Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2024 10:10:19
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

Высшая школа интеллектуальных систем и кибертехнологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки:
10.03.01 «Информационная безопасность»

Направленность (профиль):
«Организация и технологии защиты информации
(по отрасли или сфере профессиональной деятельности)»

Квалификация выпускника: **бакалавр**

Тольятти 2024

Рабочая программа дисциплины «Аудит информационной безопасности» разработана в соответствии с федеральным государственным образовательным стандартом высшего образования - бакалавриат по направлению подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства науки и высшего образования Российской Федерации от 17 ноября 2020 г. № 1427.

Составители:

старший преподаватель	Дробот О.А.
ассистент	Курцев Е.А.
(ученая степень, ученое звание)	(ФИО)

РПД обсуждена на заседании Высшей школы интеллектуальных систем и кибертехнологий

«06» 09 2024 г., протокол № 2

Директор ВШИСиКТ	к.э.н., доцент	Филиппова О.А.
	(уч.степень, уч.звание)	(ФИО)

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Цель освоения дисциплины

Целью освоения дисциплины является:

- формирование способности проводить аудит защищенности объектов информатизации в соответствии с установленными требованиями и нормативными документами;
- формирование практических навыков организации контрольных проверок работоспособности и эффективности средств защиты информации, анализа аудиторских свидетельств и документирования результатов аудита.

1.2. Перечень планируемых результатов обучения по дисциплине

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине**	**Основание (ПС)** *для профессиональных компетенций
ОПК-2.4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами	ИОПК-2.4.1. Знает требования, предъявляемые к защищенным объектам информатизации. ИОПК-2.4.2. Проводит аудит защищенности объекта информатизации.	**Знает:** требования, предъявляемые к защищенным объектам информатизации; цели, принципы, этапы и критерии аудита защищенности; виды аудиторских свидетельств и правила документирования результатов проверки. **Умеет:** определять область и критерии аудита, формировать программу и чек-листы проверки, собирать и анализировать аудиторские свидетельства, сопоставлять фактическое состояние объекта информатизации с установленными требованиями. **Владеет:** навыками планирования и проведения аудита защищенности объекта информатизации, фиксации несоответствий, подготовки обоснованных выводов и оформления отчета по результатам аудита.	-
ПК-3. Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ИПК-3.1. Оценивает работоспособность применяемых средств защиты информации с использованием штатных средств и методик. ИПК-3.2. Оценивает эффективность применяемых средств защиты информации с использованием штатных средств и методик. ИПК-3.3. Определяет уровень защищенности и доверия средств защиты информации.	**Знает:** порядок организации контрольных проверок средств защиты информации; штатные средства и методики проверки работоспособности и эффективности; показатели, критерии и документируемые результаты оценки уровня защищенности и доверия. **Умеет:** проводить контрольные проверки работоспособности и эффективности средств защиты информации по заданной методике, анализировать результаты испытаний и журналов, выявлять отклонения и определять уровень защищенности и доверия. **Владеет:** навыками подготовки исходных данных и сценариев контрольной проверки, регистрации результатов, интерпретации полученных показателей и подготовки заключения о работоспособности и эффективности применяемых средств защиты информации.	06.032 «Специалист по безопасности компьютерных систем и сетей».

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к части, формируемой участниками образовательных отношений, Блока 1. Дисциплины (модули) образовательной программы (Профессиональный модуль).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем и структура дисциплины

Общая трудоёмкость дисциплины составляет **3 з.е. (108 час.)**, их распределение по видам работ и семестрам представлено в таблице.

Виды учебных занятий и работы обучающихся	Трудоемкость, час
Общая трудоемкость дисциплины, час	**108**
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:	**86/64**
занятия лекционного типа (лекции)	40/32
занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	46/32
лабораторные работы	0/0
Самостоятельная работа всего, в т.ч.:	**22/40**
Самоподготовка по темам (разделам) дисциплины	22/40
Контроль (часы на экзамен, зачет)	**0/4**
Промежуточная аттестация	**зачет**

Примечание: *-/- объем часов соответственно для очной, очно-заочной форм обучения*

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

В процессе освоения дисциплины может применяться электронное обучение и дистанционные образовательные технологии.

В процессе освоения дисциплины обучающиеся обеспечены доступом к электронной информационно-образовательной среде и электронно-библиотечным системам.

3.1. Содержание дисциплины, структурированное по темам

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные работы, час	Практические занятия, час		
ОПК-2.4: ИОПК-2.4.1 ИОПК-2.4.2 ПК-3: ИПК-3.1 ИПК-3.2 ИПК-3.3	**ТЕМА 1. ОСНОВЫ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ТРЕБОВАНИЯ К ЗАЩИЩЕННЫМ ОБЪЕКТАМ ИНФОРМАТИЗАЦИИ** Содержание лекции: 1. Понятие, цели, задачи и виды аудита информационной безопасности. 2. Объект, предмет, область и критерии аудита. 3. Требования к защищенным объектам информатизации и источники критериев проверки. 4. Принципы независимости, объективности, достаточности и воспроизводимости аудиторских свидетельств.	7/6				Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия
	Практическая работа №1. Определение области, целей и критериев аудита для заданного объекта информатизации.			8/6		Отчёт по практической работе
	Самостоятельная работа. Изучение терминологии аудита и требований к защищенным объектам информатизации; подготовка перечня исходных документов для проверки.				4/7	Самостоятельное изучение учебных материалов
ОПК-2.4: ИОПК-2.4.1 ИОПК-2.4.2 ПК-3: ИПК-3.1 ИПК-3.2 ИПК-3.3	**ТЕМА 2. ПЛАНИРОВАНИЕ АУДИТА И ФОРМИРОВАНИЕ ПРОГРАММЫ ПРОВЕРКИ** Содержание лекции: 1. Этапы аудита: инициирование, подготовка, проведение, анализ и завершение. 2. Формирование программы аудита, календарного плана и распределение ответственности. 3. Методы получения аудиторских свидетельств: анализ документов, интервью, наблюдение, выборочная проверка, инструментальный контроль. 4. Чек-листы, рабочие документы аудитора и требования к прослеживаемости результатов.	7/6				Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия
	Практическая работа №2. Разработка программы аудита и чек-листа проверки для заданной информационной системы.			8/6		Отчёт по практической работе
	Самостоятельная работа. Подготовка структуры рабочих документов аудитора и перечня свидетельств по выбранному объекту проверки.				4/7	Самостоятельное изучение учебных материалов
ОПК-2.4: ИОПК-2.4.1 ИОПК-2.4.2 ПК-3: ИПК-3.1 ИПК-3.2 ИПК-3.3	**ТЕМА 3. АУДИТ ОРГАНИЗАЦИОННЫХ МЕР И УПРАВЛЕНИЯ ДОСТУПОМ** Содержание лекции: 1. Анализ организационно-распорядительной документации по защите информации. 2. Проверка распределения ролей, полномочий и ответственности. 3. Аудит процессов управления учетными записями, правами доступа и привилегиями. 4. Проверка процедур управления изменениями, резервного копирования,	7/5				Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия

	реагирования и непрерывности.					
	Практическая работа №3. Проведение документарной проверки организационных мер и процесса управления доступом по учебному кейсу.			8/5		Отчёт по практической работе
	Самостоятельная работа. Анализ типового комплекта локальных документов и формирование перечня возможных несоответствий.				4/7	Самостоятельное изучение учебных материалов
ОПК-2.4: ИОПК-2.4.1 ИОПК-2.4.2 ПК-3: ИПК-3.1 ИПК-3.2 ИПК-3.3	**ТЕМА 4. ТЕХНИЧЕСКИЙ АУДИТ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ** Содержание лекции: 1. Состав технического аудита: конфигурации, сетевые параметры, системное и прикладное программное обеспечение. 2. Проверка настроек идентификации, аутентификации, разграничения доступа и регистрации событий. 3. Анализ конфигураций средств защиты информации без нарушения работоспособности объекта. 4. Фиксация технических свидетельств, воспроизводимость и ограничения инструментальных проверок.	7/5				Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия
	Практическая работа №4. Анализ конфигурации учебного объекта и подготовка карты соответствия заданным требованиям защиты.			8/5		Отчёт по практической работе
	Самостоятельная работа. Подготовка перечня технических параметров и журналов, подлежащих проверке при аудите защищенности.				4/7	Самостоятельное изучение учебных материалов
ОПК-2.4: ИОПК-2.4.1 ИОПК-2.4.2 ПК-3: ИПК-3.1 ИПК-3.2 ИПК-3.3	**ТЕМА 5. КОНТРОЛЬ РАБОТОСПОСОБНОСТИ И ЭФФЕКТИВНОСТИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ** Содержание лекции: 1. Различие проверки наличия, работоспособности и эффективности средств защиты. 2. Штатные средства диагностики и методики контрольных проверок. 3. Формирование тестовых воздействий и критериев приемки в безопасной учебной среде. 4. Анализ журналов, показателей, ложных срабатываний и устойчивости настроек средств защиты.	6/5				Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия
	Практическая работа №5. Разработка и выполнение программы контрольной проверки работоспособности и эффективности заданного средства защиты информации.			7/5		Отчёт по практической работе
	Самостоятельная работа. Изучение примеров методик контроля и подготовка набора критериев работоспособности и эффективности.				3/6	Самостоятельное изучение учебных материалов
ОПК-2.4: ИОПК-2.4.1 ИОПК-2.4.2 ПК-3: ИПК-3.1 ИПК-3.2 ИПК-3.3	**ТЕМА 6. ОЦЕНКА УРОВНЯ ЗАЩИЩЕННОСТИ, ОФОРМЛЕНИЕ РЕЗУЛЬТАТОВ И ЗАВЕРШЕНИЕ АУДИТА** Содержание лекции: 1. Обобщение свидетельств и классификация выявленных несоответствий. 2. Подходы к определению уровня защищенности и доверия средств защиты	6/5				Лекция-визуализация (в т.ч. в ЭИОС) Тестирование по теме лекционного занятия

	информации. 3. Структура аудиторского отчета: факты, критерии, выводы, рекомендации и ограничения. 4. Контроль корректирующих действий, повторная проверка и закрытие результатов аудита.					
	Практическая работа №6. Подготовка итогового аудиторского отчета и заключения по результатам комплексного учебного кейса.			7/5		Отчёт по практической работе
	Самостоятельная работа. Подготовка шаблона итогового отчета и критериев подтверждения устранения выявленных несоответствий.				3/6	Самостоятельное изучение учебных материалов
	ИТОГО	**40/32**	**0/0**	**46/32**	**22/40**	

Примечание: *-/-объем часов соответственно для очной, очно-заочной форм обучения*

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

4.1. Общие методические рекомендации по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплины в форме курса, составленного на основе результатов научных исследований, проводимых университетом, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Преподавание дисциплины ведется с применением следующих видов **образовательных технологий:**

-балльно-рейтинговая технология оценивания;

- электронное обучение;

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

4.2. Методические указания для обучающихся по освоению дисциплины на занятиях лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины. Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала.

Лекционные занятия проводятся в поточной аудитории с применением мультимедийного проектора в виде учебной презентации или в ЭИОС университета.

В ходе лекционных занятий рекомендуется конспектирование учебного материала. Возможно ведение конспекта лекций в виде интеллект-карт.

Отдельные темы предлагаются для самостоятельного изучения (конспектируются).

Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиям / лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

4.3. Методические указания для обучающихся по освоению дисциплины на лабораторных работах

Подготовку к каждой лабораторной работе студент должен начать с ознакомления с планом занятия, который отражает содержание предложенной темы. Каждая выполненная работа с оформленным отчетом по ней подлежит защите преподавателю.

При оценивании лабораторных работ учитывается следующее:

–качество выполнения экспериментально-практической части работы и степень соответствия результатов работы заданным требованиям;

–качество оформления отчета по работе;

–качество устных ответов на контрольные вопросы при защите работы.

Лабораторные работы организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

4.4. Методические указания для обучающихся по освоению дисциплины на занятиях семинарского типа/ на практических занятиях

Практические (семинарские) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

Практические (семинарские) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- получение умений и навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины;
- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Практические занятия организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

4.5. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

Самостоятельная работа студентов включает:

1. Изучение учебной литературы по курсу.
2. Работу с ресурсами Интернет
3. Самостоятельное изучение учебных материалов

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы.

Для обучающихся по заочной форме обучения самостоятельная работа является основным видом учебной деятельности.

Для обеспечения самостоятельной работы обучающихся используется электронный учебный курс, созданный в ЭИОС университета http://sdo.tolgas.ru/.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Вся литература, включенная в данный перечень, представлена в виде электронных ресурсов в электронной библиотеке университета (ЭБС). Литература, используемая в печатном виде, представлена в научной библиотеке университета в объеме не менее 0,25 экземпляров на одного обучающегося.

Основная литература

1. Мартемьянов, Ю. Ф. Операционные системы. Концепции построения и обеспечения безопасности : учеб. пособие для вузов по направлению "Информац. системы и технологии" / Ю. Ф. Мартемьянов, Яковлев, Ал. В., Яковлев, Ан. В. - 2-е изд., стер. - Москва : Горячая линия -Телеком, 2020. - 332 с. : ил. - ISBN 978-5-9912-0677-8 : 455-51. - Текст : непосредственный.

2. Тенгайкин, Е. А. Эксплуатация объектов сетевого администрирования. Безопасность функционирования информационных систем. Лабораторные работы : учеб. пособие / Е. А. Тенгайкин. – Документ read. – Санкт-Петербург [и др.] : Лань, 2022. – 80 с. – URL: https://reader.lanbook.com/book/197546 (дата обращения: 02.09.2024). - Режим доступа: для авториз. пользователей. – ISBN 978-5-8114-8692-2. – Текст : электронный.

Дополнительная литература

3. Васильев, Р. Б. Управление развитием информационных систем : учеб.-метод. пособие для вузов по специальности "Приклад. информатика (по областям)" и др. междисциплин. специальностям / Р. Б. Васильев, Г. Н. Калянов, Г. А. Лёвочкина ; под ред. Г. Н. Калянова. – 2-е изд., стер. – Москва : Горячая линия -Телеком, 2018. – 376 с. : талб. – Прил. - Глоссарий. – ISBN 978-5-9912-0399-9 : 355-52. – Текст : непосредственный.

4. Дубинин, Е. А. Оценка относительного ущерба безопасности информационной системы : монография / Е. А. Дубинин, Ф. Б. Тебуева, В. В. Копытов. – Документ read. – Москва : РИОР [и др.], 2022. – 192 с. – (Научная мысль). – Прил. – URL: https://znanium.com/read?id=400262 (дата обращения: 02.09.2024). - Режим доступа: для авториз. пользователей. – ISBN 978-5-369-01371-7. - 978-5-16-101863-7. – Текст : электронный.

5. Лагоша, О. Н. Сертификация информационных систем : учеб. пособие для СПО / О. Н. Лагоша. - Изд. 3-е, стер. - Документ reader. - Санкт-Петербург [и др.] : Лань, 2023. - 109 с. - URL: https://reader.lanbook.com/book/297659 (дата обращения: 02.09.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-46102-8 : 0-00. - Текст : электронный.

6. Мельников, Д. А. Информационная безопасность открытых систем : учеб. для студентов по направлению "Приклад. информатика" / Д. А. Мельников. - Москва : Флинта [и др.], 2013. - 442 с. : табл. - ISBN 978-5-9765-1613-7. - 978-5-02-037923-7 : 442-00;379-00. - Текст : непосредственный.

7. Олифер, В. Г. Безопасность компьютерных сетей / В. Г. Олифер, Н. А. Олифер. - Москва : Горячая линия -Телеком, 2016. - 644 с. : ил. - Прил. - ISBN 978-5-9912-0420-0 : 823-90. - Текст : непосредственный.

8. Основы управления информационной безопасностью : учеб. пособие для вузов по направлениям подгот. (специальностям) укрупн. группы специальностей "Информ. безопасность" / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд., испр. - Москва : Горячая линия -Телеком, 2016. - 244 с. : ил. - (Вопросы управления информационной безопасностью. Книга 1). - Прил. - ISBN 978-5-9912-0361-6 : 400-18. - Текст : непосредственный.

9. Ситнов, А. А. Аудит информационных систем : моногр. для магистров по специальности 08.00.13 "Мат. и инструмент. методы экономики", 08.00.12 "Бухгалт. учет, статистика" и др. междисциплинар. специальностям / А. А. Ситнов, А. И. Уринцов ; Финансовый ун-т при Правительстве РФ. - Москва : ЮНИТИ-ДАНА, 2014. - 239 с. : табл. - (Magister). - Терминол. слов. - ISBN 978-5-238-02535-3 : 581-00. - Текст : непосредственный.

5.2. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы

1. 3DNEWS.RU : Электронное периодическое издание : сайт. – Москва, 1997 - . - URL: https://3dnews.ru/ (дата обращения: 02.09.2024). – Текст: электронный.
2. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 - . - URL: https://elibrary.ru (дата обращения: 02.09.2024). – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.
3. КонсультантПлюс : справочная правовая система : сайт / ЗАО «КонсультантПлюс». – Москва, 1992 - . - URL: http://www.consultant.ru (дата обращения: 02.09.2024). - Текст : электронный.
4. Электронная библиотека. Техническая литература : сайт. - URL : http://techliter.ru/ (дата обращения: 02.09.2024). - Текст : электронный.
5. Электронная библиотечная система Поволжского государственного университета сервиса : сайт / ФГБОУ ВО «ПВГУС». – Тольятти, 2010 - . - URL. : http://elib.tolgas.ru (дата обращения: 02.09.2024). - Режим доступа: для авториз. пользователей. - Текст : электронный.
6. Электронно-библиотечная система Znanium.com : сайт / ООО "ЗНАНИУМ". – Москва, 2011 - . - URL: https://znanium.com/ (дата обращения: 02.09.2024). - Режим доступа: для авториз. пользователей. - Текст : электронный.
7. Электронно-библиотечная система Лань : сайт / ООО "ЭБС ЛАНЬ". - Москва, 2011 - . - URL: https://e.lanbook.com/ (дата обращения: 02.09.2024). - Режим доступа: для авториз. пользователей. - Текст : электронный.

5.3. Программное обеспечение

Информационное обеспечение учебного процесса по дисциплине осуществляется с использованием следующего программного обеспечения (лицензионного и свободно распространяемого), в том числе отечественного производства:

№ п/п	Наименование	Условия доступа
1	Microsoft Windows	из внутренней сети университета (лицензионный договор)
2	Microsoft Office	из внутренней сети университета (лицензионный договор)
3	КонсультантПлюс	из внутренней сети университета (лицензионный договор)
4	СДО MOODLE	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)
6	Yandex	из любой точки, в которой имеется доступ к сети Интернет (свободно распространяемое)

6. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных учебным планом и рабочей программой дисциплины, оснащенные оборудованием и техническими средствами обучения.

Занятия лекционного типа. Учебные аудитории для занятий лекционного типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентации по темам лекций), обеспечивающие тематические иллюстрации, соответствующие данной программе дисциплины.

Занятия семинарского типа. Учебные аудитории для занятий семинарского типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук).

Лабораторные работы.

Для проведения лабораторных работ используется учебная аудитория «Лаборатория информационных технологий, информатики и методов программирования // Учебная аудитория для проведения занятий лекционного типа, семинарского типа, курсового проектирования, консультаций, текущего контроля и промежуточной аттестации // Помещение для хранения и профилактического обслуживания учебного оборудования (Г-413)», оснащенная следующим оборудованием: рабочие места обучающихся; Рабочее место преподавателя; Учебно-наглядные пособия, обеспечивающие тематические иллюстрации. Компьютер Аксус Intel G530\iH61\GeForceGT430\4096 Mb DDR3\500Gb\LCD 22" - 14 шт., Компьютер в сборе iP2.0 LCD - 1 шт., принтер HP 1200 - 1 шт., мобильный экран проекционный DraperLuma - 1 шт., мобильный проектор Sanyo PLC, Сетевое оборудование D-Link DES-1024D, 24-портовый; локальная сеть 100 мб с доступом в Интернет 50 мб. Лаборатория оснащена кондиционером.

Промежуточная аттестация. Для проведения промежуточной аттестации по дисциплине используются компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета и/или учебные аудитории, укомплектованные мебелью и техническими средствами обучения.

Самостоятельная работа. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интеренет» и доступом к электронной информационно-образовательной среде университета. Для организации самостоятельной работы обучающихся используются:

компьютерные классы университета;

библиотека (медиазал), имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети Интернет.

Электронная информационно-образовательная среда университета (ЭИОС). Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета (ЭИОС) http://sdo.tolgas.ru/ из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

ЭИОС университета обеспечивает:

доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;

формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

В случае реализации образовательной программы с применением электронного обучения, дистанционных образовательных технологий ЭИОС дополнительно обеспечивает:

фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательной программы;

проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети "Интернет".

7. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида, могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

8. Оценочные материалы (фонд оценочных средств) для текущего контроля успеваемости и промежуточной аттестации

8.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

Шкала оценки результатов освоения дисциплины, сформированности результатов обучения

Форма проведения промежуточной аттестации	Шкалы оценки уровня сформированности результатов обучения		Шкала оценки уровня освоения дисциплины		
	Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
зачет	допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
	пороговый	61-85,9	61-69,9	«удовлетворительно» / 3	зачтено
			70-85,9	«хорошо» / 4	зачтено
	повышенный	86-100	86-100	«отлично» / 5	зачтено

По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации в соответствии за набранными за семестр баллами (по накопительному рейтингу). Студентам, набравшим в ходе текущего контроля успеваемости по дисциплине от 61 до 100 баллов и выполнившим все обязательные виды запланированных учебных занятий, по решению преподавателя без прохождения промежуточной аттестации выставляется оценка в соответствии со шкалой оценки результатов освоения дисциплины.

***Результат обучения считается сформированным (повышенный уровень)**, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует повышенному уровню сформированности результатов обучения.*

***Результат обучения считается сформированным (пороговый уровень)**, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует пороговому уровню сформированности результатов обучения.*

***Результат обучения считается несформированным**, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений,*

качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует допороговому уровню.

Формы текущего контроля успеваемости

Формы текущего контроля	Количество контрольных точек	Количество баллов за 1 контр. точку	Макс. возм. кол-во баллов
Посещение лекционных занятий (конспект, участие в текущем тестировании)	1	10	10
Выполнение лабораторных и практических работ	6	15	90
Итого по дисциплине			100 баллов

Система оценивания представлена в электронном учебном курсе по дисциплине http://sdo.tolgas.ru/.

8.2. Типовые контрольные задания или иные материалы для ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

8.2.1. Типовые задания к практическим (семинарским) занятиям

Практическая работа № 1. Определение области и критериев аудита
Задание 1. Изучить описание учебного объекта информатизации, его назначение, состав и границы.
Задание 2. Определить заинтересованные стороны, цели аудита и проверяемые процессы.
Задание 3. Сформировать перечень критериев и требований, относительно которых будет проводиться проверка.
Задание 4. Определить виды аудиторских свидетельств, необходимые для подтверждения каждого критерия.
Задание 5. Оформить паспорт аудита: область, ограничения, критерии, источники свидетельств и ожидаемый результат.

Практическая работа № 2. Разработка программы аудита и чек-листа
Задание 1. Составить последовательность этапов аудита и перечень проверяемых вопросов.
Задание 2. Распределить вопросы по методам получения свидетельств: документы, интервью, наблюдение, техническая проверка.
Задание 3. Разработать чек-лист с критериями «соответствует / частично соответствует / не соответствует / не применимо».
Задание 4. Установить правила фиксации фактов, ссылок на свидетельства и комментариев аудитора.
Задание 5. Проверить полноту чек-листа относительно целей и области аудита.

Практическая работа № 3. Документарная проверка организационных мер и управления доступом
Задание 1. Изучить предоставленный комплект локальных документов и матрицу доступа.
Задание 2. Сопоставить установленные обязанности и полномочия с фактическим распределением ролей.
Задание 3. Проверить процедуры создания, изменения, блокирования и удаления учетных записей.
Задание 4. Зафиксировать подтверждающие свидетельства и выявленные несоответствия.
Задание 5. Сформулировать выводы по достаточности организационных мер и управления доступом.

Практическая работа № 4. Анализ технической конфигурации объекта

Задание 1. Определить перечень параметров безопасности, подлежащих проверке.

Задание 2. Собрать доступные конфигурационные данные, сведения о версиях и журналы событий.

Задание 3. Сопоставить значения параметров с заданными требованиями и критериями.

Задание 4. Зафиксировать отклонения, их местоположение и подтверждающие данные.

Задание 5. Подготовить карту соответствия технической конфигурации установленным требованиям.

Практическая работа № 5. Контрольная проверка средства защиты информации

Задание 1. Определить проверяемые функции средства защиты и критерии их работоспособности.

Задание 2. Разработать безопасный сценарий контрольной проверки и ожидаемые результаты.

Задание 3. Выполнить проверку в учебной среде с использованием штатных средств диагностики.

Задание 4. Сопоставить фактические результаты с ожидаемыми и оценить эффективность.

Задание 5. Оформить протокол проверки с выводом о работоспособности и выявленных ограничениях.

Практическая работа № 6. Подготовка итогового аудиторского отчета

Задание 1. Систематизировать выявленные факты и связать каждый факт с критерием и свидетельством.

Задание 2. Классифицировать несоответствия по значимости для защищенности объекта.

Задание 3. Сформулировать выводы без выхода за границы собранных аудиторских свидетельств.

Задание 4. Подготовить рекомендации и критерии подтверждения корректирующих действий.

Задание 5. Оформить итоговый отчет и краткое заключение для руководителя объекта.

8.3. Типовые контрольные задания или иные материалы для проведения ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Форма проведения промежуточной аттестации по дисциплине: *зачет (по результатам накопительного рейтинга или в форме компьютерного тестирования).*

Устно-письменная форма по экзаменационным билетам предполагается, как правило, для сдачи академической задолженности.

8.3.1. Перечень вопросов для подготовки к зачету

ОПК-2.4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами

1. Понятие и назначение аудита информационной безопасности.
2. Цели и задачи аудита защищенности объекта информатизации.
3. Объект, предмет и область аудита информационной безопасности.
4. Критерии аудита и источники требований к защищенному объекту информатизации.
5. Основные требования, предъявляемые к защищенным объектам информатизации.
6. Принципы объективности, независимости и доказательности аудита.
7. Этапы жизненного цикла аудита информационной безопасности.
8. Инициирование аудита и определение его целей и ограничений.
9. Программа аудита: назначение, состав и правила разработки.
10. План аудита и распределение ответственности участников проверки.
11. Аудиторский чек-лист: структура и правила применения.
12. Виды аудиторских свидетельств и требования к их достаточности.
13. Методы получения свидетельств: анализ документов, интервью, наблюдение.
14. Выборочный контроль и ограничения выборки при проведении аудита.
15. Документарный аудит организационных мер защиты информации.
16. Аудит распределения ролей, полномочий и ответственности.
17. Аудит управления учетными записями и правами доступа.
18. Аудит процедур управления изменениями и конфигурациями.
19. Аудит журналирования и регистрации событий безопасности.
20. Аудит резервного копирования и восстановления информации.
21. Аудит мер реагирования на инциденты информационной безопасности.
22. Содержание технического аудита защищенности автоматизированной системы.
23. Проверка конфигурационных параметров безопасности как метод аудита.
24. Ограничения инструментальных методов при аудите действующего объекта.
25. Фиксация фактов и обеспечение прослеживаемости аудиторских выводов.
26. Классификация выявленных несоответствий при аудите.
27. Формирование аудиторского вывода на основе собранных свидетельств.
28. Структура и содержание отчета по аудиту информационной безопасности.
29. Рекомендации по результатам аудита и требования к их обоснованности.
30. Повторная проверка и подтверждение устранения выявленных несоответствий.

ПК-3. Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации

1. Назначение контрольных проверок средств защиты информации.
2. Различие проверки наличия, работоспособности и эффективности средства защиты информации.
3. Организация контрольной проверки работоспособности средства защиты.
4. Организация контрольной проверки эффективности средства защиты.
5. Штатные средства диагностики и их роль в контрольной проверке.

6. Требования к методике проверки средства защиты информации.
7. Исходные данные для подготовки программы контрольной проверки.
8. Критерии работоспособности программного средства защиты информации.
9. Критерии работоспособности программно-аппаратного средства защиты информации.
10. Критерии работоспособности технического средства защиты информации.
11. Понятие эффективности применяемых мер и средств защиты информации.
12. Формирование безопасного тестового сценария контрольной проверки.
13. Ожидаемый результат и критерии приемки при проведении проверки.
14. Использование журналов событий при оценке работоспособности средства защиты.
15. Использование диагностических сообщений и штатной телеметрии при проверке.
16. Анализ ложных срабатываний и пропусков событий при оценке эффективности.
17. Проверка устойчивости настроек средства защиты после изменения конфигурации.
18. Контроль корректности функционирования механизмов идентификации и аутентификации.
19. Контроль корректности функционирования механизмов разграничения доступа.
20. Контроль корректности регистрации событий информационной безопасности.
21. Проверка работоспособности сетевых средств защиты информации.
22. Проверка работоспособности средств антивирусной и иной защитной обработки.
23. Проверка работоспособности криптографических механизмов штатными средствами.
24. Сопоставление фактических результатов проверки с установленными критериями.
25. Определение уровня защищенности по результатам контрольных проверок.
26. Понятие уровня доверия к средству защиты информации.
27. Связь результатов проверок с оценкой уровня защищенности и доверия.
28. Оформление протокола контрольной проверки.
29. Формулирование заключения о работоспособности и эффективности средства защиты.
30. Документирование ограничений, допущений и повторных проверок.