Межгосударственное образовательное учреждение высшего образования
«Белорусско-Российский университет»

УТВЕРЖДАЮ
Первый проректор Белорусско-Российского университета

_____ Ю.В. Машин

«17» 06 2022г.

Регистрационный № УД-09030104/б.1.В.13/р

ЗАЩИТА ИНФОРМАЦИИ
(наименование дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки: 09.03.01 «Информатика и вычислительная техника»
09.03.04 «Программная инженерия»

Направленность: Автоматизированные системы обработки информации и управления, Разработка программно-информационных систем

Квалификация (степень): бакалавр

	Форма обучения
	Очная
Курс	4
Семестр	7
Лекции, часы	30
Лабораторные работы, часы	30
Экзамен, семестр	7
Контактная работа по учебным занятиям, часы	60
Самостоятельная работа, часы	84
Всего часов / зачетных единиц	144/4

Кафедра-разработчик программы: Программное обеспечение информационных технологий

Составитель: канд. техн. наук, доцент В. В. Кутузов

Могилев, 2022

Рабочая программа составлена в соответствии с федеральным государственным образовательными стандартами высшего образования по направлениям подготовки 09.03.01 «Автоматизированные системы обработки информации и управления» и 09.03.04 «Программная инженерия» (уровень бакалавриата), утвержденные приказом № 929 от 19.09.2017 г., № 920 от 19.09.2017 г., учебными планами рег. №090301-5 и №090304-5, утвержденными 25.03.2022 г.

Рассмотрена и рекомендована к утверждению кафедрой «Программное обеспечение информационных технологий» «08» 04 2022 г., протокол № 10.

Зав. кафедрой ПОИТ _____ В. В. Кутузов

Одобрена и рекомендована к утверждению Научно-методическим советом Белорусско-Российского университета

«15» 06 2022 г., протокол № 7.

Зам. председателя
Научно-методического совета _____ С.А. Сухоцкий

Рецензент:
Мозолькова Е.В., ИО начальника управления информационных технологий ОАО «Лента»

Рабочая программа согласована:

Ведущий библиотекарь _____ Е. Н. Киселева

Начальник учебно-методического
отдела _____ В.А. Кемова

1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1 Цель учебной дисциплины

Цель учебной дисциплины - обучение студентов основным методам обеспечения информационной безопасности, средствам защиты информации, современным аппаратным и программным алгоритмам шифрования информации, построения надежных систем хранения информации, а также изучение перспективных направлений в развитии современных средств обеспечения информационной безопасности.

1.2 Планируемые результаты изучения дисциплины

В результате освоения учебной дисциплины студент должен

знать:

- основные понятия информационной безопасности;
- требования к системам защиты информации;
- принципы построения систем защиты информации;
- основные алгоритмы шифрования информации;
- методы проверки подлинности составляющих информационного процесса

уметь:

- проектировать структуру и выбирать составные компоненты систем защиты данных;
- применять методы и средства защиты компьютерной информации;
- оценивать надежность методов защиты компьютерной информации

владеть:

- навыками для оценки надежности методов защиты компьютерной информации;
- методологией проверки подлинности составляющих информационного процесса;
- технологией обеспечения информационной безопасности компьютерных систем

1.3 Место учебной дисциплины в системе подготовки студента

Дисциплина относится к блоку 1 Дисциплины (модули). Обязательная часть блока 1. Часть Блока 1. Формируемая участниками образовательных отношений.

Перечень учебных дисциплин, изучаемых ранее, усвоение которых необходимо для изучения данной дисциплины:

- Программирование;
- Практика написания программного кода;
- Базы данных;
- Основы WEB-программирования/ Технологии интернет-программирования;
- Операционные системы (5, 6 сем);

Перечень учебных дисциплин (циклов дисциплин), которые будут опираться на данную дисциплину: управление IT-проектами.

Кроме того, знания, полученные при изучении дисциплины на практических работах будут применены при прохождении преддипломной практики, а также при подготовке выпускной квалификационной работы и дальнейшей профессиональной деятельности

1.4 Требования к освоению учебной дисциплины

Освоение данной учебной дисциплины должно обеспечивать формирование следующих компетенций:

Коды формируемых компетенций	Наименование формируемых компетенций для направления подготовки 09.03.01 Информатика и вычислительная техника
ПК-12	Способен обеспечивать информационную безопасность уровня баз данных
ПК-13	Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения

Коды формируемых компетенций	Наименование формируемых компетенций для направления подготовки 09.03.04 Программная инженерия
ПК-9	Владение навыками использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных

2 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Вклад дисциплины в формирование результатов обучения выпускника (компетенций) и достижение обобщенных результатов обучения происходит путём освоения содержания обучения и достижения частных результатов обучения, описанных в данном разделе.

2.1 Содержание учебной дисциплины

Номер тем	Наименование тем	Содержание	Коды формируемых компетенций	
			09.03.01	09.03.04
1.	Основы информационной безопасности, методов и средств защиты информации	Основы информационной безопасности, методов и средств защиты информации. Методы и средства защиты информации. Рекомендуемая литература. Основные понятия и терминология информационной безопасности. Цель и объект защиты информации. Задачи в сфере обеспечения информационной безопасности. Виды информации. Классификация видов информации. Информационные системы. Классификация. Нарушители информационной безопасности. Методы защиты информации. Классификация средства защиты информации.	ПК-12 ПК-13	ПК-9
2.	Правовое и нормативное обеспечение защиты информации	Правовое и нормативное обеспечение защиты информации. Комплексный подход к обеспечению защиты объектов информационной безопасности. Классификация методов защиты информации. Законодательная база Республики Беларусь. Стандарты и рекомендации в области информационной безопасности, применяемых в рамках реализации цифровой повестки Евразийского экономического союза. Законодательная база Российской Федерации. Международное законодательство в области информационной безопасности. Стандарты ISO в области IT-безопасности	ПК-12 ПК-13	ПК-9
3.	Защита персональных данных	Персональные данные. Термины и определения. Защита персональных данных. Законодательство по защите персональных данных. Обработка персональных данных. Операторы персональных данных. Утечки персональных данных.	ПК-12 ПК-13	ПК-9

4.	Угрозы информационной безопасности	Уязвимости информации. Угрозы. Угрозы информационной безопасности. Задачи организационного обеспечения защиты информации. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Типовые модели нарушителя для различных категорий лиц. Методики оценки и моделирования угроз. Базы и банки данных угроз безопасности информации	ПК-12 ПК-13	ПК-9
5.	Управление рисками Информационной безопасности	Управление рисками информационной безопасности. Риск ориентированный подход. Общая концепция управления рисками информационной безопасности. Карты рисков. Логика снижения уровня риска до приемлемого уровня. Классификации рисков. Ущерб от реализации атаки. Методологии риск-менеджмента. Методики оценки рисков информационной безопасности	ПК-12 ПК-13	ПК-9
6.	Политика информационной безопасности в организациях	Политика информационной безопасности в организациях. Безопасность предприятия. Обеспечение безопасности организации и её персонала. Служба безопасности предприятия (организации). Функции службы безопасности. Пример структур служб безопасности. Электронные средства охраны, безопасности и контроля. Политика безопасности предприятия (организации). Рекомендуемые области разработки политики информационной безопасности	ПК-12 ПК-13	ПК-9
7.	Критическая инфраструктура. Критическая информационная инфраструктура	Критическая инфраструктура. Критическая информационная инфраструктура. Законодательство. История атак на критическую инфраструктуру. Атаки и меры защиты.	ПК-12 ПК-13	ПК-9
8.	Идентификация, аутентификация и авторизация	Идентификация, аутентификация и авторизация. Общие сведения. Классификация средств идентификации и аутентификации с точки зрения применяемых технологий. Технологии аутентификации. Двухфакторная аутентификация. Протоколы аутентификации. Биометрическая аутентификация. Аутентификация с помощью одноразовых паролей. Аутентификация с использованием токенов. Применение криптографических алгоритмов при идентификации и аутентификации	ПК-12 ПК-13	ПК-9
9.	Криптография	Криптография. Применение криптографических средств защиты информации. Шифры. Классификация криптографических алгоритмов. Примеры алгоритмов. Криптография с симметричными ключами. Криптография с асимметричными ключами. Средства криптографической защиты информации. Криптография на практике	ПК-12 ПК-13	ПК-9
10.	Электронная цифровая подпись	Электронная цифровая подпись. Электронная цифровая подпись для аутентификации данных. Алгоритмы электронной цифровой подписи. Стандарты цифровой подписи. Практика применения электронной цифровой подписи.	ПК-12 ПК-13	ПК-9
11.	Защита информации в операционных системах	Защита информации в операционных системах. Общие принципы безопасности операционных систем. Защита компьютерной информации в операционных системах Linux и Windows. Угрозы безопасности операционных систем. Средства защиты информации в операционных системах	ПК-12 ПК-13	ПК-9

12.	Сетевые атаки и защита информации в компьютерных сетях	Сетевые атаки и защита информации в компьютерных сетях. Особенности обеспечения информационной безопасности в компьютерных сетях. Основы компьютерных сетей. Угрозы безопасности в компьютерных сетях. Классификация сетевых (удаленных) атак. Протоколы. Виды сетевых атак. DoS \DDoS Атаки. Программно-аппаратные средства защиты компьютерных систем. Межсетевые экраны (Firewall). VPN. Proxy. SSH туннели. Tor. Antivirus. Мониторинг ИТ-инфраструктуры. Программное обеспечение. Программно-аппаратные средства защиты компьютерных систем.	ПК-12 ПК-13	ПК-9
13.	Защита internet ресурсов, сайтов	Защита internet ресурсов, сайтов. OWASP (Open Web Application Security Project)	ПК-12 ПК-13	ПК-9
14.	Защита приложений и баз данных	Защита приложений. Защита баз данных. Защита приложений и баз данных при их разработке.	ПК-12 ПК-13	ПК-9

2.2 Учебно-методическая карта учебной дисциплины

№ недели	Лекции (наименование тем)	Часы	Лабораторные работы	Часы	Самостоятельная работа, часы	Форма контроля знаний	Баллы (max)
	Модуль 1						
1	**Тема 1.** Основы информационной безопасности, методов и средств защиты информации	2	Лр.р. № 1. Хеширование информации	2	2	ЗЛР	3
2	**Тема 2.** Правовое и нормативное обеспечение защиты информации	2	Лр.р. № 2. Шифрование данных в ОС Linux	2	4	ЗЛР	3
3	**Тема 2.** Правовое и нормативное обеспечение защиты информации	2	Лр.р. № 2. Шифрование данных в ОС Linux	2	2	ЗЛР	4
4	**Тема 3.** Защита персональных данных	2	Лр.р. № 3. Разграничение прав доступа в ОС Linux	2	4	ЗЛР	4
5	**Тема 4.** Угрозы информационной безопасности	2	Лр.р. № 3. Разграничение прав доступа в ОС Linux	2	2	ЗЛР	4
6	**Тема 5.** Управление рисками информационной безопасности	2	Лр.р. № 4. Возможности файловых подсистем Linux для защиты информации	2	4	ЗЛР	4
7	**Тема 6.** Политика информационной безопасности в организациях	2	Лр.р. № 4. Возможности файловых подсистем Linux для защиты информации	2	2	ЗЛР	4
8	**Тема 7.** Критическая инфраструктура. Критическая информационная инфраструктура	2	Лр.р. № 5. Обеспечение целостности и доступности данных с использованием Raid, LVM.	2	4	ЗИЗ ПКУ	4 30
	Модуль 2						
9	**Тема 8**. Идентификация, аутентификация и авторизация	2	Лр.р. № 6. Изучение методов шифрования ОС Windows данных на дисках	2	2	ЗЛР	5
10	**Тема 9** Криптография	2	Лр.р. № 6. Изучение методов шифрования ОС Windows данных на дисках	2	4	ЗЛР	5
11	**Тема 1**0 Электронная цифровая подпись	2	Лр.р. № 7. Средства защиты данных в ОС Windows	2	2	ЗЛР	4

12	**Тема 11**. Защита информации в операционных системах	2	Лр.р. № 7. Средства защиты данных в ОС Windows	2	4	ЗЛР	4
13	**Тема 12.** Сетевые атаки и защита информации в компьютерных сетях	2	Лр.р. № 8. Изучение методов аудита ОС Windows	2	4	ЗЛР	4
14	**Тема 13.** Защита internet ресурсов, сайтов	2	Лр.р. № 8. Изучение методов аудита ОС Windows	2	4	ЗЛР	4
15	**Тема 14.** Защита приложений и баз данных	2	Лр.р. № 9. Основы MS Crypto API	2	4	ЗЛР ПКУ	4 30
16-18					36	ПА (экзамен)	40
	ИТОГО	30		30	84		100

Принятые обозначения:
Текущий контроль:
ЗИЗ – защита индивидуального задания.
ЗЛР – защита лабораторных работ
ПКУ – промежуточный контроль успеваемости.
ПА – промежуточная аттестация

Итоговая оценка определяется как сумма текущего контроля и промежуточной аттестации и соответствует баллам:

Экзамен

Оценка	Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
Баллы	87-100	65-86	51-64	0-50

3 ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При изучении дисциплины используется модульно-рейтинговая система оценки знаний. Применение форм и методов проведения занятий при изучении различных тем курса представлено в таблице.

№ п/п	Форма проведения занятия	Вид аудиторных занятий		Всего часов
		Лекции	лабораторные работы	
1	Мультимедиа	Темы 1–14		30
2	С использованием ЭВМ		Лр. раб. 1–9	30
	ИТОГО	30	30	60

4 ОЦЕНОЧНЫЕ СРЕДСТВА

Используемые оценочные средства по учебной дисциплине представлены в таблице и хранятся на кафедре.

№ п/п	**Вид оценочных средств**	**Количество комплектов**
1	Вопросы к экзамену	1
2	Билеты к экзамену	1
3	Задания к лабораторным работам	9
4	Индивидуальные задания	1

5 МЕТОДИКА И КРИТЕРИИ ОЦЕНКИ КОМПЕТЕНЦИЙ СТУДЕНТОВ

5.1 Уровни сформированности компетенций

Для направления подготовки: 09.03.01 «Информатика и вычислительная техника»

№ п/п	Уровни сформированности компетенции	Содержательное описание уровня	Результаты обучения
ПК-12 Способен обеспечивать информационную безопасность уровня баз данных			
ИПК-12.2. Способен обеспечивать информационную безопасность автоматизированных систем обработки информации и управления			
1	Пороговый уровень	Знает теоретические основы информационной безопасности баз данных	Может обеспечивать на базовом уровне информационную безопасность автоматизированных систем обработки информации и управления и баз данных
2	Продвинутый уровень	Владеет знаниями обеспечения информационной безопасности баз данных и систем обработки информации и управления.	Способен решать стандартные задачи профессиональной деятельности по обеспечению информационной безопасности автоматизированных систем обработки информации и управления и баз данных
3	Высокий уровень	Способен обеспечивать информационную безопасность баз данных и систем обработки информации и управления.	Способен решать нестандартный задачи профессиональной деятельности по обеспечению информационной безопасности автоматизированных систем обработки информации и управления и баз данных
ПК-13 Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения			
ИПК-13.1. Способен осуществлять администрирование сетевых устройств и программного обеспечения инфокоммуникационной системы, включая создание систем информационной безопасности ИПК-13.2. Осуществляет администрирование процесса управления безопасностью программного обеспечения инфокоммуникационной системы			
1	Пороговый уровень	Знает теоретический материал по обеспечению информационную безопасность сетевых устройств и программного обеспечения.	Знает основы администрирования сетевых устройств и программного обеспечения инфокоммуникационной системы
2	Продвинутый уровень	Владеет знаниями теоретических основ администрирования, настройки, управлению безопасности сетевых устройств и программного обеспечения.	Знает, как осуществлять администрирование сетевых устройств и программного обеспечения инфокоммуникационной системы, включая создание систем информационной безопасности
3	Высокий уровень	Владеет навыками администрирования, настройки, управлению безопасности сетевых устройств и программного обеспечения.	Знает и владеет навыками осуществлять администрирование сетевых устройств и программного обеспечения инфокоммуникационной системы, включая создание систем информационной безопасности

Для направления подготовки: 09.03.04 «Программная инженерия»

№ п/п	Уровни сформированности компетенции	Содержательное описание уровня	Результаты обучения
ПК-9. Владение навыками использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных			
ИПК-9.4. Владеет навыками применения современных методов защиты информации			
1	Пороговый уровень	Знает основы информационной безопасности. Понимает способы и протоколы безопасной передачи	Владеет теоретическими навыками применения методов защиты информации

		данных. Может оценить угрозы и риски.	
2	Продвинутый уровень	Владеет теоретическими знаниями информационной безопасности и умеет реализовывать их на практике.	Владение навыками методов защиты информации при использовании операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных
3	Высокий уровень	Владеет современными знаниями информационной безопасности и умеет реализовывать их на практике при использовании операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных.	Способен решать задачи защиты информации при использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных

5.2 Методика оценки знаний, умений и навыков студентов

Для направления подготовки: 09.03.01 «Информатика и вычислительная техника»

Результаты обучения	Оценочные средства
ПК-12 Способен обеспечивать информационную безопасность уровня баз данных	
Может обеспечивать на базовом уровне информационную безопасность автоматизированных систем обработки информации и управления и баз данных	Вопросы для защиты лабораторных работ. Вопросы к экзамену.
Способен решать стандартные задачи профессиональной деятельности по обеспечению информационной безопасности автоматизированных систем обработки информации и управления и баз данных	Вопросы для защиты лабораторных работ. Вопросы к экзамену.
Способен решать нестандартный задачи профессиональной деятельности по обеспечению информационной безопасности автоматизированных систем обработки информации и управления и баз данных	Вопросы для защиты лабораторных работ. Вопросы к экзамену.
ПК-13 Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения	
Знает основы администрирования сетевых устройств и программного обеспечения инфокоммуникационной системы	Вопросы для защиты лабораторных работ. Вопросы к экзамену.
Знает, как осуществлять администрирование сетевых устройств и программного обеспечения инфокоммуникационной системы, включая создание систем информационной безопасности	Вопросы для защиты лабораторных работ. Вопросы к экзамену.
Знает и владеет навыками осуществлять администрирование сетевых устройств и программного обеспечения инфокоммуникационной системы, включая создание систем информационной безопасности	Вопросы для защиты лабораторных работ. Вопросы к экзамену.

Для направления подготовки: 09.03.04 «Программная инженерия»

Результаты обучения	Оценочные средства
Компетенция ПК-9. Владение навыками использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных	
Владеет теоретическими навыками применения методов защиты информации	Вопросы для защиты лабораторных работ. Вопросы к экзамену.

Владение навыками методов защиты информации при использовании операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных	Вопросы для защиты лабораторных работ. Вопросы к экзамену.
Способен решать задачи защиты информации при использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных	Вопросы для защиты лабораторных работ. Вопросы к экзамену.

5.3 Критерии оценки лабораторных работ.

Студент обязан самостоятельно в полном объеме выполнить лабораторные работы согласно рабочей программе.

Задание на работы выдает ведущий занятия преподаватель.

По результатам выполнения работ студент обязан оформить отчет по лабораторной работе в соответствии с действующими в Университете требованиями по оформлению отчета.

Отсутствие отчета является причиной недопуска к сдаче лабораторной работы.

Защита отчета проводится устно, путем ответов на контрольные вопросы к работе, решения задачи по теме лабораторной работы и демонстрации навыков, полученных при выполнении работы.

При защите лабораторной работы студент имеет право пользоваться собственноручно оформленным отчетом.

При отсутствии ответов на заданные преподавателем вопросы отчет не засчитывается и баллы не выставляются.

Правильные ответы оцениваются согласно оценочным уровням сформированности компетенций по изучаемой теме.

Каждая выполненная и защищенная работа оцениваются на 3-5 баллов в зависимости от качества оформления и уровня знаний студента по тематике работы. Если по окончанию модуля лабораторная работа выполнена, но не защищена, то баллы по ней не начисляются, и она попадает в разряд задолженности.

5.4 Критерии оценки экзамена.

Экзаменационный билет включает два теоретических вопроса и одно практическое задание. Практическое задание выполняется с использованием компьютера. Содержание задание соответствует тематике, рассмотренной в процессе выполнения практических и лабораторных работ

Каждый теоретический вопрос оценивается положительной оценкой в диапазоне от 5 до 12 баллов. Практическое задание оценивается положительной оценкой в диапазоне от 5 до 16 баллов

Ответы по следующим критериям.

Теоретические вопросы:

- **12 баллов** – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, использует научную терминологию, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности, дает развернутый ответ на поставленный вопрос и четко отвечает на дополнительные вопросы.

- **10 баллов** – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности, но допускает отдельные неточности, в том числе и на дополнительные вопросы.
- **8 баллов** – студент хорошо понимает пройденный материал, отвечает правильно, умеет оценивать факты, самостоятельно рассуждает, обосновывает выводы и разъясняет их, но допускает ошибки общего характера.
- **6 баллов** – студент понимает пройденный материал, но не может теоретически обосновать некоторые выводы, допускает ошибки общего характера.
- **5 баллов** – в ответе студента имеются существенные недостатки, материал охвачен «половинчато», в рассуждениях допускаются ошибки
- **Ниже 5 баллов** – студент имеет общее представление о вопросе, ответ студента правилен лишь частично, при разъяснении материала допускаются серьезные ошибки, отсутствует техническая терминология, не может исправить ошибки с помощью наводящих вопросов;

Практическое задание:

- **16 баллов** – студент правильно и грамотно решает предложенную задачу, четко поясняет методику решения поставленной задачи, получает правильный ответ и дает обоснование результатов, четко отвечает на дополнительные вопросы.
- **14 баллов** – студент правильно и грамотно решает предложенную задачу, четко поясняет методику решения поставленной задачи, получает правильный ответ и дает обоснование результатов, отвечает не на все дополнительные вопросы.
- **12 баллов** – студент правильно и грамотно решает предложенную задачу, поясняет методику решения поставленной задачи, получает правильный, но не полный ответ и дает обоснование результатов, отвечает не на все дополнительные вопросы.
- **10 баллов** – – студент правильно и грамотно решает предложенную задачу, поясняет методику решения поставленной задачи, получает правильный, но не полный ответ и не дает полного обоснование результатов, отвечает не на все дополнительные вопросы.
- **8 баллов** студент с ошибками решает предложенную задачу, поясняет методику решения поставленной задачи, получает не полный ответ и не дает полного обоснование результатов, отвечает не на все дополнительные вопросы.
- **5 балла** – студент с ошибками решает предложенную задачу, не поясняет методику решения поставленной задачи, получает не полный ответ и не дает полного обоснование результатов, отвечает не на все дополнительные вопросы
- **Ниже 5 баллов** – студент не решает предложенную задачу.

6 МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Самостоятельная работа студентов (СРС) направлена на закрепление и углубление освоения учебного материала, развитие практических умений. СРС включает следующие виды самостоятельной работы студентов:

Перечень контрольных вопросов и заданий для самостоятельной работы студентов хранится на кафедре.

Виды самостоятельной работы

- проработка тем (вопросов), вынесенных на самостоятельное изучение;
- конспектирование учебной литературы;

- подготовка докладов;
- подготовка презентаций;
- подготовка рефератов.

Для СРС рекомендуется использовать источники, приведенные в п. 7.

7 УЧЕБНО- МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

7.1 Основная литература

№ п/п	Библиографическое описание	Гриф***	Количество экземпляров
1	Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: учеб. пособие / А.П. Жук и др. - 3-е изд., - Москва: РИОР:ИНФРА-М, 2021. – 400 с	Рек. УМО по образованию в области информационных технологий и систем связи в качестве учебного пособия для студентов высших учебных заведений»	https://znanium.com/catalog/product/1210523
2	Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. –Москва : ИНФРА-М, 2022. –201 с.	Рек. Межрегиональным учебно-методическим советом профессионального образования в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность» (квалификация «бакалавр»)	https://znanium.com/catalog/product/1844364

7.2 Дополнительная литература

№ п/п	Библиографическое описание	Гриф	Количество экземпляров
1	Герман, О. Н. Теоретико-числовые методы в криптографии : учебник для студентов вузов / О. Н. Герман, Ю. В. Нестеренко. - М. : Академия, 2012. - 272с	Учебник создан в соответствии с ФГОС по направлениям подготовки "Информационная безопасность" и "Математика"	2
2	Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с.	Допущено Учебно-методическим объединением по образованию в области прикладной информатики в качестве учебного пособия для студентов, обучающихся по направлению «Прикладная информатика»	https://znanium.com/catalog/product/1861657
3	Информационная безопасность сетей и систем : учеб. пособие / В. И. Аверченков, В. Т. Еременко, Е. А. Зайченко. – Могилев : Белорус.-Рос. ун-т, 2020. — 212с.	Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве пособия для специальности 1 -53 01 02 “Автоматизированные системы обработки информации” Президиума Совета УМО по образованию в области информатики и радиоэлектроники)	66
4	Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие для вузов / В.П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 6-е изд., стер. - М. : Академия, 2012. – 336с	Рек. МО и науки РФ в качестве учеб. пособия для студентов вузов	1
5	Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2022. — 327 с.	—	https://znanium.com/catalog/product/1865598
6	Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов / Ю. Н. Сычев. - Москва : ИНФРА-М, 2021. - 223 с.	—	https://znanium.com/catalog/product/1178148

7.3 Перечень ресурсов сети Интернет по изучаемой дисциплине

http://moodle.bru.by – Образовательный портал Белорусско-Российского университета;

http://e.biblio.bru.by/ – Электронная библиотека Белорусско-Российского университета;

https://znanium.com/ – Электронно-библиотечная система Znanium;

https://stepik.org/catalog – Российская образовательная платформа и конструктор бесплатных открытых онлайн-курсов и уроков;

https://openedu.ru – Открытое образование

https://habr.com/ru/ – Хабр. Публикации по ИТ тематикам;

7.4 Перечень наглядных и других пособий, методических рекомендаций по проведению учебных занятий, а также методических материалов к используемым в образовательном процессе техническим средствам

7.4.1 Методические рекомендации

Защита информации. Методические указания к выполнению лабораторных работ для студентов направления подготовки 09.03.01 «Информатика и вычислительная техника», 09.03.04 «Программная инженерия». – Могилев, 2022 (электронный вариант).

7.4.2 Информационные технологии

Мультимедийные презентации

Тема 1. Основы информационной безопасности, методов и средств защиты информации

Тема 2. Правовое и нормативное обеспечение защиты информации

Тема 3. Защита персональных данных

Тема 4. Угрозы информационной безопасности

Тема 5. Управление рисками информационной безопасности

Тема 6. Политика информационной безопасности в организациях

Тема 7. Критическая инфраструктура. Критическая информационная инфраструктура

Тема 8. Идентификация, аутентификация и авторизация

Тема 9. Криптография

Тема 10. Электронная цифровая подпись

Тема 11. Защита информации в операционных системах

Тема 12. Сетевые атаки и защита информации в компьютерных сетях

Тема 13. Защита internet ресурсов, сайтов

Тема 14. Защита приложений и баз данных

7.4.3 Перечень программного обеспечения, используемого в образовательном процессе

1. Виртуальная машина Hyper-V (свободно распространяемое)
2. Microsoft Office (лицензия)

8 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины содержится в паспорте лаборатории а. 517/2 , рег. № паспорта лаборатории № ПУЛ - 4 517/2-21; в паспорте лаборатории а. 518/2 , рег. № паспорта лаборатории № ПУЛ - 4 518/2-21.