

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Набережночелнинский институт (филиал)
Отделение информационных технологий и энергетических систем



УТВЕРЖДАЮ

Заместитель директора
по образовательной деятельности
НЧИ КФУ

Ахметов Н.Д.

"__" _____ 20__ г.

Программа дисциплины

Методы защиты информации

Направление подготовки: 01.03.02 - Прикладная математика и информатика

Профиль подготовки:

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2019

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО
2. Место дисциплины (модуля) в структуре ОПОП ВО
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся
4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий
 - 4.1. Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)
 - 4.2. Содержание дисциплины (модуля)
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)
6. Фонд оценочных средств по дисциплине (модулю)
 - 6.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы и форм контроля их освоения
 - 6.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания
 - 6.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы
- 6.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций
7. Перечень литературы, необходимой для освоения дисциплины (модуля)
8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)
9. Методические указания для обучающихся по освоению дисциплины (модуля)
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)
11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)
12. Средства адаптации преподавания дисциплины (модуля) к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья
13. Приложение №1. Фонд оценочных средств
14. Приложение №2. Перечень литературы, необходимой для освоения дисциплины (модуля)
15. Приложение №3. Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Программу дисциплины разработал(а)(и) Товштейн М.Я.

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО

Обучающийся, освоивший дисциплину (модуль), должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-4	Способен к разработке требований и проектированию программного обеспечения
ПК-6	Способен к обеспечению информационной безопасности на уровне баз данных

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

Должен уметь:

Должен владеть:

Должен демонстрировать способность и готовность:

В результате изучения дисциплины бакалавр должен:

ЗНАТЬ ♦

- требования к программному обеспечению защиты конфиденциальных данных,
- принципы организационной, технической и программной защиты данных, позволяющие обеспечить информационную безопасность на уровне баз данных , ♦

УМЕТЬ ♦

- ориентироваться в правовых, административно-организационных и технических средствах защиты информации с учётом требований к проектированию программного обеспечения,
- использовать программные средства, обеспечивающие информационную безопасность на уровне баз данных

ИМЕТЬ НАВЫКИ ♦

- использования криптографических методов, обеспечивающих информационную безопасность на уровне баз данных,
- разработки системы защиты информации, ♦
- применения полученных умений и знаний для проектирования программного обеспечения защиты данных

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.12 Дисциплины (модули)" основной профессиональной образовательной программы 01.03.02 "Прикладная математика и информатика ()" и относится к вариативной части.

Осваивается на 4 курсе в 8 семестре.

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) на 108 часа(ов).

Контактная работа - 50 часа(ов), в том числе лекции - 20 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 30 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 58 часа(ов).

Контроль (зачёт / экзамен) - 0 часа(ов).

Форма промежуточного контроля дисциплины: зачет в 8 семестре.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Информация как объект защиты	8	2	0	0	4
2.	Тема 2. Правовые средства защиты информации от несанкционированного доступа	8	2	0	2	8
3.	Тема 3. Угрозы информационной безопасности	8	2	0	4	2
4.	Тема 4. Административно-организационные средства защиты информации.	8	2	0	2	2
5.	Тема 5. Криптографические симметричные методы защиты информации	8	2	0	10	18
6.	Тема 6. Технические аспекты обеспечения защиты информации.	8	4	0	2	4
7.	Тема 7. Криптографические асимметричные методы защиты информации,	8	6	0	10	20
	Итого		20	0	30	58

4.2 Содержание дисциплины (модуля)

Тема 1. Информация как объект защиты

Различные определения понятия "информация": философские, техноцентрические, антропоцентрические. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 6 июля 2016 г. Основные понятия, используемые в Федеральном законе: информация, информационные технологии, информационная система, информационно-телекоммуникационная сеть, обладатель информации, доступ к информации и её конфиденциальность, предоставление информации.

Тема 2. Правовые средства защиты информации от несанкционированного доступа

Информационная безопасность - это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Защита информации - это комплекс мероприятий, направленных на обеспечение информационной безопасности. Задачи государства в сфере защиты информации

Виды государственных нормативных актов по защите информации. Информация как объект правовых отношений.

Лабораторная работа: Поиск в системе "Консультант Плюс" правовых документов и создание презентаций.

Тема 3. Угрозы информационной безопасности

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность. Атака - попытка реализации угрозы. Злоумышленник - реализатор атаки. Потенциальные злоумышленники как источники угрозы. Классификация средств защиты информации.

Угрозы информационным ресурсам предприятия.

Роль морально-этических средств защиты информации.

Лабораторная работа Разработка должностной инструкции инженера по защите информации

Тема 4. Административно-организационные средства защиты информации.

Организационные меры защиты информации: Организационные меры охраны конфиденциальных сведений на предприятиях малого бизнеса. Регламентация процессов функционирования систем, деятельность персонала по обеспечению безопасности.

Меры, осуществляемые при проектировании, строительстве и оборудовании объектов обработки данных, а также мероприятия при подборе и постановки персонала, обслуживающего систему, организация охраны и режима допуска к системе.

Организация учёта, хранения, использования и уничтожение документов и носителя информации.

Организация разграничения доступа.

Лабораторная работа Разработка презентации по документу ОАО КАМАЗ "Об организации работы по защите информации, составляющей коммерческую тайну"

Тема 5. Криптографические симметричные методы защиты информации

Криптография - это использование математических и программно-аппаратных методов для надежной защиты данных от несанкционированного доступа. Некоторые методы криптографического закрытия симметричным ключом:

-- подстановка, или замена (каждый символ исходного текста заменяется на один или несколько символов из того же или другого алфавита),

-- простая перестановка (запись сообщения по столбцам с переводом в шифротекст по строкам в один набор символов),

-- вертикальная перестановка (в первую строку по символам вписывается заданный ключ, столбцы переставляются по алфавитному порядку символов первой строки),

-- двойная перестановка (к вертикальной перестановке добавляют вертикальный столбец слева для строк и сортируют строки)

-- гаммирование (сложения сообщения с данным ключом-гаммой и вычисление остатка от деления на размерность алфавита)

-- матричная алгебра как пример применения аналитического преобразования

Лабораторные работы. Криптозащита сообщений методами шифрования симметричным ключом.

Тема 6. Технические аспекты обеспечения защиты информации.

Понятия идентификации и аутентификации. Идентификация - присвоение субъектам или объектам доступа некоторого идентификатора (метки, пароля).

Аутентификация - проверка, принадлежит ли предъявленный субъектом идентификатор этому субъекту.

Принципы аутентификации: а) пользователь знает, б) пользователь имеет,

в) пользователь есть.

Возможности нарушителя и средства защиты. Каналы утечки информации. Краткие сведения о средствах съёма и защиты информации. Защита ЭВМ и электронных носителей информации

Тема 7. Криптографические асимметричные методы защиты информации,

Применение асимметричного шифрования в обмене сообщениями. В отличие от симметричного шифрования здесь используются два ключа каждым из участников связи. Один называется открытым, так как он сообщается всем партнерам, второй ключ хранится в тайне и называется секретным, или закрытым.

Протоколы защиты канала связи. Применение сеансового ключа. Электронная цифровая подпись, сопоставление её с рукописной, методика применения.

Понятие о дайджесте сообщения и о хэш-функции.

Дайджест сообщения - это уникальная последовательность символов, однозначно соответствующая содержанию сообщения. Дайджест имеет фиксированный размер, который зависит от длины самого сообщения. Он вставляется в электронную подпись вместе со сведениями об авторе и шифруется вместе с ними.

Дайджест обеспечивает однозначное соответствие между сообщением и сжатым его эквивалентом.

Лабораторные работы. Защита сообщений методом асимметричного шифрования.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства образования и науки Российской Федерации от 5 апреля 2017 года №301)

Письмо Министерства образования Российской Федерации №14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Устав федерального государственного автономного образовательного учреждения "Казанский (Приволжский) федеральный университет"

Правила внутреннего распорядка федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"

Локальные нормативные акты Казанского (Приволжского) федерального университета

6. Фонд оценочных средств по дисциплине (модулю)

6.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы и форм контроля их освоения

Этап	Форма контроля	Оцениваемые компетенции	Темы (разделы) дисциплины
Семестр 8			
	Текущий контроль		
1	Письменная работа	ПК-4	1. Информация как объект защиты 2. Правовые средства защиты информации от несанкционированного доступа 3. Угрозы информационной безопасности 4. Административно-организационные средства защиты информации.
2	Отчет	ПК-6	5. Криптографические симметричные методы защиты информации 6. Технические аспекты обеспечения защиты информации.
3	Проверка практических навыков	ПК-4, ПК-6	7. Криптографические асимметричные методы защиты информации,
	Зачет	ПК-4, ПК-6	

6.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Форма контроля	Критерии оценивания				Этап
	Отлично	Хорошо	Удовл.	Неуд.	
Семестр 8					
Текущий контроль					
Письменная работа	Правильно выполнены все задания. Продемонстрирован высокий уровень владения материалом. Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий.	Правильно выполнена большая часть заданий. Присутствуют незначительные ошибки. Продемонстрирован хороший уровень владения материалом. Проявлены средние способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены более чем наполовину. Присутствуют серьезные ошибки. Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных заданий.	Задания выполнены менее чем наполовину. Продемонстрирован неудовлетворительный уровень владения материалом. Проявлены недостаточные способности применять знания и умения к выполнению конкретных заданий.	1
Отчет	Продемонстрирован высокий уровень владения материалом. Используются надлежащие источники в нужном количестве. Структура работы и примененные методы соответствуют поставленным задачам.	Продемонстрирован средний уровень владения материалом. Используются надлежащие источники. Структура работы и примененные методы в основном соответствуют поставленным задачам.	Продемонстрирован удовлетворительный уровень владения материалом. Используются источники, структура работы и примененные методы частично соответствуют поставленным задачам.	Продемонстрирован неудовлетворительный уровень владения материалом. Используются источники, структура работы и примененные методы не соответствуют поставленным задачам.	2

Форма контроля	Критерии оценивания				Этап
	Отлично	Хорошо	Удовл.	Неуд.	
Проверка практических навыков	Продemonстрирован высокий уровень освоения навыков, достаточный для успешного решения задач профессиональной деятельности.	Продemonстрирован хороший уровень освоения навыков, достаточный для решения большей части задач профессиональной деятельности.	Продemonстрирован удовлетворительный уровень освоения навыков, достаточный для решения отдельных задач профессиональной деятельности.	Продemonстрирован неудовлетворительный уровень освоения навыков, недостаточный для решения задач профессиональной деятельности.	3
	Зачтено		Не зачтено		
Зачет	Обучающийся обнаружил знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности, справился с выполнением заданий, предусмотренных программой дисциплины.		Обучающийся обнаружил значительные пробелы в знаниях основного учебно-программного материала, допустил принципиальные ошибки в выполнении предусмотренных программой заданий и не способен продолжить обучение или приступить по окончании университета к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.		

6.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Семестр 8

Текущий контроль

1. Письменная работа

Темы 1, 2, 3, 4

1. Какие три группы угроз информации и какие меры противодействия угрозам вам известны?
2. Какие отношения регулирует ФЗ "Об информации, информационных технологиях и о защите информации" от 6 июля 2016 г.? Как определяются понятия 'Информационная система', 'Информационные технологии', 'Обладатель информации', 'Конфиденциальность информации' ?
3. На какую информацию не может быть ограничен доступ и какие способы несанкционированного доступа вам известны?
4. Какие условия способствуют и приводят к неправомерному овладению конфиденциальной информацией?
5. Каким воздействиям может быть подвергнута информация?
6. Какими принципами следует руководствоваться при организации защиты информации?
7. Какие виды 'тайн' и какими законами они защищаются ?
8. Какие государственной тайны устанавливает ФЗ 'О государственной тайне' от 21 июля 1993 года N 5486-1 ?
9. Как определяется коммерческая тайна в ФЗ 'О коммерческой тайне' №98 от 2004 г. и что относится к информации, составляющую коммерческую тайну?
10. Какие организационные меры должны предусматриваться на предприятии для защиты конфиденциальности информации?
11. Какую ответственность устанавливают статьи Уголовного кодекса РФ за правонарушения в информационной сфере?
12. Что такое идентификация и аутентификация и какие принципы аутентификации вам известны?

Оценивание : 1 балл за развернутый ответ на один вопрос.

Пусть K - количество баллов. Тогда: $K \leq 4 \rightarrow$ НЕУД, $5 \leq K \leq 7 \rightarrow$ УДОВ, $8 \leq K \leq 10 \rightarrow$ ХОР, $11 \leq K \leq 12 \rightarrow$ ОТЛ. Всего 12 баллов.

Знание правовых и административно-организационных средств защиты информации от НСД позволяет оценить способность бакалавра к разработке требований и проектированию программного обеспечения ♦

2. Отчет

Темы 5, 6

ВОПРОСЫ, НА КОТОРЫЕ НАДО ОТВЕТИТЬ В ОТЧЁТАХ ПО ЛАБОРАТОРНЫМ РАБОТАМ

РАБОТА ♦ 1 ШИФРЫ АТБАШ И ПОЛИБИЯ

1. Что такое моноалфавитная замена?
2. Что называется ключом шифрования?
3. Каков протокол шифрования симметричным ключом?
4. Какой недостаток шифрования симметричным ключом?
5. Почему шифр получил такое название?
6. Почему шифр атбаш является шифром замены?

7. Как действуют Алиса и Боб при использовании шифра атбаш?
8. Почему шифр Полибия является примером шифрования простой подстановкой?
9. Что является ключом шифра Полибия?
10. Как действуют Алиса и Боб при использовании разных способов шифра Полибия?

РАБОТА ♦ 2. ШИФРЫ ТРИТЕМИЯ и ЦИФРОВОЙ

1. Почему шифр Тритемия является развитием шифра Полибия?
2. Как выполнить шифрование и расшифрование сообщения методом Тритемия?
3. Будет ли цифровой шифр шифром простой подстановки?
4. Какой эффект даст добавление пароля в таблицу, содержащую ключ для цифрового шифра?
5. Как выполнять шифрование и расшифрование сообщения цифровым шифром?
6. Что можно сделать для облегчения запоминания таблицы, в которой буквы алфавита размещены не по порядку?

РАБОТА ♦ 3. ШИФРЫ МНОГОАЛФАВИТНОЙ ПОДСТАНОВКИ

1. В чём преимущество многоалфавитной подстановки перед моноалфавитной подстановкой?
2. В чём сходство шифра Виженера с шифром Гронсфельда?
3. Что является ключом шифра Виженера?
4. Что такое шифр перестановки
5. В чём преимущество вертикальной перестановки перед простой перестановкой?
6. Что является ключом шифра вертикальной перестановки?
7. В чём преимущество шифров перестановки перед шифрами подстановки?
8. Что является ключом шифра простой перестановки?
9. Почему считается реализуемым шифром простой перестановки?

РАБОТА ♦ 4 ШИФРОВАНИЕ ГАММИРОВАНИЕМ

1. Что такое гаммирование?
2. В чём преимущество метода гаммирования перед другими методами шифрования?
3. Что является ключом при использовании данного метода ?
4. По каким формулам выполняется гаммирование?
5. Почему гаммирование является частным случаем многоалфавитной замены?
6. Как выполняется гаммирование при компьютерной обработке сообщений?
7. Как избежать повторения пароля для "покрытия" исходного сообщения?

РАБОТА ♦ 5 ШИФРОВАНИЕ АНАЛИТИЧЕСКИМ МЕТОДОМ

1. В чём суть аналитического метода шифрования?
2. В чём преимущество этого метода перед другими методами шифрования?
3. Что является ключом при использовании данного метода ?
4. По каким формулам выполняется данный метод?
5. Как задаётся ключ шифрования и сообщение, которое надо закрыть?
6. В чём удобство применения MS Excel для реализации аналитического метода шифрования?

Оценка отчётов: работа 1 - 2 балла, работа 2 - 2 балла, работа 3 - 4 балла, работа 4 - 5 баллов, работа 5 - 5 баллов. Всего - 18 баллов.

Работа над выполнением заданий и составление отчётов позволяет оценить способность бакалавра к обеспечению информационной безопасности на уровне баз данных.

3. Проверка практических навыков

Тема 7

ТЕМА: "ЗАЩИТА СООБЩЕНИЙ АСИММЕТРИЧНЫМИ МЕТОДАМИ ШИФРОВАНИЯ"

Дисциплина: "Методы защиты информации"

Выполнил студент Хххххххх И.О.,

группа 21711хх курс Х

Научный руководитель доцент, к.ф.-м.н. Товштейн М.Я. _____

подпись

Оценка _____

Дата "____" _____ 20__ ♦

СОДЕРЖАНИЕ

- 1) Задание ♦ 1. Проверка протокола обмена сообщениями при асимметричном шифровании (шок) _____
- 2) Задание ♦ 2. Создание защищённого канала связи при использовании симметричного шифрования сеансовым ключом ?..... _____
- 3) Задание ♦ 3. Аутентификация сообщения с помощью электронной цифровой подписи ?..... _____
- 4) Задание ♦ 4. Создание дайджеста и хеш-кода сообщения для повышения скорости передачи сообщений ?..... ?..... _____
- 5) Задание ♦ 5. Проверка протокола обмена сообщениями с дайджестом _____

Изучить методы шифрования асимметричным ключом, изложенные в брошюре СООБЩЕНИЕ ШИФРУЕМ АСИММЕТРИЧНО (см. файл <https://clck.ru/N3GdV>).

1..Получить открытые ключи для роли Алисы (Отправителя) и Боба (Получателя). (раздел ФАЙЛЫ <https://clck.ru/N3GQC>)

2..Получить закрытые ключи, отправленные каждому из вас по почте ,

3..Выполнить задания по использованию асимметричного шифрования

4.. Оформить отчёт в соответствии с данным образцом.

ОБРАЗЕЦ

◆ЗАДАНИЕ ◆ 1

ПРОВЕРКА ПРОТОКОЛА ОБМЕНА СООБЩЕНИЯМИ ПРИ АСИММЕТРИЧНОМ ШИФРОВАНИИ (ШОК)

1. Краткие теоретические сведения

2. ПРИМЕР. Позиция АЛИСЫ (фамилия) , направляемое Бобу (фамилия)

- сообщение, которое будет зашифровано

- ключи Алисы (Открытый и Закрытый) , ключ Боба - Открытый

- листинг (описание шифрования)

- шифротекст, адресованный Бобу

3. ПРИМЕР Позиция БОБА (автора отчёта), расшифровывающего сообщение Алисы (фамилия)

- шифротекст Алисы,

- ключи Боба (Открытый и Закрытый) , ключ Алисы - Открытый,

-листинг,

- раскрытое сообщение Алисы

4. Используемые источники

4.1.Товштейн М.Я. Сообщение шифруем асимметрично / М.Я. Товштейн; Набережночелнинский институт Казанского (Приволжского) федерального ун-та. ? рукопись , раздел. 1.2)

4.2. другие источники ?..

ЗАДАНИЕ ◆ 2

СОЗДАНИЕ ЗАЩИЩЁННОГО КАНАЛА СВЯЗИ ПРИ ИСПОЛЬЗОВАНИИ СИММЕТРИЧНОГО ШИФРОВАНИЯ СЕАНСОВЫМ КЛЮЧОМ

Пояснения:

а) Пункты те же, что и в задании ◆ 1

б) В качестве сеансового ключа используйте двоичный ключ для гаммирования симметричного шифрования, применённый в предыдущем цикле работ

в) В Используемых источниках указать раздел 1.3 той же брошюры, что и в задании ◆ 1

ЗАДАНИЕ ◆ 3

АУТЕНТИФИКАЦИЯ СООБЩЕНИЯ С ПОМОЩЬЮ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Пояснения:

а) пункты те же, что и в задании ◆ 1

б) В Используемых источниках указать раздел 2 той же брошюры, что и в задании ◆ 1

ЗАДАНИЕ ◆ 4

СОЗДАНИЕ ДАЙДЖЕСТА И ХЕШ-КОДА СООБЩЕНИЯ ДЛЯ ПОВЫШЕНИЯ СКОРОСТИ ПЕРЕДАЧИ СООБЩЕНИЙ

1. Краткие теоретические сведения

2. ПРИМЕР. Позиция Алисы:

а) создать сообщение из 3-х букв и одной цифрой в конце(например, 5);

б) параметры хеш-кода р и q задать простыми числами (меньшими 100 и не 17 и 19, как в брошюре);

в) проверить замечание к примеру п.3.1 про изменение дайджеста из-за изменения одного байта цифры в сообщении(например, исправить 5 на 6)

Пояснение. В Используемых источниках указать раздел 3.1 той же брошюры, что и в лаб.1

ЗАДАНИЕ ◆ 5

ПРОВЕРКА ПРОТОКОЛА ОБМЕНА СООБЩЕНИЯМИ С ДАЙДЖЕСТОМ

Пояснения:

а) пункты те же, что и в задании ◆ 1

б) В Примере используются те же данные, что и в задании ◆ 4. Не забыть использовать ЭЦП для защиты дайджеста

в) В Используемых источниках указать раздел 3.2 той же брошюры, что и в задании ◆ 1

Оценка: задание 1 - 2 балла, задание 2 - 3 балла , задание 3 - 4 балла, задание 4 - 5 баллов, задание 5 - 6 баллов.

Всего - 20 баллов.

Работа над выполнением заданий позволяет оценить не только способность бакалавра к разработке требований и проектированию программного обеспечения, но и к обеспечению информационной безопасности на уровне баз данных.

Зачет

Вопросы к зачету:

1. Понятие информации, различные определения: философские, техноцентрические, антропоцентрические. Определение, данное в ФЗ "Об информации, информационных технологиях и о защите информации"
2. Определение понятия "информация" с точки зрения физиков, кибернетиков, "технарей", философов.
3. Юридические свойства информации.
4. Принципы правового регулирования отношений в информационной сфере. Отношения, регулируемые данным законом "Об информации, информационных технологиях и о защите информации" .
5. Определение понятия "защита информации", цель защиты информации.
6. Определение понятия 'владелец' и 'пользователь информации'. Права владельца и пользователя информации.
7. Сопоставление понятий "информация документированная" и "общедоступная информация".
8. Определение "права на доступ к информации". На какую информацию не может быть ограничен доступ?
9. Правовые меры защиты информации.
10. Морально-этические меры защиты информации
11. Организационные меры защиты информации
12. Физические и технические меры защиты информации
13. Несанкционированный доступ (НСД) к информации.
14. Условия, способствующие неправомерному овладению конфиденциальной информацией..
15. Действия, приводящие к неправомерному овладению конфиденциальной информацией
16. Воздействия, которым может быть подвернута информация.
17. Характеристика групп угроз информации.
18. Источники и следствия реализации угроз информации.
19. Меры противодействия угрозам, их характеристики, примеры.
20. Принципы, которыми следует руководствоваться при организации защиты информации.
21. Идентификация и аутентификация. Принципы аутентификации..
22. Средства физической защиты объектов, требования к инженерным и техническим средствам охраны помещений, предназначенных для работы с конфиденциальной информацией.
23. Сведения, относящиеся к конфиденциальной информации.
24. Виды "тайн", защищаемые законами РФ.
25. Три степени государственной тайны, установленные ФЗ "О государственной тайне".
26. Определение коммерческой тайны в ФЗ "О коммерческой тайне". Информация, составляющая коммерческую тайну.
27. Организационные меры, предпринимаемые работодателем для защиты конфиденциальной информации.
28. Отличие симметричных от асимметричных методов криптографической защиты информации. Что понимается под ключом шифрования? Приведите примеры симметричных методов шифрования.
29. Недостатки симметричных методов шифрования и их устранение асимметричными методами. Расскажите об асимметричном методе шифрования.
30. Реализация идентификации и аутентификации в социальных и компьютерных системах.
31. Сочетание метода гаммирования с асимметричным методом шифрования для защиты канала связи между корреспондентами.
32. Достоинства и недостатки ручной подписи. Как ЭЦП борется с недостатками ручной подписи?
33. Концепция дайджеста (слепка, контрольной суммы) сообщения. Роль дайджеста в защите информации.
34. Хеш-функция, реализующая дайджест сообщения. Алгоритм её реализации.

6.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

В КФУ действует балльно-рейтинговая система оценки знаний обучающихся. Суммарно по дисциплине (модулю) можно получить максимум 100 баллов за семестр, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов.

Для зачёта:

56 баллов и более - "зачтено".

55 баллов и менее - "не зачтено".

Для экзамена:

86 баллов и более - "отлично".

71-85 баллов - "хорошо".

56-70 баллов - "удовлетворительно".

55 баллов и менее - "неудовлетворительно".

Форма контроля	Процедура оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций	Этап	Количество баллов
Семестр 8			
Текущий контроль			
Письменная работа	Обучающиеся получают задание по освещению определённых теоретических вопросов или решению задач. Работа выполняется письменно и сдаётся преподавателю. Оцениваются владение материалом по теме работы, аналитические способности, владение методами, умения и навыки, необходимые для выполнения заданий.	1	12
Отчет	Обучающийся пишет отчёт, в котором отражает выполнение им, в соответствии с полученным заданием, определённых видов работ, нацеленных на формирование профессиональных умений и навыков. Оцениваются достигнутые результаты, проявленные знания, умения и навыки, а также соответствие отчёта предъявляемым требованиям.	2	18
Проверка практических навыков	Практические навыки проверяются путём выполнения обучающимися практических заданий в условиях, полностью или частично приближенных к условиям профессиональной деятельности. Проверяется знание теоретического материала, необходимое для правильного совершения необходимых действий, умение выстроить последовательность действий, практическое владение приёмами и методами решения профессиональных задач.	3	20
Зачет	Зачёт нацелен на комплексную проверку освоения дисциплины. Обучающийся получает вопрос (вопросы) либо задание (задания) и время на подготовку. Зачёт проводится в устной, письменной или компьютерной форме. Оценивается владение материалом, его системное освоение, способность применять нужные знания, навыки и умения при анализе проблемных ситуаций и решении практических заданий.		50

7. Перечень литературы, необходимой для освоения дисциплины (модуля)

Освоение дисциплины (модуля) предполагает изучение основной и дополнительной учебной литературы. Литература может быть доступна обучающимся в одном из двух вариантов (либо в обоих из них):

- в электронном виде - через электронные библиотечные системы на основании заключенных КФУ договоров с правообладателями;

- в печатном виде - в Научной библиотеке им. Н.И. Лобачевского. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования Научной библиотекой.

Электронные издания доступны дистанционно из любой точки при введении обучающимся своего логина и пароля от личного кабинета в системе "Электронный университет". При использовании печатных изданий библиотечный фонд должен быть укомплектован ими из расчета не менее 0,5 экземпляра (для обучающихся по ФГОС 3++ - не менее 0,25 экземпляра) каждого из изданий основной литературы и не менее 0,25 экземпляра дополнительной литературы на каждого обучающегося из числа лиц, одновременно осваивающих данную дисциплину.

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля), находится в Приложении 2 к рабочей программе дисциплины. Он подлежит обновлению при изменении условий договоров КФУ с правообладателями электронных изданий и при изменении комплектования фондов Научной библиотеки КФУ.

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Нестеров С.А. Основы информационной безопасности: учебное пособие Учебное пособие. ? 5-е изд. - СПб.: Издательство ?Лань?, 2019. - 324 стр. - <https://e.lanbook.com/reader/book/114688>

Петренко В.И., Мандрица И.В. Защита персональных данных в информационных системах Практикум : Учебное пособие. ? СПб.: Издательство ?Лань?, 2019. - 108 стр. - <https://e.lanbook.com/reader/book/111916/#100>

Прохорова О. В. Информационная безопасность и защита информации : учебник/ О.В. Прохорова. ? 2-е изд. - СПб.: Издательство ?Лань?, 2019. - 124 стр. - <https://e.lanbook.com/reader/book/133924>

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид работ	Методические рекомендации
лекции	<p>Слушая лекции, необходимо уяснить цель, которую лектор ставит перед вами. Обычно он обозначает цель лекции, показывая название и план лекции. Важно внимательно слушать, отмечать наиболее существенную информацию и кратко записывать ее в тетрадь. Сравнить то, что услышано на лекции, с прочитанным и усвоенным ранее, укладывать новую информацию в собственную, уже имеющуюся, систему знаний. По ходу лекции важно подчеркивать новые термины, устанавливать их взаимосвязь с изученными ранее понятиями.</p> <p>Необходимо тщательно вслед за лектором делать записи. Если на лекции вы не получили ответа на возникшие вопросы, разрешается сразу же или в конце лекции задать их лектору. Если лектор задаёт вопросы, желательно не отмахиваться, а отвечать на них. И внимательно слушать ответы товарищей.</p>
лабораторные работы	<p>При подготовке к лабораторной работе необходимо прочитать записанную лекцию, обращая внимание на наиболее важные моменты, прочитать рекомендованный материал из учебно-методической литературы.</p> <p>Лабораторные занятия проводятся с использованием активных методов: работа в малых группах (бригадах), обсуждение проблем заказчика при анализе предметной области.</p> <p>Лабораторная работа предполагает изучение научной литературы, использование не только учебников и пособий, но и информации, содержащейся в Интернете.</p> <p>Поскольку по темам, освоенным при выполнении лабораторных работ, будут сформулированы вопросы, на которые надо будет отвечать при зачёте, студенту следует продуманно выполнять роли отправителя сообщений (Алисы) и получателя этих сообщений (Боба), помня о защите сообщений от НСД зловредной Евы.</p>
самостоятельная работа	<p>Результатом самостоятельной работы должна быть систематизация и структурирование учебного материала по изучаемой теме, включение его в уже имеющуюся у вас систему знаний. После изучения учебного материала необходимо проверить усвоение его с помощью предлагаемых вопросов. При структурировании учебного материала происходит понимание содержания самой учебной дисциплины. Поэтому остается только найти элементы этих систем и выявить существующие между ними связи и отношения.</p>
отчет	<p>В отчёте по каждой теме должны быть отражены от имени отправителя(Алисы) и получателя (Боба) следующее:</p> <ul style="list-style-type: none"> - название метода шифрования/ расшифрования; - исходное сообщение или шифротекст; - ключ (для симметричных методов - по пунктам , для асимметричных методов - открытый или закрытый соответственно роли); - способ достижения результата (с приведением таблиц, скриншотов); - результат : (а) шифротекст, предназначенный Алисой для Боба, (б) исходное сообщение, полученное Бобом от Алисы) - программа, реализующая метод.

Вид работ	Методические рекомендации
письменная работа	<p>Письменная домашняя работы и задания могут быть индивидуальными и общими. При выполнении контрольных работ, необходимо соблюдать идентичные требования к их оформлению. Следует иметь в виду, что неправильное оформление письменной работы может привести к снижению итоговой оценки. Все виды письменных работ выполняются на персональном компьютере и должны быть отпечатаны на принтере на стандартном листе белой бумаги формата А4 на одной стороне (210x297 мм). Рекомендуемый шрифт - TimesNewRoman, межстрочный интервал полуторный, 14 кегль, в таблицах - 12, в подстрочных сносках - 10. На титульном листе надписи: курсовая, контрольная работа и реферат печатаются 18 шрифтом. Подчеркивание слов и выделение их курсивом не допускается. Поля сверху, снизу по 20 мм, справа - 20 мм, слева - 30 мм, отступ первой строки абзаца - 1,25, выравнивание по ширине. Объем контрольной работы составляет 15-25 страниц включая титульный лист, оглавление, введение, список использованных источников. Титульный лист заполняется по единому образцу. В оглавлении, следующим за титульным листом, перечисляются разделы, части и параграфы с указанием номеров страниц. Названия глав (заголовки) и параграфов (подзаголовки) выделяются полужирным шрифтом, и выравниваются по центру. В конце заголовка, подзаголовка точка не ставится. Размер заголовка - 16 пт., подзаголовка - 14 пт. Каждая глава начинается с новой страницы. Расстояние между заголовком и подзаголовком, заголовком и последующим текстом, подзаголовком и предыдущим текстом отделяют двумя полуторными межстрочными интервалами (одной пустой строкой), а между подзаголовком и последующим текстом - одним полуторным межстрочным интервалом (как строки последующего текста). Страницы письменных работ должны иметь сквозную нумерацию арабскими цифрами по всему тексту. Номер страницы проставляют в центре нижнего поля страницы без точки в конце. Первой страницей письменной работы является титульный лист. Он не нумеруется. Размер шрифта, используемого для нумерации должен быть меньше, чем у основного текста. В работе второй страницей является - оглавление. При написании письменных работ обоснование того или иного положения возможно с помощью цитат из научной, справочной и иной литературы. Здесь необходимо напомнить основные правила включения в текст цитат и оформления сносок на используемые автором источники. При подготовке к зачету необходимо опираться прежде всего на лекции, а также на источники, которые разбирались на семинарах и практических занятиях в течение семестра.</p>
проверка практических навыков	<p>Важной обязанностью преподавателя является проверка практических навыков студентов. На основании этих проверок преподаватель получает представление об уровне полученных навыков и умений обучающегося.</p> <p>Как известно, именно получение практических навыков в применении методов, обеспечивающих информационную безопасность сообщений в системе защиты информации является одной из целей, которая должна быть достигнута при изучении нашей дисциплины. Наряду с формированием умений и навыков в процессе занятий обобщаются, систематизируются, углубляются и конкретизируются теоретические знания, вырабатывается способность и готовность использовать их в решении практических задач.</p> <p>Студенту нужно продемонстрировать выполнение задачи от начала до конца, причём важно убедиться в правильности выполнения задания. В нашем деле нельзя допустить промаха, поскольку его ценой может стать утечка чрезвычайно ценных данных. Поэтому наша проверка практических навыков проходит в условиях, приближённых к реальности. Студентам нравится использовать гаджеты при передаче зашифрованных сообщений через сети интернета.</p> <p>При оценке результатов применения студентом практических навыков учитывается следующее:</p> <ol style="list-style-type: none"> 1. использование теоретических знаний при выполнении заданий; 2. понимание задачи, способность предложить её решение, критически оценить решение и его последствия; 3. способность определить, проанализировать альтернативные возможности, варианты действий; 4. способность активно использовать электронные образовательные ресурсы, находить требующиеся сведения, изучать их и применять на практике; 5. способность обосновать и чётко изложить материал в отчёте; 6. способность оформить отчёт в соответствии с требованиями; ГОСТ. <p>Вот пример задания</p> <ol style="list-style-type: none"> 1. Изучить теорию шифрования асимметричным ключом, изложенную в брошюре СООБЩЕНИЕ ШИФРУЕМ АСИММЕТРИЧНО (см. файл https://clck.ru/N3GdV). 2. Получить открытые ключи для роли Алисы (Отправителя) и Боба (Получателя). (раздел ФАЙЛЫ https://clck.ru/N3GQC) 3. Получить закрытые ключи, отправленные каждому из вас по почте , 4. Выполнить задания по использованию асимметричного шифрования 5. Оформить отчёт в соответствии о данным образцом.

Вид работ	Методические рекомендации
зачет	Бакалавру следует понимать, что зачёт - это заключительный этап работы в семестре по данной дисциплине. Здесь важнейшую роль играют не только посещение занятий, но также и то, насколько внимательны и активны вы были на лекциях, при выполнении и защите лабораторные работ, при самостоятельной работе над учебно-методической литературой и интернет-источниками. Всё это проявляется при ответе на вопросы, предоставленные вам для подготовки к зачёту

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем, представлен в Приложении 3 к рабочей программе дисциплины (модуля).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Материально-техническое обеспечение образовательного процесса по дисциплине (модулю) включает в себя следующие компоненты:

Помещения для самостоятельной работы обучающихся, укомплектованные специализированной мебелью (столы и стулья) и оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду КФУ.

Учебные аудитории для контактной работы с преподавателем, укомплектованные специализированной мебелью (столы и стулья).

Компьютер и принтер для распечатки раздаточных материалов.

Мультимедийная аудитория.

Компьютерный класс.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;
- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;
- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;
- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;
- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;
- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;
- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:
- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;
- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;
- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 01.03.02 "Прикладная математика и информатика"

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.12 Методы защиты информации

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 01.03.02 - Прикладная математика и информатика

Профиль подготовки:

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2019

Основная литература:

1. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. - Москва : ФОРУМ : ИНФРА-М, 2019. - 592 с. - (Высшее образование: Бакалавриат). - ISBN 978-5-16-106148-0. - URL : <https://new.znaniyum.com/catalog/product/996789>. - Текст : электронный.
2. Баранова Е. К. Основы информатики и защиты информации: учебное пособие / Е. К. Баранова. - Москва : ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 183 с. - (Высшее образование: Бакалавриат). - ISBN 978-5-369-01169-0. - URL : <https://new.znaniyum.com/catalog/product/959916>. - Текст : электронный.
3. Никифоров С. Н. Методы защиты информации. Шифрование данных : учебное пособие / С. Н. Никифоров. - Санкт-Петербург : Лань, 2019. - 160 с. - ISBN 978-5-8114-4042-9. - URL : <https://e.lanbook.com/book/114699>. - Текст : электронный.

Дополнительная литература:

1. Никифоров С. Н. Методы защиты информации. Защищенные сети : учебное пособие / С. Н. Никифоров. - Санкт-Петербург : Лань, 2018. - 96 с. - ISBN 978-5-8114-3099-4. - URL : <https://e.lanbook.com/book/110935>. - Текст : электронный.
2. Башлы П. Н. Информационная безопасность и защита информации : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : ИЦ РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - URL : <https://new.znaniyum.com/go.php?id=405000>. - Текст : электронный.
3. Интеллектуальные системы защиты информации : учебные пособие / В. И. Васильев. - 2-е изд., испр. и доп. - Москва : Машиностроение, 2013. - 172 с. - ISBN 978-5-94275-667-3. - URL : <http://www.studentlibrary.ru/book/ISBN9785942756673.html>. - Текст : электронный

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.12 Методы защиты информации

Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Направление подготовки: 01.03.02 - Прикладная математика и информатика

Профиль подготовки:

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2019

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows 7 Профессиональная или Windows XP (Volume License)

Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Reader XI или Adobe Acrobat Reader DC

Kaspersky Endpoint Security для Windows

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань", доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "Консультант студента", доступ к которой предоставлен обучающимся. Многопрофильный образовательный ресурс "Консультант студента" является электронной библиотечной системой (ЭБС), предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Полностью соответствует требованиям федеральных государственных образовательных стандартов высшего образования к комплектованию библиотек, в том числе электронных, в части формирования фондов основной и дополнительной литературы.