2.1	Не предусмотрено	
6.3.3 Информационные справочные системы		
6.3.3.1	КонсультантПлюс – студенческая версия (Онлайн–версия КонсультантПлюс: Студент, https://student2.consultant.ru/cgi/online.cgi?req=home;rnd=0.8160556428138959)	
6.4 Правовые и нормативные документы		
6.4.1	Федеральный закон от 27 июля 2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».	
6.4.2	Федеральный закон от 26 июня 2017г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».	
6.4.3	Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 30.12.2020) "О персональных данных"	
6.4.4	Федеральный закон от 04 мая 2011г. №99-ФЗ «О лицензировании отдельных видов деятельности».	
6.4.5	Федеральный закон от 29 июня 2015г. №162-ФЗ «О стандартизации отдельных видов деятельности».	
6.4.6	Перечень сведений, отнесенных к государственной тайне. Утвержден указом Президента Российской Федерации от 30 ноября 1995г. №1203.	
6.4.7	Правила категорирования объектов критической инфраструктуры Российской Федерации. Утверждены Постановлением Правительства Российской Федерации от 08 февраля 2018г. №127.	
6.4.8	Нормативно-правовые акты государственных, муниципальных органов, предприятий в области ин-формационной безопасности	

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

1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л ИрГУПС находится – по адресу г. Иркутск, ул. Лермонтова, д.80

2	Учебная аудитория Д-415 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
3	Учебная аудитория Д-417 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
4	Учебная аудитория Д-518 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
5	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; – помещения для хранения и профилактического обслуживания учебного оборудования – А-521

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся. Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий лекции. К каждому занятию следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. 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 практическом занятии
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины
Самостоятельная работа	Обучение по дисциплине «Методология анализа информационных рисков» предусматривает активную самостоятельную работу обучающегося. В разделе 4 рабочей программы, который называется «Структура и содержание дисциплины», все часы самостоятельной работы расписаны по темам и вопросам, а также указана необходимая

	учебная литература: обучающийся изучает учебный материал, разбирает примеры и решает разноуровневые задачи в рамках выполнения как общих домашних заданий, так и индивидуальных домашних заданий (ИДЗ) и других видов работ, предусмотренных рабочей программой дисциплины. При выполнении домашних заданий обучающемуся следует обратиться к задачам, решенным на предыдущих практических занятиях, решенным домашним работам, а также к примерам, приводимым лектором. Если этого будет недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделе 6.1 «Учебная литература». Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора. Домашние задания, индивидуальные домашние задания и другие работы, предусмотренные рабочей программой дисциплины должны быть выполнены обучающимся в установленные преподавателем сроки в соответствии с требованиями к оформлению текстовой и графической документации, сформулированным в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль»
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет	

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

УТВЕРЖДЕНА
приказом ректора
от «02» июня 2023 г. № 424-1

Б1.В.ДВ.08.01 Методология анализа информационных рисков

рабочая программа дисциплины

Специальность/направление подготовки – 10.03.01 Информационная безопасность
Специализация/профиль – Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)
Квалификация выпускника – Бакалавр
Форма и срок обучения – очная форма 4 года
Кафедра-разработчик программы – Информационные системы и защита информации

Общая трудоемкость в з.е. – 2
Часов по учебному плану (УП) – 72
В том числе в форме практической подготовки (ПП) – 10
(очная)

Формы промежуточной аттестации
очная форма обучения:
зачет 7 семестр

Очная форма обучения **Распределение часов дисциплины по семестрам**

Семестр	7	**Итого**
Вид занятий	Часов по УП	**Часов по УП**
Аудиторная контактная работа по видам учебных занятий/ в т.ч. в форме ПП*	42/10	**42/10**
– лекции	28	**28**
– практические (семинарские)	14/10	**14/10**
– лабораторные		
Самостоятельная работа	30	**30**
Итого	72/10	**72/10**

* В форме ПП – в форме практической подготовки.

ИРКУТСК

Рабочая программа дисциплины разработана в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 10.03.01 Информационная безопасность, утвержденный Приказом Министерства науки и высшего образования Российской Федерации от 17.11.2020 № 1427.

Программу составил(и):
к.э.н., доцент, С.П. Серёдкин

Рабочая программа рассмотрена и одобрена для использования в учебном процессе на заседании кафедры «Информационные системы и защита информации», протокол от «2» июня 2023 г. № 12

Зав. кафедрой, к.э.н., доцент Т.К. Кириллова

1 ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1 Цели дисциплины

1	раскрытие сущности и значения методологии анализа информационных рисков реализации угроз, как основы информационной безопасности и защиты информации;
2	определение теоретических, концептуальных, методических и организационных основ информационной безопасности и защиты ценной для предприятия информации

1.2 Задачи дисциплины

1	изучить понятие «информационных активов» как основной характеристики системы оценки информационных рисков хозяйствующего субъекта;
2	определить место, роль, специфику системы оценки информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия;
3	оценить существующие методические подходы к оценке информационных рисков для выявления возможностей совершенствования данной деятельности;
4	изучить особенности организационного направления в деятельности по защите информационных активов и определение их влияния на создание и развитие системы защиты информационных активов хозяйствующего субъекта;
5	освоить методические положения по совершенствованию деятельности в сфере оценки информационных рисков хозяйствующих субъектов;
6	освоить методические подходы к оценке эффективности деятельности по защите информационных активов 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 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

Блок/часть ОПОП	Блок 1. Дисциплины / Часть, формируемая участниками образовательных отношений

2.1 Дисциплины и практики, на которых основывается изучение данной дисциплины

1	Б1.В.ДВ.03.01 Основы программирования

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

1	Б2.В.02(Пд) Производственная - преддипломная практика
2	Б3.01(Д) Подготовка к процедуре защиты выпускной квалификационной работы
3	Б3.02(Д) Защита выпускной квалификационной работы

3 ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ТРЕБОВАНИЯМИ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ		
Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения**
ПК-1 Способен организовать работу по выявлению недостатков в функционировании системы защиты и инструментальных средствах программирования	ПК-1.2 Применяет методы анализа информационных рисков в автоматизированных системах	Знать: роль информационных рисков хозяйствующего субъекта в системе управления деятельностью предприятия; основные виды информационных активов (ресурсов) хозяйствующего субъекта; основные виды угроз информационной безопасности хозяйствующего субъекта и уязвимости ресурсов, через которые они могут быть реализованы; особенности и проблемы организационного направления в деятельности по защите информационных активов; методический подход к оценке защищенности информационных активов хозяйствующего субъекта на основе учета информационных рисков; основные направления по применению защитных мероприятий с целью увеличения рискозащищенности информационных активов предприятия; способы технико-экономического обоснования мероприятий по обеспечению информационной безопасности
		Уметь: определять состав, важность и ценность конфиденциальной информации применительно к видам тайны; выявлять информационные риски реализации угроз информационным активам предприятия и иным объектам защиты; разрабатывать модели угроз и нарушителя информационной безопасности предприятия; определять направления и виды защиты информации с учетом характера рисков реализации угроз информационным активам предприятия; выявлять недостатки (уязвимости) в функционировании системы защиты информации автоматизированной системы
		Владеть: основными методами выявления информационных рисков реализации угроз конфиденциальной информации; методами определения уровня информационных рисков; методами оценки возврата инвестиций от реализации контрмер по защите информации, и их эффективности; навыками работы со специальными программными комплексами управления информационными рисками предприятия; терминологией и системным подходом к выявлению недостатков (уязвимостей) информационных систем (АС); навыками анализа угроз ИБ и уязвимостей в АС; организационными, организационно-техническими, техническими и компьютерными средствами по контролю защиты информации в АС

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	**Наименование разделов, тем и видов работ**	**Очная форма**					***Код индикатора достижения компетенции**
		Семестр	**Часы**				
			Лек	**Пр**	**Лаб**	**СР**	
1.0	**Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия.**						
1.1	Тема 1. Риски, породившие мировой финансовый кризис. Информационные риски киберпространства (кибертерроризм, риски промышленных систем, риски утечки информации, риски электронных отчетов). Государственное регулирование. Оценка рисков как основа корпоративного управления.	7	2				ПК-1.2
1.2	Тема 2. Идентификация активов (описание бизнес-процессов).	7		2/1			ПК-1.2

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ							
Код	**Наименование разделов, тем и видов работ**	**Очная форма**					***Код индикатора достижения компетенции**
		Семестр	**Часы**				
			Лек	**Пр**	**Лаб**	**СР**	
1.3	Тема 3. Термины и определения в области управления информационными рисками.	7				2	ПК-1.2
1.4	Тема 4. Антология кибератак. Наихудшие сценарии кибератак.	7				2	ПК-1.2
2.0	**Раздел 2. Основные этапы и элементы управления рисками и их оценки.**						
2.1	Тема 5. Основные элементы управления рисками информационной безопасности. Понятие риска. Количественное и качественное определение величины риска. Активы организации как ключевые факторы риска. Подходы к управлению рисками.	7	4				ПК-1.2
2.2	Тема 6. Определение ценности активов (критерии оценки ущерба, таблица ценности активов).	7		1/1			ПК-1.2
2.3	Тема 7. Типовые угрозы информационной безопасности. Типовые уязвимости информационной безопасности.	7	4				ПК-1.2
2.4	Тема 8. Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей. Профиль и жизненный цикл угрозы.	7		2/1			ПК-1.2
2.5	Тема 9. Базовый опросник для определения степени критичности систем по методу CRAMM. Опросный лист для оценки угроз по методу CRAMM. Опросный лист для оценки уязвимостей по методу CRAMM.	7				4	ПК-1.2
2.6	Тема 10. Оценка угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки риска. Подготовка отчета об оценке рисков.	7		1/1			ПК-1.2
2.7	Тема 11. Обработка рисков информационной безопасности. Процесс обработки рисков. Способы обработки риска (принятие, уменьшение, передача, избежание риска). Оценка возврата инвестиций в информационную безопасность. План обработки рисков.	7	4				ПК-1.2
2.8	Тема 12. Задание контрмер. Расчет риска реализации по всем угрозам для информационной системы после задания контрмер. Эффективность контрмеры. Эффективность комплекса контрмер. Расчет совокупной стоимости владения. Расчет возврата инвестиций.	7		1/1		4	ПК-1.2
2.9	Тема 13. Декларация о применимости механизмов контроля.	7				4	ПК-1.2
3.0	**Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов.**						
3.1	Тема 14. Инструментальные средства для управления рисками. Выбор инструментария для оценки рисков. Обзор методов и инструментальных средств управления рисками.	7	4				ПК-1.2
3.2	Тема 15. Расчет риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса; риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы; риска реализации по всем угрозам для информационной системы.	7		2/1			ПК-1.2
3.3	Тема 16. Программные продукты для управления рисками информационной безопасности.	7				2	ПК-1.2
3.4	Тема 17. Анализ современных методических подходов к обеспечению защищенности информационных активов предприятия.	7	2				ПК-1.2
3.5	Тема 18. Исследование организационной защиты информационных активов предприятия. Оценка процессов СУИБ на соответствие ISO 27001.	7		2/1			ПК-1.2
3.6	Тема 19. Законодательные и нормативные акты Российской Федерациив области защиты информации.	7				2	ПК-1.2

4 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код	Наименование разделов, тем и видов работ	Очная форма					*Код индикатора достижения компетенции
		Семестр	Часы				
			Лек	Пр	Лаб	СР	
3.7	Тема 20. Изучение документов ГТК (защита от несанкционированного доступа к информации).	7		1/1		2	ПК-1.2
3.8	Тема 21. BS ISO/IEC27001:2005 (BS 7799-2:2005). Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования. Взаимосвязь между стандартами ISO/IEC 27001:2005, BS 779993:2006 ИISO/IEC 27005:2008	7				4	ПК-1.2
4.0	**Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта.**						
4.1	Тема 22. Практические советы по внедрению системы управления рисками. Комплект типовых документов для управления рисками информационной безопасности.	7	4				ПК-1.2
4.2	Тема 23. Многофакторная модель оценки информационных рисков хозяйствующего субъекта. Укрупненная схема оценки защищенности информационных активов предприятия с учетом информационных рисков: подготовительный этап; оценка рисков информационной безопасности предприятия; управление информационными рисками; создание комплексной системы защиты информационных активов хозяйствующего субъекта; реализация программы обеспечения информационной безопасности компании; анализ эффективности вложений в информационную безопасность.	7		2/2			ПК-1.2
4.3	Тема 24. Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта.	7	4				ПК-1.2
4.4	Тема 25. Проработка лекционного материала. Подготовка к промежуточному тестированию.	7				4	ПК-1.2
	Форма промежуточной аттестации – зачет	7					
	Итого часов (без учёта часов на промежуточную аттестацию)		28	14/10		30	

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 оформлен в виде приложения № 1 к рабочей программе дисциплины и размещен 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

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.1.1	Никитин, И. А. Процессы анализа и управления рисками в области ИТ :- 2-е изд., испр. / И. А. Никитин, М. Т. Цулая. Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 167с. - Текст: электронный. - URL: https://biblioclub.ru/index.php?page=book&id=429089 (дата обращения: 14.09.2022)	Онлайн

6.1.2 Дополнительная литература

	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.2.1	Аверченков, В. И. Аудит информационной безопасности : учебное пособие - 4-е изд., стер. / В. И. Аверченков. Москва : ФЛИНТА, 2021. - 269с. - Текст:	Онлайн

	электронный. - URL: https://biblioclub.ru/index.php?page=book&id=93245 (дата обращения: 14.09.2022)	
6.1.2.2	Анисимов, А. А. Менеджмент в сфере информационной безопасности: курс лекций : курс лекций / А. А. Анисимов. Москва : Интернет-Университет Информационных Технологий (ИНТУИТ)|Бином. Лаборатория знаний, 2009. - 176с. - Текст: электронный. - URL: https://biblioclub.ru/index.php?page=book&id=232981 (дата обращения: 14.09.2022)	Онлайн
6.1.3 Учебно-методические разработки (в т. ч. для самостоятельной работы обучающихся)		
	Библиографическое описание	Кол-во экз. в библиотеке/ онлайн
6.1.3.1	- Текст: электронный. - URL: https://www.irgups.ru/eis/for_site/umkd_files/mu_9333_1480_2023_1_signed.pdf	Онлайн
6.2 Ресурсы информационно-телекоммуникационной сети «Интернет»		
6.2.1	Научная электронная библиотека «КиберЛенинка» — https://cyberleninka.ru/	
6.2.2	Научная электронная библиотека eLIBRARY.RU — https://elibrary.ru/	
6.2.3	Электронно-библиотечная система «Издательство Лань», https://e.lanbook.com/	
6.3 Программное обеспечение и информационные справочные системы		
6.3.1 Базовое программное обеспечение		
6.3.1.1	Microsoft Windows Professional 10, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.2	Microsoft Office Russian 2010, государственный контракт от 20.07.2021 № 0334100010021000013-01	
6.3.1.3	FoxitReader, свободно распространяемое программное обеспечение http://free-software.com.ua/pdf-viewer/foxit-reader/	
6.3.1.4	Adobe Acrobat Reader DC свободно распространяемое программное обеспечение https://get.adobe.com/ru/reader/enterprise/	
6.3.1.5	Яндекс. Браузер. Прикладное программное обеспечение общего назначения, Офисные приложения, лицензия – свободно распространяемое программное обеспечение по лицензии BSD License	
6.3.2 Специализированное программное обеспечение		
6.3.2.1	Не предусмотрено	
6.3.3 Информационные справочные системы		
6.3.3.1	КонсультантПлюс – студенческая версия (Онлайн–версия КонсультантПлюс: Студент, https://student2.consultant.ru/cgi/online.cgi?req=home;rnd=0.8160556428138959)	
6.4 Правовые и нормативные документы		
6.4.1	Федеральный закон от 27 июля 2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации».	
6.4.2	Федеральный закон от 26 июня 2017г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».	
6.4.3	Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 30.12.2020) "О персональных данных"	
6.4.4	Федеральный закон от 04 мая 2011г. №99-ФЗ «О лицензировании отдельных видов деятельности».	
6.4.5	Федеральный закон от 29 июня 2015г. №162-ФЗ «О стандартизации отдельных видов деятельности».	
6.4.6	Перечень сведений, отнесенных к государственной тайне. Утвержден указом Президента Российской Федерации от 30 ноября 1995г. №1203.	
6.4.7	Правила категорирования объектов критической инфраструктуры Российской Федерации. Утверждены Постановлением Правительства Российской Федерации от 08 февраля 2018г. №127.	
6.4.8	Нормативно-правовые акты государственных, муниципальных органов, предприятий в области ин-формационной безопасности	

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

1	Корпуса А, Б, В, Г, Д, Е ИрГУПС находятся по адресу г. Иркутск, ул. Чернышевского, д. 15; корпус Л ИрГУПС находится – по адресу г. Иркутск, ул. Лермонтова, д.80
2	Учебная аудитория Д-415 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
3	Учебная аудитория Д-417 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых

	работ), текущего контроля и промежуточной аттестации. Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
4	Учебная аудитория Д-518 для проведения лекционных и практических занятий, лабораторных работ, групповых и индивидуальных консультаций, курсового проектирования (выполнения курсовых работ), текущего контроля и промежуточной аттестации Основное оборудование: специализированная мебель, мультимедиапроектор, экран, (ноутбук переносной)
5	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; – помещения для хранения и профилактического обслуживания учебного оборудования – А-521

8 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Вид учебной деятельности	Организация учебной деятельности обучающегося
Лекция	Лекция (от латинского «lection» – чтение) – вид аудиторных учебных занятий. Лекция: закладывает основы научных знаний в систематизированной, последовательной, обобщенной форме; раскрывает состояние и перспективы развития соответствующей области науки и техники; концентрирует внимание обучающихся на наиболее сложных, узловых вопросах; стимулирует познавательную активность обучающихся. Во время лекционных занятий обучающийся должен уметь сконцентрировать внимание на изучаемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого весь материал, излагаемый преподавателем, обучающемуся необходимо конспектировать. На полях конспекта следует помечать вопросы, выделенные обучающимся для консультации с преподавателем. Выводы, полученные в виде формул, рекомендуется в конспекте подчеркивать или обводить рамкой, чтобы лучше запоминались. Полезно составить краткий справочник, содержащий определения важнейших понятий лекции. К каждому занятию следует разобрать материал предыдущей лекции. Изучая материал по учебнику или конспекту лекций, следует переходить к следующему вопросу только в том случае, когда хорошо усвоен предыдущий вопрос. Ряд вопросов дисциплины может быть вынесен на самостоятельное изучение. Такое задание требует оперативного выполнения. В конспекте лекций необходимо оставить место для освещения упомянутых вопросов. 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 практическом занятии
Практическое занятие	Практическое занятие – вид аудиторных учебных занятий, целенаправленная форма организации учебного процесса, при реализации которой обучающиеся по заданию и под руководством преподавателя выполняют практические задания. Практические задания направлены на углубление научно-теоретических знаний и овладение определенными методами работы, в процессе которых вырабатываются умения и навыки выполнения тех или иных учебных действий в данной сфере науки. Практические занятия развивают научное мышление и речь, позволяют проверить знания обучающихся, выступают как средства оперативной обратной связи; цель практических занятий – углублять, расширять, детализировать знания, полученные на лекции, в обобщенной форме и содействовать выработке навыков профессиональной деятельности. На практических занятиях подробно рассматриваются основные вопросы дисциплины, разбираются основные типы задач. К каждому практическому занятию следует заранее самостоятельно выполнить домашнее задание и выучить лекционный материал к следующей теме. Систематическое выполнение домашних заданий обязательно и является важным фактором, способствующим успешному усвоению дисциплины
Самостоятельная работа	Обучение по дисциплине «Методология анализа информационных рисков» предусматривает активную самостоятельную работу обучающегося. В разделе 4 рабочей программы, который называется «Структура и содержание дисциплины», все часы самостоятельной работы расписаны по темам и вопросам, а также указана необходимая учебная литература: обучающийся изучает учебный материал, разбирает примеры и решает разноуровневые задачи в рамках выполнения как общих домашних заданий, так и индивидуальных домашних заданий (ИДЗ) и других видов работ, предусмотренных рабочей программой дисциплины. При выполнении домашних заданий обучающемуся следует обратиться к задачам, решенным на предыдущих практических занятиях, решенным домашним работам, а также к примерам, приводимым лектором. Если этого будет

	недостаточно для выполнения всей работы можно дополнительно воспользоваться учебными пособиями, приведенными в разделе 6.1 «Учебная литература». Если, несмотря на изученный материал, задание выполнить не удается, то в обязательном порядке необходимо посетить консультацию преподавателя, ведущего практические занятия, и/или консультацию лектора. Домашние задания, индивидуальные домашние задания и другие работы, предусмотренные рабочей программой дисциплины должны быть выполнены обучающимся в установленные преподавателем сроки в соответствии с требованиями к оформлению текстовой и графической документации, сформулированным в Положении «Требования к оформлению текстовой и графической документации. Нормоконтроль»
Комплекс учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет	

Приложение № 1 к рабочей программе

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации

1. Общие положения

Фонд оценочных средств (ФОС) является составной частью нормативно-методического обеспечения системы оценки качества освоения обучающимися образовательной программы.

Фонд оценочных средств предназначен для использования обучающимися, преподавателями, администрацией ИрГУПС, а также сторонними образовательными организациями для оценивания качества освоения образовательной программы и уровня сформированности компетенций у обучающихся.

Задачами ФОС являются:

– оценка достижений обучающихся в процессе изучения дисциплины;

– обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс;

– самоподготовка и самоконтроль обучающихся в процессе обучения.

Фонд оценочных средств сформирован на основе ключевых принципов оценивания: валидность, надежность, объективность, эффективность.

Для оценки уровня сформированности компетенций используется трехуровневая система:

– минимальный уровень освоения, обязательный для всех обучающихся по завершению освоения образовательной программы; дает общее представление о виде деятельности, основных закономерностях функционирования объектов профессиональной деятельности, методов и алгоритмов решения практических задач;

– базовый уровень освоения, превышение минимальных характеристик сформированности компетенций; позволяет решать типовые задачи, принимать профессиональные и управленческие решения по известным алгоритмам, правилам и методикам;

– высокий уровень освоения, максимально возможная выраженность характеристик компетенций; предполагает готовность решать практические задачи повышенной сложности, нетиповые задачи, принимать профессиональные и управленческие решения в условиях неполной определенности, при недостаточном документальном, нормативном и методическом обеспечении.

2. Перечень компетенций, в формировании которых участвует дисциплина.
Программа контрольно-оценочных мероприятий.
Показатели оценивания компетенций, критерии оценки

Дисциплина «Методология анализа информационных рисков» участвует в формировании компетенций:

ПК-1. Способен организовать работу по выявлению недостатков в функционировании системы защиты и инструментальных средствах программирования

Программа контрольно-оценочных мероприятий очная форма обучения

№	Наименование контрольно-оценочного мероприятия	Объект контроля	Код индикатора достижения компетенции	Наименование оценочного средства (форма проведения*)
7 семестр				
1.0	**Раздел 1. Место и роль системы рискозащищенности информационных активов в системе управления деятельностью предприятия**			
1.1	Текущий контроль	Тема 1. Риски, породившие мировой финансовый кризис. Информационные риски киберпространства (кибертерроризм, риски промышленных систем, риски утечки информации, риски электронных отчетов). Государственное регулирование. Оценка рисков как основа корпоративного управления.	ПК-1.2	Конспект (письменно)
1.2	Текущий контроль	Тема 2. Идентификация активов (описание бизнес-процессов).	ПК-1.2	Дискуссия (устно) Конспект (письменно) В рамках ПП**: Дискуссия (устно) Конспект (письменно)
1.3	Текущий контроль	Тема 3. Термины и определения в области управления информационными рисками.	ПК-1.2	Конспект (письменно)
1.4	Текущий контроль	Тема 4. Антология кибератак. Наихудшие сценарии кибератак.	ПК-1.2	Конспект (письменно)
2.0	**Раздел 2. Основные этапы и элементы управления рисками и их оценки**			
2.1	Текущий контроль	Тема 5. Основные элементы управления рисками информационной безопасности. Понятие риска. Количественное и качественное определение величины риска. Активы организации как ключевые факторы риска. Подходы к управлению рисками.	ПК-1.2	Конспект (письменно)
2.2	Текущий контроль	Тема 6. Определение ценности активов (критерии оценки ущерба, таблица ценности активов).	ПК-1.2	Дискуссия (устно) Конспект (письменно) В рамках ПП**: Дискуссия (устно) Конспект (письменно)
2.3	Текущий контроль	Тема 7. Типовые угрозы информационной безопасности. Типовые уязвимости информационной безопасности.	ПК-1.2	Конспект (письменно)
2.4	Текущий контроль	Тема 8. Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей. Профиль и жизненный цикл угрозы.	ПК-1.2	Дискуссия (устно) Конспект (письменно) В рамках ПП**: Дискуссия (устно) Конспект (письменно)

2.5	Текущий контроль	Тема 9. Базовый опросник для определения степени критичности систем по методу CRAMM. Опросный лист для оценки угроз по методу CRAMM. Опросный лист для оценки уязвимостей по методу CRAMM.	ПК-1.2	Конспект (письменно)
2.6	Текущий контроль	Тема 10. Оценка угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки риска. Подготовка отчета об оценке рисков.	ПК-1.2	Дискуссия (устно) Конспект (письменно) В рамках ПП**: Дискуссия (устно) Конспект (письменно)
2.7	Текущий контроль	Тема 11. Обработка рисков информационной безопасности. Процесс обработки рисков. Способы обработки риска (принятие, уменьшение, передача, избежание риска). Оценка возврата инвестиций в информационную безопасность. План обработки рисков.	ПК-1.2	Конспект (письменно)
2.8	Текущий контроль	Тема 12. Задание контрмер. Расчет риска реализации по всем угрозам для информационной системы после задания контрмер. Эффективность контрмеры. Эффективность комплекса контрмер. Расчет совокупной стоимости владения. Расчет возврата инвестиций.	ПК-1.2	Дискуссия (устно) Конспект (письменно) В рамках ПП**: Дискуссия (устно) Конспект (письменно)
2.9	Текущий контроль	Тема 13. Декларация о применимости механизмов контроля.	ПК-1.2	Конспект (письменно)
3.0	**Раздел 3. Методические подходы к оценке информационных рисков хозяйствующих субъектов**			
3.1	Текущий контроль	Тема 14. Инструментальные средства для управления рисками. Выбор инструментария для оценки рисков. Обзор методов и инструментальных средств управления рисками.	ПК-1.2	Дискуссия (устно) Конспект (письменно)
3.2	Текущий контроль	Тема 15. Расчет риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса; риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы; риска реализации по всем угрозам для информационной системы.	ПК-1.2	Дискуссия (устно) Конспект (письменно) В рамках ПП**: Дискуссия (устно) Конспект (письменно)
3.3	Текущий контроль	Тема 16. Программные продукты для управления рисками информационной безопасности.	ПК-1.2	Конспект (письменно)
3.4	Текущий контроль	Тема 17. Анализ современных методических подходов к обеспечению защищенности информационных активов предприятия.	ПК-1.2	Конспект (письменно)
3.5	Текущий контроль	Тема 18. Исследование организационной защиты информационных активов предприятия. Оценка процессов СУИБ на соответствие ISO 27001.	ПК-1.2	Дискуссия (устно) Конспект (письменно) В рамках ПП**: Дискуссия (устно) Конспект (письменно)

3.6	Текущий контроль	Тема 19. Законодательные и нормативные акты Российской Федерациив области защиты информации.	ПК-1.2	Конспект (письменно)
3.7	Текущий контроль	Тема 20. Изучение документов ГТК (защита от несанкционированного доступа к информации).	ПК-1.2	Конспект (письменно) В рамках ПП**: Конспект (письменно)
3.8	Текущий контроль	Тема 21. BS ISO/IEC27001:2005 (BS 7799-2:2005). Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования. Взаимосвязь между стандартами ISO/IEC 27001:2005, BS 779993:2006 ИISO/IEC 27005:2008	ПК-1.2	Конспект (письменно)
4.0	**Раздел 4. Разработка методики оценки информационных рисков хозяйствующего субъекта**			
4.1	Текущий контроль	Тема 22. Практические советы по внедрению системы управления рисками. Комплект типовых документов для управления рисками информационной безопасности.	ПК-1.2	Конспект (письменно)
4.2	Текущий контроль	Тема 23. Многофакторная модель оценки информационных рисков хозяйствующего субъекта. Укрупненная схема оценки защищенности информационных активов предприятия с учетом информационных рисков: подготовительный этап; оценка рисков информационной безопасности предприятия; управление информационными рисками; создание комплексной системы защиты информационных активов хозяйствующего субъекта; реализация программы обеспечения информационной безопасности компании; анализ эффективности вложений в информационную безопасность.	ПК-1.2	Дискуссия (устно) Конспект (письменно) В рамках ПП**: Дискуссия (устно) Конспект (письменно)
4.3	Текущий контроль	Тема 24. Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта.	ПК-1.2	Дискуссия (устно) Конспект (письменно)
4.4	Текущий контроль	Тема 25. Проработка лекционного материала. Подготовка к промежуточному тестированию.	ПК-1.2	Конспект (письменно)
	Промежуточная аттестация	Все разделы		Зачет (собеседование) Зачет - тестирование (компьютерные технологии)

*Форма проведения контрольно-оценочного мероприятия: устно, письменно, компьютерные технологии.

**ПП – практическая подготовка

Описание показателей и критериев оценивания компетенций.

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 двухбалльная шкала: «зачтено», «не зачтено».

Перечень оценочных средств, используемых для оценивания компетенций, а также краткая характеристика этих средств приведены в таблице.

Текущий контроль

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	Дискуссия	Оценочные средства, позволяющие включить обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку зрения. Может быть использовано для оценки знаний и умений обучающихся	Перечень дискуссионных тем
2	Конспект	Особый вид текста, в основе которого лежит аналитико-синтетическая переработка информации первоисточника (исходного текста). Цель этой деятельности — выявление, систематизация и обобщение (с возможной критической оценкой) наиболее ценной (для конспектирующего) информации. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Темы конспектов

Промежуточная аттестация

№	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в ФОС
1	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 к зачету
2	Тест – промежуточная аттестация в форме зачета	Система автоматизированного контроля освоения компетенций (части компетенций) обучающимся по дисциплине (модулю) с использованием информационно-коммуникационных технологий. Может быть использовано для оценки знаний, умений, навыков и (или) опыта деятельности обучающихся	Фонд тестовых заданий

Критерии и шкалы оценивания компетенций в результате изучения дисциплины при проведении промежуточной аттестации в форме зачета. Шкала оценивания уровня освоения компетенций

Шкала оценивания	Критерии оценивания	Уровень

		освоения компетенции
«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	Компетенция не сформирована

Тест – промежуточная аттестация в форме зачета

Шкала оценивания	Критерии оценивания
«зачтено»	Обучающийся верно ответил на 70 % и более тестовых заданий при прохождении тестирования
«не зачтено»	Обучающийся верно ответил на 69 % и менее тестовых заданий при прохождении тестирования

Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Дискуссия

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Выбранная обучающимся тема (проблема) актуальна в данном курсе; представлен подробный план-конспект, в котором отражены вопросы для дискуссии; временной регламент обсуждения обоснован; даны возможные варианты ответов; использованы примеры из науки и практики
«хорошо»		Выбранная обучающимся тема (проблема) актуальна в данном курсе; представлен сжатый план-конспект, в котором отражены вопросы для дискуссии; временной регламент обсуждения обоснован; отсутствуют возможные варианты ответов; приведен один пример из практики
«удовлетворительно»		Выбранная обучающимся тема (проблема) недостаточно актуальна в данном курсе; представлен содержательно краткий план-конспект, в котором отражены вопросы для дискуссии; отсутствует временной регламент обсуждения; отсутствуют возможные варианты ответов; отсутствуют примеры из практики

«неудовлетворительно»	«не зачтено»	Выбранная обучающимся тема (проблема) не актуальна для данного курса; частично представлены вопросы для дискуссии; отсутствует временной регламент обсуждения; отсутствуют возможные варианты ответов; отсутствуют примеры из практики

Конспект

Шкалы оценивания		Критерии оценивания
«отлично»	«зачтено»	Конспект по теме выполнен в обозначенный преподавателем срок. Конспект выполнен обучающимся по заданной теме в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; раскрыл тему полностью и ответил на все вопросы преподавателя по конкретной теме конспекта. Конспект оформлен аккуратно, в наиболее оптимальной для фиксации результатов форме
«хорошо»		Конспект по теме выполнен в обозначенный преподавателем срок. Конспект выполнен обучающимся по заданной теме в полном объеме с соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; раскрыл тему не полностью и ответил на часть вопросов преподавателя по конкретной теме конспекта. Конспект оформлен аккуратно, с незначительными исправлениями
«удовлетворительно»		Конспект по теме выполнен в обозначенный преподавателем срок. Конспект выполнен обучающимся по заданной теме в не полном объеме с частичным соблюдением необходимой последовательности. Обучающийся работал полностью самостоятельно; раскрыл тему не полностью и ответил на часть вопросов преподавателя по конкретной теме конспекта. Конспект оформлен не аккуратно
«неудовлетворительно»	«не зачтено»	Конспект по теме не выполнен в обозначенный преподавателем срок. Конспект выполнен обучающимся не по заданной теме в не полном объеме без соблюдения необходимой последовательности. Обучающийся работал не самостоятельно; не раскрыл тему и не ответил на вопросы преподавателя по конкретной теме конспекта. Конспект оформлен не аккуратно

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

3.1 Типовые контрольные задания для проведения дискуссии

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для проведения дискуссии.

Образец вопросов для проведения дискуссии

Идентификация активов (описание бизнес-процессов)

Определение ценности активов (критерии оценки ущерба, таблица ценности активов)

Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей. Профиль и жизненный цикл угрозы

Оценка угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки риска. Подготовка отчета об оценке рисков

Задание контрмер. Расчет риска реализации по всем угрозам для информационной системы после задания контрмер. Эффективность контрмеры. Эффективность комплекса контрмер. Расчет совокупной стоимости владения. Расчет возврата инвестиций

Инструментальные средства для управления рисками. Выбор инструментария для оценки рисков. Обзор методов и инструментальных средств управления рисками

Расчет риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса; риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы; риска реализации по всем угрозам для информационной системы
Исследование организационной защиты информационных активов предприятия. Оценка процессов СУИБ на соответствие ISO 27001
Многофакторная модель оценки информационных рисков хозяйствующего субъекта.
Укрупненная схема оценки защищенности информационных активов предприятия с учетом информационных рисков: подготовительный этап; оценка рисков информационной безопасности предприятия; управление информационными рисками; создание комплексной системы защиты информационных активов хозяйствующего субъекта; реализация программы обеспечения информационной безопасности компании; анализ эффективности вложений в информационную безопасность
Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта

3.2 Типовые контрольные задания для написания конспекта

Контрольные варианты заданий выложены в электронной информационно-образовательной среде ИрГУПС, доступной обучающемуся через его личный кабинет.

Ниже приведен образец типовых вариантов заданий для написания конспектов.

Образец тем конспектов

Риски, породившие мировой финансовый кризис. Информационные риски киберпространства (кибертерроризм, риски промышленных систем, риски утечки информации, риски электронных отчетов). Государственное регулирование. Оценка рисков как основа корпоративного управления
Идентификация активов (описание бизнес-процессов)
Термины и определения в области управления информационными рисками
Антология кибератак. Наихудшие сценарии кибератак
Основные элементы управления рисками информационной безопасности. Понятие риска. Количественное и качественное определение величины риска. Активы организации как ключевые факторы риска. Подходы к управлению рисками
Определение ценности активов (критерии оценки ущерба, таблица ценности активов).»
Типовые угрозы информационной безопасности. Типовые уязвимости информационной безопасности
Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей. Профиль и жизненный цикл угрозы
Базовый опросник для определения степени критичности систем по методу CRAMM.Опросный лист для оценки угроз по методу CRAMM. Опросный лист для оценки уязвимостей по методу CRAMM
Оценка угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки риска. Подготовка отчета об оценке рисков
Обработка рисков информационной безопасности. Процесс обработки рисков. Способы обработки риска (принятие, уменьшение, передача, избежание риска). Оценка возврата инвестиций в информационную безопасность. План обработки рисков
Задание контрмер. Расчет риска реализации по всем угрозам для информационной системы после задания контрмер. Эффективность контрмеры. Эффективность комплекса контрмер. Расчет совокупной стоимости владения. Расчет возврата инвестиций
Декларация о применимости механизмов контроля
Инструментальные средства для управления рисками. Выбор инструментария для оценки рисков. Обзор методов и инструментальных средств управления рисками
Расчет риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса; риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы; риска реализации по всем угрозам для информационной системы
Программные продукты для управления рисками информационной безопасности

Анализ современных методических подходов к обеспечению защищенности информационных активов предприятия
Исследование организационной защиты информационных активов предприятия. Оценка процессов СУИБ на соответствие ISO 27001
Законодательные и нормативные акты Российской Федерации в области защиты информации
Изучение документов ГТК (защита от несанкционированного доступа к информации).»
BS ISO/IEC27001:2005 (BS 7799-2:2005). Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования. Взаимосвязь между стандартами ISO/IEC 27001:2005, BS 779993:2006 ИISO/IEC 27005:2008
Практические советы по внедрению системы управления рисками. Комплект типовых документов для управления рисками информационной безопасности
Многофакторная модель оценки информационных рисков хозяйствующего субъекта.
Укрупненная схема оценки защищенности информационных активов предприятия с учетом информационных рисков: подготовительный этап; оценка рисков информационной безопасности предприятия; управление информационными рисками; создание комплексной системы защиты информационных активов хозяйствующего субъекта; реализация программы обеспечения информационной безопасности компании; анализ эффективности вложений в информационную безопасность
Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта
Проработка лекционного материала. Подготовка к промежуточному тестированию

3.3 Типовые контрольные задания для проведения тестирования

Фонд тестовых заданий по дисциплине содержит тестовые задания, распределенные по разделам и темам, с указанием их количества и типа.

Структура фонда тестовых заданий по дисциплине

Индикатор достижения компетенции	Тема в соответствии с РПД	Характеристика ТЗ	Количество тестовых заданий, типы ТЗ
ПК-1.2	Тема 1. Риски, породившие мировой финансовый кризис. Информационные риски киберпространства (кибертерроризм, риски промышленных систем, риски утечки информации, риски электронных отчетов). Государственное регулирование. Оценка рисков как основа корпоративного управления.	Знание	1 – зтз
		Умение	1 – отз
		Навык и (или) опыт деятельности/действие	1 – зтз
ПК-1.2	Тема 2. Идентификация активов (описание бизнес-процессов).	Знание	1 – отз
		Умение	1 – зтз
		Навык и (или) опыт деятельности/действие	1 – отз
ПК-1.2	Тема 3. Термины и определения в области управления информационными рисками.	Знание	1 – зтз
		Умение	1 – отз
		Навык и (или) опыт деятельности/действие	1 – зтз
ПК-1.2	Тема 4. Антология кибератак. Наихудшие сценарии кибератак.	Знание	1 – отз
		Умение	1 – зтз
		Навык и (или) опыт деятельности/действие	1 – отз
ПК-1.2	Тема 5. Основные элементы управления рисками информационной безопасности. Понятие риска. Количественное и качественное определение величины риска. Активы организации как ключевые факторы риска. Подходы к управлению рисками.	Знание	1 – зтз
		Умение	1 – отз
		Навык и (или) опыт деятельности/действие	1 – зтз
ПК-1.2		Знание	1 – отз

	Тема 6. Определение ценности активов (критерии оценки ущерба, таблица ценности активов).	Умение	1 – зтз
		Навык и (или) опыт деятельности/действие	1 – отз
ПК-1.2	Тема 7. Типовые угрозы информационной безопасности. Типовые уязвимости информационной безопасности.	Знание	1 – зтз
		Умение	1 – отз
		Навык и (или) опыт деятельности/действие	1 – зтз
ПК-1.2	Тема 8. Анализ угроз и уязвимостей. Описание угроз безопасности и уязвимостей. Профиль и жизненный цикл угрозы.	Знание	1 – отз
		Умение	1 – зтз
		Навык и (или) опыт деятельности/действие	1 – отз
ПК-1.2	Тема 9. Базовый опросник для определения степени критичности систем по методу CRAMM. Опросный лист для оценки угроз по методу CRAMM. Опросный лист для оценки уязвимостей по методу CRAMM.	Знание	1 – зтз
		Умение	1 – отз
		Навык и (или) опыт деятельности/действие	1 – зтз
ПК-1.2	Тема 10. Оценка угроз и уязвимостей. Определение величины риска. Калибровка шкалы оценки риска. Подготовка отчета об оценке рисков.	Знание	1 – отз
		Умение	1 – зтз
		Навык и (или) опыт деятельности/действие	1 – отз
ПК-1.2	Тема 11. Обработка рисков информационной безопасности. Процесс обработки рисков. Способы обработки риска (принятие, уменьшение, передача, избежание риска). Оценка возврата инвестиций в информационную безопасность. План обработки рисков.	Знание	1 – зтз
		Умение	1 – отз
		Навык и (или) опыт деятельности/действие	1 – зтз
ПК-1.2	Тема 12. Задание контрмер. Расчет риска реализации по всем угрозам для информационной системы после задания контрмер. Эффективность контрмеры. Эффективность комплекса контрмер. Расчет совокупной стоимости владения. Расчет возврата инвестиций.	Знание	1 – отз
		Умение	1 – зтз
		Навык и (или) опыт деятельности/действие	1 – отз
ПК-1.2	Тема 13. Декларация о применимости механизмов контроля.	Знание	1 – зтз
		Умение	1 – отз
		Навык и (или) опыт деятельности/действие	1 – зтз
ПК-1.2	Тема 14. Инструментальные средства для управления рисками. Выбор инструментария для оценки рисков. Обзор методов и инструментальных средств управления рисками.	Знание	1 – отз
		Умение	1 – зтз
		Навык и (или) опыт деятельности/действие	1 – отз
ПК-1.2	Тема 15. Расчет риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для ресурса; риска реализации по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы; риска реализации по всем угрозам для информационной системы.	Знание	1 – зтз
		Умение	1 – отз
		Навык и (или) опыт деятельности/действие	1 – зтз
ПК-1.2	Тема 16. Программные продукты для управления рисками информационной безопасности.	Знание	1 – отз
		Умение	1 – зтз
		Навык и (или) опыт деятельности/действие	1 – отз
ПК-1.2	Тема 17. Анализ современных методических подходов к обеспечению защищенности информационных активов предприятия.	Знание	1 – зтз
		Умение	1 – отз
		Навык и (или) опыт деятельности/действие	1 – зтз
ПК-1.2	Тема 18. Исследование организационной защиты информационных активов предприятия. Оценка процессов СУИБ на соответствие ISO 27001.	Знание	1 – отз
		Умение	1 – зтз
		Навык и (или) опыт деятельности/действие	1 – отз
ПК-1.2	Тема 19. Законодательные и нормативные акты Российской Федерациив области защиты информации.	Знание	1 – зтз
		Умение	1 – отз
		Навык и (или) опыт деятельности/действие	1 – зтз
ПК-1.2	Тема 20. Изучение документов ГТК (защита от несанкционированного доступа к информации).	Знание	1 – отз
		Умение	1 – зтз

		Навык и (или) опыт деятельности/действие	1 – отз
ПК-1.2	Тема 21. BS ISO/IEC27001:2005 (BS 7799-2:2005). Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования. Взаимосвязь между стандартами ISO/IEC 27001:2005, BS 779993:2006 ИISO/IEC 27005:2008	Знание	1 – зтз
		Умение	1 – отз
		Навык и (или) опыт деятельности/действие	1 – зтз
ПК-1.2	Тема 22. Практические советы по внедрению системы управления рисками. Комплект типовых документов для управления рисками информационной безопасности.	Знание	1 – отз
		Умение	1 – зтз
		Навык и (или) опыт деятельности/действие	1 – отз
ПК-1.2	Тема 23. Многофакторная модель оценки информационных рисков хозяйствующего субъекта. Укрупненная схема оценки защищенности информационных активов предприятия с учетом информационных рисков: подготовительный этап; оценка рисков информационной безопасности предприятия; управление информационными рисками; создание комплексной системы защиты информационных активов хозяйствующего субъекта; реализация программы обеспечения информационной безопасности компании; анализ эффективности вложений в информационную безопасность.	Знание	1 – зтз
		Умение	1 – отз
		Навык и (или) опыт деятельности/действие	1 – зтз
ПК-1.2	Тема 24. Методические подходы к оценке затрат на обеспечение защищенности информационных активов хозяйствующего субъекта.	Знание	1 – отз
		Умение	1 – зтз
		Навык и (или) опыт деятельности/действие	1 – отз
ПК-1.2	Тема 25. Проработка лекционного материала. Подготовка к промежуточному тестированию.	Знание	1 – зтз
		Умение	1 – отз
		Навык и (или) опыт деятельности/действие	1 - зтз
		Итого	37 – ОТЗ 38 - ЗТЗ

Полный комплект ФТЗ хранится в электронной информационно-образовательной среде ИрГУПС и обучающийся имеет возможность ознакомиться с демонстрационным вариантом ФТЗ.

Ниже приведен образец типового варианта итогового теста, предусмотренного рабочей программой дисциплины.

1. Риск информационной безопасности:

А) Потенциальная возможность использования уязвимостей активов конкретной угрозой для причинения ущерба организации;

Б) Вероятные потери организации в результате инцидентов;

В) Возможность минимизации угрозы информационной безопасности.

2. Оценка рисков ИБ, включающая в себя:

А) Идентификацию риска ИБ и анализ риска ИБ;

Б) Идентификацию риска ИБ, анализ риска ИБ, сравнительную оценку риска ИБ; оценку остаточного риска;

В) Идентификацию риска ИБ, анализ риска ИБ, оценку остаточного риска, расчет ущерба.

3. Обработка рисков ИБ

А) Снижение, перенос, уклонение, принятие;

Б) Страхование;

В) Хеджирование.

4. Алгоритм оценки имеющихся корпоративных информационных активов включает в себя их описание по следующим категориям:

А) человеческие ресурсы (надежность персонал, информационные активы;

Б) Сервисные ресурсы, помещения, в которых обрабатывается, хранится информация;

В) Программные ресурсы, физические ресурсы (сервера, рабочие станции, сетевое и телекоммуникационное оборудование).

Ответ: 1 – А, 2 – В, 3 - Б

5. Каким методом определяется уровень риска информационного актива:

А) Метод ожидаемых потерь;

Б) Затратный метод;

В) Метод аналогий.

6. Технические каналы утечки информации возникают:

А) При использовании злоумышленником специальных технических средств промышленного шпионажа, позволяющих получать защищаемую информацию при непосредственном контакте с персоналом фирмы, документами, делами и базами данных;

Б) При использовании злоумышленником специальных технических средств промышленного шпионажа, позволяющих получать защищаемую информацию без непосредственного контакта с персоналом фирмы, документами, делами и базами данных;

В) При использовании злоумышленником специальных технических средств для воздействия на средства защиты информации;

7. Основными техническими каналами являются:

А) Визуально-оптический;

Б) Акустический;

В) Электромагнитный;

Г) Все из перечисленного.

8. Угрозы безопасности информационным активам это:

А) **Совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации;**

Б) Совокупность условий и факторов, которые могут причинить ущерб информации;

В) Совокупность условий и факторов, которые могут стать причиной нарушения информации.

9.Оценка рисков – это:

А) Выбор параметров для их описания и получение оценок по этим параметрам;

Б) Процедура выявления факторов рисков и оценки их значимости;

В) Выявление характера последствий.

10. Что такое анализ информационного риска?

Ответ: Анализ информационного риска – это систематическое использование информации для выявления угроз безопасности информации, уязвимостей информационной системы и количественной оценки вероятностей реализации угроз с использованием уязвимостей и последствий реализации угроз для информации и информационной системы, предназначенной для обработки этой информации.

11. Что такое оценка информационного риска?

Ответ: Оценка информационного риска – это общий процесс анализа информационного риска и его оценивания.

12. Какой результат реализации снижения риска?

Ответ: Внедрение мер и средств контроля и управления таким образом, чтобы остаточный риск мог быть повторно оценен как допустимый

13. Какой результат реализации сохранения риска?

Ответ: это решение о сохранении риска без каких-либо дальнейших действий

14. Какой результат реализации избежания риска?

Ответ: это отказ от деятельности или условия, вызывающего конкретный риск

15. Действиями, выполнение которых позвонил снизить риск реализации угрозы кражи средств с банковских счетов являются..

Ответ: строгое соблюдение сотрудниками положений политики информационной безопасности, своевременное обновление программного обеспечения и операционной системы, повышение информационной грамотности сотрудников.

16. Опишите последовательность действий в процессе анализа рисков информационной

безопасности?

Ответ: Определение ценности активов, оценка потенциальных потерь от реализации угрозы, анализ угроз, определение общих годовых потерь на угрозы, выбор мер по снижению, переносу или принятию риска

17. Какие мероприятия необходимо предусмотреть при управлении рисками в платежной системе?

Ответ: Определение порядка обмена информацией, необходимой для управления рисками; определение порядка обеспечения защиты информации в платежной системе; определение организационной структуры управления рисками, обеспечивающей контроль за выполнением участниками платежной системы требований к управлению рисками, установленных правилами платежной системы

18. Для снижения потенциального риска от реализации угрозы через уязвимость “SigRed” необходимо…

Ответ: Получить и применить последние обновления операционной системы, включить планировщик ядра, получить и применить последние обновления микрокода или прошивки.

3.4 Перечень теоретических вопросов к зачету

(для оценки знаний)

1. Что такое информация ограниченного доступа?
2. В каких аспектах экономической деятельности, может выступать конфиденциальная информация?
3. Дайте характеристику понятия «информационные активы организации».
4. Какова взаимосвязь понятий «информационных активов» и «системы оценки рисков информационной безопасности хозяйствующего субъекта»?
5. Определите место и роль системы защиты информационных активов в системе управления деятельностью предприятия.
6. В чем заключается суть тревожных симптомов в сфере обеспечения безопасности информационных активов?
7. В чем заключается суть тенденции увеличения количества внутренних угроз, исходящих от сотрудников организаций (инсайдеров)?
8. Рассмотрите сущность основных видов организационных каналов несанкционированного доступа к информационным активам.
9. В чем заключается суть аналитической работы по обнаружению организационных каналов несанкционированного доступа к информационным активам?
10. Раскройте сущность комплексной системы защиты информационных активов предприятий.
11. Раскройте особенности система защиты информационных активов хозяйствующего субъекта.
12. Опишите особенности организационного направления в деятельности по защите информационных активов предприятия.
13. Охарактеризуйте сущность направления в организационной защите – работе с персоналом, определении его надежности.
14. Как осуществить оценку надежности персонала, как основного источника угроз информационным активам предприятия?
15. Опишите методику оценки возможного ущерба при реализации угроз безопасности.
16. Охарактеризуйте сущность направления в организационной защите - информационно-аналитической деятельности по выявлению угроз информационным активам и управлению информационными рисками.
17. Обоснуйте позицию защищенности информационных активов с учетом информационных рисков в деятельности хозяйствующего субъекта.
18. Проведите сравнительный анализ нескольких наиболее известных методик оценки информационных рисков.
19. Какие показатели включены в основу методики оценки информационных рисков

предприятия?
20. Охарактеризуйте сущность методики и состав показателей типичной многофакторной модели оценки информационных рисков предприятия.
21. Охарактеризуйте сущность частной методики оценки надежности персонала в рамках общей методики многофакторной модели оценки информационных рисков предприятия.
22. Охарактеризуйте сущность частной методики оценки надежности технических и программно-аппаратных средств обработки информации.
23. Охарактеризуйте сущность частной методики организационно-режимных мер защиты с использованием программных комплексов анализа и управления рисками информационной системы «ГРИФ» и «КОНДОР».
24. Охарактеризуйте сущность экспертных методов по определению ценности защищаемых информационных активов.
25. Охарактеризуйте сущность методики оценки затрат на обеспечение информационной защищенности хозяйствующего субъекта.
26. Охарактеризуйте сущность эффективности оценки информационных рисков.

3.5 Перечень типовых простых практических заданий к зачету

(для оценки умений)

Задание 1. Построить модель угроз информационной безопасности (ИБ) предприятия / организации / подразделения.

Задание 2. Описать уязвимости информационной безопасности.

Задание 3. Построить модель нарушителя ИБ.

Задание 4. Опишите профиль и жизненный цикл для одной из следующих угроз:

1. Заражение компьютерным вирусом.
2. Атака на отказ в обслуживании.
3. Несанкционированный доступ к системе и хищение конфиденциальной информации.
4. Выход из строя файлового сервера.
5. Пожар в офисе.

Постарайтесь дать как широкое определение угрозе, включающее в себя большое количество различных сценариев инцидентов, так и более узкое определение, включающее в себя лишь один конкретный сценарий реализации угрозы.

Задание 5. Оцените вероятности угроз.

Задание 6. Постройте матрицу величины риска.

Задание 7. Откалибруйте шкалу оценки рисков.

Задание 8. Осуществите расчет риска информационной безопасности на основе модели угроз и уязвимостей.

3.6 Перечень типовых практических заданий к зачету

(для оценки навыков и (или) опыта деятельности)

Задание 1. Провести идентификацию активов предприятия/организации *(порядковый номер варианта выбрать в соответствии с номером учащегося в списке группы, либо выбрать организацию самостоятельно):*

1. Банк.
2. Супермаркет/магазин.
3. Научно-исследовательский институт.
4. Медицинское учреждение.
5. Торговая фирма.
6. Налоговая инспекция.
7. Агентство недвижимости.
8. Учебное заведение.
9. IT-компания.
10. Центр занятости населения.

Допускается осуществить идентификацию активов не всей организации (если она слишком велика), а один или несколько взаимодействующих между собой отделов/подразделений.

Задание 2. Осуществите расчет совокупной стоимости владения (TCO).

Задание 3. Рассчитайте затраты на контрмеры (прямые и косвенные).

Задание 4. Осуществите расчет возврата инвестиций (ROI).

Задание 5. Подготовьте отчет об оценке рисков.

Отчет об оценке рисков необходим для руководства и всех заинтересованных сторон, вовлеченных в процесс управления рисками. Другими словами, этот документ нужен для коммуникации рисков.

Краткая структура отчета об оценке рисков:

1. Введение
2. Основания, общие сведения
3. Цели и задачи
4. Методология и результаты
5. Идентификация активов и требований
6. Оценка активов и последствий
7. Анализ угроз и уязвимостей
8. Вычисление и оценивание рисков
9. Резюме рисков для руководства

9. Описание самых высоких рисков и причин их существования

10. Приложения
11. Реестры активов, требований и рисков

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

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
Дискуссия	Дискуссии проводятся во время практических занятий. Преподаватель на практическом занятии, предшествующем занятию проведения дискуссии, доводит до обучающихся тему дискуссии, количество заданий
Конспект	Защита конспектов, предусмотренных рабочей программой дисциплины, проводится во время практических занятий. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся: тему конспектов и требования, предъявляемые к их выполнению и защите

Для организации и проведения промежуточной аттестации 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 и типовые практические задания разного уровня сложности для проведения промежуточной аттестации 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. 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	Шкала оценивания
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»

Если оценка уровня сформированности компетенций обучающегося не соответствует критериям получения зачета без дополнительного аттестационного испытания, то промежуточная аттестация проводится в форме собеседования по перечню теоретических вопросов и типовых практических задач или в форме компьютерного тестирования.

Промежуточная аттестация в форме зачета с проведением аттестационного испытания проходит на последнем занятии по дисциплине.

При проведении промежуточной аттестации в форме компьютерного тестирования вариант тестового задания формируется из фонда тестовых заданий по дисциплине случайным

образом, но с условием: 50 % заданий должны быть заданиями открытого типа и 50 % заданий – закрытого типа.