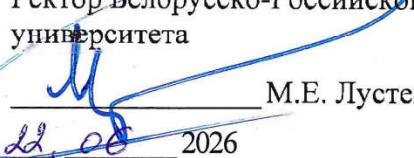


Межгосударственное образовательное учреждение высшего образования
«Белорусско-Российский университет»

Документ подписан
простой электронной подписью
Информация о владельце:
ФИО: Лустенков Михаил Евгеньевич
Должность: Ректор
Дата: 09.09.2026

УТВЕРЖДАЮ
Ректор Белорусско-Российского
университета

 М.Е. Лустенков

 2026

Регистрационный № УД-380308/Б.1.В.9/р

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
(наименование дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 38.03.02 Менеджмент

Направленность (профиль) Управление электронным бизнесом

Квалификация бакалавр

	Форма обучения
	Очная
Курс	3
Семестр	6
Лекции, часы	34
Лабораторные работы, часы	34
Зачёт, семестр	6
Контактная работа по учебным занятиям, часы	68
Самостоятельная работа, часы	40
Всего часов / зачетных единиц	108/3

Кафедра-разработчик программы: «Программное обеспечение информационных технологий»

(название кафедры)

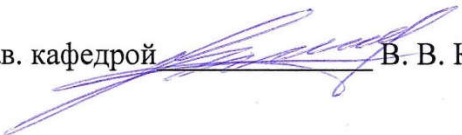
Составитель: Кутузов Виктор Владимировича, канд. техн. наук, доцент

(И.О. Фамилия, ученая степень, ученое звание)

Могилев, 2026

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования - бакалавриат по направлению подготовки 38.03.02 «Менеджмент» утвержденным приказом № 970 от 12.08.2020, учебными планами рег. №380302-2.1 утвержденными 18.02.2026.

Рассмотрена и рекомендована к утверждению кафедрой «Программное обеспечение информационных технологий» 02.03.2026, протокол № 8.

Зав. кафедрой  В. В. Кутузов

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

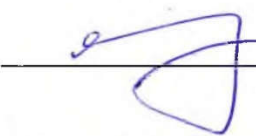
15.04.2025, протокол № 6.

Рецензент:

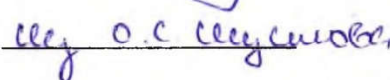
И. В. Акиншева, заведующая кафедрой программного обеспечения информационных технологий МГУ им. А.А. Кулешова, канд. техн. наук, доцент

Рабочая программа дисциплины согласована

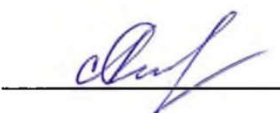
Зав. кафедрой «Маркетинг и менеджмент»

 А. В. Александров

Ведущий библиотекарь

 О. С. Сущикова

Начальник учебно-методического отдела

 О.Е. Печковская

1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1 Цель дисциплины

Целью изучения дисциплины является 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 дисциплины в системе подготовки

Дисциплина «Основы информационной безопасности» относится к Блоку 1 формируемая участниками образовательных отношений.

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

- Информатика;
- Информационные ресурсы организации;
- Программирование на языке Python;

Перечень учебных дисциплин (циклов дисциплин), которые будут опираться на данную дисциплину:

- Риск-менеджмент;
- Информационные системы корпоративного управления.

Кроме того, знания, полученные при изучении дисциплины на лабораторных занятиях будут применены при прохождении технологической (проектно-технологической) практики, организационно-управленческой практики, а также при выполнении выпускной квалификационной работы и дальнейшей профессиональной деятельности.

1.4 Требования к освоению дисциплины

Освоение данной дисциплины должно обеспечивать формирование следующих компетенций:

Коды формируемых компетенций	Наименования формируемых компетенций
ПК-1.	Способен разрабатывать и поддерживать функционирование системы внутреннего документооборота, ведение баз данных по различным показателям деятельности организации

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 дисциплины

Номер тем	Наименование тем	Содержание	Коды формируемых компетенций
1.	Основы информационной безопасности	Основы информационной безопасности. Рекомендуемая литература. Основные понятия и терминология, относящаяся к информационной безопасности. Цель и объект защиты информации. Необходимость защиты информации. Задачи в сфере обеспечения информационной безопасности. Информация. Виды информации. Классификация видов информации. Классификация защищаемой информации. Информационные системы и их классификация. Ключевые вопросы информационной безопасности: надо ли защищаться и что следует защищать? от кого надо защищаться? от чего надо защищаться? как надо защищаться? что обеспечит эффективность защиты? во что обойдется разработка, внедрение, эксплуатация, сопровождение и развитие систем защиты? Нарушители информационной безопасности. Методы защиты информации. Классификация средства защиты информации.	ПК-1
2.	Правовое и нормативное обеспечение защиты информации	Правовое и нормативное обеспечение защиты информации. Комплексный подход к обеспечению защиты объектов информационной безопасности. Законодательная база Республики Беларусь в области защиты информации и информационной безопасности в целом. Стандарты и рекомендации в области информационной безопасности, применяемых в рамках реализации цифровой повестки Евразийского экономического союза и Союзного государства. Законодательная база Российской Федерации в области защиты информации и информационной безопасности в целом. Руководящие документы ФСТЭК России.	ПК-1

		Владельцы защищаемой информации. Понятие государственная тайна, коммерческая тайна. Профессиональная тайна, служебная тайна. Международное законодательство и стандарты информационной безопасности Стандарты ISO в области IT-безопасности. Группа международных стандартов 27000 ISO/IEC 27000 Series. ISO/IEC 17799 Законодательная база США, Европы, Великобритании, Канады, Китая и других стран в вопросах информационной безопасности. Международные организации в сфере информационной безопасности	
3.	Защита персональных данных	Персональные данные. Термины и определения. Защита персональных данных. Законодательство по защите персональных данных. Штрафы за нарушения законов по защите персональных данных. Обработка персональных данных. Операторы персональных данных. Утечки персональных данных.	ПК-1
4.	Угрозы информационной безопасности	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. Уязвимости. Утечки информации. Наиболее распространенные угрозы доступности. Примеры угроз доступности. Основные угрозы целостности. Основные угрозы конфиденциальности. Методики оценки и моделирования угроз. Базы и банки данных угроз безопасности информации Моделирование угроз корпоративной инфраструктуры	ПК-1
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-1
6.	Безопасность в организациях. Политика информационной безопасности и реализация её в организациях	Безопасность предприятия (организации). Политика безопасности предприятия (организации). Политика информационной безопасности в организациях. Служба безопасности предприятия (организации). Функции службы безопасности. Пример структур служб безопасности. Обеспечение безопасности организации и её персонала. Организация внутриобъектового и пропускного режимов на предприятиях. Электронные средства охраны, безопасности и контроля. Рекомендуемые области разработки политики информационной безопасности. Внедрение политики компании в области информационной безопасности. Контроль соблюдения политики безопасности.	ПК-1

		Специализированные системы, сервисы, платформы и программное обеспечение для обеспечения информационной безопасности в организации – Системы электронного документооборота (СЭД); – Системы антивирусной защиты; – Системы мониторинга и защиты от атак из сети; – Security information and event management (SIEM) – Security Operations Center (SOC) – Security Orchestration, Automation and Response (SOAR) – Incident Response Platform (IRP) – Security Governance, Risk-management and Compliance (SGRC) – Data Leak Prevention (DPL) и др.	
7.	Практические инструменты информационной безопасности в организациях	Электронная цифровая подпись Шифрование данных Стратегии противодействия киберпреступности. Исследования киберугроз, целевых атак и группировок. Центр обеспечения безопасности (Security Operations Center (SOC)). Центр обеспечения кибербезопасности (Cybersecurity Operations Center (CSOC)). Группа экстренного реагирования на компьютерные инциденты (Computer Emergency Response Team (CERT)). Коммерческие центры мониторинга и реагирования на компьютерные инциденты (JSOC). Реагирование на инциденты информационной безопасности. Комплексный аудит информационной безопасности (современный контекст безопасности. требует принципиально нового подхода к проведению аудита; оценки только технической оснащенности уже недостаточно для гарантии готовности к сложным атакам).	ПК-1
8.	Безопасность критически важных объектов и критической информационной инфраструктуры	Безопасность критически важных объектов и критической информационной инфраструктуры. Основные термины и определения. Критическая инфраструктура. Общая характеристика критически важных объектов. Признаки принадлежности к критически важным объектам. Последствия нарушения функционирования критически важных объектов. Информационная безопасность объектов критически важных инфраструктур. Критическая информационная инфраструктура. Нормативная база, регламентирующая обеспечение информационной безопасности критически важных объектов и критической информационной инфраструктуры. История атак на критическую инфраструктуру. Угрозы. Риски. Уязвимости. Атаки и меры защиты. Системы контроля. Аудит.	ПК-1
9.	Кибербезопасность и киберпреступность	Концептуальные основы кибербезопасности. Законодательство и стандарты в вопросах кибербезопасности. Базовые меры по кибербезопасности. Виды и методы киберпреступлений. Цели и методы работы современных киберпреступников. Портрет потенциального злоумышленника. Экосистема теневого сегмента сети Интернет. Основные причины роста числа киберпреступлений. Криптовалюты и анонимные сети. Краткий обзор методов сокрытия авторства преступления и способов обналаживания похищенных средств на примере технологий VPN, Tor и криптовалюты Bitcoin	ПК-1

		Классификация киберпреступлений. Компьютерные преступления, и согласовывание их с международными нормами права. Атрибуция кибератак. Понятие источника действий в сети Интернет. Методы атрибуции источника кибератак. Возможность однозначно установить источник кибератак. Обзор практических кейсов. Основы компьютерной криминалистики. Понятие доказательств в цифровом виде. Источники сбора доказательств в цифровом виде. Методы и правовые основы компьютерно-технических экспертиз. Взаимодействие с правоохранительными органами и экспертными организациями в части расследования киберпреступлений. Основные направления деятельности Центры реагирования на кибер-инциденты.	
10.	Защита информации в операционных системах	Защита информации в операционных системах (ОС). Общие принципы безопасности операционных систем. Угрозы безопасности операционных систем. Средства защиты информации в ОС. Защита компьютерной информации в Windows, Linux и других ОС. Основы безопасности Windows. Архитектура Windows, службы, реестр, основные процессы, учетные записи, Аутентификация, NTLM, Kerberos, журналы событий. Windows Server. Active Directory. Удаленное администрирование. Удаленный рабочий стол. Основы безопасности Linux. Архитектура ядра, файловая система, БД структура каталогов, логи, основные типы событий, основные процессы, Crontab и демоны, пользователи, биты доступа файлов. Системы виртуализации. Docker. Kubernetes. DevOps. DevSecOps	ПК-1
11.	Сетевые атаки и защита информации в компьютерных сетях	Особенности обеспечения информационной безопасности в компьютерных сетях. Компьютерные сети. Сетевые модели передачи данных Угрозы безопасности в компьютерных сетях. Классификация сетевых (удаленных) атак. Обеспечение безопасности в рамках модели OSI. Уязвимости и атаки по уровням модели OSI. Сетевые атаки. DoS \DDoS Атаки. Программно-аппаратные средства защиты компьютерных систем. Технологии межсетевого экранирования (Firewall). Методы защиты компьютерных сетей от внешних угроз. Методы защиты компьютерных сетей от внутренних угроз. Мониторинг ИТ-инфраструктуры. Системы обнаружения и предотвращения атак. Программное и аппаратное обеспечение. Безопасность удаленного соединения. Организация удаленной работы через интернет. Организация виртуальных частных сетей (VPN). Proxy. SSH туннели. Tor. Организация доступа к заблокированным интернет-ресурсам и сервисам.	ПК-1
12.	Применение технологий искусственного	Искусственный интеллект (ИИ). Машинное обучение. Нейронные сети. Компьютерное зрение. ChatGPT и аналоги.	ПК-1

	интеллекта в информационной безопасности	Преимущества ИИ. Технологии ИИ и защита информации. Угрозы применения ИИ. Новые риски информационной безопасности. Использование ИИ в противоправных целях. Применение генеративных моделей для дезинформации. Дипфейки (Deep Fake. Fake News). Fake Detection. Классификация продуктов с технологиями ИИ по сценариям применения: – EDR (Endpoint Detection and Response) – NDR (Network Detection and Response) – UEBA (User and Entity Behavior Analytics) – TIP (Threat Intelligence Platform) – SIEM (Security Information and Event Management) – SOAR (Security Orchestration and Automated Response) – Средства защиты приложений (Application Security) – Антифрод (Antifraud) и др. Перспективные технологии и новые вызовы безопасности. Будущее информационной безопасности. Применение технологии Больших данных и ИИ в обеспечении кибербезопасности. Квантовые вычисления.	
13.	Обеспечение и реализация защиты информации в разрабатываемом программном обеспечении и в базах данных	Безопасная разработка и уязвимости программного кода. Разработка безопасного программного обеспечения. Угрозы и уязвимости информационной безопасности при разработке ПО. Безопасное ПО. Тестирование и анализ ПО. Фаззинг. Инструментальные среды и средства разработки и анализа ПО. Управление конфигурацией ПО. Документация разработчика ПО. Цели создание безопасного ПО и меры по их достижению. Основные нормативно-правовые акты в области создания безопасного ПО (ГОСТ Р 56939, ГОСТ Р 56546, ГОСТ Р 58412, ГОСТ Р ИСО/МЭК 18045, ГОСТ Р ИСО-МЭК 27034-1, ГОСТ Р ИСО-МЭК 27034-7 и др.). Проектирование ПО с учетом требований стандартов безопасности. Угрозы, уязвимости, риски информационной безопасности при разработке ПО - их выявление и оценка. Дефекты и уязвимости программного обеспечения. Угрозы безопасности информации при разработке ПО (по ГОСТ Р 58412). Классификация уязвимостей информационных систем (по ГОСТ Р 56546). Выявление угроз безопасности информации при разработке ПО. Оценка уровня доверия безопасности ПО (степени соответствия выявленной безопасности ПО предъявленным требованиям) (по ГОСТ Р ИСО-МЭК 27034-7). Методы и средства оценки рисков информационной безопасности при создании ПО. Организационные и технические меры по разработке безопасного ПО, реализуемых на различных стадиях жизненного цикла разработки безопасного ПО. Меры по разработке безопасного ПО, реализуемые при выполнении анализа требований к ПО. Тестирование и анализ ПО. Виды тестирования ПО. Защита ПО от взлома и несанкционированного использования. Базы данных. Администрирование баз данных. Технологии защиты баз данных. Организация защиты данных в хранилищах. Способы контроля доступа к данным и управления привилегиями Атаки на базы данных. Поиск уязвимостей к атакам SQL-injection Технология разработки и защиты баз данных.	ПК-1

14.	Технологии обеспечения безопасности веб-приложений	Основные принципы построения безопасных сайтов. Регламенты и методы разработки безопасных веб-приложений Атаки на веб-приложения. Уязвимости веб-приложений. Программное обеспечение для поиска уязвимостей в веб-приложениях. Защита веб-приложений. Безопасная аутентификация и авторизация. Проверка корректности данных, вводимых пользователем. Классификация уязвимостей Web-приложений OWASP TOP 10 и Web Application Security Consortium Threat Classification. OWASP. CVE. CWE. CVE. CVSS. KEV Получение информации о веб-приложении. Методы поиска уязвимостей в веб-приложениях. Технологии обеспечения безопасности веб-приложений.	ПК-1
15.	Экономические аспекты защиты информации и информационной безопасности в целом	Введение в экономические аспекты защиты информации и информационной безопасности в целом Экономические факторы и их роль в обеспечении информационной безопасности Информационная безопасность автоматизированных систем, угрозы и последствия нарушения безопасности автоматизированных систем Экономическая оценка обеспечения информационной безопасности автоматизированных систем Оценка затрат на обеспечение кибербезопасности автоматизированных систем Анализ затрат и выгод инвестирования в информационную безопасность Экономические проблемы информационной защиты. Виды ущерба от несанкционированного доступа (НСД) к информации. Методы оценки ущерба от НСД. Основные методы определения затрат на информационную безопасность. Оценка экономического эффекта защиты информации. Страхование как метод защиты информации. Экономическая эффективность защиты информации. Экономические последствия нарушений информационной безопасности Экономическая эффективность инвестиций в защиту информации.	ПК-1

2.2 Учебно-методическая карта дисциплины

№ недели	Лекции (наименование тем)	Часы	Лабораторные занятия	Часы	Самостоятельная работа, часы	Форма контроля знаний	Баллы (max)
	Модуль 1						
1	Тема 1. Основы информационной безопасности	2	Лр.р. № 1. Хеширование информации	2	4	ЗЛР	3
2	Тема 2. Правовое и нормативное обеспечение защиты информации	2	Лр.р. № 1. Хеширование информации	2	2	ЗЛР	3
3	Тема 2. Правовое и нормативное обеспечение защиты информации	2	Лр.р. № 2. Основы криптографии и шифрования	2	2	ЗЛР	3
4	Тема 3. Защита персональных данных	2	Лр.р. № 2. Основы криптографии и шифрования	2	2	ЗЛР	3
5	Тема 4. Угрозы информационной безопасности	2	Лр.р. № 3 Средства защиты документов Microsoft Office и PDF	2	2	ЗЛР	3

6	Тема 5. Управление рисками информационной безопасности	2	Л.р. № 4. Исследование надежности паролей и их восстановление	2	4	ЗЛР	3
7	Тема 6. Безопасность в организациях. Политика информационной безопасности и реализация её в организациях	2	Л.р. № 4. Исследование надежности паролей и их восстановление	2	2	ЗЛР	3
8	Тема 7. Практические инструменты информационной безопасности в организациях	2	Л.р. № 5. Безопасное хранение файлов на съемных носителях, диске и облачном хранилище	2	2	ТЗ ТКУ	9 30
Модуль 2							
9	Тема 8. Безопасность критически важных объектов и критической информационной инфраструктуры	2	Л.р. № 5. Безопасное хранение файлов на съемных носителях, диске и облачном хранилище	2	4	ЗЛР	3
10	Тема 9. Кибербезопасность и киберпреступность	2	Л.р. № 6. Восстановление удаленной информации	2	2	ЗЛР	3
11	Тема 10. Защита информации в операционных системах	2	Л.р. № 6. Восстановление удаленной информации	2	2	ЗЛР	3
12	Тема 11. Сетевые атаки и защита информации в компьютерных сетях	2	Л.р. № 7. Оценка рисков информационной безопасности организаций	2	2	ЗЛР	3
13	Тема 12. Применение технологий искусственного интеллекта в информационной безопасности	2	Л.р. № 7. Оценка рисков информационной безопасности организаций	2	2	ЗЛР	3
14	Тема 12. Применение технологий искусственного интеллекта в информационной безопасности	2	Л.р. № 8. Применение технологий ИИ и нейронных сетей в информационной безопасности	2	2	ЗЛР	3
15	Тема 13. Обеспечение и реализация защиты информации в разрабатываемом программном обеспечении и в базах данных	2	Л.р. № 8. Применение технологий ИИ и нейронных сетей в информационной безопасности	2	2	ЗЛР	3
16	Тема 14. Технологии обеспечения безопасности веб-приложений	2	Л.р. № 9. Средства защиты данных в ОС Windows	2	2	ЗЛР	3
17	Тема 15. Экономические аспекты защиты информации и информационной безопасности в целом	2	Л.р. № 9. Средства защиты данных в ОС Windows	2	2	ТЗ ТКУ ПА* (зачет)	6 30 40
Итого		34		34	40		100

Принятые обозначения:

ЗЛР – защита лабораторных работ;

ТКУ – текущий контроль успеваемости;

ТЗ – тестовые задания;

ПА – промежуточная аттестация.

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

Зачет

Оценка	Зачтено	Не зачтено
Баллы	51-100	0-50

3 ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При изучении дисциплины используется модульно-рейтинговая система оценки знаний студентов. 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 занятия	
1	Мультимедиа	Темы 1–15		34
2	С использованием ЭВМ		Лаб. 1–9	34
	ИТОГО	34	34	68

4 ОЦЕНОЧНЫЕ СРЕДСТВА

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

№ п/п	Вид оценочных средств	Количество комплектов
1	Вопросы к зачету	1
2	Вопросы к лабораторным работам	9
3	Тестовые задания	1

5 КРИТЕРИИ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

5.1 Формируемые компетенции и индикаторы их достижения

ПК-1. Способен разрабатывать и поддерживать функционирование системы внутреннего документооборота, ведение баз данных по различным показателям деятельности организации
ИПК-1.3. Обеспечивает безопасность информации с учетом способов ее представления
Знает основные понятия и принципы информационной безопасности, требования нормативно-правовых актов РФ, РФ и международных стандартов в области защиты информации; классификацию угроз, уязвимостей и методов криптографической защиты; принципы построения политик ИБ и организации службы безопасности; технологии защиты в ОС, сетях и веб-приложениях; методики оценки рисков; требования к безопасной разработке ПО и администрированию баз данных; функциональные возможности платформ ИБ и экономические аспекты защиты информации.
Умеет анализировать угрозы и уязвимости в системах документооборота и базах данных; выбирать и обосновывать средства защиты информации в зависимости от категории данных; настраивать средства разграничения доступа и аутентификации; проводить оценку рисков ИБ; применять криптографические методы защиты конфиденциальных документов; организовывать безопасное хранение документов с аудитом действий; выявлять признаки нарушений ИБ и использовать ПО для мониторинга событий безопасности; разрабатывать инструкции по обеспечению ИБ в подразделении.
Владеет навыками обеспечения конфиденциальности, целостности и доступности информации в системах документооборота и базах данных; методологией реализации комплексных мер защиты с учетом форматов данных; технологиями настройки средств защиты в корпоративной среде; практическими навыками применения криптографических инструментов; умениями разработки регламентов работы с конфиденциальной информацией; навыками базового аудита защищенности и подготовки рекомендаций по устранению недостатков; методами оценки экономической целесообразности мер защиты и взаимодействия с подразделениями ИБ при расследовании инцидентов.

5.2 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 и демонстрации навыков, полученных при выполнении работы. Вопросы к лабораторным работам и критерии их оценки представлены в фонде оценочных средств по данной дисциплине.

При защите лабораторной работы студент имеет право пользоваться самостоятельно подготовленным отчетом.

Каждая выполненная и защищенная лабораторная работа оцениваются в 3 балла. При этом 1 балл начисляется за выполнение работы и от 1 до 2 баллов за оформление отчета и защиту работы в зависимости от качества оформления и уровня знаний студента по тематике работы.

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

5.3 Критерии оценки зачета

Для оценки зачета используются следующие оценочные средства: тестирование.

Зачет по данной дисциплине проводится в виде теста в системе moodle.bru.by. Студенту предлагается за определённое время ответить на тест из 40 вопросов, охватывающих все изученные темы. При ответе на каждый вопрос студент должен выбрать правильный ответ из нескольких предлагаемых или сформулировать собственный ответ. Каждый правильный ответ оценивается в 1 (один) балл. Максимальное количество баллов – 40, студент получает, ответив на 100 % поставленных вопросов. Остальная шкала баллов соответствует правильным ответам на вопросы пропорционально их количеству и сложности.

Подробно средства оценивания приведены в фонде оценочных средств по данной дисциплине.

6 МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ И ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Самостоятельная работа обучающихся (СР) направлена на закрепление и углубление освоения учебного материала, развитие практических умений. СР включает следующие виды:

- работа с материалами курса, вынесенными на самостоятельное изучение;
- работа со справочной литературой;

Перечень контрольных вопросов и заданий для СР приведен в приложении и хранится на кафедре.

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

7 УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1 Основная литература

№ п/п	Библиографическое описание	Гриф	Количество экземпляров, URL
1.	Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. – Москва : Издательство Юрайт, 2026. – 349 с.	Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям	-/ https://urait.ru/bcode/583858

2.	Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. – 5-е изд., перераб. и доп. – Москва : РИОР : ИНФРА-М, 2026. – 384 с.	Допущено Учебно-методическим объединением по образованию в области прикладной информатики в качестве учебного пособия для студентов, обучающихся по направлению «Прикладная информатика»	-/ https://znanium.ru/catalog/product/2233509
----	--	--	---

7.2 Дополнительная литература

№ п/п	Библиографическое описание	Гриф	Количество экземпляров, URL
1.	Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 107 с.	Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям	-/ https://urait.ru/bcode/588741
2.	Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. – Москва : ИНФРА-М, 2023. – 201 с.	Рекомендовано 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 (степень) «бакалавр»)	-/ https://znanium.ru/catalog/product/1912987
3.	Внуков, А. А. Защита информации : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 161 с.	Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям	-/ https://urait.ru/bcode/584050
4.	Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. – Москва : ИНФРА-М, 2024. – 223 с.	Рекомендовано Межрегиональным учебно-методическим советом профессионального образования в качестве учебного пособия для студентов высших учебных заведений, обучающихся по укрупненной группе специальностей 10.05.00 «Информационная безопасность»	-/ https://znanium.com/catalog/product/2003474
5.	Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2026. — 424 с.	Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям и специальностям	-/ https://urait.ru/bcode/583156
6.	Информационная безопасность сетей и систем : учеб. пособие / В. И. Аверченко, В. Т. Еременко, Е. А. Зайченко. – Могилев : Беларус.-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

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://urait.ru> – Образовательная платформа Юрайт;
<https://stepik.org/catalog> – Российская образовательная платформа и конструктор бесплатных открытых онлайн-курсов и уроков;
<https://openedu.ru> – Открытое образование. Курсы ведущих вузов России;
<https://habr.com/ru/> – Хабр. Публикации по ИТ тематикам;
<https://infosecportal.ru> - Портал информационной безопасности
<https://regulhub.kaspersky.ru> – Kaspersky - Регуляторный хаб знаний в области информационной безопасности
<https://cybersecuritynews.com> – Cyber Security News новостная платформа, освещающая все события в кибермире на которой рассказывается о текущих угрозах, исследовательских работах, уязвимостях, утечках данных и многом другом.

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

Методические рекомендации

Основы информационной безопасности. Методические рекомендации к лабораторным работам для студентов направлений подготовки 38.03.02 Менеджмент дневной формы обучения / В. В. Кутузов. – Могилев: Белорусско-Российский университет (электронный вариант)

Информационные технологии

Мультимедийные презентации по лекционному курсу.

Тема 1. Основы информационной безопасности

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. Безопасность в организациях. Политика информационной безопасности и реализация её в организациях

Тема 7. Практические инструменты информационной безопасности в организациях

Тема 8. Безопасность критически важных объектов и критической информационной инфраструктуры

Тема 9. Кибербезопасность и киберпреступность

Тема 10. Защита информации в операционных системах

Тема 11. Сетевые атаки и защита информации в компьютерных сетях

Тема 12. Применение технологий искусственного интеллекта в информационной безопасности

Тема 13. Обеспечение и реализация защиты информации в разрабатываемом программном обеспечении и в базах данных

Тема 14. Технологии обеспечения безопасности веб-приложений

Тема 15. Экономические аспекты защиты информации и информационной безопасности в целом

Перечень программного обеспечения, используемого в образовательном процессе

Виртуальная машина Hyper-V (свободно распространяемое)

Visual Studio Code (VS Code) (свободно распространяемое)

8 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины содержится в паспорте лаборатории а. 517/2, рег. № паспорта лаборатории № ПУЛ - 4 517/2- 25; в паспорте лаборатории а. 518/2, рег. № паспорта лаборатории № ПУЛ - 4 518/2- 25; в паспорте лаборатории а. 502/2, рег. № паспорта лаборатории № ПУЛ - 4 502/2- 25.