МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ

Декан факультета
информационных технологий
/Д. Г. Демидов/

"28" апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Аудит систем управления информационной безопасностью»

Направление подготовки
10.04.01 Информационная безопасность

Профиль
Системы управления информационной безопасностью

Квалификация
Магистр

Формы обучения
Очная

Москва, 2022 г.

Разработчик(и):

Доцент кафедры «Информационная безопасность»,
к.т.н., доцент  / И.В. Калуцкий/

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

Руководитель образовательной программы
Доцент. к.т.н.  /С.А. Кесель/

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

Основной **целью** дисциплины «Аудит систем управления информационной безопасностью» является формирование у студентов знаний в области организации аудита информационной безопасности для решения задач профессиональной деятельности организационно-управленческого типа.

К **основным задачам** дисциплины «Аудит систем управления информационной безопасности» относится:

- изучение руководящих и методических документов уполномоченных федеральных органов исполнительной власти по защите информации и обеспечения безопасности критической информационной инфраструктуры;
- анализ характера обрабатываемой информации и определение перечня информации, подлежащей защите;
- выявление степени участия персонала в обработке защищаемой информации.

Обучение по дисциплине «Аудит систем управления информационной безопасностью» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	ИУК-1.1. Анализирует проблемную ситуацию как систему, осуществляет её декомпозицию и определяет связи между ее составляющими. ИУК-1.2. Определяет противоречивость и пробелы в информации, необходимой для решения проблемной ситуации, а также критически оценивает релевантность используемых информационных источников. ИУК-1.3. Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарного подходов с учетом оценки существующих рисков и возможностей их минимизации.
ПК-9. Способен проводить аудит информационной безопасности информационных систем и объектов информатизации	ИПК-9.1. Знает: каналы утечки информации. ИПК-9.2. Умеет проводить инструментальный аудит информационной безопасности информационных систем и объектов информатизации. ИПК-9.3. Владеет: методами мониторинга и аудита, выявления угроз информационно безопасности информационных систем и объектов информатизации.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к части, формируемой участниками образовательных отношений (Б1.2), частью основной образовательной программы (Б1.2.3).

Дисциплина является базовой по своим компетенциям.

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
			2
1	**Аудиторные занятия**	**72**	**2**
	В том числе:		
1.1	Лекции	18	2
1.2	Семинарские/практические занятия		2
1.3	Лабораторные занятия	54	2
2	**Самостоятельная работа**	**72**	**2**
3	**Промежуточная аттестация**		**2**
	Экзамен		2
	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. Служба информационной безопасности предприятия.	**48**	6	-	24	-	24
1.1	Тема 1. Организационные основы и принципы деятельности службы информационной безопасности.	**16**	2	-	8	-	8
1.2	Тема 2. Структура и функции службы информационной безопасности.	**16**	2	-	8	-	8
1.3	Тема 3. Цели и задачи службы информационной безопасности.	**18**	2	-	8	-	8
2	Раздел 2. Лицензирование видов деятельности.	**46**	4	-	14	-	24
3	Раздел 3. Управление службой информационной безопасности предприятия.	**50**	8	-	16	-	24

3.1	Тема 1. Организация информационно-аналитической работы.	**24**	4	-	8	-	12
3.2	Тема 2. Организация работы с персоналом предприятия.	**26**	4	-	8	-	12
Итого		**144**	**18**		**54**		**72**

3.3 Содержание дисциплины

Раздел 1. Служба информационной безопасности предприятия.

Тема 1. Организационные основы и принципы деятельности службы информационной безопасности.

Нормативно-правовые нормы организации деятельности службы информационной безопасности предприятия. Организационные основы деятельности службы информационной безопасности.

Тема 2. Структура и функции службы информационной безопасности.

Структура подразделения службы информационной в предприятии. Взаимодействие службы информационной безопасности с другими структурными подразделениями предприятия. Функции службы информационной безопасности.

Тема 3. Цели и задачи службы информационной безопасности.

Цели службы информационной в предприятии при осуществлении профильной деятельности. Задачи службы информационной безопасности предприятия в рамках осуществления профессиональной деятельности. Отчетность службы информационной безопасности руководителю предприятия.

Раздел 2. Лицензирование видов деятельности.

Нормативно-правовая база при взаимодействии с федеральными органами исполнительной власти в рамках лицензирования отдельных видов деятельности структурного подразделения обеспечивающего информационную безопасность предприятия. Проведение лицензированных работ (оказание лицензированных услуг) службой информационной безопасности предприятия в рамках подряда или договора об оказании услуг.

Раздел 3. Управление службой информационной безопасности предприятия.

Тема 1. Организация информационно-аналитической работы.

Сбор и анализ сведений о деятельности службы информационной безопасности предприятия. Составление отчетов о проделанной службой работе. Предоставление рекомендаций руководству предприятия на основании полученных и проанализированных сведений.

Тема 2. Организация работы с персоналом предприятия.

Повышение осведомленности персонала предприятия посредством оповещений, проведения обучения или прохождения персоналом курсов повышения квалификации. Реагирование на инциденты информационной безопасности, связанные с персоналом.

3.4 Тематика семинарских/практических занятий

3.4.1 Семинарские/практические занятия

Не предусмотрены учебным планом.

3.4.2 Лабораторные работы

Раздел 1. Служба информационной безопасности предприятия.

Тема 1. Организационные основы и принципы деятельности службы информационной безопасности.

Лабораторная работа 1.1. Организационные основы службы информационной безопасности.

Лабораторная работа 1.2. Принципы деятельности службы информационной безопасности.

Тема 2. Структура и функции службы информационной безопасности.

Лабораторная работа 2.1. Структура службы информационной безопасности.

Лабораторная работа 2.2. Функции службы информационной безопасности.

Тема 3. Цели и задачи службы информационной безопасности.

Лабораторная работа 3.1. Цели службы информационной безопасности.

Лабораторная работа 3.2. Задачи службы информационной безопасности.

Раздел 2. Лицензирование видов деятельности.

Лабораторная работа 4. Лицензирование отдельных видов деятельности.

Раздел 3. Управление службой информационной безопасности предприятия.

Тема 1. Организация информационно-аналитической работы.

Лабораторная работа 5.1. Организация информационно-аналитической работы.

Лабораторная работа 5.2. Организация информационно-аналитической работы.

Тема 2. Организация работы с персоналом предприятия.

Лабораторная работа 6.1. Организация работы с персоналом предприятия.

Лабораторная работа 6.2. Организация работы с персоналом предприятия.

3.5 Тематика курсовых проектов (курсовых работ)

Список примерных тем курсовых проектов (курсовых работ):

1. Методика проведения внутреннего аудита информационной безопасности на примере реального предприятия.
2. Отечественные инструменты для проведения внутреннего аудита информационной безопасности.
3. Общий список рекомендаций при проведении аудита информационной безопасности.
4. Особенности внутреннего аудита информационной безопасности в кредитно-финансовой сфере.
5. Особенности внутреннего аудита информационной безопасности в сфере здравоохранения.
6. Особенности внутреннего аудита информационной безопасности в транспортной сфере.
7. Особенности внутреннего аудита информационной безопасности в сфере связи.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. Федеральный закон от 04.05.2011 г. №99-ФЗ «О лицензировании отдельных видов деятельности», текст: электронный, – URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102147413, режим доступа: свободный.

2. 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.

3. 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.

4. 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.

5. 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 обучения по дисциплине, дополнительное программное обеспечение не предусмотрено.

4.6 Современные профессиональные базы данных и информационные справочные материалы

1. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/
2. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/

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 **10.04.01 «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;
- подготовку и оформление курсового проекта.

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;
- самостоятельная подготовка и выполнение курсового проекта;
- 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.

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
Анализирует проблемную ситуацию как систему, осуществляет её декомпозицию и определяет связи между ее составляющими.	Обучающийся не умеет или в недостаточной степени умеет анализировать проблемную ситуацию как систему, осуществлять её декомпозици	Обучающийся демонстрирует частичное умение анализировать проблемную ситуацию как систему, осуществлять её декомпозицию и определять связи	Обучающийся демонстрирует полное умение анализировать проблемную ситуацию как систему, осуществлять её декомпозицию и определять связи между ее	Обучающийся демонстрирует полное умение анализировать проблемную ситуацию как систему, осуществлять её

	ю и определять связи между ее составляющими.	между ее составляющими. . Допускаются значительные ошибки	составляющими.. Допускаются незначительные ошибки, неточности	декомпозицию и определять связи между ее составляющими. . Допускаются незначительные неточности
Определяет противоречивость и пробелы в информации, необходимой для решения проблемной ситуации, а также критически оценивает релевантность используемых информационных источников.	Обучающийся не умеет или в недостаточной степени умеет определять противоречивость и пробелы в информации, необходимой для решения проблемной ситуации, а также критически оценивать релевантность используемых информационных источников.	Обучающийся демонстрирует частичное умение определять противоречивость и пробелы в информации, необходимой для решения проблемной ситуации, а также критически оценивать релевантность используемых информационных источников. . Допускаются значительные ошибки	Обучающийся демонстрирует полное умение определять противоречивость и пробелы в информации, необходимой для решения проблемной ситуации, а также критически оценивать релевантность используемых информационных источников. . Допускаются незначительные ошибки, неточности	Обучающийся демонстрирует полное умение определять противоречивость и пробелы в информации, необходимой для решения проблемной ситуации, а также критически оценивать релевантность используемых информационных источников. . Допускаются незначительные неточности

Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарного подходов с учетом оценки существующих рисков и возможностей их минимизации.	Обучающийся не умеет или в недостаточной степени умеет разрабатывать и содержательно аргументировать стратегию решения проблемной ситуации на основе системного и междисциплинарного подходов с учетом оценки существующих рисков и возможностей их минимизации.	Обучающийся демонстрирует частичное умение разрабатывать и содержательно аргументировать стратегию решения проблемной ситуации на основе системного и междисциплинарного подходов с учетом оценки существующих рисков и возможностей их минимизации. . Допускаются значительные ошибки	Обучающийся демонстрирует полное умение разрабатывать и содержательно аргументировать стратегию решения проблемной ситуации на основе системного и междисциплинарного подходов с учетом оценки существующих рисков и возможностей их минимизации. . Допускаются незначительные ошибки, неточности	Обучающийся демонстрирует полное умение разрабатывать и содержательно аргументировать стратегию решения проблемной ситуации на основе системного и междисциплинарного подходов с учетом оценки существующих рисков и возможностей их минимизации . . Допускаются незначительные неточности
ПК-9. Способен проводить аудит информационной безопасности информационных систем и объектов информатизации				
знать: каналы утечки информации.	Обучающийся не знает или в недостаточной степени знает каналы утечки информации.	Обучающийся демонстрирует частичное знание каналов утечки информации. . Допускаются значительные ошибки	Обучающийся демонстрирует полное знание каналов утечки информации. . Допускаются незначительны	Обучающийся демонстрирует полное знание каналов утечки информации. .

			е ошибки, неточности	Допускаются незначительные неточности
уметь: проводить инструментальный аудит информационной безопасности информационных систем и объектов информатизации.	Обучающийся не умеет или в недостаточной степени умеет проводить инструментальный аудит информационной безопасности информационных систем и объектов информатизации.	Обучающийся демонстрирует частичное умение проводить инструментальный аудит информационной безопасности информационных систем и объектов информатизации. . Допускаются значительные ошибки	Обучающийся демонстрирует полное умение проводить инструментальный аудит информационной безопасности информационных систем и объектов информатизации. . Допускаются незначительные ошибки, неточности	Обучающийся демонстрирует полное умение проводить инструментальный аудит информационной безопасности информационных систем и объектов информатизации. . Допускаются незначительные неточности
владеть: методами мониторинга и аудита, выявления угроз информационно безопасности информационных систем и объектов информатизации.	Обучающийся не владеет или в недостаточной степени владеет методами мониторинга и аудита, выявления угроз информационно безопасности	Обучающийся демонстрирует частичное владение методами мониторинга и аудита, выявления угроз информационно безопасности информационных систем и объектов информатизации.	Обучающийся демонстрирует полное владение методами мониторинга и аудита, выявления угроз информационно безопасности информационных систем и объектов	Обучающийся демонстрирует полное владение методами мониторинга и аудита, выявления угроз информационно безопасности информацион

	информационных систем и объектов информатизации.	. Допускаются значительные ошибки	информатизации. . Допускаются незначительные ошибки, неточности	ных систем и объектов информатизации. . 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, написания и защиты курсового проекта (курсовой работы).

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 СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

Направление подготовки
10.04.01 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.