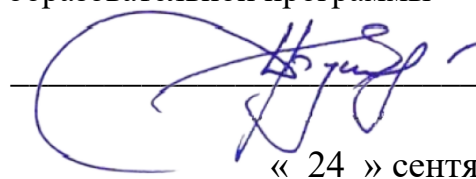


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДАЮ

Руководитель основной профессиональной
образовательной программы

 Буинцев Д.Н.
«_24_» сентября 2024 г

РАБОЧАЯ ПРОГРАММА

Дисциплины

Б1.О.24 Методы и средства криптографической защиты информации

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

10.03.01 Информационная безопасность

профиль

*Безопасность автоматизированных систем (по отрасли или в сфере
профессиональной деятельности)*

Квалификация

Бакалавр

Форма обучения

очная

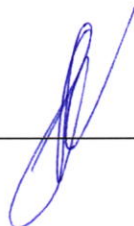
РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Южно-Сахалинск
2024

Рабочая программа дисциплины Методы и средства криптографической защиты информации составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность.

Программу составил:

Осипов Г.С., профессор кафедры информатики



Рабочая программа дисциплины Методы и средства криптографической защиты информации утверждена на заседании кафедры информатики, протокол № 8 от 19 марта 2024 г.

Исполняющий обязанности
заведующего кафедрой

Г.С. Осипов



1. Цель и задачи дисциплины

Цель дисциплины

Целью дисциплины «Методы и средства криптографической защиты информации» является формирование у студентов общих представлений о криптографических методах защиты информации, о применении криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности и об основных принципах, лежащих в основе функционирования криптографических средств защиты информации.

Задачи дисциплины

Основными задачами изучения дисциплины являются:

1. дать представление о криптографических методах защиты информации.
2. изучить математические основы современной криптографии.
3. изучить современные стандарты симметричного шифрования.
4. изучить основные криптографические алгоритмы с открытым ключом.
5. изучить криптографические функции хеширования.
6. сформировать умение применять полученные знания для компьютерной реализации криптографических алгоритмов.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Методы и средства криптографической защиты информации» относится к обязательной части Блока 1 Дисциплины (модули) подготовки студентов по направлению подготовки бакалавров 10.03.01 Информационная безопасность.

Пререквизиты дисциплины:

Для освоения данной дисциплины студент должен владеть компетенциями, сформированными основными понятиями дисциплин Математический анализ, Теоретические основы информатики, Языки и методы программирования.

Постреквизиты дисциплины:

Освоение данной дисциплины должно подготовить студентов к дальнейшему образованию в области вычислительной техники и систем обработки информации, в частности к изучению курсов: Методы оптимизации, Численные методы, Компьютерное моделирование, Web-технологии, языки и средства создания web-приложений, прохождению учебной и преддипломных практик, ведению научно-исследовательской работы.

3. Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ОПК-9	Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;	ОПК-9.1 Знает основные понятия криптографии и криптографические методы защиты информации; ОПК-9.2 Умеет определять наличие типовых технических каналов утечки информации, а также применять методики расчета и инструментального контроля показателей технической защиты информации на объектах информатизации ПК-9.3. Владеет практическими навыками обоснованного выбора и использования СКЗИ

		при решении задач профессиональной деятельности..
ОПК 4.3	Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем	ОПК-4.3.1 - Знает основные меры по защите информации в автоматизированных системах, а также содержание эксплуатационной документации автоматизированной системы; ОПК-4.3.2 - Умеет устранять выявленные уязвимости автоматизированной системы, приводящие к возникновению угроз безопасности информации, проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств; ОПК-4.3.3 - Владеет навыками осуществления автономной наладки технических и программных средств системы защиты информации автоматизированной системы.

4. Структура и содержание дисциплины (модуля)

4.1. Структура дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет 3 зачетные единицы (**108** академических часов).

Вид работы	Трудоемкость, акад. часов	
	семестр	всего
	7	
Общая трудоемкость	108	108
Контактная работа:	66	66
Лекции (Лек)	30	30
Лабораторные работы (Лаб)	30	30
Контактная работа в период теоретического обучения (КонтТО) (Проведение текущих консультаций и индивидуальная работа со студентами)	5	5
Контактная работа в период промежуточной аттестации (КонтПА)	1	1
Промежуточная аттестация экзамен	35	26
Самостоятельная работа:	7	7
- самостоятельное изучение разделов (перечислить);	0	0
- самоподготовка (проработка и повторение лекционного материала, материала учебников и учебных пособий);	2	2
- подготовка к лабораторным занятиям;	3	3
- подготовка к промежуточной аттестации и т.п.)	2	2

4.2. Распределение видов работы и их трудоемкости по разделам дисциплины (модуля)

№ п/п	Раздел дисциплины/ темы	Виды учебной работы (в часах)					Формы текущего контроля успеваемости, промежуточной аттестации
		семестр	контактная			Самостоятельная работа	
			Лекции	Практические занятия	Лабораторные занятия		
1.	Тема 1. Математические основы криптографии.	7	2	0	4		Устный опрос по теме лекции. Проверка домашнего задания.
2.	Тема 2 Основные цели и задачи криптографии		4	0	2	0	Устный опрос по теме лекции. Проверка домашнего задания.
3.	Тема 3 Историческая криптография		2	0	4	0	Устный опрос по теме лекции. Проверка домашнего задания.
4.	Тема 4. Симметричное шифрование		4	0	2	1	Устный опрос по теме лекции. Проверка домашнего задания.
5.	Тема 5 Хеширование		2	0	4	1	Устный опрос по теме лекции. Проверка домашнего задания.
6.	Тема 6. Поточное шифрование		4	0	2	1	Устный опрос по теме лекции. Проверка домашнего задания.
7.	Тема 7 ГСПЧ и проверка их качества		2	0	4	1	Устный опрос по теме лекции. Проверка домашнего задания.
8.	Тема 8. Криптография с открытым ключом		4	0	2	1	Устный опрос по теме лекции. Проверка домашнего задания.
9.	Тема 9. Электронная подпись.		2	0	4	1	Устный опрос по теме лекции. Проверка домашнего задания.
10.	Тема 10 Протоколы		4		2	1	
	экзамен				6	Устный экзамен (по билетам)	
	итого:	73	30	0	30	13	

4.3. Содержание разделов дисциплины

Тема 1 Математические основы криптографии

Криптографические методы защиты информации: шифрование, хеширование, электронная подпись.

Тема 2 Основные цели и задачи криптографии

Алгебраические структуры. Группы. Циклические группы. Кольца, кольца классов вычетов. Конечные поля. Поля Галуа. Эллиптические кривые. Понятие наибольшего общего делителя. Алгоритм Евклида, расширенный алгоритм Евклида. Сравнение первой степени с одним неизвестным. Китайская теорема об остатках. Генерация простых чисел. Тест на простоту. Алгоритмы работы с большими числами.

Тема 3 Историческая криптография

Математическая модель шифра. Классические шифры: подстановочный, перестановочный, шифр Хилла, шифры гаммирования

Тема 4. Симметричное шифрование

DES. ГОСТ 28147-89. ГОСТ Р 34.12-2015. ГОСТ Р 34.13-2015. Режимы шифрования, эммитовставка. AES.

Тема 5 Хеширование

Криптографические хеш-функции. ГОСТ Р 34.11- 2012. SHA-3.

Тема 6. Поточное шифрование

Принципы поточного шифрования. Типы поточного шифрования. Синхронные и самосинхронизирующиеся шифры. Шифр RC-4 как пример поточного алгоритма шифрования.

Тема 7 ГСПЧ и проверка их качества

Генерация случайных чисел. Псевдослучайные числа и их отличия от истинно случайных чисел. Подходы к получению псевдослучайных чисел. Критерии качества псевдослучайных чисел. Виды тестов псевдослучайных последовательностей. Тесты NIST.

Тема 8. Криптография с открытым ключом

Концепция криптографии с открытым ключом. Протокол Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль-Гамала. Криптосистема Рабина.

Тема 9. Электронная подпись.

Коды аутентичности сообщений. Электронная подпись. ГОСТ Р 34.10-2012. DSS. Инфраструктура открытого ключа.

Тема 10. Протоколы

Протокол раздельного вручения бита. Протоколы доказательства знания с нулевым разглашением. Протоколы простановки "слепых" подписей. Протоколы голосования. Протоколы безопасных вычислений

4.4 Темы и планы лабораторных занятий

Лабораторное занятие №1 (4 ч.)

Тема Математические основы криптографии

Вопросы для обсуждения:

1. Криптографические методы защиты информации.
2. Шифрование.
3. Хеширование.
4. Электронная подпись.

Лабораторное занятие №2 (2 ч.)

Тема Основные цели и задачи криптографии

Вопросы для обсуждения:

1. Сравнение первой степени с одним неизвестным.
2. Китайская теорема об остатках.
3. Генерация простых чисел.
4. Тест на простоту.
5. Алгоритмы работы с большими числами.

Лабораторное занятие №3 (4 ч.)

Тема Историческая криптография

Вопросы для обсуждения:

1. Математическая модель шифра.
2. Классические шифры: подстановочный, перестановочный.
3. Шифр Хилла.
4. Шифры гаммирования.

Лабораторное занятие №4 (2 ч.)

Тема Симметричное шифрование.

Вопросы для обсуждения:

ГОСТ 28147-89.

1. ГОСТ Р 34.12-2015.
2. ГОСТ Р 34.13-2015.
3. Режимы шифрования.

Лабораторное занятие №5 (4 ч.)

Тема Хеширование

Вопросы для обсуждения:

1. Криптографические хеш-функции.
2. ГОСТ Р 34.11- 2012.
3. SHA-3.

Лабораторное занятие №6 (2 ч.)

Тема Поточное шифрование

Вопросы для обсуждения:

1. Принципы поточного шифрования.
2. Типы поточного шифрования.
3. Синхронные и самосинхронизирующиеся шифры.
4. Шифр RC-4 как пример поточного алгоритма шифрования.

Лабораторное занятие №7 (4 ч.)

Тема ГСПЧ и проверка их качества

Вопросы для обсуждения:

1. Генерация случайных чисел.
2. Псевдослучайные числа и их отличия от истинно случайных чисел.
3. Подходы к получению псевдослучайных чисел.
4. Критерии качества псевдослучайных чисел.
5. Виды тестов псевдослучайных последовательностей.
6. Тесты NIST.

Лабораторное занятие №8 (2 ч.)

Тема. Криптография с открытым ключом

Вопросы для обсуждения:

1. Концепция криптографии с открытым ключом.
2. Протокол Диффи-Хеллмана.
3. Криптосистема RSA.
4. Криптосистема Эль-Гамала.
5. Криптосистема Рабина

Лабораторное занятие №9 (4 ч.)

Тема Электронная подпись

Вопросы для обсуждения:

1. Коды аутентичности сообщений.
2. Электронная подпись.
3. ГОСТ Р 34.10-2012.
4. Инфраструктура открытого ключа

Лабораторное занятие №10 (2 ч.)

Тема Протоколы

Вопросы для обсуждения:

1. Протокол раздельного вручения бита.
2. Протоколы доказательства знания с нулевым разглашением.
3. Протоколы простановки "слепых" подписей.
4. Протоколы голосования.
5. Протоколы безопасных вычислений

5. Темы дисциплины (модуля) для самостоятельного изучения

Не предусмотрены

6. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
	4 семестр		
1.	Тема 1. Математические основы криптографии.	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия 1	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
2.	Тема 2. Основные цели и задачи криптографии	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия 2	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
3.	Тема 3. Историческая криптография.	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия 3	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
4.	Тема 4. Симметричное шифрование	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия 4	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
5.	Тема 5. Хеширование	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия 5	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
6.	Тема 6. Поточное шифрование	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия 6	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.

7.	Тема 7. ГСПЧ и проверка их качества	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия 7	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
8.	Тема 8. Криптография с открытым ключом	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия 8	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
9.	Тема 9. Электронная подпись	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия 9	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
10	Тема 10 Протоколы	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия 10	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.

7. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине (модулю)

Примерные варианты индивидуальных заданий

Тесты

- Какой криптографический метод защиты информации предназначен для обеспечения конфиденциальности информации?
 - Хеширование
 - Электронная подпись
 - Шифрование
 - Коды аутентичности сообщений
- Для решения какой задачи обеспечения информационной безопасности предназначено хеширование?
 - Обеспечение конфиденциальности информации
 - Обеспечение неотказуемости
 - Обеспечение контроля целостности данных
 - Проверка подлинности источника данных
- Каким свойством обладают элементы a и a^{-1} в кольце классов вычетов по модулю n ?
 - $a \cdot a^{-1} = 0 \pmod{n}$
 - $a \cdot a^{-1} = -1 \pmod{n}$
 - $a \cdot a^{-1} = 1 \pmod{n}$
 - $a \cdot a^{-1} = n \pmod{n}$
- В каком случае существует значение a^{-1} по модулю n ?
 - Если a делит n
 - Если n делит a
 - Если $\text{НОД}(a, n) = 1$

г) Если $\text{НОД}(a, n) > 1$

5. Поставьте в соответствие двоичной последовательности 11001101 элемент поля Галуа $\text{GF}(2^8)$, в виде которого можно представить данную последовательность для проведения над ней криптографических преобразований.

а) $x^8 + x^7 + x^4 + x^3 + x$

б) $x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$

в) $x^7 + x^6 + x^3 + x^2 + 1$

г) $x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$

6. Чем шифр «Магма» отличается от шифра, определенного в стандарте ГОСТ 28147-89?

а) Длиной ключа

б) Это два принципиально разных симметричных блочных шифра

в) Невозможностью использования произвольной таблицы замен

г) Количеством раундов

7. Какова длина секретного ключа в шифре «Кузнечик»?

а) 64 бита

б) 128 бит

в) 256 бит

г) 512 бит

8. Какой из режимов работы симметричных блочных шифров не предназначен для обеспечения конфиденциальности информации?

а) Режим простой замены

б) Режим простой замены с сцеплением

в) Режим выработки имитовставки

г) Режим гаммирования

9. В каком из режимов работы симметричных блочных шифров результат зашифрования очередного блока открытого текста при фиксированном ключе зависит только от порядкового номера данного блока?

а) Режим простой замены

б) Режим гаммирования с обратной связью по выходу

в) Режим гаммирования

г) Режим гаммирования с обратной связью по шифртексту

10. Какой из перечисленных шифров относится к классу асимметричных шифров?

а) Магма

б) Кузнечик

в) RSA

г) AES

Примерные вопросы к экзамену

1. Алгебраические структуры. Свойства алгебраических структур. Группы, подгруппы.
2. Циклические группы.
3. Кольца. Кольца классов вычетов.
4. Поля. Поля Галуа.
5. Цели и задачи криптографии. Основные понятия.
6. Простейшие шифры: простой замены, перестановочный, аффинный.
7. Шифр Хилла.
8. Генерация простых чисел.
9. Шифры гаммирования. Шифр Вернама (одноразовый блокнот).
10. ГОСТ Р 34.12-2015. Шифр «Магма».
11. ГОСТ Р 34.12-2015. Шифр «Кузнечик».
12. Генерация псевдослучайных последовательностей и их тесты.
13. Поточное шифрование.
14. Стандарт шифрования DES.
15. Стандарт шифрования AES.
16. Криптография с открытым ключом.
17. Ранцевая криптосистема.
18. Криптосистема RSA.
19. Криптосистема Эль-Гамала.
20. Протокол Диффи-Хеллмана.
21. Алгоритмы работы с большими числами.
22. Хеш-функции. Свойства хеш-функций.
23. Коды аутентичности сообщений. Электронная подпись.
24. ГОСТ Р 34.10-2012.
25. Протокол передачи бита.
26. Слепые подписи.
27. Протоколы доказательств знания с нулевым разглашением.
28. Протоколы электронного голосования.
29. 29. Протоколы безопасных вычислений.

8. Система оценивания планируемых результатов обучения

Критерии оценивания

Оценка «отлично» выставляется студенту, глубоко и прочно усвоившему программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающему, в ответе которого увязывается теория с практикой, он показывает знакомство с литературой, правильно обосновывает и использует рациональные и современные средства решения поставленной проблемы.

Оценка «хорошо» выставляется студенту, твердо знающему программный материал, грамотно и по существу, излагающему его, который не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении поставленной задачи.

Оценка «удовлетворительно» выставляется студенту, который знает только основной программный материал, но не усвоил особенностей, допускает в ответе неточности, некорректно формулирует основные законы и правила, затрудняется в выполнении практических задач.

Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает в ответе существенные ошибки, с затруднениями выполняет практические задания.

Форма контроля	За одну работу		Всего	
	Мин. баллов	Макс. баллов	Мин. баллов	Макс. баллов
Текущий контроль:				
Активная работа на занятии	0,25	0,5	9	18
Выполнение домашнего задания	0,75	0,75	27	27
Выполнение заданий самостоятельной работы	1	3	1	3
коллоквиум	1	3	3	9
Промежуточная аттестация (экзамен)			20	43
Итого за семестр			60	100

9. Учебно-методическое и информационное обеспечение дисциплины

9.1. Основная литература

1. . Рябко, Б.Я. Основы современной криптографии и стеганографии [Электронный ресурс]: монография / Б.Я. Рябко, А.Н. Фионов. — Москва: Горячая линия Телеком, 2021. — 232 с. [Электронный ресурс]: — Режим доступа: <https://e.lanbook.com/book/111098>
2. Евсютин О.О. Криптографические методы защиты информации: методические указания для выполнения практических и самостоятельных работ: [Электронный ресурс]: — Режим доступа: <https://cloud.fb.tusur.ru/index.php/s/SeR4X5Db8nfK5QY>.
1. Панкратьев, Е. В. Введение в компьютерную алгебру : учебное пособие / Е. В. Панкратьев. — 4-е изд. — Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2023. — 324 с. — ISBN 978-5-4497-1639-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/120475.html>
2. Ряднов, А. В. Алгебраические системы. Кольца и поля : учебно-методическое пособие / А. В. Ряднов, Т. В. Меренкова, М. Е. Булатникова. — Москва : Российский университет транспорта (МИИТ), 2022. — 56 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/122047.html>
3. Ряднов, А. В. Алгебраические системы. Кольца и поля : учебно-методическое пособие / А. В. Ряднов, Т. В. Меренкова, М. Е. Булатникова. — Москва : Российский университет транспорта (МИИТ), 2021. — 56 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/122047.html>

9.2. Дополнительная литература

1. Основы криптографии: учебное пособие для вузов / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. — 3-е изд., испр. и доп. — М.: Гелиос АРВ, 2017. — 479 [1] с.
2. Основы современной криптографии: учебный курс / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. — 2-е изд., перераб. и доп. — М.: Горячая линия-Телеком, 2022. — 176 с.
3. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2022. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [Электронный ресурс]: — Режим доступа: <https://urait.ru/bcode/489919>
4. Зюзьков В.М. Компьютерная алгебра. – Томск: Изд-во Томского ун-та, 2014. - 121 с. http://www.math.tsu.ru/sites/default/files/mmf2/e-resources/Computer_algebra_Zyuzkov.pdf
5. Седов Е. Основы работы в системе компьютерной алгебры Mathematica. [Электронный ресурс]. – URL: <http://www.intuit.ru/studies/courses/4765/1039/info>

6. . Wolfram Mathematica. Русскоязычная поддержка. [Электронный ресурс]. – URL: <http://www.wolframmathematica.ru/>
7. Основы работы в системе компьютерной алгебры Mathematica: <http://www.intuit.ru/studies/courses/4765/1039/info>

9.3. Программное обеспечение

1. Microsoft Office 2010 Russian Academic OPEN 1 License (бессрочная), (лицензия 49512935);
2. Microsoft Sys Ctr Standard Sngl License/Software Assurance Pack Academic License 2 PROC (бессрочная), (лицензия 60465661)
3. Microsoft Win Home Basic 7 Russian Academic OPEN (бессрочная), (лицензия 61031351),
4. Microsoft Office 2010 Russian Academic OPEN, (бессрочная) (лицензия 61031351),
5. Microsoft Windows Proffesional 8 Russian Upgrade Academic OPEN (бессрочная), (лицензия 61031351),
6. Microsoft Internet Security&Accel Server Standart Ed 2006 English Academic OPEN, (бессрочная), (лицензия 41684549),
7. Microsoft Office Professional Plus 2010 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
8. Microsoft Windows Server CAL 2008 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
9. Microsoft Windows 10 Pro, 64 bit, Rus, OEM, Операционная система
10. Неисключительное право на использование ПО Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition.
11. Неисключительное право на использование ПО Kaspersky Security для виртуальных и облачных сред, Server, VirtSvr, License, Education Renewal
12. ABBYYFineReader 11 Professional Edition, (бессрочная), (лицензия AF11-2S1P01-102/AD),
13. Microsoft Volume Licensing Service, (бессрочная), (лицензия 62824441),
14. Microsoft Windows Pro 64bit DOEM, (бессрочная), контракт № 6-ОАЭФ2014 от 05.08.2014
15. Visual Studio Professional
16. «Антиплагиат. ВУЗ». Лицензионный договор № 5044 от 14.05. 2022 года (ежегодное продление).
17. Учебно-методический комплекс «Информационная безопасность» на 20 учебных мест;
18. Учебно-методический комплекс «Безопасность телекоммуникационных систем» на 20 учебных мест.

9.4. Профессиональные базы данных и информационные справочные системы современных информационных технологий

1. Информационная система «Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии» (<https://habr.com/>)
2. Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки- (<https://github.com/>)
3. База книг и публикаций Электронной библиотеки "Наука и Техника" (<http://www.n-t.ru>)
4. Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии (http://window.edu.ru/catalog/?p_rubr=2.2.75.6)
5. Электронная библиотечная система ZNANIUM.COM (<http://znanium.com/>)
6. Цифровая коллекция электронных версий изданий (учебники, учебные пособия, учебно-методические документы, монографии) по экономическим, естественным, техническим и гуманитарным наукам, сгруппированных по тематическим и целевым признакам.
7. Электронная библиотечная система «BOOK.ru» издательства «КноРус медиа» (<https://www.book.ru/>)
8. Интернет-университет информационных технологий (www.intuit.ru)
9. Онлайн среда разработки приложений (ideone.com)
10. Журнал «КомпьютерПресс» (www.compress.ru)

11. Издательство «Открытые системы» (www.osp.ru)
12. Издание о высоких технологиях (www.cnews.ru)
13. Справочно-правовая система «Консультант Плюс» (<http://www.consultant.ru>)
14. Polpred.com Обзор СМИ (<http://polpred.com/>)
15. Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru>)
16. Электронная библиотечная система IPRbooks (<http://www.iprbookshop.ru>)
17. Электронная библиотечная система Национальная электронная библиотека (<https://нэб.рф>)
18. Электронная библиотечная система Юрайт (<http://www.biblio-online.ru>)
19. <https://lib.tusur.ru/ru/resursy/bazy-dannyh>.

10. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

Учебные и учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

Для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

Для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

Для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

Для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

для слепых и слабовидящих:

- автоматизированным рабочим местом для людей с нарушением зрения;
- при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

для глухих и слабослышащих:

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;

для обучающихся с нарушениями опорно-двигательного аппарата:

- передвижными, регулируемые эргономическими партами СИ-1;
- компьютерной техникой со специальным программным обеспечением.

11. Материально-техническое обеспечение дисциплины (модуля)

Для преподавания и изучения дисциплины используется лекционная аудитория, обеспеченная мультимедиа проектором и сопутствующим оборудованием, интерактивной доской. Используются УМК дисциплины (на бумажном и электронном носителях), фонд научной библиотеки университета, методические и учебно-методические материалы кафедры информатики.

К рабочей программе прилагаются:

Приложение 1 – Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине (модулю);

Приложение 2 – Методические указания для обучающихся по освоению дисциплины (модуля).