Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 04.10.2023 14:33:42
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / Д.Г. Демидов /
«16» 02 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Аудит информационной безопасности»

Направление подготовки
10.03.01 Информационная безопасность

Профиль
Безопасность компьютерных систем

Квалификация
Бакалавр

Формы обучения
Очная

Москва, 2023 г.

Разработчик(и):

Доцент кафедры «Информационная безопасность»,
Доцент. к.т.н.  /С.А. Кесель/

Согласовано:
И.о. заведующего кафедрой «Информационная безопасность»,  /А.Ю. Гневшев/

Руководитель образовательной программы,  /А.Ю. Гневшев/

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине 4
2 Место дисциплины в структуре образовательной программы 5
3 Структура и содержание дисциплины 5
3.1 Виды учебной работы и трудоемкость 5
3.2 Тематический план изучения дисциплины 6
3.3 Содержание дисциплины 7
3.4 Тематика семинарских/практических занятий 8
3.5 Тематика курсовых проектов (курсовых работ) 8
4 Учебно-методическое и информационное обеспечение 9
4.1 Нормативные документы и ГОСТы 9
4.2 Основная литература 9
4.3 Дополнительная литература 10
4.4 Электронные образовательные ресурсы 10
4.5 Лицензионное и свободно распространяемое программное обеспечение 10
4.6 Современные профессиональные базы данных и информационные справочные материалы 10
5 Материально-техническое обеспечение 10
6 Методические рекомендации 11
6.1 Методические рекомендации для преподавателя по организации обучения 11
6.2 Методические указания для обучающихся по освоению дисциплины 11
7 Фонд оценочных средств 12
7.1 Методы контроля и оценивания результатов обучения 12
7.2 Шкала и критерии оценивания результатов обучения 12
7.3 Оценочные средства 17

1 Цели, задачи и планируемые результаты обучения по дисциплине

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.

Обучение по дисциплине «Аудит информационной безопасности» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.	ИОПК-10.1. Знает принципы формирования политики информационной безопасности в информационных системах; ИОПК-10.2. Умеет разрабатывать частные политики информационной безопасности информационных систем, определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, управлять процессом их реализации на объекте защиты. ИОПК-10.3. Владеет методами работы технического специалиста и поддержкой выполнения комплекса мер по обеспечению информационной безопасности, управлением процессом их реализации на объекте защиты
ПК-2. Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	ИПК-2.1. Знает организацию работы и нормативные правовые акты по аттестации объектов информатизации, методы аттестации уровня защищенности информационных систем; ИПК-2.2. Умеет участвовать в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации; ИПК-2.3. Владеет методиками проверки защищенности объектов информатизации на соответствие нормативных документов.
ПК-6. Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ИПК-6.1. Знает принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации); ИПК-6.2. Владеет методами организации и управления деятельность служб защиты информации на предприятии.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части (Б1.1), частью основной образовательной программы (Б1.1.30).

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Аналитика информационной безопасности», «Мониторинг событий и управление инцидентами (SIEM)».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы (144 часов)

3.1 Виды учебной работы и трудоемкость

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры
			6
1	**Аудиторные занятия**	**72**	**6**
	В том числе:		
1.1	Лекции	18	6
1.2	Семинарские/практические занятия		6
1.3	Лабораторные занятия	54	6
2	**Самостоятельная работа**	**72**	**6**
3	**Промежуточная аттестация**		**6**
	Экзамен		6
	Итого:	**144**	

3.2 Тематический план изучения дисциплины

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Раздел 1. Классификация информации в соответствии с российским законодательством.	**28**	4	-	8	-	16
2	Раздел 2. Типовые угрозы безопасности автоматизированных систем (АС)	**22**	2	-	8	-	12
3	Раздел 3. Настройка и эксплуатация средств обеспечения безопасности АС.	**32**	4	-	12	-	16
4	Раздел 4. Средства и методы проектирования и построения защищенных АС.	**18**	2	-	8	-	8
5	Раздел 5. Средства выявления и нейтрализации попыток нарушения безопасности АС.	**22**	2	-	8	-	12
6	Раздел 6. Виды моделей угроз. Разработка и внедрение.	**14**	2	-	8	-	4

7	Раздел 7. Разработка организационно-распорядительной и нормативно-технической документации для защищенных АС	**8**	2	-	2	-	4
Итого		**144**	**18**		**54**		**72**

3.3 Содержание дисциплины

Раздел 1. Классификация информации в соответствии с российским законодательством.

Предмет, содержание и задачи курса, его место среди других дисциплин учебного плана. Формы отчетности, основная и дополнительная литература. Информация и ее роль в современном обществе. Нормативно-правовая база для классификации информации, виды тайн и минимальный набор требований к обеспечению безопасности различных категорий информации.

Раздел 2. Типовые угрозы безопасности автоматизированных систем (АС)

Понятие угрозы и особенности типовых угроз для автоматизированных систем (АС). Автоматизированная система (АС) как объект защиты информации. Классификация и общий анализ угроз информационной безопасности в АС.

Раздел 3. Настройка и эксплуатация средств обеспечения безопасности АС.

Типовой состав средств обеспечения информационной безопасности АС. Рекомендуемые параметры настройки в зависимости от необходимого уровня обеспечения информационной безопасности. Эксплуатация и надежность средств обеспечения безопасности АС.

Раздел 4. Средства и методы проектирования и построения защищенных АС

Реализация угроз информационной безопасности путём несанкционированного доступа. Модель поведения потенциального нарушителя. Обобщённые модели систем защиты информации АС. Основные принципы обеспечения информационной безопасности АС.

Раздел 5. Средства выявления и нейтрализации попыток нарушения безопасности АС.

Системы обнаружения и предотвращения вторжений. Внедрение в периметр АС средств выявления и нейтрализации попыток нарушения безопасности АС. Аудит внедренных средств и мер.

Раздел 6. Виды моделей угроз. Разработка и внедрение.

Нормативно-правовая база для составления модели угроз информационной безопасности и модели нарушителя. Риск-ориентированный подход к оценке актуальных угроз безопасности АС. Содержание типовой модели угроз. Описание в модели угроз информационной безопасности недопустимых событий.

Раздел 7. Разработка организационно-распорядительной и нормативно-технической документации для защищенных АС.

Разработка сопроводительной документации к защищенной АС. Нормативно-правовая база защиты АС, классификация АС по уровням (классам) защищенности. Согласование мер и требований различных нормативно-правовых актов в рамках организационно-распорядительной и нормативно-технической документации предприятия.

3.4 Тематика семинарских/практических занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены учебным планом.

3.4.2 Лабораторные работы

Раздел 1. Классификация информации в соответствии с российским законодательством.

Лабораторная работа №1.1. Виды конфиденциальной информации.

Лабораторная работа №1.2. Основные требования к защите информации определенного вида.

Раздел 2. Типовые угрозы безопасности автоматизированных систем (АС).

Лабораторная работа №2.1. Классификация и общий анализ угроз, актуальных для АС.

Лабораторная работа №2.2. Типовая система защиты АС.

Раздел 3. Настройка и эксплуатация средств обеспечения безопасности АС.

Лабораторная работа №3.1. Настройка и эксплуатация системы комплексного анализа защищенности.

Лабораторная работа №3.2. Настройка и эксплуатация системы анализа защищенности сетей.

Раздел 4. Средства и методы проектирования и построения защищенных АС.

Лабораторная работа №4.1. Этапы проектирования защищенных АС.

Лабораторная работа №4.2. Построение модели защищенной АС.

Раздел 5. Средства выявления и нейтрализации попыток нарушения безопасности АС.

Лабораторная работа №5.1. Выявление инцидентов ИБ АС.

Лабораторная работа №5.2. Предотвращение и противодействие нарушениям ИБ АС.

Раздел 6. Виды моделей угроз. Разработка и внедрение.

Лабораторная работа №6.1. Разработка типовой модели угроз.

Лабораторная работа №6.2. Согласования модели угроз с организационно-распорядительной документацией предприятия.

Раздел 7. Разработка организационно-распорядительной и нормативно-технической документации для защищенных АС.

Лабораторная работа №7. Разработка комплекта организационно-распорядительной документации, необходимой для проведения аудита ИБ АС.

3.5 Тематика курсовых проектов (курсовых работ)

Курсовое проектирование по дисциплине «Аудит информационной безопасности» не предусмотрено учебным планом.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. Федеральный закон от 27.07.2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», текст: электронный, – URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264, режим доступа: свободный.

2. Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных», текст: электронный, – URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108261, режим доступа: свободный.

3. ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Национальный стандарт РФ: введен 01.01.2022: - М.: Стандартинформ, 2021.- URL: https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=10&month=12&year=2021&search=&id=242006. - Текст: электронный.

4. ГОСТ Р ИСО/МЭК 27004-2021 Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание. Национальный стандарт РФ: введен 30.11.2021: - М.: Стандартинформ, 2021.- URL: https://protect.gost.ru/document1.aspx?control=31&baseC=6&page=521&month=6&year=2008&search=&id=240761. - Текст: электронный.

5. ГОСТ Р ИСО/МЭК 27006-2020 Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Национальный стандарт РФ: введен 01.07.2021: - М.: Стандартинформ, 2020. URL: https://protect.gost.ru/document.aspx?control=7&id=238756. – Текст: электронный.

6. ГОСТ Р ИСО/МЭК 27007-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности. Национальный стандарт РФ: введен 01.06.2015: - М.: Стандартинформ, 2019. URL: https://protect.gost.ru/document.aspx?control=7&id=187871. – Текст: электронный.

4.2 Основная литература

1. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 324 с. — ISBN 978-5-507-48149-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/341267

2. Рагозин, Ю. Н. Организация и управление подразделением защиты информации на предприятии : учебное пособие / Ю. Н. Рагозин, В. А. Мельник. — Санкт-Петербург : Интермедия, 2019. — 240 с. — ISBN 978-5-4383-0180-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161357

3. Арзуманян, А. Б. Международные стандарты правовой защиты информации и информационных технологий : учебное пособие / А. Б. Арзуманян. — Ростов-на-Дону : ЮФУ, 2020. — 140 с. — ISBN 978-5-9275-3546-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/170355. — Режим доступа: для авториз. пользователей.

4.3 Дополнительная литература

1. Капгер, И. В. Управление информационной безопасностью : учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь : ПНИПУ, 2023. — 91 с. — ISBN 978-5-398-02866-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/328889. — Режим доступа: для авториз. пользователей.

2. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184. — Режим доступа: для авториз. пользователей.

4.4 Электронные образовательные ресурсы

ЭОР Разрабатывается.

4.5 Лицензионное и свободно распространяемое программное обеспечение

В рамках освоения дисциплины, дополнительное программное обеспечение не предусмотрено.

4.6 Современные профессиональные базы данных и информационные справочные материалы

В рамках освоения дисциплины, использование профессиональных баз данных и информационных справочных материалов не предусмотрено.

5 Материально-техническое обеспечение

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, допускается использование студентом собственной вычислительной техники (ноутбук).

С целью повышения качества ведения образовательной деятельности в университете создана электронная информационно-образовательная среда. Она подразумевает организацию взаимодействия между обучающимися и преподавателями через систему личных кабинетов студентов, расположенных на официальном сайте университета в информационно телекоммуникационной сети «Интернет». Созданная информационно-образовательная среда позволяет осуществлять взаимодействие между участниками образовательного процесса посредством организации дистанционного консультирования по вопросам выполнения практических заданий. В процессе самостоятельной работы студентов предусмотрена возможность получения индивидуальных консультаций преподавателя с использованием электронной почты в сети Интернет.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

3. При организации и проведения экзаменов в практико-ориентированной форме следует использовать утвержденные кафедрой Методические рекомендации.

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки **10.03.01 «Информационная безопасность».**

6.2 Методические указания для обучающихся по освоению дисциплины

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

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.

Самостоятельная работа включает изучение теоретических и практических разделов дисциплины.

Общие рекомендации по организации самостоятельной работы:

Время, которым располагает студент для выполнения учебного плана, складывается из двух составляющих: одна из них – это аудиторная работа в вузе по расписанию занятий, другая –внеаудиторная самостоятельная работа. Задания и материалы для самостоятельной работы выдаются во время учебных занятий по расписанию, на этих же занятиях преподаватель осуществляет контроль за самостоятельной работой, а также оказывает помощь студентам по правильной организации работы.

Чтобы выполнить весь объем самостоятельной работы, необходимо заниматься по 1 – 4 часа ежедневно. Начинать самостоятельные внеаудиторные занятия следует с первых же дней семестра. Первые дни семестра очень важны для того, чтобы включиться в работу, установить определенный порядок, равномерный ритм на весь семестр. Ритм в работе –это ежедневные самостоятельные занятия, желательно в одни и те же часы, при целесообразном чередовании занятий с перерывами для отдыха.

Начиная работу, не нужно стремиться делать вначале самую тяжелую ее часть, надо выбрать что-нибудь среднее по трудности, затем перейти к более трудной работе. И напоследок оставить легкую часть, требующую не столько больших интеллектуальных усилий, сколько определенных моторных действий (черчение, построение графиков и т.п.).

Следует правильно организовать свои занятия по времени: 50 минут –работа, 5-10 минут –перерыв; после 3 часов работы перерыв –20-25 минут. Иначе нарастающее утомление повлечет неустойчивость внимания. Очень существенным фактором, влияющим на

повышение умственной работоспособности, являются систематические занятия физической культурой. Организация активного отдыха предусматривает чередование умственной и физической деятельности, что полностью восстанавливает работоспособность.

Методические указания к отдельным видам деятельности:

Лекция: Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, формулировки, выводы. Помечать важные мысли. Выделять ключевые слова, термины. Делать пометки на вопросах, терминах, блоках в тексте, которые вызвали затруднения, после чего постараться найти ответ в рекомендуемой литературе. Если ответ не найден, то на консультации обратиться к преподавателю.

Лабораторная работа: Работа с конспектом лекций и методическими указаниями по выполнению лабораторной работы, просмотр рекомендуемой литературы, конспектирование основных мыслей и выводов, разработка плана выполнения лабораторной работы, предварительная формулировка возможных выводов по работе. Подготовка к практическим занятиям, проработка материала по вопросам, выносимым на практические занятия. Для более углублённого изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темой.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- экзамен.

7.2 Шкала и критерии оценивания результатов обучения

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

ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: принципы формирования политики информационной безопасности в информационных системах.	Обучающийся не знает или в недостаточной степени знает принципы формирования политики информационной безопасности в информационных системах.	Обучающийся демонстрирует частичное знание принципов формирования политики информационной безопасности в информационных системах.	Обучающийся демонстрирует полное знание принципов формирования политики информационной безопасности в информационных системах.	Обучающийся демонстрирует полное знание принципов формирования политики информационной безопасности в информационных системах.

		. Допускаются значительные ошибки	. Допускаются незначительные ошибки, неточности	. Допускаются незначительные неточности
уметь: разрабатывать частные политики информационной безопасности информационных систем, определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, управлять процессом их реализации на объекте защиты.	Обучающийся не умеет или в недостаточной степени умеет разрабатывать частные политики информационной безопасности информационных систем, определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, управлять процессом их реализации на объекте защиты.	Обучающийся демонстрирует частичное умение разрабатывать частные политики информационной безопасности информационных систем, определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, управлять процессом их реализации на объекте защиты. . Допускаются значительные ошибки	Обучающийся демонстрирует полное умение разрабатывать частные политики информационной безопасности информационных систем, определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, управлять процессом их реализации на объекте защиты. . Допускаются незначительные ошибки, неточности	Обучающийся демонстрирует полное умение разрабатывать частные политики информационной безопасности информационных систем, определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, управлять процессом их реализации на объекте защиты. . Допускаются незначительные неточности
владеть: методами работы технического специалиста и поддержкой выполнения комплекса мер по	Обучающийся не владеет или в недостаточной степени владеет методами работы технического	Обучающийся демонстрирует частичное владение методами работы технического специалиста и	Обучающийся демонстрирует полное владение методами работы технического	Обучающийся демонстрирует полное владение методами работы технического

обеспечению информационной безопасности, управлением процессом их реализации на объекте защиты.	специалиста и поддержкой выполнения комплекса мер по обеспечению информационной безопасности, управлением процессом их реализации на объекте защиты.	поддержкой выполнения комплекса мер по обеспечению информационной безопасности, управлением процессом их реализации на объекте защиты. . Допускаются значительные ошибки	специалиста и поддержкой выполнения комплекса мер по обеспечению информационной безопасности, управлением процессом их реализации на объекте защиты. . Допускаются незначительные ошибки, неточности	специалиста и поддержкой выполнения комплекса мер по обеспечению информационной безопасности, управлением процессом их реализации на объекте защиты. . Допускаются незначительные неточности
ПК-2. Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации				
знать: организацию работы и нормативные правовые акты по аттестации объектов информатизации, методы аттестации уровня защищенности информационных систем.	Обучающийся не знает или в недостаточной степени знает организацию работы и нормативные правовые акты по аттестации объектов информатизации, методы аттестации уровня защищенности информационных систем.	Обучающийся демонстрирует частичное знание организации работы и нормативных правовых актов по аттестации объектов информатизации, методов аттестации уровня защищенности информационных систем. . Допускаются значительные ошибки	Обучающийся демонстрирует полное знание организации работы и нормативных правовых актов по аттестации объектов информатизации, методов аттестации уровня защищенности информационных систем. . Допускаются незначительные ошибки, неточности	Обучающийся демонстрирует полное знание организации работы и нормативных правовых актов по аттестации объектов информатизации, методов аттестации уровня защищенности информационных систем. . Допускаются незначительные неточности
уметь: участвовать в организации и сопровождении аттестации объекта информатизации по	Обучающийся не умеет или в недостаточной степени умеет участвовать в организации и	Обучающийся демонстрирует частичное умение участвовать в организации и сопровождении	Обучающийся демонстрирует полное умение участвовать в организации и сопровождении	Обучающийся демонстрирует полное умение участвовать в организации и сопровождени

требованиям безопасности информации.	сопровождении аттестации объекта информатизации по требованиям безопасности информации.	аттестации объекта информатизации по требованиям безопасности информации. . Допускаются значительные ошибки	аттестации объекта информатизации по требованиям безопасности информации. . Допускаются незначительные ошибки, неточности	и аттестации объекта информатизации по требованиям безопасности информации. . Допускаются незначительные неточности
владеть: методиками проверки защищенности объектов информатизации на соответствие нормативных документов.	Обучающийся не владеет или в недостаточной степени владеет методиками проверки защищенности объектов информатизации на соответствие нормативных документов.	Обучающийся демонстрирует частичное владение методиками проверки защищенности объектов информатизации на соответствие нормативных документов. . Допускаются значительные ошибки	Обучающийся демонстрирует полное владение методиками проверки защищенности объектов информатизации на соответствие нормативных документов. . Допускаются незначительные ошибки, неточности	Обучающийся демонстрирует полное владение методиками проверки защищенности объектов информатизации на соответствие нормативных документов. . Допускаются незначительные неточности
ПК-6. Способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.				
знать: принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации).	Обучающийся не знает или в недостаточной степени знает принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации).	Обучающийся демонстрирует частичное знание принципов формирования комплекса мер по обеспечению информационной безопасности предприятия (организации). . Допускаются значительные ошибки	Обучающийся демонстрирует полное знание принципов формирования комплекса мер по обеспечению информационной безопасности предприятия (организации). . Допускаются незначительные	Обучающийся демонстрирует полное знание принципов формирования комплекса мер по обеспечению информационной безопасности предприятия (организации). .

			ошибки, неточности	Допускаются незначительные неточности
владеть: методами организации и управления деятельность служб защиты информации на предприятии.	Обучающийся не владеет или в недостаточной степени владеет методами организации и управления деятельность служб защиты информации на предприятии.	Обучающийся демонстрирует частичное владение методами организации и управления деятельность служб защиты информации на предприятии. . Допускаются значительные ошибки	Обучающийся демонстрирует полное владение методами организации и управления деятельность служб защиты информации на предприятии. . Допускаются незначительные ошибки, неточности	Обучающийся демонстрирует полное владение методами организации и управления деятельность служб защиты информации на предприятии. . Допускаются незначительные неточности

Форма промежуточной аттестации: экзамен.

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.

7.3 Оценочные средства

7.3.1 Текущий контроль

Текущий контроль успеваемости студентов осуществляется в процессе проведения лабораторных работ.

7.3.2 Промежуточная аттестация

Оценочные средства для промежуточной аттестации

Экзамен

Список вопросов для экзамена

1. Аудит ИБ. Концепция IA*4
2. Оценочные стандарты и спецификации ИБ.
3. Состав, основные стандарты и спецификации.
4. В каком нормативном правовом акте закреплены все виды конфиденциальной информации?
5. Что такое персональные данные в соответствии с ФЗ-152?
6. Какую информацию запрещено относить к конфиденциальной в соответствии с законом РФ?
7. Раскройте понятие "конфиденциальный документ"
8. Перечислите 4 вида тайн относящихся к персональным данным. В случае если Вам известно больше видов тайн относящихся к ПД их следует перечислить.
9. В каком случае фотографию можно отнести к биометрическим персональным данным?
10. Может ли являться оператором персональных данных физическое лицо?
11. Какие действия можно производить с персональными данными?
12. Перечислите классификационные группы персональных данных по признаку свободы оборота.
13. Кто является основным ответственным за определение уровня классификации информации?
14. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
15. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
16. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
17. Основной документ, на основе которого проводится политика информационной безопасности?
18. Коммерческая тайна это….
19. Государственная тайна это…
20. Банковская тайна это….

21. Профессиональная тайна…
22. Как называется тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений?
23. Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем.
24. Стандарт «Общие Критерии». Концепция, основные понятия и определения.
25. Стандарт «Общие Критерии». Оценочные уровни доверия (ОУД)
26. СТО БР ИББС Структура, концепция, основные понятия и определения.
27. СТО БР ИББС Проведение аудита соответствия кредитно-финансовой организации требованиям СТО БР ИББС.
28. PCI DSS Структура, концепция, основные понятия и определения.
29. PCI DSS Проведение аудита соответствия требованиям PCI DSS
30. PCI DSS Проведение самооценки соответствия требованиям PCI DSS
31. PCI DSS Основные требования (12 требований)

Пример билета.

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

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1
по дисциплине

«АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки
10.03.01 Информационная безопасность

ВОПРОСЫ:

1. Коммерческая тайна это...
2. Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем.
3. Кто является основным ответственным за определение уровня классификации информации?

Утверждено: _____ / _____ / «__» _____ 20__г.