МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ФИТКБ

_____/Гусев П.Ю./

28.02.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Методическое обеспечение анализа защищенности информационных систем и сетей»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация специализация N 7 "Анализ безопасности информационных систем"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2023

Автор программы _____ К.А. Разинкин

Заведующий кафедрой Систем информационной безопасности _____ А.Г. Остапенко

Руководитель ОПОП _____ А.Г. Остапенко

Воронеж 2023

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины овладение принципами и методами организа-

ции процесса анализа защищенности автоматизированной системы и сетей, методиками применяется для определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях, отнесенных к государственным и муниципальным информационным системам, информационным системам персональных данных, значимым объектам критической информационной инфраструктуры Российской Федерации.

1.2. Задачи освоения дисциплины

- сформировать у студентов способность применения методов научных исследований при проведении разработок в области защиты информации в автоматизированных системах, в частности для процесса анализа защищенности автоматизированной системы и сетей
- способствование развитию навыков разработки методик и тестов для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Методическое обеспечение анализа защищенности информационных систем и сетей» относится к дисциплинам обязательной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Методическое обеспечение анализа защищенности информационных систем и сетей» направлен на формирование следующих компетенций:

ОПК-8 - Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах;

ОПК-7.2. - Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации;

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**
ОПК-8	знать методологические основы научных исследований при проведении разработок в области защиты информации в автоматизированных системах
	уметь обрабатывать результаты научных исследований в части анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации
ОПК-7.2.	знать содержание, порядок подготовки и выполнения работ по обеспечению анализа защищенности информационных систем и сетей в соответствии с ти-

	повой методикой анализа защищенности информационных систем и сетей и законодательной и нормативной базой аудита иб
	уметь разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Методическое обеспечение анализа защищенности информационных систем и сетей» составляет 9 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры	
		9	10
Аудиторные занятия (всего)	144	72	72
В том числе:			
Лекции	72	36	36
Практические занятия (ПЗ)	72	36	36
Самостоятельная работа	180	72	108
Курсовой проект	+		+
Виды промежуточной аттестации - зачет, зачет с оценкой	+	+	+
Общая трудоемкость: академические часы зач.ед.	 324 9	 144 4	 180 5

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	СРС	Всего, час
	Базовые сведения о проверке и оценке уровня безопасности компьютерных систем	Проверки и оценки уровня ИБ организации. Оценка уязвимостей компьютерной системы Разновидности проверок и оценок уровня ИБ организации. Рынок аналитических услуг в сфере ИБ. Место и роль аудита в модели обеспечения ИБ.	12	12	30	54
	Оценка уровня безопасности компьютерных систем: общие понятия и определения	Оценка уровня безопасности компьютерных систем: общие понятия и определения Базовые определения. Принципы и формы аудита ИБ организации Оценка уязвимостей компьютерной системы Особенности автоматизированных информационных систем как объектов аудита ИБ. Исходная концептуальная схема (пара-	12	12	30	54

		дигма) проведения аудита ИБ.				
	Типовая методика анализа защищенности информационных систем и сетей	Изучение исходных данных по АС; оценка рисков, связанных с наличием угроз безопасности в отношении ресурсов АС; анализ механизмов организационного уровня, политики; безопасности организации и организационно-распорядительной документации и оценка их соответствия требованиям существующих нормативных документов, а также их адекватности существующим рискам; ручной анализ конфигурационных файлов маршрутизаторов, межсетевых экранов (МЭ) и прокси-серверов, осуществляющих управление межсетевыми взаимодействиями, почтовых и DNS-серверов, а также других критических элементов сетевой инфраструктуры; сканирование внешних сетевых адресов локальной вычислительной системы (ЛВС) из сети Интернет; сканирование ресурсов ЛВС изнутри; анализ конфигурации серверов и рабочих станций ЛВС при помощи специализированных программных средств.	12	12	30	54
	Законодательная и нормативная база аудита ИБ.	Структура международных стандартов по ИБ. Область применения. Процессная модель управления ИБ. Оценка зрелости системы управления ИБ. Стандарты проведения оценки уровня безопасности компьютерных систем Структура международных стандартов по ИБ. Область применения. Процессная модель управления ИБ. Оценка зрелости системы управления ИБ. ISO 27001 (В 7799 - 2:2005). ISO 27002 (BS 7799 - 1:2005). Стандарты ISO/IEC и ГОСТ ИСО/МЭК 27005, BS 7799-3. Анализ рисков ИБ. Общие критерии (ГОСТ Р ИСО/МЭК 15408). Руководящие документы ФСТЭК России аудит в целях сертификации средств защиты и аттестации объектов нформатизации.Ста Банка России СТО БР ИББС-CoBit. Стандарт аудита PCI DSS. Соответствие и взаимодействие международного и российского подходов и методов аудита безопасности. Стандарт аудита PCI DSS.	12	12	30	54
	Методология оценки уровня безопасности компьютерных систем. Организация процесса оценки уровня безопасности компьютерных систем.	Основные этапы и методы работ по проведению аудита ИБ. Программа аудита ИБ. Основные этапы и методы работ по проведению аудита ИБ. Программа аудита ИБ. Сбор свидетельств (исходной информации) для проведения аудита ИБ. Рекомендации по планированию аудита ИБ. Рекомендации по моделированию. Этапы проведения внутреннего и внешнего аудитов ИБ: общее и различия. Стадии аудита ИБ: планирование; подготовка; моделирование; тестирование; анализ; разработка предложений, документирование. Договор о проведении внешнего аудита ИБ. Порядок планирования аудита. Методы аудита:	12	12	30	54

		экспертно-аналитические; экспертно-инструментальные; моделирование действий злоумышленника. Методы сбора исходных данных: опрос, наблюдение, анализ. Методы анализа собранных свидетельств. Аудиторская группа: состав, права и обязанности, роли, привлечение технических специалистов. Обязанности проверяемой организации во время аудита ИБ.				
	Инструментальные средства оценки уровня безопасности компьютерных систем	Методы и инструментальные средства проведения аудита ИБ. Программные средства анализа и управления. Оценка уязвимостей компьютерной системы средствами Dallas Lock. Инструментарий базового уровня - справочные и методические материалы. Инструментарий для обеспечения повышенного уровня безопасности. ПО идентификации и оценки защищаемых ресурсов, угроз, уязвимостей и мер защиты в сфере компьютерной и физической безопасности предприятия. СОВ, их применение и примеры систем. Сохранение доказательств вторжений. Стандарты в области обнаружения вторжений.	12	12	30	54
		Итого	**72**	**72**	**180**	**324**

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины предусматривает выполнение курсовых проектов в 10 семестрах для очной формы обучения.

Примерная тематика курсового проекта: «Разработка формализованной модели угроз информационной безопасности на предприятии»

Задачи, решаемые при выполнении курсового проекта:

1. Осуществление постоянного и непрерывного прогнозирования угроз.
2. Обоснование выводов и реализации эффективных методов создания, развития и совершенствования системы информационной безопасности.
3. Непрерывное управления системой информационной безопасности и контроля над ней.
4. Объединение в единый, целостный механизм средств и методов, обеспечивающих информационную безопасность и эффективность использования информационных ресурсов.

Курсовой проект включат в себя графическую часть и расчетно-пояснительную записку.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

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

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-8	знать методологические основы научных исследований при проведении разработок в области защиты информации в автоматизированных системах	знание методологических основ научных исследований при проведении разработок в области защиты информации в автоматизированных системах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь обрабатывать результаты научных исследований в части анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации	умение обрабатывать результаты научных исследований в части анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ОПК-7.2.	знать содержание, порядок подготовки и выполнения работ по обеспечению анализа защищенности информационных систем и сетей в соответствии с типовой методикой анализа защищенности информационных систем и сетей и законодательной и нормативной базой аудита иб	знание содержание, порядок подготовки и выполнения работ по обеспечению анализа защищенности информационных систем и сетей в соответствии с типовой методикой анализа защищенности информационных систем и сетей и законодательной и нормативной базой аудита иб	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации	умение разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 9, 10 семестре для очной формы обучения по двух/четырехбалльной системе:

«зачтено»

«не зачтено».

Компетенция	Результаты обучения, характеризующие	Критерии оценивания	Зачтено	Не зачтено

	сформированность компетенции			
ОПК-8	знать методологические основы научных исследований при проведении разработок в области защиты информации в автоматизированных системах	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь обрабатывать результаты научных исследований в части анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ОПК-7.2.	знать содержание, порядок подготовки и выполнения работ по обеспечению анализа защищенности информационных систем и сетей в соответствии с типовой методикой анализа защищенности информационных систем и сетей и законодательной и нормативной базой аудита иб	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

или
«отлично»;
«хорошо»;
«удовлетворительно»;
«неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-8	знать методологические основы научных исследований при проведении разработок в области защиты информации в автоматизированных системах	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов

	уметь обрабатывать результаты научных исследований в части анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ОПК-7.2.	знать содержание, порядок подготовки и выполнения работ по обеспечению анализа защищенности информационных систем и сетей в соответствии с типовой методикой анализа защищенности информационных систем и сетей и законодательной и нормативной базой аудита иб	Тест	Выполнение теста на 90-100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1) Содержит ли «Протокол аттестационных испытаний ОИ на соответствие требованиям по ЗИ от несанкционированного доступа» данные о средствах контроля защищенности информации?

Ответ:

(1) Да

(2) Нет

2) Какие разделы включает в себя «Заключение по результатам аттестационных испытаний ОИ на соответствие требованиям по безопасности информации»?

Ответ:

(1) Условия и порядок проведения аттестационных испытаний

(2) Замечания и рекомендации по результатам аттестационных испытаний

(3) Проверка подсистемы управления доступом

(4) Анализ исходных данных об объекте информатизации

3) Какие разделы включает в себя «Протокол аттестационных испытаний объекта информатизации на соответствие требованиям по защите информации от несанкционированного доступа»?

Ответ:

(1) Проверка подсистемы обеспечения целостности

(2) Анализ условий размещения объекта информатизации

(3) Анализ выполнения требований по защите информации на объекте информатизации от утечки по техническим каналам

(4) Замечания и рекомендации по результатам аттестационных испытаний

4) Как называется мера доверия, которая может быть оказана архитектуре, инфраструктуре, программно-аппаратной реализации системы и методам управления её конфигурацией и целостностью?

Ответ:

(1) эффективность безопасности

(2) гарантированность безопасности

(3) непрерывность безопасности

(4) надежность безопасности

5) При проведении тестового преодоления защиты внешними аудиторами договор с заказчиком таких услуг должен предусматривать:

Ответ:

(1) конкретный детализированный план тестового проникновения

(2) порядок уведомления всех заинтересованных сотрудников предприятия-заказчика о предстоящем тестовом проникновении

(3) снятие ответственности с аудитора за возможный ущерб, который может быть нанесен в процессе такого проникновения

6) К негативным факторам, ограничивающим передачу на аутсорсинг функций по обеспечению информационной безопасности, относятся:

Ответ:

(1) высокий уровень затрат на услуги, предоставляемыми сторонними организациями-поставщиками услуг

(2) доступ предприятия-поставщика услуг к конфиденциальной информации

(3) потенциальная возможность перехвата и утечки информации в процессе оказания услуг сторонней организацией

7) Как в методике FRAP осуществляется определение защищаемых активов?

Ответ:

(1) по результатам заполнения опросных листов и автоматизированного анализа (сканирования) сетей

(2) по результатам изучения документации на систему

(3) по результатам заполнения опросных листов, изучения документации на систему, использования инструментов автоматизированного анализа (сканирования) сетей

8) Что из перечисленного характерно для методики OCTAVE?

Ответ:

(1) весь процесс анализа автоматизирован, производится на основании параметрических функций

(2) весь процесс анализа производится силами сотрудников организации, без привлечения внешних консультантов

(3) весь процесс анализа производится силами внешних консультантов, без привлечения сотрудников организации

9) Какие из перечисленных критериев оценки и управления рисками используются в методике RiskWatch?

Ответ:

(1) годовые потери (Annual Loss Expectancy, ALE) и оценка возврата инвестиций (Return on Investment, ROI)

(2) угрозы, исходящие от человека-нарушителя, действующего через сеть передачи данных

(3) влияние потерь на HR - аспект деятельности организации

10) При вычислении вероятности влияния результирующий уровень вероятности определяется на основании двух значений. Первое значение определяет вероятность существования уязвимости в текущей среде. Что определяет второе значение?

Ответ:

(1) изменения останова сервера по причине физического износа оборудования

(2) вероятность существования уязвимости исходя из эффективности текущих элементов контроля

(3) вероятность существования уязвимости при гипотетических параметрах системы

7.2.2 Примерный перечень заданий для решения стандартных задач

1) Какие программные средства используются для анализа защищенности операционных систем Microsoft

Ответ:

(1) MBSA

(2) PowerChute

(3) XSpider 7.0

2) Содержит ли «Заключение по результатам аттестационных испытаний ОИ на соответствие требованиям по безопасности информации» рекомендации по ЗИ на ОИ в ходе его эксплуатации?

Ответ:

(1) Да

(2) Нет

3) Каким термином обозначается анализ регистрационной информации системы защиты?

Ответ:

(1) мониторинг

(2) аудит

(3) аккредитация

(4) сертификация

4) Назовите основные функции систем анализа защищенности

Ответ:

(1) обнаружение уязвимостей в сетевой инфраструктуре

(2) анализ и предоставление рекомендаций по устранению уязвимостей

(3) предоставление различных отчетов

5) Что можно отнести к системам анализа защищенности

Ответ:

(1) XSpider

(2) Internet

(3) Nessus

6) В каком случае система анализа защищенности пытается определить наличие уязвимости без фактического подтверждения ее наличия

Ответ:

(1) идентификация

(2) сканирование

(3) зондировани

7) В каком случае система анализа защищенности имитирует ту атаку, которая использует проявленную уязвимость

Ответ:

(1) идентификация

(2) сканирование

(3) зондирование

8) Какой метод позволяет делать вывод об уязвимостях, опираясь на информацию в заголовке ответа на запрос сканера безопасности

Ответ:

(1) проверка заголовков

(2) активные зондирующие проверки

(3) имитация атак

9) Какой метод позволяет убедиться, присутствует или нет на анализируемом ПК уязвимость

Ответ:

(1) идентификация

(2) сканирование

(3) зондирование

10) Какой метод сравнивает фрагменты сканируемого программного обеспечения с сигнатурой известной уязвимости, хранящейся в базе данных системы анализа защищенности

Ответ:

(1) проверка заголовков

(2) активные зондирующие проверки

(3) имитация атак

7.2.3 Примерный перечень заданий для решения прикладных задач

1) Какой метод основан на использовании различных дефектов в программном обеспечении и реализует подход зондирования

Ответ:

(1) проверка заголовков

(2) активные зондирующие проверки

(3) имитация атак

2) Какой метод реализует подход сканирования

Ответ:

(1) проверка заголовков

(2) активные зондирующие проверки

(3) имитация атак

3) Что можно отнести к активным зондирующим проверкам

Ответ:

(1) анализ заголовков почтовой программы

(2) проверка контрольных сумм

(3) проверка даты сканируемого ПО

4) Назовите основные функции MBSA

Ответ:

(1) обнаружение основных уязвимостей

(2) проверка наличия рекомендованных к установке обновлений системы безопасности

(3) автоматизаци работы планировщика сканирования

5) Какая проверка MBSA выводит настройки реестра, запрещающие анонимным пользователям просмотр списка учетных записей

Ответ:

(1) Macro Security

(2) Parent Paths

(3) Restrict Anonymous

6) Системы анализа защищенности помогают предотвратить:

Ответ:

(1) известные атаки

(2) новые виды атак

(3) нетипичное поведение пользователей

7) Системы анализа защищенности выявляют уязвимости путем:

Ответ:

(1) диалогов с пользователями

(2) пассивного анализа

(3) активного опробования

8) Согласно стандарту X.700, в число функций управления безопасностью входят:

Ответ:

(1) создание инцидентов

(2) реагирование на инциденты

(3) устранение инцидентов

9) Выделите утверждение, верное в отношении защиты сетей.

Ответ:

(1) уровень защищенности сети определяется уровнем защищенности ее самого «сильного» звена

(2) уровень защищенности сети определяется суммой уровней защищенности ее звеньев

(3) уровень защищенности сети определяется уровнем защищенности ее самого «слабого» звена

(4) уровень защищенности сети не зависит напрямую от защищенности ее отдельных звеньев

10) Чем характеризуется степень сопротивляемости механизма защиты?

Ответ:

(1) вероятностью его преодоления

(2) количеством угроз, которым этот механизм препятствует

(3) величиной потерь в случае успешного прохождения

(4) стоимостью механизма защиты

7.2.4 Примерный перечень вопросов для подготовки к зачету

Проверки и оценки уровня ИБ организации. Оценка уязвимостей компьютерной системы

Разновидности проверок и оценок уровня ИБ организации. Рынок аналитических услуг в сфере ИБ. Место и роль аудита в модели обеспечения ИБ.

Оценка уровня безопасности компьютерных систем: общие понятия и определения

Базовые определения. Принципы и формы аудита ИБ организации

Оценка уязвимостей компьютерной системы

Особенности автоматизированных информационных систем как объектов аудита ИБ.

Исходная концептуальная схема (парадигма) проведения аудита ИБ.

Изучение исходных данных по АС; оценка рисков, связанных с наличием угроз безопасности в отношении ресурсов АС; анализ механизмов организационного уровня, политики; безопасности организации и организационно-распорядительной документации и оценка их соответствия требованиям существующих нормативных документов, а также их адекватности существующим рискам; ручной анализ конфигурационных файлов маршрутизаторов, межсетевых экранов (МЭ) и прокси-серверов, осуществляющих управление межсетевыми взаимодействиями, почтовых и DNS-серверов, а также других критических элементов сетевой инфраструктуры; сканирование внешних сетевых адресов локальной вычислительной системы (ЛВС) из сети Интернет; сканирование ресурсов ЛВС изнутри; анализ конфигурации серверов и рабочих станций ЛВС при помощи специализированных программных средств.

7.2.5 Примерный перечень заданий для решения прикладных задач

Структура международных стандартов по ИБ. Область применения. Процессная модель управления ИБ. Оценка зрелости системы управления ИБ. Стандарты проведения оценки уровня безопасности компьютерных систем

Структура международных стандартов по ИБ. Область применения. Процессная модель управления ИБ. Оценка зрелости системы управления ИБ. ISO 27001 (В 7799 - 2:2005). ISO 27002 (BS 7799 - 1:2005). Стандарты ISO/IEC и ГОСТ ИСО/МЭК 27005, BS 7799-3. Анализ рисков ИБ. Общие критерии (ГОСТ Р ИСО/МЭК 15408). Руководящие документы ФСТЭК России аудит в целях сертификации средств защиты и аттестации объектов нформатизации.Ста Банка России СТО БР ИББС- CoBit. Стандарт аудита PCI DSS. Соответствие и взаимодействие международного и российского

подходов и методов аудита безопасности.

Стандарт аудита PCI DSS. Основные этапы и методы работ по проведению аудита ИБ. Программа аудита ИБ. Основные этапы и методы работ по проведению аудита ИБ. Программа аудита ИБ. Сбор свидетельств (исходной информации) для проведения аудита ИБ. Рекомендации по планированию аудита ИБ. Рекомендации по моделированию. Этапы проведения внутреннего и внешнего аудитов ИБ: общее и различия. Стадии аудита ИБ: планирование; подготовка; моделирование; тестирование; анализ; разработка предложений, документирование. Договор о проведении внешнего аудита ИБ. Порядок планирования аудита. Методы аудита: экспертно-аналитические; экспертно-инструментальные; моделирование действий злоумышленника. Методы сбора исходных данных: опрос, наблюдение, анализ. Методы анализа собранных свидетельств. Аудиторская группа: состав, права и обязанности, роли, привлечение технических специалистов. Обязанности проверяемой организации во время аудита ИБ.

Методы и инструментальные средства проведения аудита ИБ. Программные средства анализа и управления. Оценка уязвимостей компьютерной системы средствами Dallas Lock.

Инструментарий базового уровня - справочные и методические материалы. Инструментарий для обеспечения повышенного уровня безопасности. ПО идентификации и оценки защищаемых ресурсов, угроз, уязвимостей и мер защиты в сфере компьютерной и физической безопасности предприятия. СОВ, их применение и примеры систем. Сохранение доказательств вторжений. Стандарты в области обнаружения вторжений.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Базовые сведения о проверке и оценке уровня безопасности компьютерных систем	ОПК-8, ОПК-7.2.	Тест, защита практических работ, требования к курсовому проекту
2	Оценка уровня безопасности компьютерных систем: общие понятия и определения	ОПК-8, ОПК-7.2.	Тест, защита практических работ, требования к курсовому проекту

3	Типовая методика анализа защищенности информационных систем и сетей	ОПК-8, ОПК-7.2.	Тест, защита практических работ, требования к курсовому проекту
4	Законодательная и нормативная база аудита ИБ.	ОПК-8, ОПК-7.2.	Тест, защита практических работ, требования к курсовому проекту
5	Методология оценки уровня безопасности компьютерных систем. Организация процесса оценки уровня безопасности компьютерных систем.	ОПК-8, ОПК-7.2.	Тест, защита практических работ, требования к курсовому проекту
6	Инструментальные средства оценки уровня безопасности компьютерных систем	ОПК-8, ОПК-7.2.	Тест, защита практических работ, требования к курсовому проекту проекту

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

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Защита курсовой работы, курсового проекта или отчета по всем видам практик осуществляется согласно требованиям, предъявляемым к работе, описанным в методических материалах. Примерное время защиты на одного студента составляет 20 мин.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература

1. Бондарев, В. В. Анализ защищенности и мониторинг компьютерных сетей. Методы и средства : учебное пособие / В. В. Бондарев. — Москва : МГТУ им. Н.Э. Баумана, 2017. — 228 с. — ISBN 978-5-7038-4757-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103518

2. Колегов, Д. Н. Лабораторный практикум по основам анализа защищенности веб-приложений : учебное пособие / Д. Н. Колегов. — Томск : ТГУ, 2014. — 59 с. — Текст : электронный // Лань : электронно-библиотечная си-

стема. — URL: https://e.lanbook.com/book/76815

Дополнительная литература

1. Золотарев, В. В. , Федорова, Н.А. З 80 Анализ защищенности автоматизированных систем: Учебное пособие / В. В. Золотарев, Н. А. Федорова; СибГАУ. – Красноярск, 2007. – 93 с.

https://www.studmed.ru/view/zolotarev-vv-fedorova-na-analiz-zaschischennosti-avtomatizirovannyh-sistem_8fe5e8ab036.html

2. Вострецова, Е.В. В78 Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019.— 204 с.

https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

http://att.nica.ru
http://www.edu.ru/
http://window.edu.ru/window/library
http://www.intuit.ru/catalog/
http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp
https://cchgeu.ru/education/cafedras/kafsib/?docs
http://www.eios.vorstu.ru
http://e.lanbook.com/ (ЭБС Лань)
http://IPRbookshop.ru/ (ЭБСIPRbooks)

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой.

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Методическое обеспечение анализа защищенности информационных систем и сетей» читаются лекции, проводятся практические занятия, выполняется курсовой проект.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Практические занятия направлены на приобретение практических

навыков расчета

– Оценка угроз информационной безопасности.
– Актуальные угрозы.
– Способы реализации угроз ИБ. Действия по реализации угроз ИБ.
– Стандарты оценки угроз ИБ.

Занятия проводятся путем решения конкретных задач в аудитории.

Методика выполнения курсового проекта изложена в учебно-методическом пособии. Выполнять этапы курсового проекта должны своевременно и в установленные сроки.

Контроль усвоения материала дисциплины производится проверкой курсового проекта, защитой курсового проекта.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом, зачетом с оценкой три дня эффективнее всего использовать для повторения и систематизации материала.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП
1	2	3	4