Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Проректор
_____ / А.А. Кирсанкин/
«__»_____ 2026 г.

Рабочая программа учебной дисциплины

АНАЛИЗ УЯЗВИМОСТЕЙ И ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

образовательной программы высшего образования –
программы специалитета

10.05.03 Информационная безопасность автоматизированных систем
Специализация №5 «Безопасность открытых информационных систем»

Форма обучения: очная

Курган 2026

Рабочая программа дисциплины «Анализ уязвимостей и тестирование на проникновение информационных систем» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» (Безопасность открытых информационных систем), утвержденным для очной формы обучения «27» июня 2025 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» «02» сентября 2026, протокол № 1.

Рабочую программу составил:
канд. биол. наук, доцент А.В. Человечкова

Согласовано:

Заведующий кафедрой «БИАС»
канд. тех. наук, доцент Д.И. Дик

Начальник Управления
образовательной деятельности И.В. Григоренко

Специалист по учебно-методической
работе Учебно-методического
отдела Г.В. Казанкова

1. ОБЪЕМ ДИСЦИПЛИНЫ

Очная форма

Всего: 4 зачетных единицы трудоемкости (144 академических часа)

Вид учебной работы	На всю дисциплину	Семестр
		11
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**64**	**64**
Лекции	32	32
Лабораторные работы	32	32
Самостоятельная работа, всего часов в том числе:	**80**	**80**
Подготовка к зачету	18	18
Другие виды самостоятельной работы (изучение тем, подготовка к лабораторным работам и рубежному контролю)	62	62
Вид промежуточной аттестации	**зачет**	**зачет**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**144**	**144**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Анализ уязвимостей и тестирование на проникновение информационных систем» относится к части, формируемой участниками образовательных отношений дисциплинам Блока Б1.

Изучение дисциплины базируется на результатах обучения, сформированных при изучении следующих дисциплин: Безопасность операционных систем; Информационная безопасность распределённых информационных систем; Реагирование на инциденты информационной безопасности; Тестирование программного обеспечения.

Результаты обучения по дисциплине необходимы для изучения дисциплин «Безопасная разработка программного обеспечения», для прохождения преддипломной практики, а также для выполнения выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью дисциплины «Анализ уязвимостей и тестирование на проникновение информационных систем» является формирование у обучающихся теоретических знаний и практических навыков по обнаружению, анализу и устранению уязвимостей, а также проведению санкционированного тестирования на проникновение (пентеста).

Задачи дисциплины:

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

Компетенции, формируемые в результате освоения дисциплины:

- Способен определять угрозы безопасности, реализация которых может привести к нарушению безопасности информации в открытых информационных системах (ПК-4);
- Способен оценивать эффективность систем защиты информации, функционирующих в открытых информационных системах (ПК-8).

Индикаторы и дескрипторы части соответствующей компетенции, формируемой в процессе изучения дисциплины «Анализ уязвимостей и тестирование на проникновение информационных систем», оцениваются при помощи оценочных средств.

Планируемые результаты обучения по дисциплине «Анализ уязвимостей и тестирование на проникновение информационных систем», индикаторы достижения компетенций ПК-4, ПК-8, перечень оценочных средств представлены в таблице.

№ п/п	Код индикатора достижения компетенции	Наименование индикатора достижения компетенции	Код планируемого результата обучения	Планируемые результаты обучения	Наименование оценочных средств
1.	ИД-1 ПК-4	– Знать: основные угрозы безопасности	З (ИД-1 ПК-4)	Знает: основные угрозы и уязвимости безопасности	Вопросы теста
2.	ИД-2 ПК-4	– Уметь: реализовывать защиту открытых информационных систем	У (ИД-2 ПК-4)	Умеет: реализовывать защиту систем с помощью программно-аппаратных средств	Комплекс имитационных задач
3.	ИД-3 ПК-4	– Владеть: методами по реализации защиты от нарушения безопасности открытых информационных систем	В (ИД-3 ПК-4)	Владеет: навыками по обнаружению и устранению уязвимостей	Комплекс имитационных задач
4.	ИД-1 ПК-8	– Знать: эффективные способы защиты информации в системах	З (ИД-1 ПК-8)	Знает: основные уязвимости и эффективные способы защиты информации в системах	Вопросы теста
5.	ИД-2 ПК-8	– Уметь: оценивать эффективность систем защиты	У (ИД-2 ПК-8)	Умеет: оценивать эффективность систем защиты и обеспечивать тестирование систем на проникновение	Комплекс имитационных задач
6.	ИД-3 ПК-8	– Владеть: навыками оценки эффективности систем защиты информации в открытых системах	В (ИД-3 ПК-8)	Владеет: навыки анализа программных реализаций на предмет оценки эффективности систем защиты информации	Комплекс имитационных задач

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план.

Рубеж	Номер раздела, темы	Наименование раздела, темы	Количество часов контактной работы с преподавателем	
			Очная	
			Лекции	Лабор.
Рубеж 1	Тема 1	*Актуальные виды угроз безопасности*	2	-
	Тема 2	*Угрозы, уязвимости и атаки. Основы управления угрозами и уязвимостями безопасности*	6	6
	Тема 3	*Методики анализа угроз и уязвимостей ИБ*	6	9
		1-ый рубежный контроль	Тестирование	1
Рубеж 2	Тема 4	*Способы и средства выявления управления угрозами и уязвимостями ИБ*	6	10
	Тема 5	*Способы формирования моделей угроз ИБ*	6	5
	Тема 6	*Современные методы и средства управления угрозами и уязвимостями безопасности информационных систем*	6	-
		2-ый рубежный контроль	Тестирование	1
		Всего:	**32**	**32**

4.2. Содержание лекционных занятий

Тема 1. Актуальные виды угроз безопасности.

Актуальные виды угроз безопасности. Угрозы. Классификация угроз безопасности. Модели угроз и модель нарушителя. Утечки информации. Каналы утечек информации. Классификация каналов утечек информации.

Тема 2. Угрозы, уязвимости и атаки. Основы управления угрозами и уязвимостями безопасности.

Типы уязвимостей. Mitre Att&ck, НПА и ГОСТы.

ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей».

ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем».

ГОСТ Р 58142-2018 «Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 1. Использование доступных источников для идентификации потенциальных уязвимостей»

ГОСТ Р 58143-2018 «Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 2. Тестирование проникновения”

ГОСТ Р 58412-2019 «Угрозы безопасности информации при разработке программного обеспечения».

Структуры, способы построения и функционирования систем управления угрозами безопасности (TIP), систем обнаружения уязвимостей (VAS).

Тема 3. Методики анализа угроз и уязвимостей ИБ.

Базы данных уязвимостей (БД УиУ ФСТЭК России). Типовые уязвимости и ошибки конфигураций (CVE). Стандарты оценки уязвимостей (SCAP). Методика и единая система оценки уязвимостей (CVSS). Открытый язык описания уязвимостей и их оценки (OVAL). Методика ФСТЭК России оценки уязвимостей ИБ: «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств» (утв. Федеральной службой по техническому и экспортному контролю 28 октября 2022 г.)

Тема 4. Способы и средства выявления управления угрозами и уязвимостями ИБ.

Способы управления угрозами. Технология Threat Inteligence (TI). Технология сканирование и обнаружения уязвимостей (External Attack Surface Management). Виды обнаружения уязвимостей. Варианты анализа защищенности (тестирование пассивное и активное). Сканеры сети. Сканеры операционных систем. Анализ DVL. Сканеры СУБД. Сканеры веб-приложений. Анализ DVWA, BurpSuite, OWASP ZAP. Средства активного тестирования (пентеста) для выявления уязвимости ИБ (FW Metasploit/Armitage). Применение средств тестирования и средств пентеста. Анализ отечественных программных средств анализа уязвимостей (Сканер-ВС, XSpider, RedChack, Ревизор сети, ScanOVAL) и программных средств из открытого ПО (OpenSCAP). Открытые системы управления угрозами (Threat Intelligence Platform): MISP, OpenIOC, OpenCTI.

Тема 5. Способы формирования моделей угроз ИБ.

Формирование актуальных угроз, анализ метрик, вычисление параметров метрик по методике CVSS и методике оценке уязвимостей ФСТЭК России для различного типа информационных систем (ИС ПДн, ГИС и др.). Разработка графического представления моделей в нотациях IDEF, UML, EPC и BMPN. Обоснование выбора средств защиты информации для локализации угроз ИБ.

Тема 6. Современные методы и средства управления угрозами и уязвимостями безопасности информационных систем.

Современные методы и средства управления угрозами и уязвимостями безопасности информационных систем.

4.3 Лабораторные работы

Номер темы	Наименование темы	Наименование тем лабораторных работ.	Норматив времени, час.
			очная

2	*Угрозы, уязвимости и атаки. Основы управления угрозами и уязвимостями безопасности*	Лабораторная работа № 1. Понятие угрозы и уязвимости и атаки. Классификация и классификаторы уязвимостей.	6
3	*Методики анализа угроз и уязвимостей ИБ*	Лабораторная работа №2. Аппаратная уязвимость в специальном ПО. Методики оценки уязвимостей.	9
	1-ый рубежный контроль	***Тестирование***	***1***
4	*Способы и средства выявления управления угрозами и уязвимостями ИБ*	Лабораторная работа №3. Управление угрозами. Средства активного тестирование беспроводных сетей на проникновение: разведка в беспроводной сети, инструменты тестирования, анализ беспроводного трафика.	10
5	*Способы формирования моделей угроз ИБ*	Лабораторная работа №4 Анализ метрик. Методики вычисление параметров метрик.	5
	2-ой рубежный контроль	***Тестирование***	***1***
		Итого	**32**

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной работе.

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения лабораторных работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале лабораторной работы.

Преподавателем запланировано применение на лабораторных работах технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

Для текущего контроля успеваемости по очной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на лабораторных работах в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным работам, подготовку к рубежным контролям и подготовку к зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы
Очная форма

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем:	**44**
Актуальные виды угроз безопасности	7
Угрозы, уязвимости и атаки. Основы управления угрозами и уязвимостями безопасности	7
Методики анализа угроз и уязвимостей ИБ	7
Способы и средства выявления управления угрозами и уязвимостями ИБ	7
Способы формирования моделей угроз ИБ	8
Современные методы и средства управления угрозами и уязвимостями безопасности информационных систем	8
Подготовка к лабораторным работам (по 1 часа на каждое занятие)	16
Подготовка к рубежным контролям (по 1часа на каждый рубежный контроль)	2
Подготовка к зачету	18
Всего:	**80**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности обучающихся в КГУ (очная форма).
2. Отчеты обучающихся по лабораторным работам.
3. Банк тестовых заданий к рубежным контролям № 1, № 2 (очная форма).
4. Вопросы к зачету.

6.2. Система балльно-рейтинговой оценки работы обучающихся по дисциплине

№	Наименование	Содержание					
1	Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы *(доводятся до*	Распределение баллов					
		Вид учебной работы:	Посещение лекций	Выполнение лабораторной работы	Рубежный контроль №1	Рубежный контроль №2	Зачет

	сведения обучающихся на первом учебном занятии)	Балльная оценка:	$0,5_б$ х 16= $8_б$	$10_б$ х 4 =$40_б$	11	11	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета		60 и менее баллов – неудовлетворительно; не зачтено; 61…73 – удовлетворительно; зачтено; 74… 90 – хорошо; 91…100 – отлично				
3	Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов		Для допуска к промежуточной аттестации по дисциплине за семестр, обучающийся должен набрать по итогам текущего и рубежного контроля не менее 51 баллов. В случае если обучающийся набрал менее 51 балла, то к аттестационным испытаниям он не допускается. Для получения зачета без проведения процедуры промежуточной аттестации обучающемуся необходимо набрать в ходе текущего и рубежных контролей не менее 61 балла. В этом случае итог балльной оценки, получаемой обучающимся, определяется по количеству баллов, набранных им в ходе текущего и рубежного контролей. При этом, на усмотрение преподавателя, бальная оценка обучающегося может быть повышена за счет получения дополнительных баллов за академическую активность. Обучающийся, имеющий право на получение оценки без проведения процедуры промежуточной аттестации, может повысить ее путем сдачи аттестационного испытания. В случае получения обучающимся на аттестационном испытании 0 баллов итог бальной оценки по дисциплине не снижается. За академическую активность в ходе освоения дисциплины, участие в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности обучающемуся могут быть начислены дополнительные баллы. Максимальное количество дополнительных баллов за академическую активность составляет 30. Основанием для получения дополнительных баллов являются: - выполнение дополнительных заданий по дисциплине; дополнительные баллы начисляются преподавателем; - участие в течение семестра в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности КГУ.			
4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) обучающихся для получения недостающих баллов в конце семестра		В случае если к промежуточной аттестации (зачету) набрана сумма менее 51 баллов, обучающемуся необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.				

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования.

Перед проведением каждого рубежного контроля преподаватель прорабатывает с обучающимися основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. Варианты тестовых заданий состоят для 1 и 2 рубежного контроля из 11 вопросов. На каждое тестирование при рубежном контроле обучающемуся отводится 1 академический час.

Баллы обучающемуся выставляются в зависимости от числа правильно выбранных ответов. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании. Помножив полученное значение на 100%, можно привести итоговую оценку к традиционной следующим образом:

«неудовлетворительно» – менее 50%

«удовлетворительно» – 50% - 70%

«хорошо» – 70% - 90%

«отлично» – 90% - 100% .

Преподаватель оценивает в баллах результаты тестирования каждого обучающегося по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

Зачет проводится в форме ответов на вопросы билета. Билет состоит из 2 вопросов. Вопросы к зачету доводятся до обучающихся на последней лекции в семестре. На подготовку ответа обучающемуся отводится 1 астрономический час. Каждый вопрос оценивается до 15 баллов.

Результаты успеваемости и зачета заносятся преподавателем в зачетную ведомость, которая сдается в организационный отдел института в день зачета, а также выставляются в зачетную книжку обучающегося.

6.4. Примеры оценочных средств для рубежного контроля и зачета

1-ый рубежный контроль

Вопрос 1. Что такое уязвимость в контексте информационной безопасности?

а) атака на систему;

б) ошибка в логике работы программы;

в) слабое место в системе, которое может быть использовано злоумышленником;

г) сбой в электропитании.

Вопрос 2. Что представляет собой MITRE ATT&CK?

а) метод описания уязвимостей;

б) методика тестирования на проникновение;

в) база знаний о тактиках и техниках атак;

г) программное обеспечение для защиты данных.

Вопрос 3. Что включает SCAP?

а) методология тестирования программного обеспечения;

б) протокол автоматизации управления данными безопасности;

в) протокол автоматизации выявления уязвимостей;

г) база уязвимостей.

2-ой рубежный контроль

Вопрос 1. Какой инструмент относится к платформам Threat Intelligence?

а) MISP;
б) ZAP;
в) Hydra;
г) Nessus.

Вопрос 2. Какой тип тестирования использует Metasploit?

а) пассивный;
б) активный;
в) статистический.

Вопрос 3. Какой формат используется в CVE для идентификатора уязвимости?

а) CVE-год-номер;
б) ID: год: уровень;
в) CWE: номер;
г) CVSS-номер.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Классификация уязвимостей по источнику их возникновения.
2. Классификация атак на информационные системы.
3. Этапы процесса управления уязвимостями.
4. Структура и функции систем управления угрозами (TIP).
5. Структура и функции систем анализа уязвимостей (VAS).
6. Назначение и структура ГОСТ Р 56545–2015.
7. Назначение и структура ГОСТ Р 56546–2015.
8. Описание требований ГОСТ Р 58142–2018.
9. Описание положений ГОСТ Р 58412–2019 по угрозам при разработке ПО.
10. Принципы оценки уязвимостей по методике ФСТЭК России.
11. Типовые программные уязвимости.
12. Уязвимости в веб-приложениях: описание и примеры.
13. Уязвимости операционных систем и сетевых сервисов.
14. Уязвимости СУБД и средств хранения данных.
15. Классификация уязвимостей по ГОСТ Р 56546–2015.
16. Структура базы данных CVE и механизм регистрации уязвимостей.
17. Функции и содержание БД УиУ ФСТЭК России.
18. Структура и элементы стандарта SCAP.
19. Назначение и применение языка OVAL.
20. Методология CVSS: уровни критичности и формулы.
21. Сравнение методик оценки уязвимостей: CVSS и методика ФСТЭК.
22. Применение сканеров веб-приложений: OWASP ZAP и Burp Suite.
23. Применение средств пентеста: Metasploit, Armitage.
24. Анализ уязвимостей в DVWA и DVL.
25. Применение отечественных сканеров: Сканер-ВС, XSpider, ScanOVAL.

26. Применение свободного ПО для анализа уязвимостей: OpenSCAP.
27. Принципы и структура технологии Threat Intelligence.
28. Обзор платформ управления угрозами: MISP, OpenCTI, OpenIOC.
29. Внедрение External Attack Surface Management в инфраструктуру.
30. Принципы формирования модели угроз безопасности информации.

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежного контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

1. Васильева Е. Н. Угрозы безопасности информационных технологий. / [Электронный ресурс]: учеб. пособие / Е.Н. Васильева, В.В. Цехановский, 2005. - 63 с.

2. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс]: учебное пособие / Ю. Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 253 с.: ил. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=276557

3. Основы защиты информации в современных информационных системах: учебное пособие / Н. Ю. Бабанов, А. А. Евстифеев, А. П. Мартынов [и др.]. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2022. — 175 с. — ISBN 978-5-9515-0491-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/132622.html

4. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности. – М.: «Академия», 2009. - 272 с.

5. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс] - Москва: ДМК Пресс, 2014. - 702 с. - ISBN 978-5-94074-768-0. - Доступ ЭБС «Консультант студента».

6. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учебное пособие для вузов 2-е изд., испр. и доп. [Электронный ресурс] - Москва: Горячая линия - Телеком, 2013. - 338 с. - ISBN 978-5-9912-0328-9. - Доступ ЭБС «Консультант студента».

7.2. Дополнительная литература

1. Скулкин, О. Шифровальщики : как реагировать на атаки с использованием программ- вымогателей : [16+] / О. Скулкин ; науч. ред. А. Алексеев ; ред. К. Ахметов ; пер. с англ. А. Власюк. – Москва : Альпина Паблишер, 2023. – 205 с. : ил. – Режим доступа: по подписке. –

URL:https://biblioclub.ru/index.php?page=book&id=707831 (дата обращения: 01.09.2026). – ISBN 978-5-206-00080-1. – Текст : электронный.

2. Лапонина, О. Р. Протоколы безопасного сетевого взаимодействия [Электронный ресурс]: курс/ О. Р. Лапонина. - 2-е изд., исправ. - Москва: ИНТУИТ, 2016. - 462 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=429094

3. Касперски, К. Техника сетевых атак. Т. 1 / Крис Касперски. – М.: Солон-Р, 2001. – 400 с.

4. Олифер, В.Г. Компьютерные сети: Принципы, технологии, протоколы: учебное пособие для студентов вузов / В. Г. Олифер, Н. А. Олифер. – 3-е изд. – М.; СПб.; Нижний Новгород: Питер, 2007. – 957, с.

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Электронный фонд правовой и нормативно-технической документации - http://docs.cntd.ru;
2. ЭБС «Лань» - https://e.lanbook.com/;
3. ЭБС «Znanium» - https://znanium.com/;
4. ЭБС «Консультант студента» - https://www.studentlibrary.ru;
5. Национальный Открытый Университет «ИНТУИТ» - https://intuit.ru;
6. Единое окно доступа к образовательным ресурсам. – http://window.edu.ru/;
7. Научная электронная библиотека - http://elibrary.ru/;
8. Электронная библиотека КГУ - http://dspace.kgsu.ru/xmlui/;
9. Информационный онлайн портал ISO27000.ru - http://www.iso27000.ru/;
10. Безопасность - http://groteck.ru/security.
11. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining Васильев В. И., Вульфин А. М., Кириллова А.Д., Кучкарова Н. В. URL:Glava2/Index1.phphttps://sccs.intelgr.com /archive/2021-03/04-Vasilyev.pdf
12. Разработка типовой методики анализа уязвимостей в веб-приложениях при проведении сертификационных испытаний по требованиям безопасности информации Барабанов А.В., ФедичевА.В. https://cyberleninka.ru/article/n/ razrabotka-tipovoymetodiki-analiza-uyazvimostey-v-veb-prilozheniyah-pri-proveden ii-sertifikatsionnyh-ispytaniy-po-trebovaniyam/viewer

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1. ЭБС «Лань».
2. ЭБС «Консультант студента».
3. ЭБС «Znanium.com».
4. «Гарант» - справочно-правовая система.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение по реализации дисциплины осуществляется в соответствии с требования ФГОС ВО по данной образовательной программе.

11. Для студентов, обучающихся с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн. Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1. Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений, обучающихся принимается с учетом мнения ведущего преподавателя и доводится до сведения обучающихся.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины
«Анализ уязвимостей и тестирование на проникновение информационных систем»

образовательной программы высшего образования –
программы специалитета

10.05.03 Информационная безопасность автоматизированных систем
Специализация №5 «Безопасность открытых информационных систем»

Трудоемкость дисциплины: 4 з.е. (144 академических часа – очная форма обучения)

Семестр: В (очная форма обучения)

Курс: 6 (очная форма обучения)

Форма промежуточной аттестации: зачет

Содержание дисциплины. Основные разделы.

Актуальные виды угроз безопасности. Угрозы, уязвимости и атаки. Основы управления угрозами и уязвимостями безопасности. Методики анализа угроз и уязвимостей ИБ. Способы и средства выявления управления угрозами и уязвимостями ИБ. Способы формирования моделей угроз ИБ. Современные методы и средства управления угрозами и уязвимостями безопасности информационных систем.

ЛИСТ
регистрации изменений (дополнений) в рабочую программу учебной дисциплины
«Анализ уязвимостей и тестирование на проникновение информационных систем»

Изменения / дополнения в рабочую программу
на 20___ / 20___ учебный год:

_____
_____
_____
_____
_____
_____

Ответственный преподаватель _____ / Человечкова А.В. /

Изменения утверждены на заседании кафедры «___»_____20___ г.,
Протокол № ___

Заведующий кафедрой _____ «___»_____20___ г.

Изменения / дополнения в рабочую программу
на 20___ / 20___ учебный год:

_____
_____
_____
_____
_____
_____

Ответственный преподаватель _____ / Человечкова А.В. /

Изменения утверждены на заседании кафедры «___»_____20___ г.,
Протокол № ___

Заведующий кафедрой _____ «___»_____20___ г.