Межгосударственное образовательное учреждение высшего образования
«Белорусско-Российский университет»

УТВЕРЖДАЮ
Первый проректор Белорусско-Российского университета

_____ Ю.В. Машин
22.12 2023

Регистрационный № УД-090301/04/5.1.В./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	**3, 4**
Семестр	6, 7
Лекции, часы	48
Лабораторные работы, часы	46
Зачет	6
Экзамен, семестр	7
Контактная работа по учебным занятиям, часы	94
Самостоятельная работа, часы	122
Всего часов / зачетных единиц	216/6

Кафедра-разработчик программы: Программное обеспечение информационных технологий

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

Могилев, 2023

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, № 920 от 19.09.2017, учебными планами рег. №090301-2.1 и №090304-2.1, утвержденными 28.04.2023.

Рассмотрена и рекомендована к утверждению кафедрой «Программное обеспечение информационных технологий» «11» ноября 2023 г., протокол № 04.

Зав. кафедрой «Программное обеспечение информационных технологий»  В. В. Кутузов

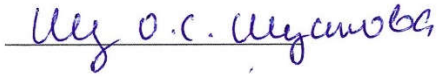
Одобрена и рекомендована к утверждению Научно-методическим советом Белорусско-Российского университета

«20» декабря 2023 г., протокол № 3

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

Рецензент:
И. В. Акиншева, заведующая кафедрой программного обеспечения информационных технологий МГУ имени А. А. Кулешова, к.т.н., доцент

Рабочая программа согласована:

Ведущий библиотекарь 

Начальник учебно-методического
отдела  О.Е. Печковская

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:

- Информатика;
- Программирование;
- Объектно-ориентированное 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 темы	Наименование тем	Содержание	Коды формируемых компетенций	
			09.03.01	09.03.04
	6 семестр			
1.	Основы защиты информации и информационной безопасности	Основы защиты информации и 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-12 ПК-13	ПК-9
2.	Правовое и нормативное обеспечение защиты информации (Законодательство РБ и РФ)	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	ПК-12 ПК-13	ПК-9

		государства. Законодательная база Российской Федерации в области защиты информации и информационной безопасности в целом. Руководящие документы ФСТЭК России. Владельцы защищаемой информации. Понятие государственная тайна, коммерческая тайна. Профессиональная тайна, служебная тайна.		
3.	Международное законодательство и стандарты информационной безопасности	Международное законодательство в области информационной безопасности и защиты информации. Структура и состав информационного законодательства Информация как объект права. Цели и задачи международных нормативных актов по ИБ. Роль стандартов информационной безопасности. Актуальные проблемы ИБ, освещаемые в международных стандартах. Критерии безопасности информационных технологий: – Критерии безопасности компьютерных систем министерства обороны США («Оранжевая книга»); – Европейские критерии безопасности информационных технологий; – Федеральные критерии безопасности информационных технологий; – Канадские критерии безопасности компьютерных систем; – Общие критерии оценки защищённости информационных технологий (Единые критерии безопасности информационных технологий.) – Common Criteria for Information Technology Security Evaluation, (Common Criteria), ISO/IEC 15408. 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 (Международные профессиональные объединения в сфере информационной безопасности. Специализированные международные организации в сфере информационной безопасности)	ПК-12 ПК-13	ПК-9
4.	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-12 ПК-13	ПК-9
5.	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	ПК-12 ПК-13	ПК-9

		угрозы целостности. Основные угрозы конфиденциальности. Методики оценки и моделирования угроз. Базы и банки данных угроз безопасности информации Моделирование угроз корпоративной инфраструктуры		
6.	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
7.	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. Специализированное 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 (SCO) – Security Orchestration, Automation and Response (SOAR) – Incident Response Platform (IRP) – Security Governance, Risk-management and Compliance (SGRC) – Data Leak Prevention (DPL) и др.	ПК-12 ПК-13	ПК-9
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	ПК-12 ПК-13	ПК-9

		контроля. Аудит.		
9.	Идентификация, аутентификация и авторизация	Идентификация, аутентификация и авторизация. Общие сведения. Правовое и нормативное обеспечение, стандарты по вопросам идентификации, аутентификации и авторизации. 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
10.	Криптография	Криптография. Криптоанализ. 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. Программное обеспечение для шифрования, дешифрования. Перспективные технологии криптографии. Квантовая криптография.	ПК-12 ПК-13	ПК-9
11.	Электронная цифровая подпись	Электронная цифровая подпись (ЭЦП). Необходимость использования ЭЦП. ЭЦП для аутентификации данных. Алгоритмы ЭЦП. Стандарты цифровой подписи. Нормативно-правовая база ЭЦП. Практика применения ЭЦП. Программное обеспечение для работы с ЭЦП. Электронно-цифровая подпись в СЭД. Организация хранения документов с ЭЦП. Удостоверяющие центры. Инфраструктура управления открытыми ключами.	ПК-12 ПК-13	ПК-9
12.	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-12 ПК-13	ПК-9

13.	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-12 ПК-13	ПК-9
14.	Применение технологий искусственного интеллекта в информационной безопасности	Искусственный интеллект (ИИ). Машинное обучение. Нейронные сети. Компьютерное зрение. ChatGPT и аналоги. 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.	ПК-12 ПК-13	ПК-9
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	ПК-12 ПК-13	ПК-9

		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.		
	7 семестр			
1.	Обеспечение и реализация защиты информации в разрабатываемом программном обеспечении	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.	ПК-12 ПК-13	ПК-9
2.	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-12 ПК-13	ПК-9

3.	Защита баз данных	Базы данных. Администрирование баз данных. Технологии защиты баз данных. Организация защиты данных в хранилищах. Способы контроля доступа к данным и управления привилегиями Алгоритм проведения процедуры резервного копирования Модели восстановления SQL-сервера Резервное копирование баз данных. Восстановление баз данных. Аутентификация и авторизация пользователей. Назначение серверных ролей и ролей баз данных. Авторизация пользователей при получении доступа к ресурсам. Настройка безопасности агента SQL Дополнительные параметры развертывания и администрирования AD DS. Обеспечение безопасности служб AD DS. Мониторинг, управление и восстановление AD DS. Атаки на базы данных. Поиск уязвимостей к атакам SQL-injection Технология разработки и защиты баз данных.	ПК-12 ПК-13	ПК-9
4.	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 обналичивания похищенных средств на примере технологий VPN, Tor и криптовалюты Bitcoin 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.	ПК-12 ПК-13	ПК-9
5.	Киберпреступность, виды и методы осуществления киберпреступлений	Ландшафт угроз кибербезопасности (методы и техники атакующих постоянно совершенствуются, злоумышленники используют новые инструменты и векторы атак, которые не детектируются стандартными средствами защиты). Современный контекст безопасности. Сложность атак. Hi-Tech Crime Trends как источник стратегической информации о глобальном ландшафте киберугроз и прогнозах их развития. Информационная безопасность и преступность.	ПК-12 ПК-13	ПК-9

		Понятия киберпреступности и киберпреступления. Международные масштабы киберпреступности. Хакерские группировки. Международное сотрудничество в целях противодействия киберпреступности. Деятельность Интерпола, Европола в борьбе с киберпрступностью. Конвенция о киберпреступности. Международные стандарты. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (незаконный доступ, получение данных, незаконный перехват информационных ресурсов, искажение информации). Преступления, связанные с контентом (детская порнография, расизм, агрессивные высказывания и др.). Преступления, связанные с нарушением интеллектуальных прав. Преступления, связанные с применением компьютеров и компьютерных технологий (компьютерное мошенничество, использование персональных данных, полученных незаконным путем, кибертерроризм, отмывание денег, др.). Правовые возможности борьбы с киберпреступностью. Ответственность за совершение киберпреступлений. Виды и методы киберпреступлений. Цели и методы работы современных киберпреступников, обзор практических ситуаций (кейсов). Портрет потенциального злоумышленника. Модель угроз и модель нарушителя. Экосистема теневого сегмента сети Интернет. Основные причины роста числа киберпреступлений. Криптовалюты и анонимные сети. Основы криптографии. Краткий обзор методов сокрытия авторства преступления и способов обналичивания похищенных средств.		
6.	Кибербезопасность индустриальных систем, инфраструктуры и в отраслях в целом	Новые угрозы безопасности для высокотехнологичных предприятий. Кибербезопасность индустриальных систем в цифрах. Ландшафт угроз. Риски. Industrial CyberSecurity. Кибербезопасность систем промышленной автоматизации. Кибербезопасность транспортной инфраструктуры. Кибербезопасность в отраслях промышленности (финансы, транспорт, строительство, машиностроение, энергетика, медицина, связь и т.д.) Эволюция технологий информационной безопасности кибер-физических систем с точки зрения теории управления. Обеспечение кибер-устойчивости информационных систем цифровой индустрии. Кибер-устойчивость сетей с гибкой топологией. Обнаружение инцидентов безопасности в магистральных сетях передачи данных. Технологии SIEM для промышленного интернета вещей. Создание доверенной среды обмена данными для цифровой индустрии. Методология аутентификации в сетях цифровой индустрии. Тестирование защищенности кибер-физических систем.	ПК-12 ПК-13	ПК-9
7.	Стратегия и тактика противодействия киберпреступности	Стратегии противодействия киберпреступности. Исследования киберугроз, целевых атак и группировок. Центр обеспечения безопасности (Security Operations Center (SOC)). Центр обеспечения кибербезопасности (Cybersecurity Operations Center (CSOC)).	ПК-12 ПК-13	ПК-9

		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. Своевременная идентификация, локализация и ликвидация инцидентов по всему миру. Использование данных Threat Intelligence & Attribution для восстановления хронологии инцидента и приведения ИТ-инфраструктуру в стабильное состояние в кратчайшие сроки. Расследования высокотехнологичных преступлений. Борьба с компьютерными, финансовыми, корпоративными преступлениями по всему миру. Анализ вредоносного кода при расследовании киберпреступлений. Компьютерная криминалистика, полезные практики, необходимые для обеспечения высокого уровня кибербезопасности. Киберучения. Киберучения в формате Red Teaming. Киберполигоны. Имитация целевых атак и регулярное противодействие им. 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). Полный цикл проверок для всестороннего аудита инфраструктуры и оценки защищенности компании от сложных киберугроз. Аудит. Сертификация. Применение технологий искусственного интеллекта, машинного обучения, глубокого обучения, нейронных сетей в вопросах кибербезопасности. Новые технологии. Новые риски. Новые технологии защиты.		

2.2 Учебно-методическая карта учебной дисциплины

6 семестр

№ недели	Лекции (наименование тем)	Часы	Лабораторные работы	Часы	Самостоятельная работа, часы	Форма контроля знаний	Баллы (max)
	Модуль 1						
1	**Тема 1.** Основы защиты информации и информационной безопасности	2	Лр.р. № 1. Хеширование информации	2	2	ЗЛР	5
2	**Тема 2.** Правовое и нормативное обеспечение защиты информации (Законодательство РБ и РФ)	2			4		
3	**Тема 3.** Международное законодательство и стандарты информационной безопасности	2	Лр.р. № 2. Исследование надежности паролей и их восстановление	2	4	ЗЛР	5
4	**Тема 4.** Защита персональных данных	2			4		
5	**Тема 5.** Угрозы информационной безопасности	2	Лр.р. № 3. Шифрование данных	2	4	ЗЛР	5

6	**Тема 6.** Управление рисками информационной безопасности	2			4		
7	**Тема 7.** Безопасность в организациях. Политика информационной безопасности и реализация её в организациях	2	Лр.р. № 4. Архивирование и резервное копирование данных	2	4	ЗЛР	5
8	**Тема 8.** Безопасность критически важных объектов и критической информационной инфраструктуры	2			4	ТЗ ПКУ	10 30
	Модуль 2						
9	**Тема 9.** Идентификация, аутентификация и авторизация	2	Лр.р. № 5. Восстановление удаленной информации	2	4	ЗЛР	5
10	**Тема 9.** Идентификация, аутентификация и авторизация	2			4		
11	**Тема 10.** Криптография	2	Лр.р. № 6. Оценка рисков информационной безопасности организаций в соответствии с требованиями СТБ 34.101.70-2016	2	4	ЗЛР	5
12	**Тема 11.** Электронная цифровая подпись	2			4		
13	**Тема 12.** Защита информации в операционных системах	2	Лр.р. № 6. Оценка рисков информационной безопасности организаций в соответствии с требованиями СТБ 34.101.70-2016	2	4	ЗЛР	5
14	**Тема 13.** Сетевые атаки и защита информации в компьютерных сетях	2			4		
15	**Тема 13.** Сетевые атаки и защита информации в компьютерных сетях	2	Лр.р. № 7. Ознакомление с ChatGPT и применение его в решении вопросов информационной безопасности	2	4	ЗЛР	5
16	**Тема 14.** Применение технологий искусственного интеллекта в информационной безопасности	2				ТЗ	10
17	**Тема 15.** Экономические аспекты защиты информации и информационной безопасности в целом	2				ПКУ	30
17						ПА (зачет)	40
	ИТОГО	34		16	58		100

7 семестр

№ недели	Лекции (наименование тем)	Часы	Лабораторные работы	Часы	Самостоятельная работа, часы	Форма контроля знаний	Баллы (max)
	Модуль 1						
1	**Тема 1.** Обеспечение и реализация защиты информации в разрабатываемом программном обеспечении	2	Лр.р. № 1. Шифрование данных в ОС Linux	2	1	ЗЛР	3
2			Лр.р. № 1. Шифрование данных в ОС Linux	2	2	ЗЛР	3
3	**Тема 2.** Технологии обеспечения безопасности веб-приложений	2	Лр.р. № 2. Разграничение прав доступа в ОС Linux	2	2	ЗЛР	4
4			Лр.р. № 2. Разграничение прав доступа в ОС Linux	2	2	ЗЛР	4
5	**Тема 3.** Защита баз данных	2	Лр.р. № 3. Возможности файловых подсистем Linux для защиты информации	2	2	ЗЛР	4
6			Лр.р. № 3. Возможности файловых подсистем Linux для защиты информации	2	2	ЗЛР	4
7	**Тема 4.** Кибербезопасность и киберпреступность	2	Лр.р. № 4. Обеспечение целостности и доступности данных с использованием Raid, LVM.	2	2	ЗЛР	4
8			Лр.р. № 4. Обеспечение целостности и доступности данных с использованием Raid, LVM.	2	2	ЗИЗ ПКУ	4 30
	Модуль 2						
9	**Тема 5**. Киберпреступность, виды и методы осуществления киберпреступлений	2	Лр.р. № 5. Изучение методов шифрования ОС Windows данных на дисках	2	1	ЗЛР	5
10			Лр.р. № 5. Изучение методов шифрования ОС Windows данных на дисках	2	2	ЗЛР	5
11	**Тема 6** Кибербезопасность индустриальных систем, инфраструктуры и в отраслях в целом	2	Лр.р. № 6. Средства защиты данных в ОС Windows	2	2	ЗЛР	4
12			Лр.р. № 6. Средства защиты данных в ОС Windows	2	2	ЗЛР	4
13	**Тема 7.** Стратегия и тактика противодействия киберпреступности	2	Лр.р. № 7. Изучение методов аудита ОС Windows	2	2	ЗЛР	4
14			Лр.р. №7. Изучение методов аудита С Windows	2	2	ЗЛР	4
15			Лр.р. №8. Основы MS Crypto API	2	2	ЗЛР ПКУ	4 30
16-18					36	ПА (экзамен)	40
	ИТОГО	14		30	64		100

Принятые обозначения:
Текущий контроль:
ЗИЗ – защита индивидуального задания.
ТЗ – тестовые 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:

Зачет

Оценка	Зачтено	Не зачтено
Баллы	51-100	0-50

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 1–15 Темы 1–7		48
2	С использованием ЭВМ		Лр. раб. 1–7 Лр. раб. 1–8	46
	ИТОГО	48	46	94

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 зачету	1
2.	Вопросы к экзамену	1
3.	Билеты к экзамену	1
4.	Задания к лабораторным работам	15
5.	Индивидуальные задания	1
6.	Контрольные задания для проведения рейтинг-контроля	1
7.	Тестовые 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			
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
ПК-13 Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения			
ИПК-13.2. Осуществляет администрирование процесса управления безопасностью программного обеспечения инфокоммуникационной системы			
1	Пороговый уровень	Знает теоретический материал по основам управления безопасностью программного обеспечения инфокоммуникационной системы	Знает основы управления безопасностью программного обеспечения инфокоммуникационной системы
2	Продвинутый уровень	Владеет знаниями теоретических основ администрирования процесса управления безопасностью программного обеспечения инфокоммуникационной системы	Знает, как осуществлять администрирование процесса управления безопасностью программного обеспечения инфокоммуникационной системы
3	Высокий уровень	Владеет навыками администрирования процесса управления безопасностью программного обеспечения инфокоммуникационной системы	Знает и владеет навыками осуществлять администрирование процесса управления безопасностью программного обеспечения инфокоммуникационной системы

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 данных. Может оценить угрозы и риски.	Владеет теоретическими навыками применения методов защиты информации
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. Тестовые задания. Тематики индивидуальных заданий. Вопросы к зачету. 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. Тестовые задания. Тематики индивидуальных заданий. Вопросы к зачету. 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. Тестовые задания. Тематики индивидуальных заданий. Вопросы к зачету. Вопросы к экзамену.
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)	
Знает основы администрирования сетевых устройств и программного обеспечения инфокоммуникационной системы	Вопросы для защиты лабораторных работ. Тестовые задания. Тематики индивидуальных заданий. Вопросы к зачету. Вопросы к экзамену.
Знает, как осуществлять администрирование сетевых устройств и программного обеспечения инфокоммуникационной системы, включая создание систем информационной безопасности	Вопросы для защиты лабораторных работ. Тестовые задания. Тематики индивидуальных заданий. Вопросы к зачету. Вопросы к экзамену.
Знает и владеет навыками осуществлять администрирование сетевых устройств и программного обеспечения инфокоммуникационной	Вопросы для защиты лабораторных работ. Тестовые задания. Тематики индивидуальных заданий.

системы, включая создание систем информационной безопасности	Вопросы к зачету. Вопросы к экзамену.
ПК-13 Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения (ИПК-13.2. Осуществляет администрирование процесса управления безопасностью программного обеспечения инфокоммуникационной системы)	
Знает основы управления безопасностью программного обеспечения инфокоммуникационной системы	Вопросы для защиты лабораторных работ. Тестовые задания. Тематики индивидуальных заданий. Вопросы к зачету. Вопросы к экзамену.
Знает, как осуществлять администрирование процесса управления безопасностью программного обеспечения инфокоммуникационной системы	Вопросы для защиты лабораторных работ. Тестовые задания. Тематики индивидуальных заданий. Вопросы к зачету. Вопросы к экзамену.
Знает и владеет навыками осуществлять администрирование процесса управления безопасностью программного обеспечения инфокоммуникационной системы	Вопросы для защиты лабораторных работ. Тестовые задания. Тематики индивидуальных заданий. Вопросы к зачету. 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. Тестовые задания. Вопросы к зачету. 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. Тестовые задания. Вопросы к зачету. 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. Тестовые задания. Вопросы к зачету. 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 тестовых заданий.

Выполненные тестовые задания оценивается в диапазоне до 10 баллов в зависимости от уровня знаний студента по тематике тестовых заданий. Если по окончанию модуля тестовые задания не выполнены, то баллы по ней не начисляются и она попадает в разряд задолженности.

5.5 Критерии оценки индивидуальных заданий.

При подготовке индивидуальных заданий по вопросам информационной безопасности важно проявить глубокое понимание темы, представить четкую и обоснованную позицию с опорой на достоверные источники. На все источники необходимо давать ссылки. Текст должен логически соединять различные разделы, убедительно проводя читателя от начала до конца работы, которое в итоге должно показывать итоги, выводы работы. Важным аспектом является оригинальность мыслей и анализа, включая как теоретические данные, так и собственные исследования или кейс-анализ. Стилистическое и грамматическое исполнение индивидуального задания должно быть аккуратным, а форматирование соответствовать требованиям ГОСТов. Практическая ценность предложенных индивидуальной работы и решений, отраженных в ней, играет ключевую роль при оценке работы. Оценивается работа в диапазоне до 4 баллов.

5.6 Критерии оценки зачета.

Контрольное задание включает 2 теоретических вопроса. Теоретические вопросы выбираются из разных дидактических единиц. Каждый вопрос оценивается положительной оценкой в диапазоне от 10 до 20 баллов.

Ответы на вопросы оцениваются по следующим критериям.

Теоретические вопросы:

- **19-20 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.
- **17-18 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.
- **15-16 баллов** – студент хорошо понимает пройденный материал, отвечает правильно, умеет оценивать факты, самостоятельно рассуждает, обосновывает выводы и разъясняет их, но допускает ошибки общего характера.
- **13-14 баллов** – студент понимает пройденный материал, но не может теоретически обосновать некоторые выводы, допускает ошибки общего характера.

- **11-12 баллов** – студент отвечает в основном правильно на поставленный вопрос, но чувствуется механическое заучивание материала, отсутствует логическая последовательность при изложении ответа, не может ответить на дополнительные вопросы.
- **10 баллов** – в ответе студента имеются существенные недостатки, материал охвачен «половинчато», в рассуждениях допускаются ошибки
- **Ниже 10 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;

5.7 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	Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. – Москва : Издательство Юрайт, 2024. – 309 с.	Рекомендовано Учебно-методическим отделом высшего образования в качестве учебника для студентов высших учебных заведений, обучающихся по инженерно-техническим направлениям	https://urait.ru/bcode/537000
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, 2024. – 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.ru/catalog/product/2082642

7.2 Дополнительная литература

№ п/п	Библиографическое описание	Гриф	Количество экземпляров
1	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
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	Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 3-е изд. – Москва : РИОР : ИНФРА-М, 2023. – 400 с.	Рекомендовано УМО по образованию в области информационных технологий и систем связи в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению подготовки «Инфокоммуникационные технологии и системы связи» квалификации (степени) «бакалавр» и квалификации (степени) «магистр»	https://znanium.ru/catalog/product/1912992
4	Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. – 3-е изд., испр. и доп. – Москва : ИНФРА-М, 2022. – 327 с.	Рекомендовано Учебно-методическим объединением вузов Российской Федерации по образованию в области историко-архивоведения в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению «Информационная безопасность»	https://znanium.com/catalog/product/1865598
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, 2024. – 473 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/536132
6	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

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

http://jisp.ru – Журнал «Проблемы информационной безопасности. Компьютерные системы»

https://habr.com/ru/hub/infosecurity/ Хабр. Портал сообщества IT-специалистов: раздел информационная безопасность, зашита данных

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.

https://cisoclub.ru – CISOCLUB информационный портал и профессиональное сообщество специалистов по информационной безопасности.

https://cisoclub.ru/category/reports/ – CISOCLUB: Отчеты и исследования по информационной безопасности

https://safe-surf.ru – Безопасность пользователей в сети Интернет

https://www.securitylab.ru – SecurityLab.ru – информационный портал, оперативно и ежедневно рассказывающий о событиях в области защиты информации, интернет-права и новых технологиях

https://codeib.ru – Код ИБ - экосистема проектов по информационной безопасности

https://ctfnews.ru – Всё о CTF в России

https://stepik.org/course/127 – курс по аудиту безопасности веб-проектов от Mail.ru Group. Будет полезен тем, кто только начинает изучать категорию web.

https://bdu.fstec.ru/threat – Банк данных угроз безопасности информации

http://fstec.ru/ – Портал ФСТЭК

https://csrc.nist.gov/publications/sp - NIST SP 800 Series – Специальные публикации Национального Института Стандартов и Технологий США

https://cybershafarat.com/wp-content/uploads/2023/04/D0A0D09AD09D_Issledovanie_AI.pdf – Инструменты ИИ в руках злоумышленников – классификация угроз и способы противодействия

http://multilang.pravo.by/ru – Национальный центр правовой информации Республики Беларусь. «ЮРИДИЧЕСКИЙ СЛОВАРЬ»

https://mgimo.ru/upload/iblock/559/Tom%202.pdf – Международная информационная безопасность: Теория и практика: В трех томах. Том 2: Сборник документов (на русском языке) / Под общ. ред. А. В. Крутских. – М.: Издательство «Аспект Пресс», 2019. – 784 с.

http://aciso.ru/files/news/uchebnik.pdf – Назаров, Д. М. Основы обеспечения безопасности персональных данных в организации : учеб. пособие / Д. М. Назаров, К. М. Саматов ; М-во науки и высш. образования Рос. Федерации, Урал. гос. экон. ун-т. – Екатеринбург : Изд-во Урал. гос. экон. ун-та, 2019. – 118 с.

https://pravo.by/document/?guid=3871&p0=P223s0001 – Проект новой Концепции национальной безопасности Республики Беларусь (2023)

https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf – Постановление Совета Безопасности Республики Беларусь 18.03.2019 № 1 «КОНЦЕПЦИЯ информационной безопасности Республики Беларусь»

https://pravo.by/document/?guid=3871&p0=h10800455 – Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»

https://president.gov.by/bucket/assets/uploads/documents/2023/40uk.pdf – Указ № 40 от 14 февраля 2023 «О кибербезопасности»

https://www.oac.gov.by/activity/cybersecurity-centers-list/recommendations-determining-rights – Рекомендации по определению прав и обязанностей заместителя руководителя государственного органа и иной организации по вопросам обеспечения кибербезопасности

http://kgb.by/ru/zakon170-3/ – Закон Республики Беларусь от 19 июля 2010 г. N 170-З «О государственных секретах»

https://www.oac.gov.by/public/content/files/files/law/resolutions-sm/2014-783.pdf – Постановление Совета Министров Республики Беларусь от 12 августа 2014 г. № 783 «О служебной информации ограниченного распространения и информации, составляющей коммерческую тайну»

https://www.oac.gov.by/public/content/files/files/law/laws-rb/113-z.pdf – Закон Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи»

https://pravo.by/upload/docs/op/H12100099_1620939600.pdf – Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных»

https://cpd.by/storage/2023/02/NPK-22.02.2023.pdf – Постатейный комментарий к Закону Республики Беларусь «О защите персональных данных» – Минск : Национальный центр защиты персональных данных, 2023 – 202 с.

https://cpd.by/storage/2022/05/algoritm_dejstvij_operatora_razjasnenie.pdf – Алгоритм приведения деятельности операторов, уполномоченных лиц в соответствие с требованиями Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных»

https://pravo.by/document/?guid=3871&p0=F01900068 – ПЕРЕЧЕНЬ стандартов и рекомендаций в области информационной безопасности, применяемых в рамках реализации цифровой повестки Евразийского экономического союза. Рекомендации Коллегии Евразийской экономической комиссии от 12 марта 2019 г. № 9

http://www.scrf.gov.ru/security/information/document112/ – Концепция Конвенции ООН об обеспечении международной информационной безопасности

https://regulhub.kaspersky.ru/ – Регуляторный хаб знаний в области информационной безопасности

https://www.youtube.com/watch?v=qfxj-vHr5lU – Законодательные требования РФ по информационной безопасности 2023 | Алексей Лукацкий

http://www.kremlin.ru/acts/bank/24157 – Федеральный закон РФ от 27 июля 2006 г. № 149-ФЗ «Об информации, информатизации и защите информации»

http://www.kremlin.ru/acts/bank/24154 – Федеральный закон РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

http://www.kremlin.ru/acts/bank/21227 – Федеральный закон РФ от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне»

http://www.kremlin.ru/acts/bank/32938 – Федеральный закон РФ от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»

http://www.kremlin.ru/acts/bank/42128 – Федеральный закон РФ от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

https://docs.cntd.ru/document/1200101777 – ГОСТ Р ИСО/МЭК 15408 «Критерии оценки безопасности информационных технологий»

https://docs.cntd.ru/document/1200101777 – ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель (Information technology. Security techniques. Evaluation criteria for IT security. Part 1. Introduction and general model)

https://docs.cntd.ru/document/1200105710 – ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности (Information technology. Security techniques. Evaluation criteria for IT security. Part 2. Security functional components)

https://docs.cntd.ru/document/1200105711 – ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности (Information technology. Security techniques. Evaluation criteria for IT security. Part 3. Security assurance requirements)

https://docs.cntd.ru/document/1200105309 – ГОСТ Р ИСО/МЭК 18045-2013. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий (Information technology - Security techniques – Methodology for IT security evaluation)

https://docs.cntd.ru/document/1200159380 – ГОСТ Р 58142-2018 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 1. Использование доступных источников для идентификации

потенциальных уязвимостей

https://docs.cntd.ru/document/1200095100 – ГОСТ Р 58143-2018 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 2. Тестирование проникновения

https://rppa.ru/_media/analitika/gdpr_01.10.2023.pdf – Алексей Мунтян. Рассмотрение механизмов и специфики применения Генерального регламента ЕС о защите данных (GDPR)

https://www.enforcementtracker.com – База сведений о штрафов за нарушение GDPR

https://www.cloudav.ru/upload/iblock/447/PAD_PAD360%20-%20Whitepaper%20-%20Критические%20инфраструктуры.pdf – Критическая инфраструктура

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 рекомендации к лабораторным работам для студентов направлений подготовки 09.03.01 «Информатика и вычислительная техника» и 09.03.04 «Программная инженерия» / сост. В. В. Кутузов, Е. А. Зайченко. - Могилев : Белорус.-Рос. ун-т.

7.4.2 Информационные технологии

Мультимедийные презентации

6 семестр

Тема 1. Основы защиты информации и информационной безопасности

Тема 2. Правовое и нормативное обеспечение защиты информации (Законодательство РБ и РФ)

Тема 3. Международное законодательство и стандарты информационной безопасности

Тема 4. Защита персональных данных

Тема 5. Угрозы информационной безопасности

Тема 6. Управление рисками информационной безопасности

Тема 7. Безопасность в организациях. Политика информационной безопасности и реализация её в организациях

Тема 8. Безопасность критически важных объектов и критической информационной инфраструктуры

Тема 9. Идентификация, аутентификация и авторизация

Тема 10. Криптография

Тема 11. Электронная цифровая подпись

Тема 12. Защита информации в операционных системах

Тема 13. Сетевые атаки и защита информации в компьютерных сетях

Тема 14. Применение технологий искусственного интеллекта в информационной безопасности

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

7 семестр

Тема 1. Обеспечение и реализация защиты информации в разрабатываемом программном обеспечении

Тема 2. Технологии обеспечения безопасности веб-приложений

Тема 3. Защита баз данных

Тема 4. Кибербезопасность и киберпреступность

Тема 5. Киберпреступность, виды и методы осуществления киберпреступлений

Тема 6. Кибербезопасность индустриальных систем, инфраструктуры и в отраслях в целом

Тема 7. Стратегия и тактика противодействия киберпреступности

7.4.3 Перечень программного обеспечения, используемого в образовательном процессе

1. Виртуальная машина Hyper-V (свободно распространяемое)
2. Visual Studio Code (VS Code) (свободно распространяемое)

8 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины содержится в паспорте лаборатории ауд. 517/2, рег. № паспорта лаборатории № ПУЛ - 4 517/2-23; в паспорте лаборатории ауд. 518/2, рег. № паспорта лаборатории № ПУЛ - 4 518/2-23.