МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

_____ Филиппович А.Ю.

"01" сентября 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Анализ рисков информационной безопасности»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль)
«Обеспечение информационной безопасности распределенных информационных систем»

Квалификация (степень) выпускника
Специалист

Форма обучения
Очная
Год приема - 2019

Москва 2019 г.

1. Цели освоения дисциплины

К **основным целям** освоения дисциплины «Анализ рисков информационной безопасности» следует отнести:

- приобретение студентами знаний, умений и навыков в области подготовки о проведения оценки рисков информационной безопасности автоматизированных систем.

К **основным задачам** освоения дисциплины «Анализ рисков информационной безопасности» следует отнести:

- изучение основных понятий технологии анализа рисков информационной безопасности;
- знакомство с нормативным обеспечением анализа рисков;
- умение оценивать активы, угрозы и безопасность информационных систем;
- ознакомление с современными методиками оценки рисков, принципами построения систем управления рисками информационной безопасности и прикладными средствами автоматизации процесса анализа рисков.

2. Место дисциплины в структуре ООП специалитета

Дисциплина «Анализ рисков информационной безопасности» относится к числу профессиональных учебных дисциплин вариативной части цикла (Б1.2) основной образовательной программы (дисциплины по выбору- Б.1.ДВ.3).

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Организационное и правовое обеспечение информационной безопасности» – сущность и понятие информации, информационной безопасности и характеристику ее составляющих, источники и классификацию угроз информационной безопасности, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации, основные меры по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические);

«Программно-аппаратные средства обеспечения информационной безопасности » – основные методы и программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, компьютерных сетях, автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности, источники и классификацию угроз информационной безопасности, основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации, классификацию защищаемой информации по видам тайны и степеням конфиденциальности, классификацию и оценку угроз информационной безопасности для объекта информатизации;

«Управление информационной безопасностью» - основные методы управления информационной безопасностью.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать	Перечень планируемых результатов обучения по дисциплине
ПК-5	способностью проводить анализ рисков информационной безопасности автоматизированной системы (далее – ИБ АС)	**знать:** основные понятия и принципы анализа и оценки рисков; **уметь:** классифицировать и оценивать угрозы информационной безопасности для автоматизированных систем; **владеть:** методами и средствами анализа и оценки рисков.
ПК-17	способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе (далее - АС) и выявлять каналы утечки информации	**знать:** особенности сертификации и аттестации автоматизированных систем по требованиям безопасности; **владеть:** методами и средствами выявления угроз безопасности автоматизированным системам;
ПК-22	способностью участвовать в формировании политики информационной безопасности (далее - ИБ) организации и контролировать эффективность ее реализации	**знать:** принципы функционирования автоматизированных систем; **уметь:** разрабатывать модели угроз и модели нарушителя безопасности автоматизированных систем;
ПК-27	способностью выполнять полный объем работ, связанных с реализацией частных политик ИБ АС, осуществлять мониторинг и аудит безопасности АС	**уметь:** классифицировать и оценивать угрозы информационной безопасности для автоматизированных систем; **владеть:** методами и средствами выявления угроз безопасности автоматизированным системам; методами и средствами анализа и оценки рисков.

ПСК-7.2	Способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	**владеть:** навыками анализа структурных и функциональных схем технологических процессов обработки информации в автоматизированных системах.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **4** зачетные единицы, т.е. **144** академических часов (лекции – 36 часов, лабораторные занятия – 36 часов, ,самостоятельная работа – 72 часа, форма контроля – экзамен) в 6 семестре.

Структура и содержание дисциплины по срокам и видам работы отражены в приложении.

Содержание разделов дисциплины

Тема 1. Анализ рисков в области информационной безопасности

Информационная безопасность бизнеса. Проблемы обоснования стоимости корпоративной системы защиты информации. Службы информационной безопасности. Основные функции специалистов, ответственных за информационную безопасность. Основные этапы работы по обеспечению режима информационной безопасности. Постановка задачи анализа рисков. Национальные особенности защиты информации.

Тема 2. Стандарты управления рисками

Национальные стандарты управления рисками информационной безопасности: ГОСТ Р ИСО/МЭК семейств 17799, 27000, 13335, 13569, 18044, 18045. Международные стандарты управления рисками: CobiT, ITIL, BSI, COSO, SAS70, NIST-800. Обзор основных стандартов. Ведомственные и корпоративные стандарты управления рисками информационной безопасности.

Тема 3. Технологии анализа рисков

Вопросы анализа рисков и управления ими. Идентификация рисков. Оценивание рисков. Качественные и количественные методики оценки рисков. Выбор допустимого уровня рисков. Выбор контрмер и оценка их эффективности. Разработка корпоративной методики анализа рисков.

Тема 4. Средства анализа рисков

Инструментарии базового уровня. Средства полного анализа рисков. Комплекс оценки рисков «ГРИФ». Методики и инструменты CORAS, CRAMM, Babel Enterprise, RiskWatch. Экспертная система «АванГард».

Тема 5. Управление информационными рисками

Основные элементы управления рисками информационных систем. Система управления информационными рисками.

5. Образовательные технологии

Методика преподавания дисциплины и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:
- подготовка к выполнению практических работ с использованием видеоуроков;
- проведение интерактивных лекционных и практических занятий в форме видеоуроков;
– подготовка, представление и обсуждение презентаций на практических занятиях;
– использование интерактивных форм проведения занятий;

Удельный вес занятий, проводимых в интерактивных формах, определен образовательной программой, особенностью контингента обучающихся и содержанием дисциплины и в целом по дисциплине составляет 25% (18 часов) аудиторных занятий. Занятия лекционного типа составляют 50% (36 часов) от объема аудиторных занятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:
- подготовка и выступление на практическом занятии с презентацией на тему: «Методы и средства анализа рисков ИБ» (индивидуально для каждого обучающегося) и с ее обсуждением;
- подготовка к выполнению практических работ
- экзамен;

Образцы контрольных вопросов и заданий для проведения текущего контроля,, экзаменационных билетов, приведены в приложении.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

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

В результате освоения дисциплины формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ПК-5	способность проводить анализ рисков информационной безопасности автоматизированной системы
ПК-17	способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации
ПК-22	способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации

ПК-27	способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы
ПСК-7.2	Способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин, практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины, описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

ПК-5 - способность проводить анализ рисков информационной безопасности автоматизированной системы				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: основные понятия и принципы анализа и оценки рисков.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: основные понятия и принципы анализа и оценки рисков.	Обучающийся демонстрирует неполное соответствие следующих знаний: основные понятия и принципы анализа и оценки рисков. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации	Обучающийся демонстрирует частичное соответствие следующих основные понятия и принципы анализа и оценки рисков, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях	Обучающийся демонстрирует полное соответствие знаний: основные понятия и принципы анализа и оценки рисков, свободно оперирует приобретенными знаниями

уметь: классифицировать и оценивать угрозы информационной безопасности для автоматизированных систем.	Обучающийся не умеет или в недостаточной степени умеет классифицировать и оценивать угрозы информационной безопасности для автоматизированных систем.	Обучающийся демонстрирует неполное соответствие следующих умений: классифицировать и оценивать угрозы информационной безопасности для автоматизированных систем. Допускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании умениями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих умений: классифицировать и оценивать угрозы информационной безопасности для автоматизированных систем. Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся демонстрирует полное соответствие следующих умений: классифицировать и оценивать угрозы информационной безопасности для автоматизированных систем. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности
владеть: методами и средствами анализа и оценки рисков.	Обучающийся не владеет или в недостаточной степени владеет методами и средствами анализа и оценки рисков	Обучающийся владеет в неполном объеме методами и средствами анализа и оценки рисков, допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей, Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях	Обучающийся частично владеет методами и средствами анализа и оценки рисков, навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет методами и средствами анализа и оценки рисков, свободно применяет полученные навыки в ситуациях повышенной сложности
ПК-17 - способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации				
знать: особенности сертификации и аттестации автоматизированных систем по требованиям безопасности.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: особенности сертификации и аттестации автоматизированных систем по требованиям безопасности.	Обучающийся демонстрирует неполное соответствие следующих знаний: особенности сертификации и аттестации автоматизированных систем по требованиям безопасности. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации	Обучающийся демонстрирует частичное соответствие следующих знаний: особенности сертификации и аттестации автоматизированных систем по требованиям безопасности, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях	Обучающийся демонстрирует полное соответствие следующих знаний: особенности сертификации и аттестации автоматизированных систем по требованиям безопасности, свободно оперирует приобретенными знаниями
владеть: методами и средствами выявления угроз безопасности автоматизированным системам.	Обучающийся не владеет или в недостаточной степени владеет методами и средствами выявления угроз безопасности автоматизированным системам.	Обучающийся владеет методами и средствами выявления угроз безопасности автоматизированным системам. допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей, Обучающийся испытывает значительные затруднения при применении навыков в новых	Обучающийся частично владеет методами и средствами выявления угроз безопасности автоматизированным системам, навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе	Обучающийся в полном объеме владеет методами и средствами выявления угроз безопасности автоматизированным системам, свободно применяет полученные навыки в ситуациях повышенной сложности

		ситуациях	умений на новые, нестандартные ситуации	
ПК-22 способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации				
знать: принципы функционирования автоматизированных систем.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: принципы функционирования автоматизированных систем.	Обучающийся демонстрирует неполное соответствие следующих знаний принципы функционирования автоматизированных систем. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации	Обучающийся демонстрирует частичное соответствие следующих знаний: принципы функционирования автоматизированных систем, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях	Обучающийся демонстрирует полное соответствие следующих знаний принципы функционирования автоматизированных систем, свободно оперирует приобретенными знаниями
уметь: разрабатывать модели угроз и модели нарушителя безопасности автоматизированных систем.	Обучающийся не умеет или в недостаточной степени умеет разрабатывать модели угроз и модели нарушителя безопасности автоматизированных систем.	Обучающийся демонстрирует неполное соответствие следующих умений: разрабатывать модели угроз и модели нарушителя безопасности автоматизированных систем. Допускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании умениями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих умений: разрабатывать модели угроз и модели нарушителя безопасности автоматизированных систем. Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации	Обучающийся демонстрирует полное соответствие следующих умений: разрабатывать модели угроз и модели нарушителя безопасности автоматизированных систем. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности
ПК-27 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы				
уметь: классифицировать и оценивать угрозы информационной безопасности для автоматизированных систем.	Обучающийся не умеет или в недостаточной степени умеет классифицировать и оценивать угрозы информационной безопасности для автоматизированных систем.	Обучающийся демонстрирует неполное соответствие следующих умений: классифицировать и оценивать угрозы информационной безопасности для автоматизированных систем. Допускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании умениями при их переносе на новые ситуации	Обучающийся демонстрирует частичное соответствие следующих умений: классифицировать и оценивать угрозы информационной безопасности для автоматизированных систем. Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации	Обучающийся демонстрирует полное соответствие следующих умений: осуществлять классифицировать и оценивать угрозы информационной безопасности для автоматизированных систем. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности

владеть: методами и средствами выявления угроз безопасности автоматизированным системам; методами и средствами анализа и оценки рисков.	Обучающийся не владеет или в недостаточной степени владеет методами и средствами выявления угроз безопасности автоматизированным системам; методами и средствами анализа и оценки рисков.	Обучающийся владеет методами и средствами выявления угроз безопасности автоматизированным системам; методами и средствами анализа и оценки рисков, допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей, Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях	Обучающийся частично владеет методами и средствами выявления угроз безопасности автоматизированным системам; методами и средствами анализа и оценки рисков, навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации	Обучающийся в полном объеме владеет методами и средствами выявления угроз безопасности автоматизированным системам; методами и средствами анализа и оценки рисков, свободно применяет полученные навыки в ситуациях повышенной сложности
ПСК-7.2 Способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах				
владеть: навыками анализа структурных и функциональных схем технологических процессов обработки информации в автоматизированных системах критически важных объектов.	Обучающийся не владеет или в недостаточной степени владеет навыками анализа структурных и функциональных схем технологических процессов обработки информации в автоматизированных системах критически важных объектов	Обучающийся владеет навыками анализа структурных и функциональных схем технологических процессов обработки информации в автоматизированных системах критически важных объектов, допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей, Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях.	Обучающийся частично владеет навыками анализа структурных и функциональных схем технологических процессов обработки информации в автоматизированных системах критически важных объектов, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет навыками анализа структурных и функциональных схем технологических процессов обработки информации в автоматизированных системах критически важных объектов, свободно применяет полученные навыки в ситуациях повышенной сложности.

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине, при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине проводится преподавателем, ведущим занятия по дисциплине методом экспертной оценки. По итогам промежуточной

аттестации по дисциплине выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно»,

К промежуточной аттестации допускаются только студенты, выполнившие все виды учебной работы, предусмотренные рабочей программой по дисциплине (которые прошли промежуточный контроль, выполнили практические работы, выступили с докладом по презентации).

Шкала оценивания	**Описание**
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент в основном демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены некоторые ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Удовлетворительно	Студент демонстрирует удовлетворительное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются умеренные ошибки, проявляется неполное наличие знаний, умений, навыков по ряду показателей, студент испытывает затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

Фонды оценочных средств представлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины.

а) основная литература:

1. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А., Симонов С.В. – М. : Компания АйТи ; ДМК Пресс, 2005.
2. Астахов А.М. Искусство управления информационными рисками –М.: ДМК Пресс, 2010.

3. Зегжда П.Д., Калинин М.О. Управление информационной безопасностью компьютерных систем. – СПб. : Изд-во Политехн. ун-та, 2012.
4. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности. - М. , 2011.
5. Калинин М. О. Теория и системы управления информационной безопасностью. Анализ рисков информационной безопасности : лаб. практикум / М. О. Калинин. – СПб. : Изд-во Политехн. ун-та, 2010.

б) дополнительная литература:

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации". Принят Государственной Думой 8 июля 2006 года.
2. ГОСТ Р ИСО/МЭК 13335-2007 "Информационная технология. Методы и средства обеспечения безопасности".
3. ГОСТ Р ИСО/МЭК 27001-2006. «Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования». .
4. ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности информационных технологий».
5. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».
6. ГОСТ Р ИСО/МЭК 13569-2007. «Финансовые услуги. Рекомендации по информационной безопасности».
7. ГОСТ Р ИСО/МЭК 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».
8. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая Линия – Телеком, 2004.
9. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: Учебн. пособие для вузов. М: Горячая линия – Телеком, 2006. – 544 с.

в) программное обеспечение и интернет-ресурсы:

1. Операционная система Windows 7 или более поздней версии или аналог.
2. Microsoft Office XP или более поздней версии или аналог.
3. Антивирусное ПО «Kaspersky Antivirus» 7.0 или более поздней версии или аналог.
4. Инструментальные средства анализа рисков.

8. Материально-техническое обеспечение дисциплины.

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, компьютер, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки специалистов **10.05.03** «**Информационная безопасность автоматизированных систем»**.

Программу составил:
доцент, к.т.н. Федоров Н.В

Программа утверждена на заседании кафедры «Информационная безопасность» «29» августа 2019 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

Приложение.

Структура и содержание дисциплины «Анализ рисков информационной безопасности» по направлению подготовки 10.05.03 «Информационная безопасность автоматизированных систем» (специалист)

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб	СРС	КСР	К.Р.	К.П.	ДЗ	Реферат	К/р	Э	З
	Восьмой семестр														
1	Информационная безопасность бизнеса. Проблемы обоснования стоимости корпоративной системы защиты информации. Службы информационной безопасности.			2	2		4								
2	Основные функции специалистов, ответственных за информационную безопасность. Основные этапы работы по обеспечению режима информационной безопасности. Постановка задачи анализа рисков. Национальные особенности защиты информации.			2	2		4								
3	Национальные стандарты управления рисками информационной безопасности: ГОСТ Р ИСО/МЭК семейств 17799, 27000, 13335, 13569, 18044, 18045..			2	2		6								
4	Международные стандарты управления рисками: CobiT, ITIL, BSI, COSO, SAS70, NIST-800. Обзор основных стандартов			2	2		4								
5	Ведомственные и корпоративные стандарты управления рисками информационной безопасности.			2	2		4								
6	Вопросы анализа рисков и управления ими.			2	2		4								
7	Идентификация рисков.			2	2		5				+				
8	Оценивание рисков.			3	3		5				+				
9	Качественные и количественные методики оценки рисков.			2	2		4				+				
10	Выбор допустимого уровня рисков			2	2		4				+				

11	. Выбор контрмер и оценка их эффективности.			3	3		4				+					
12	Разработка корпоративной методики анализа рисков.			2	2		4				+					
13	Инструментарии базового уровня. Средства полного анализа рисков.			2	2		4				+					
14	Комплекс оценки рисков «ГРИФ».			2	2		4				+					
15	Методики и инструменты CORAS, CRAMM, Babel Enterprise, RiskWatch.			2	2		4				+					
16	Экспертная система «АванГард».			2	2		4				+					
17	Основные элементы управления рисками информационных систем. Система управления информационными рисками.			2	2		4									
	Форма аттестации		19-21											Э		
	Всего часов по дисциплине в шестом семестре			36	36		72									
	Всего часов по дисциплине			36	36		72									

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»

ОП (профиль): ««Обеспечение информационной безопасности распределенных информационных систем

Форма обучения: очная

Вид профессиональной деятельности: научно-исследовательская; проектно-конструкторская; контрольно-аналитическая; организационно-управленческая; эксплуатационная.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Анализ рисков информационной безопасности»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Домашние задания
Экзамен

Составитель: к.т.н.,проф. Федоров Н.В.

Москва, 2019 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Анализ рисков информационной безопасности					
ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **профессиональные и профессионально-специализированные компетенции**					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетенций**	**Форма оценочного средства****	**Степени уровней освоения компетенций**
ИНДЕКС	**ФОРМУЛИРОВКА**				
ПК-5	способность проводить анализ рисков информационной безопасности автоматизированной системы (далее – ИБ АС)	**знать:** основные понятия и принципы анализа и оценки рисков; **уметь:** классифицировать и оценивать угрозы информационной безопасности для автоматизированных систем; **владеть:** методами и средствами анализа и оценки рисков.	лекция, самостоятельная работа, практические занятия	Домашние задания экзамен	**Базовый уровень** **знать:** основные понятия и принципы анализа и оценки рисков; **уметь:** классифицировать и оценивать угрозы информационной безопасности для автоматизированных систем; **владеть:** методами и средствами анализа и оценки рисков. -
ПК-17	способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе (далее - АС) и выявлять каналы утечки информации	**знать:** особенности сертификации и аттестации автоматизированных систем по требованиям безопасности; **владеть:** методами и средствами выявления угроз безопасности автоматизированным системам;	лекция, самостоятельная работа, практические занятия	Домашние задания экзамен	**Базовый уровень:** **знать:** особенности сертификации и аттестации автоматизированных систем по требованиям безопасности; **владеть:** методами и средствами выявления угроз безопасности автоматизированным системам -

ПК-22	способность участвовать в формировании политики информационной безопасности (далее - ИБ) организации и контролировать эффективность ее реализации	**знать:** принципы функционирования автоматизированных систем; **уметь:** разрабатывать модели угроз и модели нарушителя безопасности автоматизированных систем;	лекция, самостоятельная работа, практические занятия	Домашние задания экзамен	**Базовый уровень** **знать:** принципы функционирования автоматизированных систем **уметь:** - разрабатывать модели угроз и модели нарушителя безопасности автоматизированных систем;
ПК-27	способностью выполнять полный объем работ, связанных с реализацией частных политик ИБ АС, осуществлять мониторинг и аудит безопасности АС	**уметь:** классифицировать и оценивать угрозы информационной безопасности для автоматизированных систем; **владеть:** методами и средствами выявления угроз безопасности автоматизированным системам; методами и средствами анализа и оценки рисков.	лекция, самостоятельная работа, практические занятия	Домашние задания экзамен	**Базовый уровень** **уметь:** классифицировать и оценивать угрозы информационной безопасности для автоматизированных систем; **владеть:** методами и средствами выявления угроз безопасности автоматизированным системам
ПСК-7.2	Способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	**владеть:** навыками анализа структурных и функциональных схем технологических процессов обработки информации в автоматизированных системах критически важных объектов;	лекция, самостоятельная работа, практические занятия	Домашние задания экзамен	**владеть:** навыками анализа структурных и функциональных схем технологических процессов обработки информации в автоматизированных системах критически важных объектов;

Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы

Домашние задания.

1. Анализ рисков информационной безопасности с использованием модели информационных потоков.

2. Анализ рисков информационной безопасности с использованием модели угроз и уязвимостей.

3. Управление рисками информационной безопасности согласно ГОСТ Р ИСО/МЭК 17799. Составление правил политик безопасности.

4. Управление рисками информационной безопасности по ГОСТ Р ИСО/МЭК 17799. Анализ выполнения правил политик безопасности

5. Расчет рисков информационной безопасности по методике RiskWatch.

6. Методика анализа рисков информационной безопасности CORAS.

Оценочные средства для промежуточной аттестации

Экзамен

Список вопросов для экзамена по дисциплине

1. Информационная безопасность бизнеса.
2. Проблемы обоснования стоимости корпоративной системы защиты информации.
3. Службы информационной безопасности.
4. Основные функции специалистов, ответственных за информационную безопасность.
5. Основные этапы работы по обеспечению режима информационной безопасности.
6. Постановка задачи анализа рисков.
7. Национальные особенности защиты информации.
8. Национальные стандарты управления рисками информационной безопасности: ГОСТ Р ИСО/МЭК семейств 17799, 27000, 13335, 13569, 18044, 18045.
9. Международные стандарты управления рисками: CobiT, ITIL, BSI, COSO, SAS70, NIST-800.
10. Обзор основных стандартов.
11. Ведомственные и корпоративные стандарты управления рисками информационной безопасности.
12. Вопросы анализа рисков и управления ими.
13. Идентификация рисков.
14. Оценивание рисков.

15. Качественные и количественные методики оценки рисков.
16. Выбор допустимого уровня рисков.
17. Выбор контрмер и оценка их эффективности.
18. Разработка корпоративной методики анализа рисков.
19. Инструментарии базового уровня.
20. Средства полного анализа рисков.
21. Комплекс оценки рисков «ГРИФ».
22. Методики и инструменты CORAS
23. Методики и инструменты CRAMM,
24. Методики и инструменты Babel Enterprise
25. Методики и инструменты RiskWatch.
26. Экспертная система «АванГард».
27. Основные элементы управления рисками информационных систем.
28. Система управления информационными рисками.

Пример билета

1. Постановка задачи анализа рисков.
2. Методики и инструменты CRAMM