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

«Аудит 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 «Аудит информационной безопасности» следует отнести:

- изучение студентами видов, практических методов и средств проведения аудита информационной безопасности (ИБ).

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

- формирование понимания процессов проверки и оценки ИБ, принципов организации процессов аудита и анализа рисков ИБ и подготовки отчетных документов;
- ознакомление с основными стандартами в области аудита ИБ, практическими приемами проведения аудита, методами сбора данных, оценки рисков и анализа защищенности;
- обучение инструментальным средствам проведения аудита ИБ.

2. Место дисциплины в структуре ООП

Дисциплина «Аудит информационной безопасности» относится к числу профессиональных учебных дисциплин специализации части цикла (Б1) основной образовательной программы (Б.1.ДС.4).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы информационной безопасности», «Информационная безопасность автоматизированных систем»..

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

В результате освоения дисциплины (модуля) 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-22	Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	**знать:** • организационно-правовую документацию предприятий (устав, положение о предприятии), работающих в сфере защиты информации; • основные методы и технологию управления службой защиты информации. **уметь:**

		• применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. **владеть:** • навыками работы с нормативными правовыми актами; • методами формирования требований по защите информации.
ПК-24	Способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	**знать:** • основные стандарты, регламентирующие управление качеством информационной безопасности. **уметь:** • применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. **владеть:** • методами организации и управления деятельностью служб защиты информации на предприятии;
ПК-27	Способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	**знать:** • порядок проведения категорирования технических средств и систем и аттестации объектов информатизации (выделенных помещений) требованиям безопасности информации. **уметь:** • реализовывать системы защиты информации в соответствии со стандартами по оценке защищенных систем. **владеть:** • навыками определения наиболее вероятных угроз безопасности в отношении ресурсов ИС и уязвимостей защиты, делающих возможным осуществление этих угроз; • методами и средствами выявления угроз безопасности объекту информатизации.

ПСК-7.3	Способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем	**знать:** • теоретические основы построения и функционирования информационных систем аудита; • организацию аудита информационной безопасности информационной системы. **уметь:** • применять отечественные и зарубежные стандарты для проектирования, разработки и оценки защищенности объектов. **владеть:** • методами обработки результатов анализа данных аудита и содержащие оценку уровней защищенности объекта информатизации или соответствие ее требованиям стандартов; • методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часов (лекции – 36 час, лабораторные занятия – 36 час, самостоятельная работа - 72 часов, форма контроля – экзамен) в 8 семестре.

Структура и содержание дисциплины «Аудит информационной безопасности» по срокам и видам работы отражены в приложении.

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 у обучающихся:

- выполнение лабораторных работ в лабораториях вуза;
- индивидуальные и групповые консультации студентов преподавателем, в том числе в виде защиты выполненных заданий в рамках самостоятельной работы;
- посещение профильных конференций и работа на мастер-классах экспертов и специалистов индустрии;
- посещение лекций.

Самостоятельная внеаудиторная работа студентов составляет 50% от общего объема дисциплины и состоит из:

- подготовки к выполнению и подготовки к защите лабораторных работ;
- чтения литературы и освоения дополнительного материала в рамках тематики дисциплины;
- подготовки к текущей аттестации;
- подготовки к промежуточной аттестации.

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:

- экзамен.

Образцы вопросов к экзамену приведены в приложении.

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

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

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ПК-22	Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации
ПК-24	Способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности
ПК-27	Способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы
ПСК-7.3	Способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися

дисциплин (модулей), 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 (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю):

ПК-22 Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации

Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). 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, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.
уметь	Обучающийся не умеет или в недостаточной степени умеет выполнять действия, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3).	Обучающийся демонстрирует неполное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность умений, по ряду показателей,	Обучающийся демонстрирует частичное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Умения освоены, но допускаются незначительные ошибки, неточности,	Обучающийся демонстрирует полное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Свободно оперирует приобретенными умениями, применяет их в ситуациях

		обучающийся испытывает значительные затруднения при оперировании умениями при их переносе на новые ситуации.	затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	повышенной сложности.
владеть	Обучающийся не владеет или в недостаточной степени владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3).	Обучающийся в неполном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей. Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях.	Обучающийся частично владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Свободно применяет полученные навыки в ситуациях повышенной сложности.

ПК-24 Способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей,	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.

		обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	операциях.	
уметь	Обучающийся не умеет или в недостаточной степени умеет выполнять действия, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3).	Обучающийся демонстрирует неполное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). 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 умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся демонстрирует полное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
владеть	Обучающийся не владеет или в недостаточной степени владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3).	Обучающийся в неполном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей. Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях.	Обучающийся частично владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Свободно применяет полученные навыки 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				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). 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, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенными знаниями.
уметь	Обучающийся не умеет или в недостаточной степени умеет выполнять действия, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3).	Обучающийся демонстрирует неполное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). 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 умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся демонстрирует полное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.

владеть	Обучающийся не владеет или в недостаточной степени владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3).	Обучающийся в неполном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей. Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях.	Обучающийся частично владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Свободно применяет полученные навыки в ситуациях повышенной сложности.

ПСК-7.3 Способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Допускаются значительные	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Но допускаются незначительные	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3). Свободно оперирует

		ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	ошибки, неточности, затруднения при аналитических операциях.	приобретенными знаниями.
уметь	Обучающийся не умеет или в недостаточной степени умеет выполнять действия, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3).	Обучающийся демонстрирует неполное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). 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 умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся демонстрирует полное соответствие умений, указанных в индикаторах компетенций дисциплины «Уметь» (см. п. 3). Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
владеть	Обучающийся не владеет или в недостаточной степени владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3).	Обучающийся в неполном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей. Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях.	Обучающийся частично владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет приемами, методами и иными умениями, указанными в индикаторах компетенций дисциплины «Владеть» (см. п. 3). 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 (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

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 демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
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 средствпредставлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины

1. Основная литература:

- Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. – 3-е изд., стер. – Москва : Флинта, 2016. – 269 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93245 (дата обращения: 19.08.2019). – Библиогр. в кн. – ISBN 978-5-9765-1256-6. – Текст : электронный.
- Аудит информационной безопасности органов исполнительной власти : учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, М.В. Рудановский. – 4-е изд., стер. – Москва : Флинта, 2016. – 100 с. – (Организация и технология защиты информации). – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93259 (дата обращения: 19.08.2019). – Библиогр.: с. 83-84. – ISBN 978-5-9765-1277-1. – Текст : электронный.

2. Дополнительная литература:

- Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. – Ростов-на-Дону : Издательство Южного федерального университета, 2016. – 74 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=493175 (дата обращения: 19.08.2019). – Библиогр. в кн. – ISBN 978-5-9275-2364-1. – Текст : электронный.
- Галатенко, В.А. Основы информационной безопасности: Курс лекций : учебное пособие / В.А. Галатенко ; под ред. В.Б. Бетелина. – Изд. 3-е. – Москва : Интернет-Университет Информационных Технологий, 2006. – 208 с. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=233063 (дата обращения: 19.08.2019). – ISBN 5-9556-0052-3. – Текст : электронный.

8. Материально-техническое обеспечение дисциплины

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

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

Оборудование и аппаратура:

1. Операционная система Microsoft Windows.
2. Веб-браузер Chrome.

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, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

10. Методические рекомендации для преподавателя

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

Программу составил:

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 «Аудит 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
	8 семестр														
1	Понятие аудита безопасности. Методы анализа данных при аудите ИБ. Анализ информационных рисков предприятия. Методы оценивания информационных рисков.	8	1-2	4		4	8								
2	Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии Европейских стран. Германский стандарт BSI. Британский стандарт BS 7799. Международный стандарт ISO 17799. Международный стандарт ISO 15408 «Общие критерии». Стандарт COBIT. Стандарты по безопасности		3-4	4		4	8								

	информационных технологий в России.															
3	Основные понятия ОК. Методология оценки безопасности информационных технологий по ОК. Оценка уровня доверия функциональной безопасности информационной технологии. Обзор классов и семейств ОК.		5-6	4		4	8									
4	Анализ видов используемых программных продуктов. Система CRAMM. Система КОНДОР. Сетевые сканеры.		7-8	4		4	8									
5	Задачи и содержание работ при проведении аудита ИБ. Подготовка предприятия к проведению аудита ИБ. Планирование процедуры аудита ИБ. Организация и проведение работ по аудиту. Алгоритм проведения аудита безопасности предприятия. Перечень и систематизация данных, необходимых для проведения аудита ИБ. Выработка рекомендаций и подготовка отчетных документов. Экономическая оценка обеспечения ИБ.		9-10	4		4	8									
6	Информационная безопасность бизнеса. Развитие службы информацион2/6 ной безопасности. Международная практика защиты информации. Модель Symantec LifeCycle Security. Постановка		11-12	4		4	8									

	задачи анализа рисков. Модель Gartner Group. Модель Carnegie Mellon University. Различные взгляды на защиту информации. Национальные особенности защиты информации. Особенности отечественных нормативных документов. Учет остаточных рисков.															
7	Международный стандарт ISO 17799. Обзор стандарта BS 7799. Развитие стандарта BS 7799 (ISO 17799). Сравнение стандартов ISO 17799 и BSI. Стандарт США NIST 800-30. Алгоритм описания информационной системы. Идентификация угроз и уязвимостей. Организация защиты информации. Ведомственные и корпоративные стандарты управления ИБ. XBSS-спецификации сервисов безопасности X/Open. Стандарт NASA «Безопасность информационных технологий». Концепция управления рисками MITRE.		13-14	4		4	8									
8	Вопросы анализа рисков и управления ими. Идентификация рисков. Оценивание рисков. Измерение рисков. Выбор допустимого уровня риска. Выбор контрмер и оценка их		15-16	4		4	8									

	эффективности. Разработка корпоративной методики анализа рисков. Постановка задачи. Методы оценивания информационных рисков. Табличные методы оценки рисков. Методика анализа рисков Microsoft.														
9	Инструментарий базового уровня. Справочные и методические материалы. COBRA. RA Software Tool. Средства полного анализа рисков. Метод CRAMM. Пример использования метода CRAMM. Средства компании MethodWare. Экспертная система «АванГард». RiskWatch.		17-18	4		4	8								
	Форма аттестации	8	19-21							.				Э	
	Всего часов по дисциплине во восьмом семестре			36		36	72								
	Всего часов по дисциплине			36		36	72								

Приложение к
рабочей программе

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗРВАНИЯ

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: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая

.

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Аудит информационной безопасности»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

список вопросов к экзамену.

Составители:

Москва, 2019 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Аудит информационной безопасности					
ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетен**	**Форма оценоч-ного**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ПК-22	Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	**знать:** • организационно-правовую документацию предприятий (устав, положение о предприятии), работающих в сфере защиты информации; • основные методы и технологию управления службой защиты информации. **уметь:** • применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. **владеть:** • навыками работы с нормативными правовыми актами; • методами формирования требований по защите информации.	самостоятельная работа, лабораторные занятия, лекции	экзамен	**Базовый уровень:** **знать:** • основные методы и технологию управления службой защиты информации. **уметь:** • применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. **владеть:** • навыками работы с нормативными правовыми актами; **Повышенный уровень:** Знать организационно-правовую документацию предприятий (устав, положение о предприятии), работающих в сфере защиты информации; основные методы и технологию управления службой защиты информации. применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. навыками работы с нормативными правовыми актами; методами формирования требований по защите информации.

ПК-24	Способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	**знать:** • основные стандарты, регламентирующие управление качеством информационной безопасности. **уметь:** • применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. **владеть:** • методами организации и управления деятельностью служб защиты информации на предприятии.	самостоятельная работа, лабораторные занятия, лекции	экзамен	**Базовый уровень:** **знать:** • основные стандарты, регламентирующие управление качеством информационной безопасности. **уметь**: • применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. **владеть:** методами организации и управления деятельностью служб защиты информации на предприятии. **Повышенный уровень:** основные стандарты, регламентирующие управление качеством информационной безопасности. применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. методами организации и управления деятельностью служб защиты информации на предприятии.

ПК-27	Способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	**знать:** • порядок проведения категорирования технических средств и систем и аттестации объектов информатизации (выделенных помещений) требованиям безопасности информации. **уметь:** • реализовывать системы защиты информации в соответствии со стандартами по оценке защищенных систем. **владеть:** • навыками определения наиболее вероятных угроз безопасности в отношении ресурсов ИС и уязвимостей защиты, делающих возможным осуществление этих угроз; • методами и средствами выявления угроз безопасности объекту информатизации.	самостоятельная работа, лабораторные занятия, лекции	экзамен	**Базовый уровень:** **знать:** • порядок проведения категорирования технических средств и систем и аттестации объектов информатизации (выделенных помещений) требованиям безопасности информации. **уметь:** • реализовывать системы защиты информации в соответствии со стандартами по оценке защищенных систем. **владеть:** методами и средствами выявления угроз безопасности объекту информатизации. **Повышенный уровень**: порядок проведения категорирования технических средств и систем и аттестации объектов информатизации (выделенных помещений) требованиям безопасности информации. методами и средствами выявления угроз безопасности объекту информатизации. реализовывать системы защиты информации в соответствии со стандартами по оценке защищенных систем.

ПСК-7.3	Способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем	**знать:** • теоретические основы построения и функционирования информационных систем аудита; • организацию аудита информационной безопасности информационной системы. **уметь:** • применять отечественные и зарубежные стандарты для проектирования, разработки и оценки защищенности объектов. **владеть:** • методами обработки результатов анализа данных аудита и содержащие оценку уровней защищенности объекта информатизации или соответствие ее требованиям стандартов; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.	самостоятельная работа, лабораторные занятия, лекции	экзамен	**Базовый уровень:** **знать:** • теоретические основы построения и функционирования информационных систем аудита; **уметь:** • применять отечественные и зарубежные стандарты для проектирования, разработки и оценки защищенности объектов. **владеть:** • методами обработки результатов анализа данных аудита и содержащие оценку уровней защищенности объекта информатизации или соответствие ее требованиям стандартов; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов. **Повышенный уровень:** теоретические основы построения и функционирования информационных систем аудита; организацию аудита информационной безопасности информационной системы. применять отечественные и зарубежные стандарты для проектирования, разработки и оценки защищенности объектов. • методами обработки результатов анализа данных аудита и содержащие оценку уровней защищенности объекта информатизации или соответствие ее требованиям стандартов; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

Приложение 2
к рабочей программе

Оценочные средства для промежуточной аттестации

Список вопросов для экзамена по дисциплине

1. Понятие аудита безопасности.
2. Методы анализа данных при аудите ИБ.
3. Анализ информационных рисков предприятия.
4. Методы оценивания информационных рисков.
5. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга).
6. Гармонизированные критерии Европейских стран.
7. Германский стандарт BSI.
8. Британский стандарт BS 7799.
9. Международный стандарт ISO 17799.
10. Международный стандарт ISO 15408 «Общие критерии».
11. Стандарт COBIT.
12. Стандарты по безопасности информационных технологий в России.
13. Основные понятия ОК.
14. Методология оценки безопасности информационных технологий по ОК.
15. Оценка уровня доверия функциональной безопасности информационной технологии.
16. Обзор классов и семейств ОК.
17. Назначение стандарта ISO 17799 для управления информационной безопасностью.
18. Практика прохождения аудита и получения сертификата ISO 17799.
19. Анализ видов используемых программных продуктов.
20. Система CRAMM.
21. Система КОНДОР.
22. Сетевые сканеры.
23. Задачи и содержание работ при проведении аудита ИБ.
24. Подготовка предприятия к проведению аудита ИБ.
25. Планирование процедуры аудита ИБ.
26. Организация и проведение работ по аудиту.
27. Алгоритм проведения аудита безопасности предприятия.
28. Перечень и систематизация данных, необходимых для проведения аудита ИБ.
29. Выработка рекомендаций и подготовка отчетных документов.
30. Экономическая оценка обеспечения ИБ.