МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета _____ Гусев П.Ю.

«31» августа 2021 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Анализ уязвимостей компьютерных систем и сетей»

Специальность 10.05.01 Компьютерная безопасность

Специализация специализация № 4 "Безопасность компьютерных систем и сетей (связь, информационные и коммуникационные технологии)"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2021

Автор программы _____ /Соколова Е.С./

Заведующий кафедрой Систем информационной безопасности _____ /Остапенко А.Г./

Руководитель ОПОП _____ / Остапенко А.Г./

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины изучение студентом основных видов уязвимостей, методов и средств их анализа и устранения

1.2. Задачи освоения дисциплины

- ✓ формирование навыков экспертизы качества и надежности реализаций программных и программно-аппаратных средств обеспечения информационной безопасности;
- ✓ формирование навыков анализа программных реализаций на предмет наличия уязвимостей.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Анализ уязвимостей компьютерных систем и сетей» относится к дисциплинам части, формируемой участниками образовательных отношений блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Анализ уязвимостей компьютерных систем и сетей» направлен на формирование следующих компетенций:

ПК-4.5 - Способен анализировать уязвимости и угрозы информационной безопасности в компьютерных системах и сетях

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-4.5	знать классификацию и классификаторы основных критических программные и аппаратные уязвимости, а также регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России.
	уметь анализировать компьютерную систему с целью определения уровня защищённости и доверия и оценивает риски, связанные с осуществлением угроз безопасности в отношении компьютерной системы с последующим формированием предложений по устранению выявленных уязвимостей

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Анализ уязвимостей компьютерных 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)	126	54	72
В том числе:			
Лекции	72	36	36
Практические занятия (ПЗ)	54	18	36

Самостоятельная работа	126	18	108
Часы на контроль	72	36	36
Виды промежуточной аттестации - экзамен	+	+	+
Общая трудоемкость: академические часы зач.ед.	 324 9	 108 3	 216 6

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
1	Введение в анализ уязвимостей	Понятие угрозы и уязвимости и атаки. Классификация и классификаторы уязвимостей. Понятия "уязвимость кода", "уязвимость конфигурации", "уязвимость архитектуры", "организационная уязвимость", "многофакторная уязвимость". База данных общеизвестных уязвимостей информационной безопасности CVE (англ. Common Vulnerabilities and Exposures). Обзор банка данных угроз безопасности информации Федеральная служба по техническому и экспортному контролю ФСТЭК России. Регламент включения информации об уязвимостях программного обеспечения и программ- ноаппаратных средств в банк данных угроз безопасности информации ФСТЭК России. Стандарт Common Vulnerability Scoring System (CVSS). ГОСТ Р 56546-2015. ГОСТ Р 58142-2018 МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045 Классификация уязвимостей информационных систем. Классификация эксплойтов. Анализ стандартов и методик тестирования на проникновение. Уязвимости нулевого дня. Обзор наиболее распространенных и критических уязвимостей.	12	8	20	40
2	Аппаратные уязвимости	Аппаратная уязвимость категории утечка по стороннему каналу (Meltdown). Группа аппаратных уязвимостей – Spectre. Уязвимости микропрограмм в постоянных запоминающих устройствах, уязвимости микропрограмм в программируемых логических интегральных схемах, уязвимости базовой системы ввода-вывода, уязвимости ПО контроллеров управления, интерфейсов управления и другие уязвимости. Уязвимости в портативных технических средствах. уязвимости в сетевом (коммуникационном, телекоммуникационном) оборудовании. уязви-	12	8	20	40

		мости в средствах защиты информации.				
3	Программные уязвимости	Уязвимости в общесистемном (общем) ПО. Уязвимости в прикладном ПО. Уязвимости в специальном ПО	12	8	20	40
4	Методы и инструменты анализа уязвимостей в сфере информационной безопасности	Методы: экспертный и статистический анализ, анализ документации, сканирование уязвимостей, моделирование атак, тестирование на проникновение, визуализация данных. Методология тестирования на проникновение: разведка, сканирование и перечисление, получение доступа, повышение привелеги, поддержание доступа, заметание следов, составление отчёта. Получение отпечатка сбор информации: разведка по открытым источникам, использование общих ресурсов, запрос сведений о регистрации, анализ записей DNS, получение сведений о маршрутизации, автоматизированные инструменты для снятия отпечатков и сбора информации. Методы сканирования и уклонения: сканирование портов, сетевые сканеры, автоматическое сканирование уязвимостей. Тестирование web-приложений: веб-анализ, межсайтовые сценарии, SQL – иньекция. Тестирование беспроводных сетей на проникновение: разведка в беспроводной сети, инструменты тестирования, анализ беспроводного трафика. Мобильное тестирование на проникновение с Kali NetHunter. Инструменты анализа уязвимостей Kali Linux.	36	30	66	132
		Итого	**72**	**54**	**126**	**252**

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 не предусматривает выполнение курсового проекта (работы) или контрольной работы.

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
ПК-4.5	знать классификацию и классификаторы основных критических программные и аппаратные уязвимости, а	знание классификации и классификаторов основных критических программные и	Выполнение работ в срок, предусмотренный в рабочих про-	Невыполнение работ в срок, предусмотренный в рабочих

	также регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России.	аппаратные уязвимости, а также регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России.	граммах	программах
	уметь анализировать компьютерную систему с целью определения уровня защищённости и доверия и оценивает риски, связанные с осуществлением угроз безопасности в отношении компьютерной системы с последующим формированием предложений по устранению выявленных уязвимостей	умение анализировать компьютерную систему с целью определения уровня защищённости и доверия и оценивает риски, связанные с осуществлением угроз безопасности в отношении компьютерной системы с последующим формированием предложений по устранению выявленных уязвимостей	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 четырехбалльной системе:

«отлично»;

«хорошо»;

«удовлетворительно»;

«неудовлетворительно».

Компетенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Отлично**	**Хорошо**	**Удовл.**	**Неудовл.**
ПК-4.5	знать классификацию и классификаторы основных критических программные и аппаратные уязвимости, а также регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России.	Тест	Выполнение теста на 90- 100%	Выполнение теста на 80-90%	Выполнение теста на 70-80%	В тесте менее 70% правильных ответов
	уметь анализировать	Решение	Задачи ре-	Продемонстр	Проде-	Задачи не

	компьютерную систему с целью определения уровня защищённости и доверия и оценивает риски, связанные с осуществлением угроз безопасности в отношении компьютерной системы с последующим формированием предложений по устранению выявленных уязвимостей	стандартных практических задач	шены в полном объеме и получены верные ответы	ирован верный ход решения всех, но не получен верный ответ во всех задачах	монстр ирован верный ход решения в большинстве задач	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. Что такое эксплойт?

(1) компьютерная программа, нейтрализующая уязвимости в программном обеспечении

(2) компьютерная программа, использующая уязвимости в программном обеспечении и применяемая для проведения атаки на вычислительную систему

(3) компьютерная программа, содержащая уязвимости

2. К какому классу относится уязвимость, появившаяся в результате разработки программного обеспечения без учета требований по безопасности информации?

Ответ:

(1) уязвимость архитектуры

(2) уязвимость кода

(3) многофакторная уязвимость

3. К какому классу относится уязвимость, появившаяся в результате выбора, компоновки компонентов программного обеспечения, содержащих уязвимости?

(1) уязвимость архитектуры
(2) уязвимость кода
(3) многофакторная уязвимость

4. Common Vulnerabilities and Exposures (CVE) это…

(1) база данных угроз информационной безопасности
(2) база данных общеизвестных уязвимостей
(3) база данных эксплоитов
(4) база данных наиболее крупных атак на вычислительные системы в мире

5. Что такое CVE Numbering Authority (CNA)?

(1) идентификатор уязвимости
(2) организации, которым разрешено назначать CVE ID уязвимостям в согласованных за ними областях
(3) эксплоит уязвимости
(4) количество уязвимостей одного типа

6. Что такое Primary CAN?

(1) идентификатор уязвимости
(2) организации, которым разрешено назначать CVE ID уязвимостям в согласованных за ними областях
(3) эксплоит уязвимости
(4) организация, курирующая ведение CVE

7. Для чего используется CVSS?

(1) для оценки угроз
(2) для оценки потенциала нарушителя
(3) для оценки уязвимостей

8. Какая версия стандарта CVSS является актуальной?

(1) первая
(2) вторая
(3) третья
(4) четвертая

9. Какие метрики используются для оценки уязвимостей в CVSS?

(1) базовые
(2) стандартные
(3) контекстные
(4) временные
(5) постоянные

10.В описании угрозы в Банке данных угроз безопасности информации в качестве источника угрозы указаны…

(1) минимальные возможности внешнего или внутреннего нарушителя, необходимые для реализации угрозы
(2) максимальные возможности внешнего или внутреннего нарушителя, необходимые для реализации угрозы
(3) минимальные возможности внутреннего нарушителя, необходимые для реализации угрозы
(4) максимальные возможности внешнего нарушителя, необходимые для реализации угрозы

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Как в CVSS называются характеристики уязвимости, которые не зависят от среды и не меняются со временем?

базовые
контекстные
временные

2. Как в CVSS называются характеристики уязвимости, которые могут

измениться со временем?

базовые

контекстные

временные

4. Как в CVSS называются характеристики уязвимости, которые зависят от среды?

базовые

контекстные

временные

5. Какая базовая метрика CVSS отражает удаленность злоумышленника для использования уязвимости?

вектор атаки

сложность доступа

требуемые привилегии

масштаб

6. Какая базовая метрика CVSS показывает, могут ли отличаться уязвимый и атакуемый компоненты?

вектор атаки

сложность доступа

требуемые привилегии

масштаб

7. Какая базовая метрика CVSS отражает сложность реализации атаки?

вектор атаки

сложность доступа

требуемые привилегии

масштаб

8. Какая метрика CVSS отражает степень конфиденциальности информации о существовании уязвимости и достоверность известных технических деталей?

масштаб

степень достоверности отчета

уровень исправления

зрелость эксплойта

9. Какие метрики CVSS применяются, если аналитик хочет уточнить оценку уязвимости исходя из инфраструктуры и других параметров конкретной организации?

базовые

контекстные

временные

10. Какие метрики CVSS используются опционально?

базовые

контекстные

временные

11. Что содержит вектор уязвимости в CVSS?

итоговую численную оценку уязвимости

значения метрик для уязвимости

перечень метрик для уязвимости без их значений

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Что означает система защиты с полным перекрытием?

(1) для половины (и более) уязвимостей есть устраняющие барьеры
(2) для любой уязвимости есть устраняющий ее барьер
(3) у любой уязвимости есть риск ее реализации
(4) количество уязвимостей меньше, чем количество препятствующих им барьеров

2. При отсутствии в системе барьеров, «перекрывающих» выявленные уязвимости, степень сопротивляемости механизма защиты принимается равной...

(1) 0
(2) 1

3. Защищенность системы защиты определяется как величина…

(1) обратная суммарному количеству рисков
(2) обратная остаточному риску
(3) обратная уязвимости
(4) равная сумме всех уязвимостей

3. Что из нижеперечисленного относится к оперативным методам повышения безопасности?

(1) систематическое тестирование
(2) предотвращение ошибок в CASE-технологиях
(3) обязательная сертификация
(4) программная избыточность

4. Что из нижеперечисленного относится к мерам предотвращения угроз безопасности?

(1) систематическое тестирование
(2) предотвращение ошибок в CASE-технологиях
(3) обязательная сертификация
(4) программная избыточность

5. Выделите внешние по отношению к объекту уязвимости дестабилизирующие факторы и угрозы безопасности:

(1) ошибки персонала при эксплуатации
(2) ошибки программирования
(3) сбой и отказы аппаратуры ЭВМ
(4) ошибки алгоритмизации задач

6. Выделите внутренние по отношению к объекту уязвимости дестабилизирующие факторы и угрозы безопасности:

(1) ошибки персонала при эксплуатации
(2) ошибки программирования
(3) сбой и отказы аппаратуры ЭВМ
(4) ошибки алгоритмизации задач

7. На каких принципах должна строиться архитектура ИС?

(1) проектирование на принципе закрытых систем
(2) проектирование на принципе открытых систем
(3) усиление самого сильного звена
(4) усиление самого слабого звена
(5) эшелонирование обороны

8. Злоумышленники часто используют для атак:
(1) уязвимости Web-серверов
(2) уязвимости X-Window
(3) уязвимости почтовых серверов

10. Nessus - это:
Ответ:
(1) сканер портов
(2) сканер уязвимостей без встроенного сканера портов
(3) сканер уязвимостей со встроенным сканером портов

7.2.5 Примерный перечень заданий для решения прикладных задач

Понятие угрозы и уязвимости и атаки. Классификация и классификаторы уязвимостей. Понятия "уязвимость кода", "уязвимость конфигурации", "уязвимость архитектуры", "организационная уязвимость", "многофакторная уязвимость". База данных общеизвестных уязвимостей информационной безопасности CVE (англ. Common Vulnerabilities and Exposures). Обзор банка данных угроз безопасности информации Федеральная служба по техническому и экспортному контролю ФСТЭК России. Регламент включения информации об уязвимостях программного обеспечения и программ- но-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России. Стандарт Common Vulnerability Scoring System (CVSS). ГОСТ Р 56546-2015. ГОСТ Р 58142-2018 МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045 Классификация уязвимостей информационных систем. Классификация эксплойтов. Анализ стандартов и методик тестирования на проникновение. Уязвимости нулевого дня. Обзор наиболее распространенных и критических уязвимостей.

Аппаратная уязвимость категории утечка по стороннему каналу (Meltdown). Группа аппаратных уязвимостей – Spectre. Уязвимости микропрограмм в постоянных запоминающих устройствах, уязвимости микропрограмм в программируемых логических интегральных схемах, уязвимости базовой системы ввода-вывода, уязвимости ПО контроллеров управления, интерфейсов управления и другие уязвимости. Уязвимости в портативных технических средствах. уязвимости в сетевом (коммуникационном, телекоммуникационном) оборудовании. уязвимости в средствах защиты информации.

Уязвимости в общесистемном (общем) ПО. Уязвимости в прикладном ПО. Уязвимости в специальном ПО

Методы: экспертный и статистический анализ, анализ документации, сканирование уязвимостей, моделирование атак, тестирование на проникновение, визуализация данных. Методология тестирования на проникновение: разведка, сканирование и перечисление, получение доступа, повышение привелеги, поддержание доступа, заметание следов, составление отчёта. Получение отпечатка сбор информации: разведка по открытым источникам, использование общих ресурсов, запрос сведений о регистрации, анализ записей DNS, получение сведений о маршрутизации, автоматизированные инструменты для снятия отпечатков и сбора информации. Методы сканирования и уклонения: сканирование портов, сетевые сканеры, автоматическое сканирование уязвимостей. Тестирование web-приложений: веб-анализ, межсайтовые сценарии, SQL – иньекция. Тестирование беспроводных сетей на проникновение: разведка в беспроводной сети, инструменты тестирования, анализ беспроводного трафика. Мобильное тестирование на проникновение с Kali NetHunter. Инструменты анализа уязвимостей Kali Linux.

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

(Например: 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	Введение в анализ уязвимостей	ПК-4.5	Тест, защита практических работ
2	Аппаратные уязвимости	ПК-4.5	Тест, защита практических работ
3	Программные уязвимости	ПК-4.5	Тест, защита практических работ
4	Методы и инструменты анализа уязвимостей в сфере информационной безопасности	ПК-4.5	Тест, защита практических работ
5	Введение в анализ уязвимостей	ПК-4.5	Тест, защита практи-

			ческих работ
6	Аппаратные уязвимости	ПК-4.5	Тест, защита практических работ

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.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература

Информационная безопасность. Практические аспекты : учебник / Л. Х. Сафиуллина, А. Р. Касимова, Я. С. Рябов [и др.]. — Санкт-Петербург : Интермедия, 2021. — 240 с. — ISBN 978-5-4383-0205-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161340

Алѐшкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) : учебное пособие / А. С. Алѐшкин, С. А. Лесько, Д. О. Жуков. — Москва : РТУ МИРЭА, 2020. — 152 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167600

Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299

Дополнительная литература

Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Высшее образование). —

ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493262

Давидюк, Н. В. Мониторинг безопасности информационных систем : учебное пособие / Н. В. Давидюк, И. М. Космачева. — Санкт-Петербург : Интермедия, 2020. — 116 с. — ISBN 978-5-4383-0204-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161352

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)

Банк данных угроз безопасности информации. Электрон. дан. - Режим доступа: http://www.bdu.fstec.ru

Стандарт Common Vulnerabilities and Exposures. Электрон. дан. - Режим доступа: http://cve.mitre.org

База данных с информационными бюллетенями (Secunia Advisories), содержащими сведения об обнаруженных угрозах и уязвимостях ПО Secunia Advisory and Vulnerability Database Электрон. дан. - Режим доступа: https://secuniaresearch.flexerasoftware.com/community/advisories

База уязвимостей VND (Vulnerability Notes Database Электрон. дан. - Режим доступа: https://www.kb.cert.org/vuls

База сценариев эксплуатации уязвимостей Exploit Database Электрон. дан. - Режим доступа: https://www.exploit-db.com

Агрегатор информации об уязвимостях CVEDetails. Электрон. дан. - Режим доступа: https://www.cvedetails.com

Information Security Информационная безопасность. Электрон. дан. - Режим доступа: http://www.itsec.ru

Securitylab.ru by Positive Technologies. Электрон. дан. - Режим доступа: https://www.securitylab.ru/

Anti-Malware.ru. Электрон. дан. - Режим доступа: https://www.anti-malware.ru/news

Iso27000.ru Искусство управления информационной безопасностью. Электрон. дан. - Режим доступа: http://www.iso27000.ru/

SecurityPolicy.ru Документы по информационной безопасности. Электрон. дан. - Режим доступа: http://securitypolicy.ru/

SearchInform – Информационная безопасность. Электрон. дан. - Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/

Информационная безопасность предприятия. Электрон. дан. - Режим доступа: Ekrost.ru

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 «Анализ уязвимостей компьютерных систем и сетей» читаются лекции, проводятся практические занятия.

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 анализа аппаратных и программных уязвимостей. Занятия проводятся путем решения конкретных задач в аудитории.

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 энцик-

	лопедий, 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 расчет- нографических 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 экзаменом, экзаменом 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