

Министерство науки и высшего образования Российской Федерации
Муромский институт (филиал)
федерального государственного бюджетного образовательного учреждения высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(МИ ВлГУ)**

Кафедра ЭиВТ

«УТВЕРЖДАЮ»
Заместитель директора по УР
_____ Д.Е. Андрианов
_____ 04.06.2019

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Защита информации

Направление подготовки

09.03.01 Информатика и вычислительная техника

Профиль подготовки

Вычислительные машины, комплексы, системы и сети

Семестр	Трудоем- кость, час./зач. ед.	Лек- ции, час.	Практи- ческие занятия, час.	Лабора- торные работы, час.	Консультация, час.	Конт- роль, час.	Всего (контактная работа), час.	СРС, час.	Форма промежу- точного контроля (экз., зач., зач. с оц.)
8	144 / 4	12	12	12	3,2	0,35	39,55	77,8	Экз.(26,65)
Итого	144 / 4	12	12	12	3,2	0,35	39,55	77,8	26,65

Муром, 2019 г.

1. Цель освоения дисциплины

Цель дисциплины: обеспечение студентов знаниями в области защиты информации от несанкционированного доступа техническими и криптографическими средствами.

Задачи дисциплины: освоение студентами знаний по возможным каналам утечки информации, по механизмам предотвращения несанкционированного доступа к информации, методам подавления каналов утечки информации, по методам криптографической защиты информации, передаваемой по открытым каналам связи, по существующим стандартам в этой области.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина базируется на дисциплинах "Математика", "Физика", "Информатика", "Электротехника, электроника и схемотехника", "Дискретная математика", "Программирование". Результаты изучения дисциплины "Защита информации" используются обучающимися при подготовке ВКР.

3. Планируемые результаты обучения по дисциплине

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения средства компетенции	Результаты обучения по дисциплине	
ПК-10 Способен оценить угрозы информационной безопасности и выбрать современные средства защиты информации	ПК-10.1 Знает нормативные документы по защите информации.	Знать нормативные документы по защите информации Владеть навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	вопросы к устному опросу, тест
	ПК-10.2 Разрабатывает модель угроз и методы защиты от них для информационных систем.	Знать о существующих угрозах информационной безопасности и их источниках Уметь разрабатывать модель угроз и методы защиты от них для информационных систем.	
	ПК-10.3 Умеет использовать средства защиты информации.	Знать о существующих средствах обеспечения информационной безопасности и тенденциях их развития Уметь выбирать и использовать средства защиты от основных классов угроз Владеть навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

4.1. Форма обучения: очная

Уровень базового образования: среднее общее.

Срок обучения 4г.

4.1.1. Структура дисциплины

№ п\п	Раздел (тема) дисциплины	Семестр	Контактная работа обучающихся с педагогическим работником							Самостоятельная работа	Форма текущего контроля успеваемости (по неделям семестра), форма промежуточной аттестации(по семестрам)
			Лекции	Практические занятия	Лабораторные работы	Контрольные работы	КП / КР	Консультация	Контроль		
1	Каналы утечки информации и технические средства защиты.	8	2	2						22	устный опрос, отчеты по практическим работам, экзаменационное тестирование
2	Криптографические методы защиты.	8	10	10	12					55,8	устный опрос, отчеты по лабораторным и практическим работам, экзаменационное тестирование
Всего за семестр		144	12	12	12			3,2	0,35	77,8	Экз.(26,65)
Итого		144	12	12	12			3,2	0,35	77,8	26,65

4.1.2. Содержание дисциплины

4.1.2.1. Перечень лекций

Семестр 8

Раздел 1. Каналы утечки информации и технические средства защиты.

Лекция 1.

Задачи защиты информации. Каналы утечки информации, принципы и методы защиты (2 часа).

Раздел 2. Криптографические методы защиты.

Лекция 2.

Криптографическая защита информации. Методы защиты с секретным и открытым ключом (2 часа).

Лекция 3.

Шифры с секретным ключом. Блочные и потоковые шифры. Шифры DES, ГОСТ 28147-89, RC6, AES (2 часа).

Лекция 4.

Криптосистемы с открытым ключом. Шифры Шамира, Эль-Гамала и RSA (2 часа).

Лекция 5.

Электронная или цифровая подпись. Электронная подпись на базе шифров Эль-Гамала и RSA. Криптографические протоколы с открытым ключом (2 часа).

Лекция 6.

Теоретическая стойкость криптосистем. Методы взлома шифрованной информации и надежность криптографической защиты информации (2 часа).

4.1.2.2. Перечень практических занятий

Семестр 8

Раздел 1. Каналы утечки информации и технические средства защиты.

Практическое занятие 1

Каналы утечки информации. Электрические и электромагнитные каналы (2 часа).

Раздел 2. Криптографические методы защиты.

Практическое занятие 2

Примеры простейших методов шифрования (2 часа).

Практическое занятие 3

Алгоритмы блочного шифрования и дешифрования с секретным ключом DES (2 часа).

Практическое занятие 4

Алгоритмы шифрования и дешифрования с секретным ключом по ГОСТ 28147-89 (2 часа).

Практическое занятие 5

Теория чисел в задачах шифрования и дешифрования информации (2 часа).

Практическое занятие 6

Алгоритмы шифрования и дешифрования с открытым ключом (2 часа).

4.1.2.3. Перечень лабораторных работ

Семестр 8

Раздел 2. Криптографические методы защиты.

Лабораторная 1.

Классические симметричные криптосистемы (4 часа).

Лабораторная 2.

Разработка программы шифрования и дешифрования по алгоритму DES (4 часа).

Лабораторная 3.

Разработка программы шифрования и дешифрования с открытым ключом (4 часа).

4.1.2.4. Перечень тем и учебно-методическое обеспечение самостоятельной работы

Перечень тем, вынесенных на самостоятельное изучение:

1. Задачи защиты информации. Классификация информации по степени секретности, принадлежности и виду ее носителя.
2. Основные способы защиты информации.
3. Основные каналы утечки информации из контролируемых зон.
4. Виды и технические средства разведок. Технические средства защиты информации от утечки.
5. Классификация каналов утечки информации по лежащим в их основе физическим законам.
6. Средства выявления каналов утечки информации.
7. Алгоритмы первых криптографических систем.
8. Классификация шифров по степени стойкости. Методы взлома шифрованной информации.
9. Блочные и потоковые шифры.
10. Особенности криптографических систем с секретным и открытым ключом.
11. Алгоритм шифрования с секретным ключом DES.
12. Алгоритмы нахождения наибольшего общего делителя, наименьшего общего кратного и составления таблицы простых чисел.
13. Быстрый алгоритм умножения и возведения в степень по модулю заданного числа. Решение сравнений.
14. Шифры с открытым ключом Диффи - Шелмана, Шамира, Эль-Гамала и RSA.
15. Алгоритмы электронной или цифровой подписи. Предъявляемые к подписи требования.
16. Случайные числа в криптографии.

Для самостоятельной работы используются методические указания по освоению дисциплины и издания из списка приведенной ниже основной и дополнительной литературы.

4.1.2.5. Перечень тем контрольных работ, рефератов, ТР, РГР, РПР

Не планируется.

4.1.2.6. Примерный перечень тем курсовых работ (проектов)

Не планируется.

4.2 Форма обучения: заочная

Уровень базового образования: среднее общее.

Срок обучения 5л.

Семестр	Трудоем- кость, час./ зач. ед.	Лек- ции, час.	Прак- тические занятия, час.	Лабора- торные работы, час.	Консультация, час.	Конт- роль, час.	Всего (контак- тная работа), час.	СРС, час.	Форма промежуточного контроля (экз., зач., зач. с оц.)
9	144 / 4	4	4	8	2	0,6	18,6	116,75	Экз.(8,65)
Итого	144 / 4	4	4	8	2	0,6	18,6	116,75	8,65

4.2.1. Структура дисциплины

№ п\п	Раздел (тема) дисциплины	Семестр	Контактная работа обучающихся с педагогическим работником							Самостоятельная работа	Форма текущего контроля успеваемости (по неделям семестра), форма промежуточной аттестации(по семестрам)
			Лекции	Практические занятия	Лабораторные работы	Контрольные работы	КП / КР	Консультация	Контроль		
1	Каналы утечки информации и технические средства защиты.	9	2							39	устный опрос, экзаменационное тестирование
2	Криптографические методы защиты.	9	2	4	8					77,75	устный опрос, отчеты по лабораторным и практическим работам, экзаменационное тестирование
Всего за семестр		144	4	4	8	+		2	0,6	116,75	Экз.(8,65)
Итого		144	4	4	8			2	0,6	116,75	8,65

4.2.2. Содержание дисциплины

4.2.2.1. Перечень лекций

Семестр 9

Раздел 1. Каналы утечки информации и технические средства защиты.

Лекция 1.

Задачи защиты информации. Каналы утечки информации, принципы и методы защиты (2 часа).

Раздел 2. Криптографические методы защиты.

Лекция 2.

Криптографическая защита информации. Методы защиты с секретным и открытым ключом (2 часа).

4.2.2.2. Перечень практических занятий

Семестр 9

Раздел 2. Криптографические методы защиты.

Практическое занятие 1.

Теория чисел в задачах шифрования и дешифрования информации (2 часа).

Практическое занятие 2.

Алгоритмы шифрования и дешифрования с открытым ключом (2 часа).

4.2.2.3. Перечень лабораторных работ

Семестр 9

Раздел 1. Криптографические методы защиты.

Лабораторная 1.

Разработка программы шифрования по алгоритму DES. Разработка программы дешифрования по алгоритму DES (4 часа).

Лабораторная 2.

Разработка программы шифрования и дешифрования с открытым ключом (4 часа).

4.2.2.4. Перечень тем и учебно-методическое обеспечение самостоятельной работы

Перечень тем, вынесенных на самостоятельное изучение:

1. Задачи защиты информации. Классификация информации по степени секретности, принадлежности и виду ее носителя.

2. Основные способы защиты информации.

3. Основные каналы утечки информации из контролируемых зон.

4. Виды и технические средства разведок. Технические средства защиты информации от утечки.

5. Классификация каналов утечки информации по лежащим в их основе физическим законам.

6. Средства выявления каналов утечки информации.

7. Алгоритмы первых криптографических систем.

8. Классификация шифров по степени стойкости. Методы взлома шифрованной информации.

9. Блочные и потоковые шифры.

10. Особенности криптографических систем с секретным и открытым ключом.

11. Алгоритм шифрования с секретным ключом DES.

12. Алгоритмы нахождения наибольшего общего делителя, наименьшего общего кратного и составления таблицы простых чисел.

13. Быстрый алгоритм умножения и возведения в степень по модулю заданного числа. Решение сравнений.

14. Шифры с открытым ключом Диффи - Шелмана, Шамира, Эль-Гамала и RSA.

15. Алгоритмы электронной или цифровой подписи. Предъявляемые к подписи требования.

16. Случайные числа в криптографии.

Для самостоятельной работы используются методические указания по освоению дисциплины и издания из списка приведенной ниже основной и дополнительной литературы.

4.2.2.5. Перечень тем контрольных работ, рефератов, ТР, РГР, РПР

1. Криптографическая защита информации. Методы защиты с секретным и открытым ключом.

2. Шифры с секретным ключом. Блочные и потоковые шифры. Шифры DES, ГОСТ 28147-89, RC6, AES.

3. Криптосистемы с открытым ключом. Шифры Шамира, Эль-Гамала и RSA.

4. Электронная подпись на базе шифров Эль-Гамала и RSA.

5. Криптографические протоколы с открытым ключом.

6. Теоретическая стойкость криптосистем.
7. Методы взлома шифрованной информации и надежность криптографической защиты информации.

4.2.2.6. Примерный перечень тем курсовых работ (проектов)

Не планируется.

5. Образовательные технологии

В процессе изучения дисциплины применяется контактная технология преподавания (за исключением самостоятельно изучаемых студентами вопросов). При проведении лабораторных и практических работ применяется имитационный или симуляционный подход. Шаги решения задач студентам демонстрируются при помощи мультимедийной техники. В дальнейшем студенты самостоятельно решают аналогичные задания.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Фонды оценочных материалов (средств) приведены в приложении.

7. Учебно-методическое и информационное обеспечение дисциплины.

7.1. Основная учебно-методическая литература по дисциплине

1. Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. – М.: Техносфера, 2021. – 482 с. [сайт]. – URL: <https://www.iprbookshop.ru/108023>
2. Фороузан, Б. А. Криптография и безопасность сетей: учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. – М.: ИНТУИТ, Ай Пи Ар Медиа, 2021. – 776 с. [сайт]. – URL: <https://www.iprbookshop.ru/102017>
3. Джонс, К. Д. Инструментальные средства обеспечения безопасности: учебное пособие / К. Д. Джонс, М. Шема, Б. С. Джонсон. – М.: ИНТУИТ, Ай Пи Ар Медиа, 2021. – 913 с. [сайт]. – URL: <https://www.iprbookshop.ru/102011>
4. Гулак, М. Л. Аудит информационной безопасности. Прикладная статистика: учебное пособие / М. Л. Гулак, М. Ю. Рытов, О. М. Голембиовская. – М.: Ай Пи Ар Медиа, 2020. – 121 с. [сайт]. – URL: <https://www.iprbookshop.ru/97630>
5. Шинаков, К. Е. Анализ рисков безопасности информационных систем персональных данных: монография / К. Е. Шинаков, М. Ю. Рытов, О. М. Голембиовская. – М.: Ай Пи Ар Медиа, 2020. – 236 с. [сайт]. – URL: <https://www.iprbookshop.ru/95150>
6. Милославская, Н. Г. Управление информационной безопасностью. Конспект лекций: учебное пособие / Н. Г. Милославская, А. И. Толстой. – М.: Национальный исследовательский ядерный университет «МИФИ», 2020. – 534 с. [сайт]. – URL: <https://www.iprbookshop.ru/125513>
7. Галатенко, В. А. Основы информационной безопасности: учебное пособие / В. А. Галатенко. – 3-е изд. – М.: ИНТУИТ, Ай Пи Ар Медиа, 2020. – 266 с. [сайт]. – URL: <https://www.iprbookshop.ru/97562>
8. Полянская, О. Ю. Инфраструктуры открытых ключей: учебное пособие / О. Ю. Полянская, В. С. Горбатов. – Москва, Саратов: ИНТУИТ, Ай Пи Ар Медиа, 2020. – 452 с. [сайт]. – URL: <https://www.iprbookshop.ru/89439>
9. Басалова, Г. В. Основы криптографии: учебное пособие / Г. В. Басалова. – Москва, Саратов: ИНТУИТ, Ай Пи Ар Медиа, 2020. – 282 с. [сайт]. – URL: <https://www.iprbookshop.ru/89455>
10. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. – Саратов: Профобразование, 2019. – 702 с. [сайт]. – URL: <https://www.iprbookshop.ru/87995>
11. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. – Саратов: Профобразование, 2019. – 543 с. [сайт]. – URL: <https://www.iprbookshop.ru/87992>

12. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. – 2-е изд. – Саратов: Профобразование, 2019. – 446 с. [сайт]. – URL: <https://www.iprbookshop.ru/87998>
13. Этапы формирования модели угроз и модели нарушителя информационной безопасности с учетом изменений законодательства Российской Федерации: учебное пособие / О. М. Голембиовская, М. Ю. Рытов, К. Е. Шинаков [и др.]. – Саратов: Вузовское образование, 2021. – 265 с. [сайт]. – URL: <https://www.iprbookshop.ru/109162>

7.2. Дополнительная учебно-методическая литература по дисциплине

1. Фомин, Д. В. Защита информации: специализированные аттестованные программные и программно-аппаратные средства: практикум / Д. В. Фомин. – Саратов: Вузовское образование, 2021. – 218 с. [сайт]. – URL: <https://www.iprbookshop.ru/110329>
2. Епишкина, А. В. Нормативное регулирование в области защиты информации. Конспект лекций: учебное пособие / А. В. Епишкина, С. В. Запечников. – М.: Национальный исследовательский ядерный университет «МИФИ», 2021. – 116 с. [сайт]. – URL: <https://www.iprbookshop.ru/125496>
3. Данилова, О. Т. Методы и средства компьютерной экспертизы: учебное пособие / О. Т. Данилова. – Омск: Омский государственный технический университет, 2021. – 124 с. [сайт]. – URL: <https://www.iprbookshop.ru/124838>
4. Солонская, О. И. Средства защиты информации: учебное пособие / О. И. Солонская. – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2021. – 89 с. [сайт]. – URL: <https://www.iprbookshop.ru/117115>
5. Велигура, А. Н. Комбинаторика и теория графов для кибербезопасности. Конспект лекций: учебное пособие / А. Н. Велигура. – М.: Национальный исследовательский ядерный университет «МИФИ», 2021. – 200 с. [сайт]. – URL: <https://www.iprbookshop.ru/125492>
6. Фомичев, В. М. Элементы теории информации в защите информации: учебное пособие для академического бакалавриата / В. М. Фомичев. – М.: Прометей, 2021. – 218 с. [сайт]. – URL: <https://www.iprbookshop.ru/125693>
7. Хаулет, Т. Защитные средства с открытыми исходными текстами. Практическое руководство по защитным приложениям: учебное пособие / Т. Хаулет. – М.: ИНТУИТ, Ай Пи Ар Медиа, 2020. – 607 с. [сайт]. – URL: <https://www.iprbookshop.ru/97544>
8. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А. И. Белоус, В. А. Солодуха. – Москва, Вологда: Инфра-Инженерия, 2020. – 692 с. [сайт]. – URL: <https://www.iprbookshop.ru/98349>
9. Защита Web-приложений: учебное пособие / А. В. Скрыпников, Д. В. Арапов, В. В. Денисенко, Т. Д. Герасимова. – Воронеж: Воронежский государственный университет инженерных технологий, 2020. – 76 с. [сайт]. – URL: <https://www.iprbookshop.ru/106438>
10. Ильин, М. Е. Теоретико-числовые методы в криптографии. Ч.1: учебное пособие / М. Е. Ильин, К. А. Ципоркова. – Рязань: Рязанский государственный радиотехнический университет, 2020. – 112 с. [сайт]. – URL: <https://www.iprbookshop.ru/121800>
11. Пилиди, В. С. Математические основы защиты информации: учебное пособие / В. С. Пилиди. – Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2019. – 308 с. [сайт]. – URL: <https://www.iprbookshop.ru/95786>
12. Брюхомицкий, Ю. А. Безопасность информационных технологий. В 2 частях. Ч.1: учебное пособие / Ю. А. Брюхомицкий. – Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2020. – 171 с. [сайт]. – URL: <https://www.iprbookshop.ru/107943>
13. Масюк, М. А. Основные понятия и правовые основы защиты информации: учебное пособие / М. А. Масюк, А. А. Попов, Е. В. Касьянова. – Красноярск: Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, 2020. – 82 с. [сайт]. – URL: <https://www.iprbookshop.ru/116643>
14. Скрипник, Д. А. Общие вопросы технической защиты информации: учебное пособие / Д. А. Скрипник. – 3-е изд. – Москва, Саратов: ИНТУИТ, Ай Пи Ар Медиа, 2020. – 424 с. [сайт]. – URL: <https://www.iprbookshop.ru/89451>

15. Скрипник, Д. А. Обеспечение безопасности персональных данных: учебное пособие / Д. А. Скрипник. – 3-е изд. – Москва, Саратов: ИНТУИТ, Ай Пи Ар Медиа, 2020. – 121 с. [сайт]. – URL: <https://www.iprbookshop.ru/89449>
16. Косолапов, Ю. В. Криптографические протоколы на основе линейных кодов: учебное пособие / Ю. В. Косолапов. – Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2020. – 98 с. [сайт]. – URL: <https://www.iprbookshop.ru/100176>
17. Суворова, Г. М. Информационная безопасность: учебное пособие / Г. М. Суворова. – Саратов: Вузовское образование, 2019. – 214 с. [сайт]. – URL: <https://www.iprbookshop.ru/86938>
18. Богульская, Н. А. Модели безопасности компьютерных систем: учебное пособие / Н. А. Богульская, М. М. Кучеров. – Красноярск: Сибирский федеральный университет, 2019. – 206 с. [сайт]. – URL: <https://www.iprbookshop.ru/100055>
19. Жиль, Земор Курс криптографии / Земор Жиль; перевод В. В. Шуликовская. – Москва, Ижевск: Регулярная и хаотическая динамика, Институт компьютерных исследований, 2019. – 256 с. [сайт]. – URL: <https://www.iprbookshop.ru/91941>
20. Зенков, А. В. Основы информационной безопасности: учебное пособие / А. В. Зенков. – Москва, Вологда: Инфра-Инженерия, 2022. – 104 с. [сайт]. – URL: <https://www.iprbookshop.ru/124242>
21. Ревнивых, А. В. Информационная безопасность в организациях: учебное пособие / А. В. Ревнивых. – М.: Ай Пи Ар Медиа, 2021. – 83 с. [сайт]. – URL: <https://www.iprbookshop.ru/108227>

7.3. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

В образовательном процессе используются информационные технологии, реализованные на основе информационно-образовательного портала института (www.mivlgu.ru/iop), и инфокоммуникационной сети института:

- предоставление учебно-методических материалов в электронном виде;
- взаимодействие участников образовательного процесса через локальную сеть института и Интернет;
- предоставление сведений о результатах учебной деятельности в электронном личном кабинете обучающегося.

Информационные справочные системы:

Информационно-поисковая система Консультант Плюс <http://www.consultant.ru>

Информационный портал Совета Безопасности Российской Федерации <http://www.scrf.gov.ru/security/information/>

Информационно-аналитический портал iso27000.ru <http://iso27000.ru>

Информационно-образовательный портал МИ ВлГУ <https://www.mivlgu.ru/iop/>

Научная электронная библиотека "eLibrary" <http://elibrary.ru>

Электронная библиотека ВлГУ <https://dspace.www1.vlsu.ru/>

Электронная библиотека «ЭВРИКА» <http://elib.mivlgu.local/>

Курс: Основы информационной безопасности

<http://www.intuit.ru/studies/courses/10/10/info>

Курс: Стандарты информационной безопасности

<http://www.intuit.ru/studies/courses/30/30/info>

Курс: Криптографические основы безопасности

<http://www.intuit.ru/studies/courses/28/28/info>

Программное обеспечение:

Microsoft Visual Studio (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

iprbookshop.ru
consultant.ru
iso27000.ru
intuit.ru
mivlgu.ru/iop

8. Материально-техническое обеспечение дисциплины

Лаборатория сетевых технологий и систем пространственного позиционирования
Компьютер IN WIN - 12 шт.; проектор NEC Projector NP40G; экран настенный, акустическая система

Лекционная аудитория
Проектор ACER P1100 DLP Projector EMEA; Компьютер Celeron 1.8 GHz; Экран настенный; Акустическая система;

Лаборатория программирования и лицензионного программного обеспечения
Компьютер Kraftway Credo KC 36 - 12 шт.; проектор NEC Projector VT595G; экран настенный; акустическая система.

9. Методические указания по освоению дисциплины

Для успешного освоения теоретического материала обучающийся: знакомится со списком рекомендуемой основной и дополнительной литературы; уточняет у преподавателя, каким дополнительным пособиям следует отдать предпочтение; ведет конспект лекций и прорабатывает лекционный материал, пользуясь как конспектом, так и учебными пособиями.

На практических занятиях пройденный теоретический материал подкрепляется решением задач по основным темам дисциплины. Занятия проводятся в компьютерном классе, используя специальное программное обеспечение. Каждой подгруппе обучающихся преподаватель выдает задачу, связанную с разработкой и программной реализацией алгоритмов обработки информации. В конце занятия обучающие демонстрируют полученные результаты преподавателю и при необходимости делают работу над ошибками.

До выполнения лабораторных работ обучающийся изучает соответствующий раздел теории. Перед занятием студент знакомится с описанием заданий для выполнения работы, внимательно изучает содержание и порядок проведения лабораторной работы. Лабораторная работа проводится в компьютерном классе. Обучающиеся выполняют индивидуальную задачу компьютерного моделирования в соответствии с заданием на лабораторную работу. Полученные результаты исследований сводятся в отчет и защищаются по традиционной методике в классе на следующем лабораторном занятии. Необходимый теоретический материал, индивидуальное задание, шаги выполнения лабораторной работы и требование к отчету приведены в методических указаниях, размещенных на информационно-образовательном портале института.

Самостоятельная работа оказывает важное влияние на формирование личности будущего специалиста, она планируется обучающимся самостоятельно. Каждый обучающийся самостоятельно определяет режим своей работы и меру труда, затрачиваемого на овладение учебным содержанием дисциплины. Он выполняет внеаудиторную работу и изучение разделов, выносимых на самостоятельную работу, по личному индивидуальному плану, в зависимости от его подготовки, времени и других условий.

Форма заключительного контроля при промежуточной аттестации – экзамен. Для проведения промежуточной аттестации по дисциплине разработаны фонд оценочных средств и бально-рейтинговая система оценки учебной деятельности студентов. Оценка по дисциплине выставляется в информационной системе и носит интегрированный характер, учитывающий результаты оценивания участия студентов в аудиторных занятиях, качества и своевременности выполнения заданий в ходе изучения дисциплины и промежуточной аттестации.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению *09.03.01 Информатика и вычислительная техника* и профилю подготовки *Вычислительные машины, комплексы, системы и сети*

Рабочую программу составил ст. преподаватель *Холкина Н.Е.*_____

Программа рассмотрена и одобрена на заседании кафедры *ЭиВТ* протокол № 34 от 29.05.2019 года.

Заведующий кафедрой *ЭиВТ* _____*Кропотов Ю.А.*
(Подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии факультета ФРЭКС

протокол № 9 от 31.05.2019 года.

Председатель комиссии ФРЭКС _____*Белов А.А.*
(Подпись)

Лист актуализации рабочей программы дисциплины

Программа одобрена на 2020/2021 учебный год.

Протокол заседания кафедры № 24 от 27.05.2020 года.

Заведующий кафедрой ЭиВТ _____ *Кропотов Ю.А.*
(Подпись)

Программа одобрена на 2021/2022 учебный год.

Протокол заседания кафедры № 32 от 19.05.2021 года.

Заведующий кафедрой ЭиВТ _____ *Белов А.А.*
(Подпись)

Программа одобрена на 2022/2023 учебный год.

Протокол заседания кафедры № 34 от 11.05.2022 года.

Заведующий кафедрой ЭиВТ _____ *Белов А.А.*
(Подпись)

Фонд оценочных материалов (средств) по дисциплине
Защита информации

1. Оценочные материалы для проведения текущего контроля успеваемости по дисциплине

Варианты заданий к лабораторным и практическим работам и перечень контрольных вопросов приведены в методических указаниях:

1) Методические указания для практических занятий доступны по ссылке: <https://www.mivlgu.ru/iop/mod/resource/view.php?id=7695>

2) Методические указания для лабораторных занятий доступны по ссылке: <https://www.mivlgu.ru/iop/mod/resource/view.php?id=7698>

Вопросы для устного опроса:

1. Возможные каналы утечки информации, классификация информации по виду и степени секретности, по способам хранения и защиты.
2. Организационные и технические средства защиты информации. Требования, предъявляемые к техническим средствам хранения информации, расположенным в контролируемых зонах.
3. Электромагнитные, электрические и акустические каналы утечки информации из контролируемых зон. Технические средства разведок.
4. Принципы криптографической защиты информации. Исторические методы шифрования. Понятие совершенного шифра.
5. Криптографические системы защиты информации с секретным ключом и схема секретной связи.
6. Блочные и потоковые шифры. Шифры DES и ГОСТ 28147-89.
7. Криптографические системы с открытым ключом. Криптосистема Диффи – Хеллмана и ее недостатки.
8. Определение односторонней функции и роль этой функции в криптосистемах с открытым ключом. Пример односторонней функции возведения в степень. Алгоритм быстрого возведения в степень по модулю некоторого числа.
9. Элементы теории чисел. Понятие простого числа. Решето Эратосфена. Свойства сумм и произведений целых по модулю чисел.
10. Доказать, что мощность множества простых чисел бесконечна. Формула, определяющая показатель, с которым данное простое число «р» входит в произведение $n!$
11. Функция и теорема Эйлера. Нахождение функции Эйлера.
12. Алгоритм разложения отношения двух целых чисел в цепную дробь. Задачи сравнения и алгоритмы их решения.
13. Алгоритм решения задачи деления по модулю целых чисел.
14. Теорема Ферма и решение многочленов по модулю.
15. Алгоритм шифра с открытым ключом Шамира.
16. Алгоритм шифра с открытым ключом Эль-Гамала.
17. Алгоритм шифра с открытым ключом RSA.
18. Методы взлома шифров и надежность криптографических систем защиты информации.
19. Цифровая подпись и ее реализация на базе шифра Эль-Гамала.
20. Цифровая подпись и ее реализация на базе шифра RSA.
21. Криптографические протоколы с открытым ключом.
22. Эллиптические кривые и вычисления на них. Математические основы.
23. Криптографические системы с совершенной секретностью. Определение и условия совершенной секретности.
24. Хеш-функции и методы формирования случайных чисел в криптографии.
25. Тесты для проверки генераторов случайных и псевдослучайных чисел.

Общее распределение баллов текущего контроля по видам учебных работ для студентов

Рейтинг-контроль 1	2 отчета по практическим	до 10 баллов
Рейтинг-контроль 2	3 отчета по практическим и 1 отчета по лабораторным работам	до 20 баллов
Рейтинг-контроль 3	3 отчета по практическим и 2 отчета по лабораторным работам	до 30 баллов
Посещение занятий студентом		0
Дополнительные баллы (бонусы)		0
Выполнение семестрового плана самостоятельной работы		0

2. Промежуточная аттестация по дисциплине

Перечень вопросов к экзамену / зачету / зачету с оценкой.

Перечень практических задач / заданий к экзамену / зачету / зачету с оценкой (при наличии)

Для проведения экзаменационного тестирования используются задания в тестовой форме, приведённые далее (в разделе 3).

Методические материалы, характеризующих процедуры оценивания

На основе типовых заданий программным комплексом информационно-образовательного портала МИ ВлГУ формируются в автоматическом режиме тестовые задания для студентов. Программный комплекс формирует индивидуальные задания для каждого зарегистрированного в системе студента и устанавливает время прохождения тестирования. Результатом тестирования является процент правильных ответов, с учетом индивидуального семестрового рейтинга студента формируется итоговая оценка.

Максимальная сумма баллов, набираемая студентом по дисциплине равна 100.

Оценка в баллах	Оценка по шкале	Обоснование	Уровень сформированности компетенций
Более 80	«Отлично»	Содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному	Высокий уровень
66-80	«Хорошо»	Содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками	Продвинутый уровень

50-65	«Удовлетворительно»	Содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки	<i>Пороговый уровень</i>
Менее 50	«Неудовлетворительно»	Содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки	<i>Компетенции не сформированы</i>

3. Задания в тестовой форме по дисциплине

Примеры заданий:

К особенностям асимметричных систем шифрования относятся алгоритмы шифрования и расшифрования являются открытыми
 алгоритмы шифрования и расшифрования являются секретными
 открытый ключ и криптограмма могут быть отправлены по незащищённым каналам связи

Псевдослучайная последовательность, выработанная по заданному алгоритму для шифрования открытых данных и расшифровывания зашифрованных данных это?

Полный перечень тестовых заданий с указанием правильных ответов, размещен в банке вопросов на информационно-образовательном портале института по ссылке <https://www.mivlgu.ru/iop/question/edit.php?courseid=611&category=35187%2C20588&qbshowtext=0&recurse=0&showhidden=0>

Оценка рассчитывается как процент правильно выполненных тестовых заданий из их общего числа.