ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

Институт приоритетных технологий

Кафедра информационной безопасности

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование
дисциплины (модуля): **Методики проведения инструментального аудита**

Уровень ОПОП: Специалитет

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей (по отрасли или в сфере профессиональной деятельности)

Форма обучения: Очная

Срок обучения: 2024 - 2030 уч. г.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.01 Компьютерная безопасность (приказ № 1459 от 26.11.2020 г.) и учебного плана, утвержденного Ученым советом (от 26.05.2023 г., протокол № 9)

Разработчики:
Никишова А. В., кандидат технических наук, доцент

Программа рассмотрена и утверждена на заседании кафедры, протокол № 08 от 30.08.2023 года

Зав. кафедрой Какорина О. А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины - обеспечение упорядоченной и эффективной работы информационных систем в условиях существования внешних угроз и уязвимостей ее компонентов.

Задачи дисциплины:

- Изучение методов работы с современными базами данных уязвимостей программного обеспечения
- Знакомство с программными средствами проведения автоматизированных процедур по аудиту ИС
- Изучение программных средств управления аудитом

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Методики проведения инструментального аудита» относится к обязательной части учебного плана.

Дисциплина изучается на 5 курсе.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование компетенций, определенных учебным планом в соответствии с ФГОС ВО.

Выпускник должен обладать следующими общепрофессиональными компетенциями (ОПК):

- ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях

Знания, умения, навыки, формируемые по компетенции в рамках дисциплины

Студент должен знать:

средства и методы хранения и передачи аутентификационной информации; механизмы реализации атак в сетях TCP/IP; основные протоколы идентификации и аутентификации абонентов сети; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений

Студент должен уметь:

формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты

Студент должен владеть навыками:

настройки межсетевых экранов; владеет методиками анализа сетевого трафика

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Десятый семестр
Контактная работа (всего)	**80**	**80**
Лабораторные	32	32
Лекции	32	32
Практические	16	16
Самостоятельная работа (всего)	**100**	**100**
Виды промежуточной аттестации	**36**	**36**
Экзамен	36	36
Общая трудоемкость часы	**216**	**216**
Общая трудоемкость зачетные единицы	**6**	**6**

5. Содержание дисциплины

5.1. Содержание дисциплины: Лабораторные (32 ч.)

Десятый семестр. (32 ч.)

Тема 1. Экспертный аудит информационной безопасности (2 ч.)

1. Определены следующие показатели качества выделенного помещения:
— освещенность помещения;
— наличие средств прегражденияотраженного света: ширмы, шторы, и др.;
— просторность помещения;
— наличие генератора шума;
— наличие 20 посадочных мест;
— наличие генератора зашумления
2. С помощью 3х экспертов определите наиболее значимые показатели качества выделенного помещения с точки зрения его защищенности.
3. Проверьте гипотезу о согласованности мнений экспертов.
4. Постройте гистограмму ранжирования показателей качества выделенного помещения.
5. Примите решение об основных показателях качества, наиболее влияющих на защищенность выделенного помещения.

Тема 2. Экспертный аудит информационной безопасности (2 ч.)

С помощью метода мозгового штурма сформировать перечень угроз для выделенного помещения.

Тема 3. Экспертный аудит информационной безопасности (2 ч.)

Используя метод попарных сравнений, сформируйте список актуальных угроз.

Тема 4. Инструментальный аудит информационной безопасности (2 ч.)

1) Опишите входные данные модели информационных потоков.
2) Опишите основные понятия и допущения модели информационных потоков.
3) Опишите порядок расчета рисков модели информационных потоков.
4) Опишите порядок учета применяемых контрмер.

Тема 5. Инструментальный аудит информационной безопасности (2 ч.)

1) Опишите входные данные модели анализа угроз и уязвимостей.
2) Опишите основные понятия и допущения модели анализа угроз и уязвимостей.
3) Опишите порядок расчета рисков модели анализа угроз и уязвимостей.

Тема 6. Инструментальный аудит информационной безопасности (2 ч.)

С помощью программы ГРИФ из состава Digital Security Office проведите анализ рисков организации в соответствии с заданием преподавателя.

Тема 7. Получение свидетельств аудита (2 ч.)

Собрать свидетельства аудита.

Тема 8. Получение обнаружений аудита (2 ч.)

По имеющимся свидетельствам аудита получить обнаружения аудита.

Тема 9. План аудита (2 ч.)

Составить план аудита организации по ГОСТ Р ИСО 19011 — 2021.

Тема 10. Программа аудита (2 ч.)

Составить программу аудита по ГОСТ Р ИСО 19011 — 2021.

Тема 11. Инструменты эксплуатации уязвимостей (2 ч.)

Изучить инструменты эксплуатации уязвимостей

Тема 12. Сканирование портов (2 ч.)

Тестирование на проникновение с помощью сканера портов NMAP

Тема 13. Сканирование уязвимостей (2 ч.)

Инструментальный аудит с помощью сканера уязвимостей OpenVAS.

Тема 14. Сканирование беспроводных сететей (2 ч.)

Провести тестирование безопасности беспроводных сетей с помощью утилиты Aircrack-ng

Тема 15. Инструменты мониторинга трафика (2 ч.)

Инструментальный аудит с помощью сниффера для перехвата и анализа сетевого трафика Wireshark.

Тема 16. Анализ уязвимостей в веб-приложениях (2 ч.)

Сканеры веб-уязвимостей.

5.2. Содержание дисциплины: Лекции (32 ч.)

Десятый семестр. (32 ч.)

Тема 1. Стуктура и свойства процессов и систем (2 ч.)

Основные понятия аудита информационной безопасности, основные этапы проведения аудита, способы проведения.

Тема 2. Способы контроля и проверки процессов и систем (2 ч.)

Виды аудита безопасности. Состав работ по проведению работ аудита безопасности. Сбор исходных данных. Разработка рекомендаций по повышению уровня защиты АС предприятия.

Тема 3. Внутренний и внешний аудит (2 ч.)

Понятие внутреннего и внешнего аудита. Перечень исходных данных, необходимых для аудита безопасности.

Тема 4. Методологические основы аудита информационной безопасности (2 ч.)

Основная схема методики аудита информационной безопасности. Органы государсвенной власти, уполномоченные осуществлять мероприятия по контролю и надзору.

Тема 5. Правовые основы аудита информационной безопасности (2 ч.)

Основные нормативные правовые акты, регулирующие требования к проведению аудита и являющиеся основными в сфере информационной безопасности в Российской Федерации.

Тема 6. Этапы проведения инструментального аудита (2 ч.)

1. Разведка.
2. Сканирование и перечисление.
3. Получение доступа.
4. Повышение привилегий.
5. Поддержание доступа.
6. Заметание следов.
7. Составление отчета.

Тема 7. Средства обнаружения вторжений. Средства межсетевого экранирования (2 ч.)

Средства обнаружения вторжений. Средства межсетевого экранирования.

Тема 8. Средства криптографической защиты информации (2 ч.)

Средства криптографической защиты информации

Тема 9. Средства резервного копирования информации (2 ч.)

Средства резервного копирования.

Тема 10. Инструменты эксплуатации уязвимостей (2 ч.)

Инструменты экспулуатации уязвимостей

Тема 11. Тестирование на проникновение (2 ч.)

Предварительное соглашение на взаимодействие. Сбор разведданных. Моделирование угроз. Анализ уязвимостей. Эксплуатация. Составление отчета.

Тема 12. Методы и инструменты тестирования безопасности (2 ч.)

Тестирование на проникновение
Тестирование на основе кода
Тестирование на основе сценария угроз
Тестирование на утечку информации
Тестирование на наличие недостатков аутентификации и авторизации

Тема 13. Сканеры портов (2 ч.)

Сканеры портов.

Тема 14. Инструменты шифрования (2 ч.)

Различные программы для шифрования

Тема 15. Инструменты мониторинга трафика (2 ч.)

Различные программы для мониторинга трафика.

Тема 16. Сканеры веб-уязвимостей (2 ч.)

Сетевые сканеры безопасности.

5.3. Содержание дисциплины: Практические (16 ч.)

Десятый семестр. (16 ч.)

Тема 1. Современный подход к информационной безопасности информационных систем (2 ч.)

Современный подход к информационной безопасности информационных систем

Тема 2. Политика безопасности распределенной информационной системы (2 ч.)

Политика безопасности распределенной информационной системы.

Тема 3. Модель нарушителя распределенной информационной системы (2 ч.)

Построение модели нарушителя.

Тема 4. Безопасность систем управления базами данных (2 ч.)

Безопасность систем управления базами данных распределенной информационной системы. Общие положения. Угрозы СУБД. Методы борьбы. Агрегирование данных. Покушение на высокую доступность.

Тема 5. Безопасность данных и WEB-сервисов (2 ч.)

Безопасность данных и WEB-сервисов.

Тема 6. Система контроля доступа в распределенных ИС (2 ч.)

Система контроля доступа

Тема 7. Средства обнаружения вторжений. Средства межсетевого экранирования (2 ч.)

Средства обнаружения вторжений.

Тема 8. Средства криптографической защиты информации (2 ч.)

Средства криптографической защиты информации

6. Виды самостоятельной работы студентов по дисциплине

Десятый семестр (100 ч.)

Вид СРС: Ознакомление с нормативными документами (50 ч.)

Тематика заданий СРС:

Изучить содержание нормативно-правовых документов в области проведения аудита и оценки рисков информационной безопасности:

1. ГОСТ Р 56275-2014
2. ГОСТ Р ИСО 31000-2010
3. ГОСТ Р 58771-2019
4. ГОСТ Р ИСО/МЭК 27007-2014
5. ГОСТ Р ИСО/МЭК 27006-2008.

Вид СРС: Подготовка рефератов (50 ч.)

Тематика заданий СРС:

Реферат – письменная работа объемом 8–10 страниц. Это краткое и точное изложение сущности какого-либо вопроса, темы.

Тему реферата студент выбирает из предложенных преподавателем или может предложить свой вариант. В реферате нужны развернутые аргументы, рассуждения, сравнения. Содержание темы излагается объективно от имени автора.

Функции реферата. Информативная, поисковая, справочная, сигнальная, коммуникативная. Степень выполнения этих функций зависит от содержательных и формальных качеств реферата и целей.

Требования к языку реферата. Должен отличаться точностью, краткостью, ясностью и простотой.

Структура реферата.

1. Титульный лист.
2. Оглавление (на отдельной странице). Указываются названия всех разделов (пунктов плана)

реферата и номера страниц, указывающие начало этих разделов в тексте реферата.
3. Введение. Аргументируется актуальность исследования, т.е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками, перечисляются положения, которые должны быть обоснованы. Обязательно формулируются цель и задачи реферата.
4. Основная часть. Подчиняется собственному плану, что отражается в разделении текста на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала. В случае если используется чья-либо неординарная мысль, идея, то обязательно нужно сделать ссылку на того автора, у кого взят данный материал.
5. Заключение. Последняя часть научного текста. В краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования.
6. Приложение. Может включать графики, таблицы, расчеты.
7. Библиография (список литературы). Указывается реально использованная для написания реферата литература. Названия книг располагаются по алфавиту с указанием их выходных данных.
При проверке реферата оцениваются:
- знание фактического материала, усвоение общих представлений, понятий, идей;
- характеристика реализации цели и задач исследования;
- степень обоснованности аргументов и обобщений;
- качество и ценность полученных результатов;
- использование литературных источников;
- культура письменного изложения материала;
- культура оформления материалов работы.

Тематика рефератов:
1. Аудит ИБ.
2.Стандарты СУИБ.
3.Сертификация в сфере ИБ.
4. Направления ИБ.
5. Анализ рисков ИБ.
6. Оценка рисков ИБ.
7. Психология восприятия рисков ИБ.
8. Моделирование угроз ИБ.
9.Программные средства аудита ИБ.
10. SaaS-решение для аудита ИБ.
11. Инциденты ИБ.
12. BYOD.
13.Облачная безопасность.
14. Тесты на проникновение.
15.Безопасность АСУ ТП.

7. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Фонд оценочных средств. Оценочные материалы

8.1. Показатели и критерии оценивания компетенций, шкалы оценивания

В рамках изучаемой дисциплины студент демонстрирует уровни овладения компетенциями:

Повышенный уровень:

обучающийся демонстрирует глубокое знание учебного материала; способен использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных ситуациях; способен анализировать, проводить сравнение и обоснование выбора методов решения практико-ориентированных заданий

Базовый уровень:

обучающийся способен понимать и интерпретировать освоенную информацию; демонстрирует осознанное владение учебным материалом и учебными умениями, навыками и способами деятельности, необходимыми для решения практико-ориентированных заданий

Пороговый уровень:

обучающийся обладает необходимой системой знаний и владеет некоторыми умениями; демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий на репродуктивном уровне

Уровень ниже порогового:

система знаний, необходимая для решения учебных и практико-ориентированных заданий, не сформирована; обучающийся не владеет основными умениями, навыками и способами деятельности

Уровень сформированности компетенции	Шкала оценивания для промежуточной аттестации	Шкала оценивания по БРС
	Экзамен, зачет с оценкой	
Повышенный	5 (отлично)	91 и более
Базовый	4 (хорошо)	71 – 90
Пороговый	3 (удовлетворительно)	60 – 70
Ниже порогового	2 (неудовлетворительно)	Ниже 60

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели
Отлично	Обучающийся демонстрирует: систематизированные, глубокие и полные знания по всем разделам учебной дисциплины, а также по основным вопросам, выходящим за ее пределы; точное использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы; безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач; выраженную способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации; полное и глубокое усвоение основной, и дополнительной литературы, по изучаемой учебной дисциплине; умение свободно ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку, использовать научные достижения других дисциплин; творческую самостоятельную работу на учебных занятиях, активное творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Хорошо	Обучающийся демонстрирует: систематизированные, глубокие и полные знания по всем разделам учебной дисциплины; использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы и обобщения; владение инструментарием учебной дисциплины (методами комплексного анализа, техникой информационных технологий), умение его использовать в постановке и решении научных и профессиональных задач; способность решать сложные проблемы в рамках учебной дисциплины; свободное владение типовыми решениями; усвоение основной и дополнительной литературы, рекомендованной рабочей программой по учебной дисциплине; умение ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку; активную самостоятельную работу на учебных занятиях, систематическое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.
Удов-летвори-тельно	Обучающийся демонстрирует: достаточные знания в объеме рабочей программы по учебной дисциплине; использование научной терминологии, грамотное, логически правильно изложение ответа на вопросы, умение делать выводы без существенных ошибок; владение инструментарием учебной дисциплины, умение его использовать в решении учебных и профессиональных задач; способность самостоятельно применять типовые решения в рамках изучаемой дисциплины; усвоение основной литературы, рекомендованной рабочей программой по дисциплине; умение ориентироваться в базовых теориях, концепциях и направлениях по дисциплине; работу на учебных занятиях под руководством преподавателя, фрагментарное участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.
Неудов-летвори-тельно	Обучающийся демонстрирует: фрагментарные знания в рамках изучаемой дисциплины; знания отдельных литературных источников, рекомендованных рабочей программой по учебной дисциплине; неумение использовать научную терминологию учебной дисциплины, наличие в ответе грубых, логических ошибок; пассивность на занятиях или отказ от ответа, низкий уровень культуры исполнения заданий.

8.2. Вопросы, задания текущего контроля

В целях освоения компетенций, указанных в рабочей программе дисциплины, предусмотрены следующие вопросы, задания текущего контроля:

- ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях

Студент должен знать:

средства и методы хранения и передачи аутентификационной информации; механизмы реализации атак в сетях TCP/IP; основные протоколы идентификации и аутентификации абонентов сети; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений

Вопросы, задания:

1. Перечислите этапы программы аудита информационной безопасности.

2. Перечислите действующие стандарты и руководства по аудиту информационной безопасности.

3. Дайте определение: анализ рисков организации, угрозы и уязвимости объекта информатизации.

Студент должен уметь:

формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты

Задания:

1. Составьте программу аудита информационной безорасности для выделенного помещения
2. С помощью модели информационных потоков провести анализ рисков организации
3. С помощью модели анализа угроз и уязвимостей провести анализ рисков организации

Студент должен владеть навыками:

настройки межсетевых экранов; владеет методиками анализа сетевого трафика

Задания:

1. Провести аудит средств межсетевого экранирования.
2. Настроить средство межсетевого экранирования в соответствии с заданными требованиями безопасности.
3. Настроить политику межсетевого экрана.

8.3. Вопросы промежуточной аттестации

Десятый семестр (Экзамен)

1. Процессный подход и информационная безопасность
2. Цели контроля и проверки процессов и систем
3. Программа аудита информационной безопасности
4. Стандарты и руководства по аудиту информационной безопасности
5. Понятия аудита иформационной безопасности
6. Виды аудита информационной безопасности
7. Внутренний и внешний аудит
8. Основные нормативные правовые акты
9. Способы проведения аудита информационной безопасности
10. Данные необходимые для проведени аудита информационной безопасности
11. Методика проведения аудита информационной безопасности
12. Средства проведения аудита информационной безопасности
13. Оценка уровня бузопасности
14. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга)
15. Международный стандарт ISO 17799
16. Система КОНДОР
17. Выработка рекомендаций и подготовка отчетных документов
18. Экономическая оценка обеспечения ИБ
19. Назначение стандарта ISO 17799 для управления информационной безопасностью
20. Стандарты по безопасности информационных технологий в России

8.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Промежуточная аттестация обучающихся ведется непрерывно и включает в себя:

для дисциплин, завершающихся (согласно учебному плану) зачетом/зачетом с оценкой (дифференцированным зачетом), – текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и оценивание окончательных результатов обучения по дисциплине;

для дисциплин, завершающихся (согласно учебному плану) экзаменом, – текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и семестровую аттестацию (экзамен) – оценивание окончательных результатов обучения по дисциплине.

По дисциплинам, завершающимся зачетом/зачетом с оценкой, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 100 баллов.

Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля.

По дисциплинам, завершающимся экзаменом, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 60 баллов.

Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля и количества баллов, набранных на семестровой аттестации (экзамене).

Система оценивания.

В соответствии с Положением о балльно-рейтинговой системе оценки успеваемости обучающихся Волгоградского государственного университета предусмотрена возможность предоставления студентам выполнения дополнительных заданий повышенной сложности (не включаемых в перечень обязательных и, соответственно, в перечень обязательного текущего контроля успеваемости) и получения за выполнение таких заданий «премиальных» баллов, - для поощрения обучающихся, демонстрирующих выдающие способности.

Оценка качества освоения образовательной программы включает текущий контроль успеваемости, промежуточную аттестацию обучающихся и государственную итоговую аттестацию выпускников.

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на протяжении семестра. К основным формам текущего контроля можно отнести:

Форма текущего контроля: Контрольная работа

контрольные работы применяются для оценки знаний, умений, навыков по дисциплине или ее части. Контрольная работа, как правило, состоит из небольшого количества средних по трудности вопросов, задач или заданий, требующих поиска обоснованного ответа. Может занимать часть или полное учебное занятие с разбором правильных решений на следующем занятии.

Форма текущего контроля: Устный опрос, собеседование

устный опрос, собеседование являются формой оценки знаний и предполагают специальную беседу преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной. Процедуры направлены на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме и т.п.

Форма текущего контроля: Письменные задания или лабораторные работы

письменные задания являются формой оценки знаний и предполагают подготовка письменного ответа, решение специализированной задачи, выполнение теста. являются формами контроля и средствами применения и реализации полученных обучающимися знаний, умений и навыков в ходе выполнения учебно-практической задачи, связанной с получением значимого результата с помощью реальных средств деятельности. Рекомендуются для проведения в рамках тем (разделов), наиболее значимых в формировании компетенций. Тест является простейшей формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин. Тест состоит из небольшого количества элементарных задач; может предоставлять возможность выбора из перечня ответов; занимает часть учебного занятия (10–30 минут); правильные решения разбираются на том же или следующем занятии; частота тестирования определяется преподавателем.

Промежуточная аттестация, как правило, осуществляется в конце семестра и может завершать изучение, как отдельной дисциплины, так и ее раздела (разделов) /модуля (модулей). Промежуточная аттестация помогает оценить более крупные совокупности знаний, умений и навыков, в некоторых случаях – даже формирование определенных компетенций.

К формам промежуточного контроля можно отнести:

Форма промежуточной аттестации: Экзамен

экзамен по дисциплине или ее части имеет цель оценить сформированность компетенций, теоретическую подготовку студента, его способность к творческому мышлению, приобретенные им навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач. Форма проведения, как правило, предусматривает ответы на вопросы экзаменационного билета, выполнение которых направленно на проверку сформированности компетенций по соответствующей учебной дисциплине.

Методика формирования результирующей оценки:

Десятый семестр

1. Контрольная работа - от 0 до 0 баллов
2. Устный опрос, собеседование - от 0 до 0 баллов
3. Письменные задания или лабораторные работы - от 0 до 0 баллов
4. Экзамен - от 0 до 40 баллов

9. Перечень основной и дополнительной учебной литературы

9.1 Основная литература

1. Шаньгин Владимир Федорович Информационная безопасность компьютерных систем и сетей [Электронный ресурс]: учебное - ФОРУМ, 2017. - 416 с. - Режим доступа: http://new.znanium.com/go.php?id=775200

2. Баранова Елена Константиновна Информационная безопасность и защита информации [Электронный ресурс]: учебное - Издание перераб. и доп. - РИОР, 2018. - 336 с. - Режим доступа: http://new.znanium.com/go.php?id=957144

9.2 Дополнительная литература

1. Бирюков Андрей Александрович Информационная безопасность: защита и нападение [Электронный ресурс]: - Издание 2 - ДМК Пресс, 2017. - 434 с. - Режим доступа: http://znanium.com/go.php?id=1028060

2. Васильева Т.Ю., Куприянов А.И., Мельников В.П. Информационная безопасность [Электронный ресурс]: учебное - КноРус, 2018. - Режим доступа: http://www.book.ru/book/929884

В качестве учебно-методического обеспечения могут быть использованы другие учебные, учебно-методические и научные источники по профилю дисциплины, содержащиеся в электронно-библиотечных системах, указанных в п. 11.2 «Электронно-библиотечные системы».

9.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://lib.volsu.ru - Электронная библиотека Волгоградского государственного университета

10.Методические указания по освоению дисциплины для лиц с ОВЗ и инвалидов

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по индивидуальной траектории в рамках индивидуального учебного плана (при необходимости), изучение данной дисциплины базируется на следующих возможностях:
- индивидуальные консультации преподавателя;
- максимально полная презентация содержания дисциплины в ЭИОС (в частности, полнотекстовые лекции, презентации, аудиоматериалы, тексты для перевода и анализа и т.п.).

11. Перечень информационных технологий

В учебном процессе активно используются информационные технологии с применением современных средств телекоммуникации; электронные учебники и обучающие компьютерные программы. Каждый обучающийся обеспечен неограниченным доступом к электронной информационно-образовательной среде (ЭИОС) университета. ЭИОС предоставляет открытый доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к электронным библиотечным системам и электронным образовательным ресурсам.

11.1 Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)

Программное обеспечение:
1. Microsoft Windows 7 Professional, 11 лицензий, номер 60357707
2. Microsoft Windows 7 Home Premium, 1 лицензия, OEM-лицензия
3. Microsoft Windows 8.1 Home, 1 лицензия OEM-лицензия
4. Microsoft Office 2007 Standart, 1 лицензия, номер 43847745
5. Microsoft Office 2016, 1 лицензия, Сублицензионный договор No 31604241628 от 21.11.16
6. LibreOffice 12 лицензий (свободно-распространяемое программное обеспечение)
7. FreeBSD, 1 лицензия FreeBSD license свободное программное обеспечение
8. Oracle VM VirtualBox, 14 лицензий GNU GPL свободное программное обеспечение
9. Mozila FireFox, 13 лицензий Mozilla Public License 2.0 (MPL) свободное программное обеспечение
10. Visual Studio Community 2017, 13 лицензий, учебное программное обеспечение
11. Python 2.7, 13 лицензий PSFL (свободно-распространяемое программное обеспечение)

11.2 Современные профессиональные базы данных и информационно-справочные системы, в т.ч. электронно-библиотечные системы
(обновление выполняется еженедельно)

Название	Краткое описание	URL-ссылка
Научная электронная библиотека	Крупнейший российский информационный портал в области науки, технологии, медицины и образования.	http://elibrary.ru/
ЭБС "Лань"	Электронно-библиотечная система	https://e.lanbook.com/

ЭБС Znanium.com	Электронно-библиотечная система	https://znanium.com/
ЭБС BOOK.ru	Электронно-библиотечная система	https://www.book.ru/
ЭБС Юрайт	Электронно-библиотечная система	https://www.biblio-online.ru/
Scopus	Scopus – крупнейшая единая база данных, содержащая аннотации и информацию о цитируемости рецензируемой научной литературы, со встроенными инструментами отслеживания, анализа и визуализации данных. В базе содержится 23700 изданий от 5000 международных издателей, в области естественных, общественных и гуманитарных наук, техники, медицины и искусства.	http://www.scopus.com/
Web of Science	Наукометрическая реферативная база данных журналов и конференций. С платформой Web of Science вы можете получить доступ к непревзойденному объему исследовательской литературы мирового класса, связанной с тщательно отобранным списком журналов, и открыть для себя новую информацию при помощи скрупулезно записанных метаданных и ссылок.	https://apps.webofknowledge.com/
КонсультантПлюс	Информационно-справочная система	http://www.consultant.ru/
Гарант	Информационно-справочная система по законодательству Российской Федерации	http://www.garant.ru/
Научная библиотека ВолГУ им О.В. Иншакова		http://library.volsu.ru/

12. Материально-техническое обеспечение дисциплины

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, лабораторного типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и
промежуточной аттестации.
Специализированная мебель:
1. Столы – 8 шт.
2. стулья – 16 шт.
3. парта со скамьей – 8 шт.
4. рабочее место преподавателя (стол и стул) – 1 шт.
Демонстрационное оборудование:
1. Проектор BenQ MX 505
2. Экран проекционный
3. Доска (магнитная, маркерная)
Рабочие места на базе вычислительной техники (18 шт):
1.Моноблок VPS 5000 (16 шт.);
2. Ноутбук Acer AS5738G;
3. Ноутбук HP Pavilion экран 15,6” Intel Pentium N3540.
Сетевое оборудование:
1. Wi-Fi роутер ASUS RT-N10
2. Концентратор.
3. Комплекс "Сетевое оборудование "Cisco" часть 1

Специализированная мебель:

1. парта со скамьей – 40 шт.
2. учебные места – 80 шт.
3. рабочее место преподавателя (стол и стул) – 1 шт.

Демонстрационное оборудование:

1. Доска (магнитная, меловая)
2. Мультимедийное оборудование