Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 01.11.2023 12:25:33
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / А.Ю. Филиппович /
«28» мая 2020 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 по защите информации

Форма обучения
Очная
Год приема - 2020

Москва 2020 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 базовой части цикла (Б.1) основной образовательной программы (Б.1.35).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Организационное и правовое обеспечение информационной безопасности», «Физические основы информационной безопасности», «Техническая защита информации», «Разработка технических текстов и документации», «Введение в аналитику информационной безопасности», «Аналитика информационной безопасности».

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-14	Способен 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-16	Способен 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-19	Способен 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.
ОПК-5.3.	Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	**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 (лабораторные занятия – 72 час, самостоятельная работа - 72 часов, форма контроля – экзамен) в 6 семестре.

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

5. Образовательные технологии

Методика преподавания дисциплины «Аудит информационной безопасности» 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:

- посещение лекций;
- выполнение лабораторных работ в лабораториях вуза;
- индивидуальные и групповые консультации студентов преподавателем, в том числе в виде защиты выполненных заданий в рамках самостоятельной работы.

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 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:

- выполнение лабораторных работ;
- экзамен.

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-14	Способен участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации
ПК-16	Способен обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности
ПК-19	Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы
ОПК-5.3.	Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах

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-14 Способен 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	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.

		затруднения при оперировании знаниями при их переносе на новые ситуации.		
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-16 Способен 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 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.

ПК-19 Способен 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.

ОПК-5.3. Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах				
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.

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 средств представлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины

1. **Основная литература:**
   - Петренко, В.И. Защита персональных данных в информационных системах : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». – Ставрополь : СКФУ, 2016. – 201 с. : схем. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=459205 (дата обращения: 18.08.2019). – Текст : электронный.
   - Новая парадигма защиты и управления персональными данными в Российской Федерации и зарубежных странах в условиях развития систем обработки данных в сети Интернет : монография / А.С. Дупан, А.К. Жарова, В.М. Елин и др. ; под ред. А.С. Дупан ; Высшая школа экономики, Национальный исследовательский университет. – Москва : Издательский дом Высшей школы экономики, 2016. – 343 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=486427 (дата обращения: 18.08.2019). – Библиогр. в кн. – ISBN 978-5-7598-1386-6 (в обл.). – Текст : электронный.

2. **Дополнительная литература:**
   - Аверченков, В.И. Защита персональных данных в организации : монография / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. – 3-е изд., стер. – Москва : Флинта, 2016. – 124 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=93260 (дата обращения: 18.08.2019). – Библиогр.: с. 107-109. – ISBN 978-5-9765-1273-3. – Текст : электронный.
   - Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 253 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 18.08.2019). – Библиогр. в кн. – ISBN 978-5-4475-3946-7. – DOI 10.23681/276557. – 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. Компьютер с операционной системой Microsoft Windows.

Программное обеспечение и интернет-ресурсы:

1. Веб-браузер Chrome.
2. Microsoft Office.

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: доц. Кесель С.А.

Программа утверждена на заседании кафедры “Информационная безопасность” «28» мая 2020 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
	6 семестр														
1	Классификация информации в соответствии с российским законодательством.	6	1-4			16	16								
2	Типовые угрозы безопасности автоматизированных систем (АС)		5-7			12	12								
3	Настройка и эксплуатация средств обеспечения безопасности АС.		8-11			16	16								
4	Средства и методы проектирования и построения защищенных АС.		12-13			8	8								
5	Средства выявления и нейтрализации попыток нарушения безопасности АС.		14-16			12	12								
6	Виды моделей угроз. Разработка и внедрение.		17			4	4								
7	Разработка организационно-распорядительной и нормативно-		18			4	4								

	технической документации для защищенных АС														
	Форма аттестации	6	19-21							.				Э	
	Всего часов по дисциплине во первом семестре					72	72								
	Всего часов по дисциплине					72	72								

Приложение к
рабочей программе

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
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 зачету

Составители: доц. Кесель С.А.

Москва, 2020 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-14	Способен 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-16	Способен 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-19	Способен 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.

ОПК-5.3.	Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	**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 зачета по дисциплине

1. Аудит ИБ. Концепция IA*4
2. Оценочные стандарты и спецификации ИБ. Состав, основные стандарты и спецификации.
3. В каком нормативном правовом акте закреплены все виды конфиденциальной информации?
4. Что такое персональные данные в соответствии с ФЗ-152?
5. Какую информацию запрещено относить к конфиденциальной в соответствии с законом РФ?
6. Раскройте понятие "конфиденциальный документ"
7. Перечислите 4 вида тайн относящихся к персональным данным. В случае если Вам известно больше видов тайн относящихся к ПД их следует перечислить.
8. В каком случае фотографию можно отнести к биометрическим персональным данным?
9. Может ли являться оператором персональных данных физическое лицо?
10. Какие действия можно производить с персональными данными?
11. Перечислите классификационные группы персональных данных по признаку свободы оборота.
12. Кто является основным ответственным за определение уровня классификации информации?
13. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
14. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
15. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
16. Основной документ, на основе которого проводится политика информационной безопасности?
17. Коммерческая тайна это….
18. Государственная тайна это…
19. Банковская тайна это….
20. Профессиональная тайна…
21. Как называется тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений?
22. Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем.
23. Стандарт «Общие Критерии». Концепция, основные понятия и определения.
24. Стандарт «Общие Критерии». Оценочные уровни доверия (ОУД)
25. СТО БР ИББС Структура, концепция, основные понятия и определения.
26. СТО БР ИББС Проведение аудита соответствия кредитно-финансовой организации требованиям СТО БР ИББС.
27. . PCI DSS Структура, концепция, основные понятия и определения.
28. PCI DSS Проведение аудита соответствия требованиям PCI DSS

29. 24. PCI DSS Проведение самооценки соответствия требованиям PCI DSS
30. PCI DSS Основные требования (12 требований)