МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Заведующий кафедрой

_____

«_____» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА

дисциплины:	«Разработка безопасного программного обеспечения»
направление подготовки:	09.03.01 Информатика и вычислительная техника
направленность (профиль):	Информационная безопасность компьютерных систем и сетей
форма обучения:	Очная

Рабочая программа рассмотрена на заседании кафедры математики и прикладных информационных технологий

Протокол № _____ от «_____» _____2024г.

1. Цели и задачи освоения дисциплины

Цели дисциплины:

«Разработка безопасного программного обеспечения» является подготовка специалистов, способных создавать надежное и защищенное программное обеспечение, устойчивое к различным видам атак и уязвимостей.

Задачи дисциплины:

- изучение фундаментальных принципов и концепций безопасности программного обеспечения;
- освоение методологий и стандартов разработки безопасного ПО на всех этапах жизненного цикла;
- понимание типов угроз и уязвимостей в программном обеспечении;
- изучение методов анализа безопасности кода и выявления потенциальных проблем;
- освоение практик безопасного программирования для различных языков и платформ;
- изучение механизмов защиты данных и управления доступом;
- понимание принципов безопасной архитектуры и проектирования систем;
- освоение инструментов и технологий для обеспечения безопасности ПО;
- изучение методик тестирования безопасности программного обеспечения;
- развитие навыков оценки рисков и управления безопасностью в процессе разработки ПО.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к части, формируемая участниками образовательных отношений. Необходимыми условиями для освоения дисциплины являются:

Знания:

1. Понимание концепции оценки профессиональных рисков (ОПР) в контексте разработки ПО.
2. Изучение методологий и инструментов для проведения ОПР в IT-проектах.
3. Классификация источников рисков в программном обеспечении.
4. Методы идентификации потенциальных опасностей и рисков в процессе разработки ПО.
5. Базовые принципы оценки вероятности и последствий рисков в IT-сфере.

Умения:

1. Анализируйте различные аспекты разработки ПО для выявления потенциальных рисков.

2. Применяйте методы оценки рисков в контексте безопасности программного обеспечения.

3. Разрабатывайте стратегии управления рисками на разных этапах жизненного цикла ПО.

4. Интегрируйте результаты ОПР в процессы разработки и поддержки ПО.

5. Коммуницируйте результаты оценки рисков и рекомендаций по их снижению заинтересованным сторонам проекта.

Навыки:

1. Использование инструментов для автоматической оценки рисков в коде.

2. Проведение экспертных оценок рисков на основе анализа специфики проекта.

3. Создание и обновление документации по оценке рисков в проекте.

4. Организация и проведение собеседований с командой для обсуждения рисков.

5. Постоянное мониторинг и актуализация оценки рисков в процессе разработки и эксплуатации ПО.

Содержание дисциплины может служить основой для прохождения учебной и производственной практик, подготовки к выполнению выпускной квалификационной работы и профессиональной деятельности.

3. Результаты обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Таблица 3.1

Код и наименование компетенции	Код и наименование индикатора достижения компетенции (ИДК)	Код и наименование результата обучения по дисциплине (модулю)
ПКС–1. Способен обеспечивать информационную безопасность компьютерных систем и сетей.	ПКС–1.1. Управляет информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; планирует восстановление сетевой инфокоммуникационной системы; документирует ошибки в работе сетевых устройств и программного обеспечения; обеспечивает безопасность баз данных; предотвращает потери и повреждения данных при сбоях.	Знать: З1–управление информационной безопасностью; администрирование процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения
		Уметь: У1–управлять информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения.
		Владеть: В1–методикой управления информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения.

ПКС–3. Способен проводить оценку уровня безопасности компьютерных систем и сетей, а также проводить тестирование программного обеспечения на защищенность.	ПКС–3.1. Оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Знать: З2–уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.
		Уметь: У2–оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.
		Владеть: В2–оценкой уровня безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.

4. Объем дисциплины

Общий объем дисциплины составляет 3 зачётных единицы, 108 часов.

Таблица 4.1

Форма обучения	Курс/ семестр	Аудиторные занятия / контактная работа, час.			Самостоятельная работа, час.	Контроль, час	Форма промежуточной аттестации
		Лекции	Практические занятия	Лабораторные занятия			
Очная	4/8	12	-	22	47	27	Экзамен

5. Структура и содержание дисциплины

5.1. Структура дисциплины

- очная форма обучения (ОФО)

Таблица 5.1

№ п/п	Структура дисциплины		Аудиторные занятия, час.			СРС, час.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1	Введение в разработку безопасного ПО	2	-	4	8	14	ПКС – 1.1. ПКС – 3.1.	Теоретические вопросы к коллоквиуму №1
2	2	Анализ уязвимостей и рисков	2	-	4	8	14	ПКС – 1.1. ПКС – 3.1.	Теоретические вопросы к коллоквиуму №1
3	3	Безопасное проектирование	2	-	4	8	1	ПКС – 1.1. ПКС – 3.1.	Теоретические вопросы к коллоквиуму №2
4	4	Безопасное программирование и защита данных	2	-	4	8	14	ПКС – 1.1. ПКС – 3.1.	Теоретические вопросы к коллоквиуму №2
5	5	Аутентификация,	2	-	4	8	14	ПКС – 1.1.	Теоретические

		авторизация и защита от сетевых атак						ПКС – 3.1.	вопросы к коллоквиуму №3
6	6	Тестирование безопасности и управление безопасностью в процессе разработки	2	-	2	7	11	ПКС – 1.1. ПКС – 3.1.	Теоретические вопросы к коллоквиуму №3
7	Экзамен		-	-	-	27	27	ПКС – 1.1. ПКС – 3.1.	Вопросы к экзамену
Итого:			12	-	22	74	108	X	X

- заочная форма обучения (ЗФО): не реализуется
- очно-заочная форма обучения (ОЗФО): не реализуется

5.2. Содержание дисциплины

5.2.1. Содержание разделов дисциплины (дидактические единицы)

Раздел 1. Введение в разработку безопасного ПО

Определение безопасности ПО и ее важность. Основные принципы безопасности

Типы угроз и атак на ПО. Стандарты и методологии разработки безопасного ПО.

Раздел 2. Анализ уязвимостей и рисков

Методы выявления уязвимостей (статический анализ, динамический анализ). Классификация уязвимостей (OWASP Top 10, CWE). Оценка рисков и приоритизация исправлений. Инструменты для автоматического сканирования на уязвимости.

Раздел 3. Безопасное проектирование

Принципы безопасной архитектуры. Паттерны и антипаттерны безопасности. Безопасная реализация функциональности. Использование шаблонов проектирования для повышения безопасности.

Раздел 4. Безопасное программирование и защита данных

Языковые особенности и их влияние на безопасность. Обработка ошибок и исключений. Управление памятью и предотвращение утечек. Безопасное использование API и библиотек. Шифрование данных (симметричное и асимметричное). Хеширование и подписывание сообщений. Управление ключами и сертификатами. Безопасное хранение паролей.

Раздел 5. Аутентификация, авторизация и защита от сетевых атак

Механизмы аутентификации (пароли, биометрия, токены). Протоколы аутентификации (OAuth, OpenID Connect). Системы авторизации и управление доступом. Безопасность сессий и управления состоянием. Основные протоколы безопасности (HTTPS, SSH).

Фильтрация входящего трафика и брандмауэры. Детекция и предотвращение вторжений (IDS/IPS). Безопасность веб-приложений (CSRF, XSS)

Раздел 6. Тестирование безопасности и управление безопасностью в процессе разработки

Виды тестирования безопасности (black box, white box, gray box). Методики ручного тестирования на проникновение. Автоматизация тестирования безопасности. Интеграция безопасности в CI/CD процессы. Интеграция безопасности в жизненный цикл разработки. Согласование требований безопасности. Мониторинг и аудит безопасности. Реагирование на инциденты и управление уязвимостями.

5.2.2. Содержание дисциплины по видам учебных занятий

Лекционные занятия

Таблица 5.2.1

№ п/п	Номер раздела дисциплины	Объем, час.			Тема лекции
		ОФО	ЗФО	ОЗФО	
1	1	2	-	-	Введение в разработку безопасного ПО
2	2	2	-	-	Анализ уязвимостей и рисков
3	3	2	-	-	Безопасное проектирование
4	4	2	-	-	Безопасное программирование и защита данных
5	5	2	-	-	Аутентификация, авторизация и защита от сетевых атак
6	6	2	-	-	Тестирование безопасности и управление безопасностью в процессе разработки
Итого:		12	-	-	X

Практические занятия

Практические работы учебным планом не предусмотрены

Лабораторные работы

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.			Тема лабораторного занятия
		ОФО	ЗФО	ОЗФО	
1	1	4	-	-	Введение в разработку безопасного ПО
2	2	4	-	-	Анализ уязвимостей и рисков
3	3	4	-	-	Безопасное проектирование
4	4	4	-	-	Безопасное программирование и защита данных
5	5	4	-	-	Аутентификация, авторизация и защита от сетевых атак
6	6	2	-	-	Тестирование безопасности и управление безопасностью в процессе разработки
Итого:		22	-	-	X

Самостоятельная работа студента

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час.			Тема	Вид СРС
		ОФО	ЗФО	ОЗФО		
1	1	8	-	-	Введение в реверс инжиниринг	Изучение теоретического материала для выполнения лабораторной работы
2	2	8	-	-	Введение в разработку безопасного ПО	Изучение теоретического материала для выполнения лабораторной работы
3	3	8	-	-	Анализ уязвимостей и рисков	Изучение теоретического материала для выполнения лабораторной работы
4	4	8	-	-	Безопасное проектирование	Изучение теоретического материала для выполнения лабораторной работы
5	5	8	-	-	Безопасное программирование и защита данных	Изучение теоретического материала для выполнения лабораторной работы
6	6	7	-	-	Аутентификация, авторизация и защита от сетевых атак	Изучение теоретического материала для выполнения лабораторной работы
7	7	27	-	-	Экзамен	Изучение вопросов и подготовка к экзамену
Итого:		74	-	-	X	X

5.2.3. Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

- визуализация учебного материала в PowerPoint в диалоговом режиме (лекционные занятия);
- работа в малых группах (практические занятия);
- разбор практических ситуаций (практические занятия).

6. Тематика курсовых работ/проектов

Курсовые работы/проекты учебным планом не предусмотрены.

7. Контрольные работы

Контрольные работы учебным планом не предусмотрены.

8. Оценка результатов освоения дисциплины

8.1. Критерии оценивания степени полноты и качества освоения компетенций в соответствии с планируемыми результатами обучения приведены в Приложении 1.

8.2. Рейтинговая система оценивания степени полноты и качества освоения компетенций обучающихся очной формы обучения представлена в таблице 8.1.

Таблица 8.1

№ п/п	Виды мероприятий в рамках текущего контроля	Количество баллов
1	Коллоквиум № 1	0-30
	ИТОГО за первую текущую аттестацию	0-30
2	Коллоквиум № 2	0-30
	ИТОГО за вторую текущую аттестацию	0-30
3	Коллоквиум № 3	0-40
	ИТОГО за третью текущую аттестацию	0-40
	ВСЕГО	0-100

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Перечень рекомендуемой литературы представлен в Приложении 2.

9.2. Современные профессиональные базы данных и информационные справочные системы:

– Электронный каталог/Электронная библиотека ТИУ http://webirbis.tsogu.ru/
– Цифровой образовательный ресурс – библиотечная система IPR SMART — https://www.iprbookshop.ru/
– Электронно-библиотечная система «Консультант студента» www.studentlibrary.ru
– Электронно-библиотечная система «Лань» https://e.lanbook.com
– Образовательная платформа ЮРАЙТ www.urait.ru
– Научная электронная библиотека ELIBRARY.RU http://www.elibrary.ru
– Национальная электронная библиотека (НЭБ)
– Библиотеки нефтяных вузов России :
– Электронная нефтегазовая библиотека РГУ нефти и газа им. Губкина http://elib.gubkin.ru/
– Электронная библиотека Уфимского государственного нефтяного технического университета http://bibl.rusoil.net/
– Библиотечно-информационный комплекс Ухтинского государственного технического университета УГТУ http://lib.ugtu.net/books.

9.3. Лицензионное и свободно распространяемое программное обеспечение, в т.ч. отечественного производства:

- Microsoft Windows;
- Microsoft Office;
- Oracle VirtualBox;
- OpenVAS;
- Nmap;
- Wireshark;
- John the Ripper;

- Snort;
- SecretNetStudio;
- VipNet;
- OpenVPN;
- КриптоПро;

10. Материально-техническое обеспечение дисциплины

Помещения для проведения всех видов работы, предусмотренных учебным планом, укомплектованы необходимым оборудованием и техническими средствами обучения.

Таблица 10.1

Обеспеченность материально-технических условий реализации ОПОП ВО

№ п/п	Наименование учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно – наглядных пособий	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1	2	3	4
1.	Разработка безопасного программного обеспечения	Лекционные занятия: Учебная аудитория для проведения занятий лекционного типа; групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Оснащенность: Учебная мебель: столы, стулья. Моноблок - 1 шт., проектор - 1 шт., проекционный экран - 1 шт., акустическая система (колонки) - 4 шт., микрофон - 1 шт., документ-камера - 1 шт., телевизор - 2 шт.	625039, г. Тюмень, ул. Мельникайте, д. 70.
		Лабораторные занятия: Учебная аудитория для проведения (лабораторных занятий); групповых и индивидуальных консультаций; текущего контроля и промежуточной аттестации. Оснащенность: Учебная мебель: столы, стулья. Моноблоки, проектор - 1 шт., проекционный экран - 1 шт., акустическая система (колонки) - 4 шт., микрофон - 1 шт., документ-камера - 1 шт., телевизор - 2 шт.	625039, г. Тюмень, ул. Мельникайте, д. 70

11. Методические указания по организации СРС

11.1. Методические указания по подготовке к практическим занятиям.

Важной формой самостоятельной работы студента является систематическая и планомерная подготовка к лабораторному занятию. После лекции студент должен познакомиться с планом лабораторных занятий и списком обязательной и дополнительной литературы, которую необходимо прочитать, изучить и законспектировать. Разъяснение по вопросам новой темы студенты получают у преподавателя в конце предыдущего лабораторного занятия.

Подготовка к лабораторному занятию требует, прежде всего, чтения рекомендуемых источников и монографических работ. Важным этапом в самостоятельной работе студента является повторение материала по конспекту лекции. Одна из главных составляющих внеаудиторной подготовки – работа с книгой. Она предполагает: внимательное прочтение, критическое осмысление содержания, обоснование собственной позиции по дискуссионным моментам, постановки интересующих вопросов, которые могут стать предметом обсуждения на практическом занятии.

В начале практического занятия должен присутствовать организационный момент и вступительная часть. Преподаватель произносит краткую вступительную речь, где формулируются основные вопросы и проблемы, способы их решения в процессе работы.

В конце каждой темы подводятся итоги, предлагаются темы докладов, выносятся вопросы для самоподготовки. Как средство контроля и учета знаний студентов в течение семестра проводятся контрольные работы.

Практические занятия являются одной из важнейших форм обучения студентов: они позволяют студентам закрепить, углубить и конкретизировать знания по курсу алгебры и теории чисел, подготовиться к научно-исследовательской деятельности. В процессе работы на практических занятиях обучающийся должен совершенствовать умения и навыки самостоятельного анализа источников и научной литературы, что необходимо для научно-исследовательской работы.

Усвоенный материал необходимо научиться применять при решении практических задач.

Успешному осуществлению внеаудиторной самостоятельной работы способствуют тестирования. Они обеспечивают непосредственную связь между студентом и преподавателем (по ним преподаватель судит о трудностях, возникающих у студентов в ходе учебного процесса, о степени усвоения предмета, о помощи, какую надо указать, чтобы устранить пробелы в знаниях); они используются для осуществления контрольных функций.

11.2. Методические указания по организации самостоятельной работы.

Самостоятельная работа является одной из важнейших форм изучения любой дисциплины. Она позволяет систематизировать и углубить теоретические знания, закрепить

умения и навыки, способствует развитию умений пользоваться научной и учебно-методической литературой. Познавательная деятельность в процессе самостоятельной работы требует от студента высокого уровня активности и самоорганизованности.

В учебном процессе выделяют два вида самостоятельной работы: аудиторная и внеаудиторная.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа студентов представляет собой логическое продолжение аудиторных занятий. Затраты времени на выполнение этой работы регламентируются рабочим учебным планом. Режим работы выбирает сам обучающийся в зависимости от своих способностей и конкретных условий.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Самостоятельная работа включает в себя работу с конспектом лекций, изучение и конспектирование рекомендуемой литературы, подготовка мультимедиа-сообщений/докладов, подготовка реферата, тестирование, решение задач и упражнений по образцу, решение вариативных задач, выполнение чертежей, схем, расчетов (графических работ), решение ситуационных (профессиональных) задач, подготовка к деловым играм, проектирование и моделирование разных видов и компонентов профессиональной деятельности, научно-исследовательскую работу и др.

Контроль результатов внеаудиторной самостоятельной работы студентов может осуществляться в пределах времени, отведенного на обязательные учебные занятия по дисциплине и внеаудиторную самостоятельную работу студентов по дисциплине, может проходить в письменной, устной или смешанной форме.

Работа на лекции – это сложный процесс, который включает в себя такие элементы как слушание, осмысление и, собственно, конспектирование. Для того, чтобы лекция выполнила свое назначение, важно подготовиться к ней и ее записи еще до прихода преподавателя в аудиторию, поскольку в первые минуты лекции объявляется тема лекции, формулируется ее основная цель. Без этого дальнейшее восприятие лекции становится сложным. Важно научиться слушать преподавателя во время лекции. Здесь не следует путать такие понятия как слышать и слушать. Слушание лекции состоит из нескольких этапов, начиная от слышания (первый шаг в процессе осмысленного слушания) и заканчивая оценкой сказанного.

Чтобы процесс слушания стал более эффективным, нужно разделять качество общения с лектором, научиться поддерживать непрерывное внимание к выступающему. Для оптимизации процесса слушания следует:

1. научиться выделять основные положения. Нельзя понять и запомнить все, что говорит выступающий, однако можно выделить основные моменты. Для этого необходимо обращать внимание на вводные слова, словосочетания, фразы, которые используются, как правило, для перехода к новым положениям, выводам и обобщениям;

2. во время лекции осуществлять поэтапный анализ и обобщение, услышанного. Необходимо постоянно анализировать и обобщать положения, раскрываемые в речи говорящего. Стараясь представить материал обобщенно, мы готовим надежную базу для экономной, свернутой его записи. Делать это лучше всего по этапам, ориентируясь на момент логического завершения одного вопроса (подвопроса, тезиса и т.д.) и перехода к другому;

3. готовность слушать выступление лектора до конца.

Слушание является лишь одним из элементов хорошего усвоения лекционного материала.

Поток информации, который сообщается во время лекции необходимо фиксировать, записывать – научиться вести конспект лекции, где формулировались бы наиболее важные моменты, основные положения, излагаемые лектором. Для ведения конспекта лекции следует использовать тетрадь. Ведение конспекта на листочках не рекомендуется, поскольку они не так удобны в использовании и часто теряются. При оформлении конспекта лекции необходимо оставлять поля, где студент может записать свои собственные мысли, возникающие параллельно с мыслями, высказанными лектором, а также вопросы, которые могут возникнуть в процессе слушания, чтобы получить на них ответы при самостоятельной проработке материала лекции, при изучении рекомендованной литературы или непосредственно у преподавателя в конце лекции.

Составляя конспект лекции, следует оставлять значительный интервал между строчками. Это связано с тем, что иногда возникает необходимость вписать в первоначальный текст лекции одну или несколько строчек, имеющих принципиальное значение и почерпнутых из других источников. Расстояние между строками необходимо также для подчеркивания слов или целых групп слов (такое подчеркивание вызывается необходимостью привлечь внимание к данному месту в тексте при повторном чтении). Обычно подчеркивают определения, выводы.

Главным отличием конспекта лекции от текста является свертывание текста. При ведении конспекта удаляются отдельные слова или части текста, которые не выражают значимую информацию, а развернутые обороты речи заменяют более лаконичными или же

синонимичными словосочетаниями. При конспектировании основную информацию следует записывать подробно, а дополнительные и вспомогательные сведения, примеры – очень кратко. Особенно важные моменты лекции, на которые следует обратить особое внимание лектор, как правило, читает в замедленном темпе, что позволяет сделать их запись дословной. Также важно полностью без всяких изменений вносить в тетрадь схемы, таблицы, чертежи и т.п., если они предполагаются в лекции. Для того, чтобы совместить механическую запись с почти дословным фиксированием наиболее важных положений, можно использовать системы условных сокращений. В первую очередь сокращаются длинные слова и те, что повторяются в речи лектора чаще всего. При этом само сокращение должно быть по возможности кратким.

Приложение 1

Планируемые результаты обучения для формирования компетенции и критерии их оценивания

Дисциплина: Разработка безопасного программного обеспечения

Код, направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): Информационная безопасность компьютерных систем и сетей

Код компетенции	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
		1 - 2	3	4	5
1	2	3	4	5	6
ПКС–1	З1–управление информационной безопасностью; администрирование процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения	Не знает управление информационной безопасностью; администрирование процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения	Удовлетворительно знает управление информационной безопасностью; администрирование процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения	Хорошо знает управление информационной безопасностью; администрирование процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения	Отлично знает управление информационной безопасностью; администрирование процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения
	У1–управлять информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и	Не умеет управлять информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и	Удовлетворительно умеет управлять информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых	Хорошо умеет управлять информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью	В совершенстве умеет управлять информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью

	программного обеспечения.	программного обеспечения.	устройств и программного обеспечения.	сетевых устройств и программного обеспечения.	сетевых устройств и программного обеспечения.
	В1–методикой управления информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения.	Не владеет методикой управления информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения.	Удовлетворительно владеет методикой управления информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения.	Хорошо владеет методикой управления информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения.	В совершенстве владеет методикой управления информационной безопасностью; администрирует процесс конфигурирования и управления безопасностью сетевых устройств и программного обеспечения.
ПКС – 3	З2 – уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Не знает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Удовлетворительно знает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Хорошо знает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Отлично знает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.
	У2 – оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Не умеет оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Удовлетворительно умеет оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	Хорошо умеет выбирать оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	В совершенстве умеет оценивает уровень безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.
	В2 – оценкой уровня безопасности	Не владеет оценкой уровня безопасности	Удовлетворительно владеет оценкой уровня	Хорошо владеет оценкой уровня	В совершенстве владеет оценкой

	компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.	уровня безопасности компьютерных систем и сетей; разрабатывает тестовые случаи, управляет процессом тестирования программного обеспечения.

Приложение 2

КАРТА

обеспеченности дисциплины учебной и учебно-методической литературой

Дисциплина: Разработка безопасного программного обеспечения

Код, направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): Информационная безопасность компьютерных систем и сетей

№ п/п	Название учебного, учебно-методического издания, автор, издательство, вид издания, год издания	Количество экземпляров в БИК	Контингент обучающихся, использующих указанную литературу	Обеспеченность обучающихся литературой, %	Наличие электронного варианта в ЭБС (+/-)
1	Ванина, А. Г. Персональная кибербезопасность : учебное пособие (курс лекций) / А. Г. Востокин, С. В. Архитектура операционных систем : учебное пособие / С. В. Востокин. - Самара : Самарский университет, 2023. - 84 с. - URL: https://e.lanbook.com/book/406658.	ЭР*	30	100	+
2	Ванина, А. Г. Персональная кибербезопасность : учебное пособие (курс лекций) / А. Г. Ванина, Д. В. Орёл, С. В. Аникуев. — Ставрополь : Северо-Кавказский федеральный университет, 2022. — 137 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/135721.html.	ЭР*	30	100	+
3	Бизянов, Е. Е. Системное программирование : учебное пособие / Е. Е. Бизянов. - Москва, Вологда : Инфра-Инженерия, 2024. - 192 с. - URL: https://www.iprbookshop.ru/143252.html.	ЭР*	30	100	+
4	Парасич, И. В. Алгоритмический язык СИ. Примеры и задания : учебное пособие для вузов. Ч. 2 / И. В. Парасич. - Санкт-Петербург : Лань, 2024. - 68 с. - URL: https://e.lanbook.com/book/434096.	ЭР*	30	100	+
5	Рацеев, С. М. Реализации некоторых криптосистем и корректирующих кодов : учебное пособие для вузов / С. М. Рацеев. - Санкт-Петербург : Лань, 2024. - 288 с. - URL: https://e.lanbook.com/book/356009.	ЭР*	30	100	+

*ЭР – электронный ресурс для автор. пользователей доступен через Электронный каталог/Электронную библиотеку ТИУ http://webirbis.tsogu.ru/