



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.01.02 Защита данных

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Направленность (профиль): Компьютерное моделирование и анализ данных

Квалификация (степень): бакалавр

Форма обучения: очная

Институт: математики, естествознания и техники

Кафедра: математического моделирования, компьютерных технологий и информационной безопасности

	очная форма	очно-заочная форма	заочная форма
Курс	1		
Семестр	2		

Лекции	18		
Лабораторные занятия			
Практические (семинарские) занятия	18		
в т.ч. практическая подготовка	2		
Форма(ы) промежуточной аттестации	Экзамен - 0,3		
Контроль	9		
Иные формы работы	-		
Самостоятельная работа	98,7		

Всего часов: 144

Трудовое количество: 4 зачетных единиц

Разработчики рабочей программы:

к.п.н., доцент, Т.А. Щучка,

ассистент О.Ю. Андропова

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины: понимание основных понятий, методов и технологий, используемых для защиты информации; предоставление обучаемым знаний основных типов и способов защиты информации; приобретение студентами умения проектировать системы защиты информации; овладение современными программными и аппаратными средствами защиты информации.

Задачи изучения дисциплины:

- освоение базовых понятий и терминов в области защиты данных;
- ознакомление с современными инструментами и программным обеспечением для защиты данных;
- ознакомление с процессом разработки и внедрения политики безопасности данных в организациях;
- изучение различных типов угроз и способов их минимизации;
- обеспечение информационной безопасности в современных условиях и основные факторы, влияющие на ее защиту;
- определение взаимосвязи национальных интересов и национальной безопасности.

Место дисциплины в структуре ОПОП: реализуется в рамках части, формируемой участниками образовательных отношений, блока Б1. Дисциплины (модули).

Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
УК-10	Знать: – правовые нормы, противодействующие проявлениям экстремизма, терроризма, коррупционного поведения в профессиональной деятельности, основные меры юридической ответственности за совершение деяний экстремистской, террористической и коррупционной направленности.	Знает; – правовые нормы, действующие в области в области защиты данных, а именно знает законы, регулирующие сбор и обработку персональных данных.
	Уметь: – анализировать, толковать и применять правовые нормы о противодействии экстремизму, терроризму, коррупционному поведению в профессиональной деятельности и повседневной жизни.	Умеет: – планировать, организовать и проводить мероприятия, направленные на соблюдение правовых норм в области защиты данных.

	<p>Владеть:</p> <ul style="list-style-type: none"> – навыками работы с законодательными нормами, противодействующими проявлениям экстремизма, терроризма, коррупционного поведению в профессиональной деятельности и повседневной жизни. 	<p>Владеет:</p> <ul style="list-style-type: none"> – навыками работы с законодательными нормами о защите данных; – навыками проведения оценки рисков в области защиты данных.
ПКС-1	<p>Знать:</p> <ul style="list-style-type: none"> – возможности существующей программно-технической архитектуры; – методологию разработки программного обеспечения и технологию программирования; – методы и средства проектирования программного обеспечения; – типовые решения, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения. 	<p>Знает:</p> <ul style="list-style-type: none"> – современные архитектуры информационных систем для поддержки интеграции с инструментами для шифрования, аутентификации и управления доступом; – способы реализации многоуровневой защиты, включая защиту на уровне сети, приложений и данных; – стандартные протоколы безопасности для защиты данных; – библиотеки для реализации шифрования и других криптографических функций.
	<p>Уметь:</p> <ul style="list-style-type: none"> – проводить оценку и обоснование рекомендуемых решений; – вырабатывать варианты реализации программного обеспечения; – применять методы и средства проектирования программного обеспечения, структур данных, программных интерфейсов. 	<p>Умеет:</p> <ul style="list-style-type: none"> – проводить анализ рисков, связанных с защитой данных, и оценивать эффективность различных методов и технологий защиты; – обосновывать выбор тех или иных решений по защите данных; – адаптировать существующие решения по защите данных; – применять методы проектирования программного обеспечения, которые обеспечивают безопасность данных.
	<p>Владеть:</p> <ul style="list-style-type: none"> – анализом возможностей реализации требований к программному обеспечению; – навыками распределения заданий между программистами в соответствии с техническими спецификациями; – методами проектирования структур данных; – методами проектирования программных интерфейсов; – навыками осуществления обучения и наставничества. 	<p>Владеет:</p> <ul style="list-style-type: none"> – анализом возможностей реализации требований к защите данных; – навыками распределения задач среди команды разработчиков, учитывая их опыт и специализацию в области защиты данных; – методами проектирования структур данных, которые обеспечивают безопасное и эффективное хранение конфиденциальной информации.

II. СОДЕРЖАНИЕ И ОБЪЕМ ДИСЦИПЛИНЫ

с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

Очная форма обучения

№	Наименование разделов и тем	Всего часов	Ауд. занятия			Сам. раб.
			ЛК	ЛБ	ПЗ	
2 семестр						
	Раздел 1. Основы защиты данных	134,7	18		18	98,7
1.	Тема 1. Защита информации, целостность и конфиденциальность данных. Санкционированный доступ к информации	7	1			6
2.	Тема 2. Необходимость защиты информации в современном мире	14	1		2	4
3.	Тема 3. Авторское право. Охрана авторского права государством	14	2		2	10
4.	Тема 4. Законодательство, регулирующее защиту информации	16	2		2	12
5.	Тема 5. Каналы утечки информации	14	2		2	10
6.	Тема 6. Программные средства защиты. Объекты и назначение программной защиты	14	2		2	10
7.	Тема 7. Подходы к выбору средств защиты	14	2		2	10
8.	Тема 8. Программные средства защиты и борьбы с пиратством	16	2		2	12
9.	Тема 9. Защита информационных систем системами криптографии данных	16	2		2	12
10.	Тема 10. Хакерские атаки и методы защиты от них	16,7	2		2	12,7
	Экзамен	0,3				
	Контроль	9				
	Итого за 2 семестр	144	18		18	98,7
	в т.ч. практическая подготовка	2				
	ИТОГО	144	18		18	98,7

Очно-заочная форма обучения не реализуется

Заочная форма обучения не реализуется

III. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И

ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Текущая аттестация проводится в форме реферата.

Примерная тематика рефератов

1. Основы законодательства о защите данных.
2. Методы оценки рисков в области защиты данных: подходы и лучшие практики.
3. Роль технологий шифрования в защите данных.
4. Кибербезопасность и защита данных, как предотвратить утечку информации.
5. Влияние социальных медиа на защиту данных.
6. Защита данных в облачных вычислениях.
7. Автоматизация процессов защиты данных: преимущества и недостатки.
8. Политики конфиденциальности, как создать эффективный документ для пользователей.
9. Роль искусственного интеллекта в защите данных.
10. Интеллектуальная собственность в условиях рыночной экономики.
11. Электронная подпись.
12. Использование защит для отражения хакерских атак.
13. Программная защита при передаче данных.
14. Методы борьбы с фишинговыми атаками.
15. Законодательство о персональных данных.
16. Защита авторских прав.
17. Банковская безопасность.
18. Программные средства анализа локальных сетей на предмет уязвимостей.
19. Безопасность применения платежных систем - законодательство и практика.
20. Методы несанкционированного доступа к информации.

Промежуточная аттестация обучающихся осуществляется в форме экзамена во 2 семестре с использованием следующих оценочных материалов:

Вопросы к экзамену (2 семестр, очная форма обучения)

1. Защита информации, целостность и конфиденциальность данных. Санкционированный доступ к информации
2. Основные понятия в области информационно-технической безопасности.
3. Авторское право.
4. Составляющие информационно-технической безопасности.
5. Классификация информации по степеням конфиденциальности.
6. Концепция защиты информации.
7. Обзор российских и международных правовых подходов к обеспечению информационной безопасности.
8. Основные законы, регулирующие защиту информации в Российской Федерации.

9. Основные каналы утечки информации.
10. Средства обеспечения безопасности компьютерных сетей.
11. Средства анализа защищенности сетевых сервисов.
12. Средства анализа защищенности операционных систем.
13. Средства анализа защищенности приложений.
14. Средства обнаружения атак.
15. Варианты установки системы обнаружения атак.
16. Проблема надежности и достоверности информации.
17. Надежность и достоверность информации.
18. Механизмы и средства защиты сетей.
19. Возможности средств анализа защищенности.
20. Основные определения криптографии.
21. Алгоритмы симметричного шифрования.
22. Основные функции антивируса.
23. Межсетевые экраны.
24. Виды угроз.
25. Основные нарушения.
26. Характер происхождения угроз (умышленные и естественные факторы).
27. Источники угроз.
28. Предпосылки появления угроз. Классы каналов несанкционированного получения информации.
29. Причины нарушения целостности информации.
30. Сетевые защищенные протоколы.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Внуков А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/537247> (дата обращения: 03.04.2024).
2. Чернова Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 327 с. — (Высшее образование). — ISBN 978-5-534-16772-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/542739> (дата обращения: 03.04.2024).

4.2. Дополнительная литература

1. Ищейнов В. Я. Информационная безопасность и защита информации : теория и практика : учебное пособие : [16+] / В. Я. Ищейнов. — Москва ; Берлин : Директ-Медиа, 2020. — 271 с. : схем., табл. — Режим доступа: по подписке. — URL: <https://biblioclub.ru/index.php?page=book&id=571485> (дата обращения: 03.04.2024). —

Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный.

2. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/555950> (дата обращения: 03.04.2024).

V. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№ пп	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
1.	http://edu.ru/	Российское образование: Федеральный портал. Включает ссылки на порталы и сайты образовательных учрежде- ний; государственные обра- зовательные стандарты; нор- мативные документы; ката- лог экскурсий и обучающих программ.	Свободный доступ
2.	http://citforum.ru/database/osbd/contents.shtml	Информационно-аналитиче- ские материалы	Свободный доступ

VI. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1.	http://www.biblioclub.ru	Электронно-библиотечная система (ЭБС) Университетская библиотека он- лайн	Регистрация через лю- бой университетский компьютер. В дальнейшем предо- ставляется неограничен- ный индивидуальный доступ из любой точки, в которой имеется до- ступ к сети Интернет
2.	www.garant.ru	Информационно-правовой портал	Свободный доступ
3.	www.elibrary.ru	Российский информационный пор- тал в области науки, технологии, медицины и образования	Свободный доступ

4.	www.consultant.ru	Российская компьютерная справочно-правовая система	Свободный доступ
----	----------------------------------------------------------	----------------------------------------------------	------------------

VII. ЛИЦЕНЗИОННОЕ И СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

При реализации учебной дисциплины применяется следующее лицензионное и свободно распространяемое программное обеспечение:

- Microsoft Windows;
- Microsoft Office;
- LibreOffice;
- реляционная система управления базами данных с открытым исходным кодом – MySQL.

VIII. ОБОРУДОВАНИЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБУЧЕНИЯ, НЕОБХОДИМЫЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Учебные занятия проводятся в аудиториях, укомплектованных специализированной мебелью, в том числе стационарными или переносными техническими средствами обучения (проектор, экран, компьютер/ноутбук).

Лабораторные занятия, групповые и индивидуальные консультации, текущая и промежуточная аттестации проводятся в специализированных классах, оснащенных автоматизированными рабочими местами с компьютерами.

Самостоятельная работа проводится в кабинетах, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.