МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное
бюджетное образовательное учреждение
высшего образования

«ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

_____

«___»_____ 2024г.

РАБОЧАЯ ПРОГРАММА

дисциплины:	Программно-аппаратные средства защиты информации
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

Цель освоения дисциплины: овладение теоретическими знаниями и умениями, развитие навыков практических действий по выбору и применению программно-аппаратных средств обеспечения информационной безопасности».

Задачи освоения дисциплины:

- изучение нормативных правовых и организационных основ обеспечения информационной безопасности;
- изучение методов и процедур выявления угроз информационной безопасности и оценки степени их опасности;
- изучение классов и видов программно-аппаратных средств обеспечения информационной безопасности и механизмов построения с их помощью систем защиты информации;
- практическая отработка способов и порядка выбора и применения программно-аппаратных средств обеспечения информационной безопасности;
- развитие исследовательских и аналитических навыков, интеллектуального потенциала.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к дисциплинам части учебного плана, формируемой участниками образовательных отношений.

Необходимыми условиями для освоения дисциплины являются:

- знание теоретических основ информационных и сетевых технологий и информационной безопасности;
- умение разрабатывать алгоритмы и реализовывать их с использованием языков программирования;
- владение навыками использования информационно-коммуникационных технологий в практической деятельности.

Содержание дисциплины является логическим продолжением содержания дисциплины «Информационная безопасность» и 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 индикаторов достижения компетенций (ИДК)	Код и наименование результата обучения по дисциплине
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) теоретические основы обеспечения информационной безопасности
		Уметь (У1) планировать восстановление сетевой инфокоммуникационной системы; документировать ошибки в работе сетевых устройств и программного обеспечения
		Владеть (В1) практическими навыками администрирования процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; обеспечения безопасности баз данных
ПКС-2. Способен осуществлять техническое обслуживание и	ПКС-2. 1. Осуществляет администрирование и техническое обслуживание программно-	Знать (З2) теоретические основы обеспечения информационной безопасности в операционных системах

администрирование средств защиты информации и процесса управления безопасностью сетевых устройств и программного обеспечения в компьютерных системах и сетях.	аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях; средств защиты информации прикладного и системного программного обеспечения.	и компьютерных системах и сетях с использованием программных и программно-аппаратных средств обеспечения информационной безопасности
		Уметь (У2) планировать и организовывать мероприятия по техническому обслуживанию программно-аппаратных средств защиты информации, средств защиты информации прикладного и системного программного обеспечения
		Владеть (В2) практическими навыками внедрения, настройки и администрирования программно-аппаратных средств защиты информации, средств защиты информации прикладного и системного программного обеспечения

4. Объем дисциплины

Общий объем дисциплины составляет 4 зачетных единиц, 144 часа.

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	3/6	16	-	32	60	36	Экзамен
заочная	-	-	-	-	-	-	-

5. Структура и содержание дисциплины

5.1. Структура дисциплины.

очная форма обучения (ОФО)

Таблица 5.1.1

№ п/п	Структура дисциплины		Аудиторные занятия, час.			СРС, час.	Всего, час.	Код ИДК	Оценочные средства
	Номер раздела	Наименование раздела	Л.	Пр.	Лаб.				
1	1	Правовые и организационные основы информационной безопасности	3	-	6	12	21	ПКС-1.1 ПКС-2.1	Задание на лабораторную работу
2	2	Основные методы и средства реализации отдельных функциональных требований по защите информации и данных	3	-	7	12	22		
3	3	Программно-аппаратные средства защиты программ	3	-	6	12	21		
4	4	Программно-аппаратные средства	4	-	7	12	23		

		защиты от несанкционированного доступа к информации, хранимой в ПЭВМ							
5	5	Программно-аппаратные средства защиты информации в сетях передачи данных	3	-	6	12	21		
6	Экзамен		-	-	-	36	36	ПКС-1.1 ПКС-2.1	Вопросы к экзамену
Итого:			16		32	96	144	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. Правовые и организационные основы информационной безопасности. Основные понятия в области информационной безопасности. Нормативно-правовые акты, специальные нормативные документы и документы национальной (международной) системы стандартизации в области информационной безопасности. Система органов обеспечения информационной безопасности в Российской Федерации. Лицензирование деятельности в области технической защиты информации. Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации. Анализ сетевых угроз информационной безопасности. Классификация ПАСОИБ. Функциональные возможности ПАСОИБ.

Раздел 2. Основные методы и средства реализации отдельных функциональных требований по защите информации и данных. Классификация функциональных требований по защите информации и данных. Принципы действия и технологические особенности программно-аппаратных средств, реализующих отдельные функциональные требования по защите информации и данных и их взаимодействие с общесистемными компонентами вычислительных систем. Методы обеспечения идентификации и аутентификации. Методы криптографической защиты. Методы и средства хранения ключевой информации. Методы и средства ограничения доступа к компонентам вычислительных систем. Характеристика методов и средства привязки программного обеспечения к аппаратному окружению и физическим носителям. Методы аудита безопасности. Методы обеспечения доступа к системе защиты и управления безопасностью. Методы обеспечения целостности системы защиты.

Раздел 3. Программно-аппаратные средства защиты программ. Классификация аппаратных компонентов средств защиты программ. Классификация программных компонентов средств защиты программ. Структура программного обеспечения. Способы встраивания средств защиты в программное обеспечение. Способы определения факта незаконного использования программ. Способы защиты программ от незаконного использования. Способы изучения кода программ. Способы защиты программ от изучения кода. Основные принципы обеспечения безопасности программ. Понятие изолированной программной среды.

Раздел 4. Программно-аппаратные средства защиты от несанкционированного доступа к информации, хранимой в ПЭВМ. Классификация программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ. Характеристики программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ. Понятие электронного замка. Принципы построения и функционирования электронных замков. Механизмы контроля аппаратной конфигурации ПЭВМ. Общие принципы разграничения доступа пользователей к устройствам ПЭВМ. Основные принципы криптографической защиты информации.

Раздел 5. Программно-аппаратные средства защиты информации в сетях передачи данных. Классификация программно-аппаратных средств защиты информации в сетях передачи данных. Принципы построения и функционирования межсетевых экранов в сетях передачи данных. Программно-аппаратные средства межсетевого экранирования. Основные принципы защиты информации при передаче по каналам связи. Программно-аппаратные средства защиты информации при передаче по каналам связи. Основные принципы разграничения доступа к сетевым ресурсам. Основные принципы обнаружения сетевых атак. Программно-аппаратные средства обнаружения сетевых атак. Основные принципы защиты от сетевых атак. Программно-аппаратные средства защиты от сетевых атак. Основные принципы управления безопасностью сети. Программно-аппаратные средства управления безопасностью сети. Обзор штатных средств сетевого оборудования, предназначенных для защиты информации при передаче по каналам связи. Способы применения штатных средств сетевого оборудования, предназначенных для защиты информации при передаче по каналам связи.

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	3			Правовые и организационные основы информационной безопасности
2	2	3			Основные методы и средства реализации отдельных функциональных требований по защите информации и данных
3	3	3			Программно-аппаратные средства защиты программ
4	4	4			Программно-аппаратные средства защиты от несанкционированного доступа к информации, хранимой в ПЭВМ
5	5	3			Программно-аппаратные средства защиты информации в сетях передачи данных
Итого:		16			-

Лабораторные работы

Таблица 5.2.2

№ п/п	Номер раздела дисциплины	Объем, час.			Тема практического занятия
		ОФО	ЗФО	ОЗФО	
1	1	6			Правовые и организационные основы информационной безопасности
2	2	7			Основные методы и средства реализации отдельных функциональных требований по защите информации и данных
3	3	6			Программно-аппаратные средства защиты программ
4	4	7			Программно-аппаратные средства защиты от несанкционированного доступа к информации, хранимой в ПЭВМ
5	5	6			Программно-аппаратные средства защиты информации в сетях передачи данных
Итого:		32			-

Практические занятия

Практические занятия учебным планом не предусмотрены.

Самостоятельная работа студента

Таблица 5.2.3

№ п/п	Номер раздела дисциплины	Объем, час.			Тема	Вид СРС
		ОФО	ЗФО	ОФО		
1	1	12			Правовые и организационные основы информационной безопасности	Подготовка к лабораторным работам
2	2	12			Основные методы и средства реализации отдельных функциональных требований по защите информации и данных	Подготовка к лабораторным работам
3	3	12			Программно-аппаратные средства защиты программ	Подготовка к лабораторным работам
4	4	12			Программно-аппаратные средства защиты от несанкционированного доступа к информации, хранимой в ПЭВМ	Подготовка к лабораторным работам
5	5	12			Программно-аппаратные средства защиты информации в сетях передачи данных	Подготовка к лабораторным работам
6	1-5	36			Экзамен	Подготовка к экзамену
Итого:		96				

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

- ИКТ – технологии (визуализация учебного материала в PowerPoint в диалоговом режиме);
- обучение в сотрудничестве (коллективная, групповая работа);
- технология проблемного обучения.

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 текущая аттестация		
1	Лабораторная работа № 1	0-15
2	Лабораторная работа № 2	0-15
	ИТОГО за первую текущую аттестацию	**0-30**
2 текущая аттестация		
3	Лабораторная работа № 3	0-15
4	Лабораторная работа № 4	0-15

	ИТОГО за вторую текущую аттестацию	**0-30**
3 текущая аттестация		
5	Лабораторная работа № 5	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;
- 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;
- Электронная справочная система нормативно-технической документации «Технорматив»;
- ЭКБСОН – информационная система доступа к электронным каталогам библиотек сферы образования и науки.

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

- Microsoft Windows;
- Microsoft Office;
- Oracle VirtualBox;
- VipNet;
- Snort;
- SecretNetStudio;
- КриптоПроCSP.

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.	Программно-аппаратные средства защиты информации	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 лабораторным 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. 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 лабораторного 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.

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

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, изучение мультимедиалекций, расположенных в свободном доступе, решение ситуационных (профессиональных) задач, проектирование и моделирование разных видов и компонентов профессиональной деятельности, научно-исследовательскую работу и др.

Приложение 1

Планируемые результаты обучения для формирования компетенции и критерии их оценивания

Дисциплина: Программно-аппаратные средства защиты информации
Код, направление подготовки: 09.03.01 «Информатика и вычислительная техника»
Направленность (профиль): Информационная безопасность компьютерных систем и сетей

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
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) теоретические основы обеспечения информационной безопасности	Не знает теоретические основы обеспечения информационной безопасности	Знает на низком уровне теоретические основы обеспечения информационной безопасности	Знает на среднем уровне теоретические основы обеспечения информационной безопасности	Знает в совершенстве теоретические основы обеспечения информационной безопасности
		Уметь (У1) планировать восстановление сетевой инфокоммуникационной системы; документировать ошибки в работе сетевых устройств и программного обеспечения	Не умеет планировать восстановление сетевой инфокоммуникационной системы; документировать ошибки в работе сетевых устройств и программного обеспечения	Умеет на низком уровне планировать восстановление сетевой инфокоммуникационной системы; документировать ошибки в работе сетевых устройств и программного обеспечения	Умеет на среднем уровне планировать восстановление сетевой инфокоммуникационной системы; документировать ошибки в работе сетевых устройств и программного обеспечения	Умеет в совершенстве планировать восстановление сетевой инфокоммуникационной системы; документировать ошибки в работе сетевых устройств и программного обеспечения
		Владеть (В1) практическими навыками администрирования процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; обеспечения безопасности баз данных	Не владеет практическими навыками администрирования процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; обеспечения безопасности баз данных	Владеет на низком уровне практическими навыками администрирования процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; обеспечения безопасности баз данных	Владеет на среднем уровне практическими навыками администрирования процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; обеспечения безопасности баз данных	Владеет в совершенстве практическими навыками администрирования процесса конфигурирования и управления безопасностью сетевых устройств и программного обеспечения; обеспечения безопасности баз данных

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
ПКС-2. Способен осуществлять техническое обслуживание и администрирование средств защиты информации и процесса управления безопасностью сетевых устройств и программного обеспечения в компьютерных системах и сетях.	ПКС-2. 1. Осуществляет администрирование и техническое обслуживание программно-аппаратных средств защиты информации в операционных системах и компьютерных системах и сетях; средств защиты информации прикладного и системного программного обеспечения.	Знать (З2) теоретические основы обеспечения информационной безопасности в операционных системах и компьютерных системах и сетях с использованием программных и программно-аппаратных средств обеспечения информационной безопасности	Не знает теоретические основы обеспечения информационной безопасности в операционных системах и компьютерных системах и сетях с использованием программных и программно-аппаратных средств обеспечения информационной безопасности	Знает на низком уровне теоретические основы обеспечения информационной безопасности в операционных системах и компьютерных системах и сетях с использованием программных и программно-аппаратных средств обеспечения информационной безопасности	Знает на среднем уровне теоретические основы обеспечения информационной безопасности в операционных системах и компьютерных системах и сетях с использованием программных и программно-аппаратных средств обеспечения информационной безопасности	Знает в совершенстве теоретические основы обеспечения информационной безопасности в операционных системах и компьютерных системах и сетях с использованием программных и программно-аппаратных средств обеспечения информационной безопасности
		Уметь (У2) планировать и организовывать мероприятия по техническому обслуживанию программно-аппаратных средств защиты информации, средств защиты информации прикладного и системного программного обеспечения	Не умеет планировать и организовывать мероприятия по техническому обслуживанию программно-аппаратных средств защиты информации, средств защиты информации прикладного и системного программного обеспечения	Умеет на низком уровне планировать и организовывать мероприятия по техническому обслуживанию программно-аппаратных средств защиты информации, средств защиты информации прикладного и системного программного обеспечения	Умеет на среднем уровне планировать и организовывать мероприятия по техническому обслуживанию программно-аппаратных средств защиты информации, средств защиты информации прикладного и системного программного обеспечения	Умеет в совершенстве планировать и организовывать мероприятия по техническому обслуживанию программно-аппаратных средств защиты информации, средств защиты информации прикладного и системного программного обеспечения

Код компетенции	Код, наименование ИДК	Код и наименование результата обучения по дисциплине	Критерии оценивания результатов обучения			
			1-2	3	4	5
		Владеть (В2) практическими навыками внедрения, настройки и администрирования программно-аппаратных средств защиты информации, средств защиты информации прикладного и системного программного обеспечения	Не владеет практическими навыками внедрения, настройки и администрирования программно-аппаратных средств защиты информации, средств защиты информации прикладного и системного программного обеспечения	Владеет на низком уровне практическими навыками внедрения, настройки и администрирования программно-аппаратных средств защиты информации, средств защиты информации прикладного и системного программного обеспечения	Владеет на среднем уровне практическими навыками внедрения, настройки и администрирования программно-аппаратных средств защиты информации, средств защиты информации прикладного и системного программного обеспечения	Владеет в совершенстве практическими навыками внедрения, настройки и администрирования программно-аппаратных средств защиты информации, средств защиты информации прикладного и системного программного обеспечения

Приложение 2

КАРТА
обеспеченности дисциплины учебной и учебно-методической литературой

Дисциплина: «Программно-аппаратные средства защиты информации»
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	Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/449285	ЭР*	30	100	+
2	Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/513300	ЭР*	30	100	+
3	Программно-аппаратные средства защиты информационных систем : учебное пособие / Ю. Ю. Громов, О. Г. Иванова, К. В. Стародубов, А. А. Кадыков. — Тамбов : ТГТУ, 2017. — 194 с. — ISBN 978-5-8265-1737-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/319553	ЭР*	30	100	+
4	Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2019. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/125739	ЭР*	30	100	+

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

Лист согласования 00ДО-0000758810

Внутренний документ "Программно-аппаратные средства защиты информации_2024_09.03.01_ИБКСб"

Ответственный: Кармацкая Елена Александровна

Согласовано

Серийный номер ЭП	Должность	ФИО	ИО	Виза	Комментарий	Дата
	Заведующий кафедрой, имеющий ученую степень доктора наук	Барбаков Олег Михайлович		Согласовано		
	Директор	Каюкова Дарья Хрисановна		Согласовано		
	Специалист 1 категории		Радичко Диана Викторовна	Согласовано		