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
_____ Н.Д. Ахметов
"___"_____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: 2018

Содержание

Программу дисциплины разработал(а)(и) доцент, к.н. (доцент) Каримов В.С. (Кафедра системного анализа и информатики, Отделение информационных технологий и энергетических систем), VSKarimov@kpfu.ru ; доцент, к.н. (доцент) Товштейн М.Я. (Кафедра системного анализа и информатики, Отделение информационных технологий и энергетических систем), motbrecia@gmail.com

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
ОПК-4	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-5	Способность осуществлять целенаправленный поиск информации о новейших научных и технологических достижениях в сети Интернет и в других источниках

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

- комплексный характер защиты информационной системы,

- принципы организационной, технической и программной защиты конфиденциальных данных , основы криптографии,

Должен уметь:

- ориентироваться в государственных нормативных актах по защите информации,

- использовать программно-технические средства, обеспечивающие безопасность хранения, жизнедеятельности и передачи информации при её разработке и эксплуатации в

Должен владеть:

- навыками принятия мер противодействия угрозам безопасности информации, разрабатывать систему защиты информации.

Должен демонстрировать способность и готовность:

В результате изучения дисциплины бакалавр должен:

знать

- комплексный характер защиты информационной системы,

- принципы организационной, технической и программной защиты конфиденциальных данных , основы криптографии,

уметь

- ориентироваться в государственных нормативных актах по защите информации,

- использовать программно-технические средства, обеспечивающие безопасность хранения, жизнедеятельности и передачи информации при её разработке и эксплуатации в различных средах.

иметь навыки

- принимать меры противодействия угрозам безопасности информации, разрабатывать систему защиты информации.

- емонстрировать, полученные умения и знания на практике.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.ОД.8 Дисциплины (модули)" основной профессиональной образовательной программы 01.03.02 "Прикладная математика и информатика ()" и относится к обязательным дисциплинам.

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 4 зачетных(ые) единиц(ы) на 144 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 - 94 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 защиты2	8	2	0	0	4
2.	Тема 2. Правовые средства защиты информации от несанкционированного доступа	8	2	0	4	14
3.	Тема 3. Угрозы информационной безопасности предприятия	8	2	0	2	14
4.	Тема 4. Административно-организационные средства защиты информации.	8	2	0	2	12
5.	Тема 5. Технические аспекты обеспечения защиты информации.	8	2	0	2	8
6.	Тема 6. Криптографические симметричные методы защиты информации.	8	4	0	10	20
7.	Тема 7. Криптографические асимметричные методы защиты информации,	8	6	0	10	22
	Итого		20	0	30	94

4.2 Содержание дисциплины (модуля)

Тема 1. Информация как объект защиты2

Различные определения понятия "информация": философские, техноцентрические, антропоцентрические. Определение, данное в Федеральном законе ""Об информации, информационных технологиях и о защите информации" от 6 июля 2016 г . Информатизация общества на современном этапе, основные принципы информатизации общества.

Тема 2. Правовые средства защиты информации от несанкционированного доступа

Информационная безопасностью - это защищенн&#65533;ость информации и поддерживающей инфраструктуры от случайных или предна&#65533;меренных воздействий естественного или искусственного характера, которые могут на&#65533;нести неприем&#65533;лемый ущерб субъектам информационных отношений, в том числе вла&#65533;дельцам и пользовате&#65533;лям информации и поддерживающей инфраструктуры.

Защита информации - это комплекс мероприятий, направленных на обеспечение ин&#65533;формационной безопасности.

Доктрина информационной безопасности РФ.

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

Тема 3. Угрозы информационной безопасности предприятия

Угроза - это потенциальная возможность определенным образом нарушить информацио&#65533;нную безопасность. Атака - попытка реализации угрозы. Злоумышленник - реализатор атаки. Потенциальные злоумышленни&#65533;ки как ис&#65533;точниками угрозы.Классификация средств защиты информации.

Угрозы информационным ресурсам предприятия.

Роль морально-этических средств защиты 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. Организация явного или скрытого контроля за работой пользователей

Тема 5. 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 6. 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 аналитическго преобразования

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 применении.

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 шифруемая вместе с ними.

Дайджест обеспечивает однозначное соответствие между сообщением и сжатым его эквивалентом.

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	Устный опрос	ОПК-4	1. Информация как объект защиты2
2	Презентация	ОПК-4	2. Правовые средства защиты информации от несанкционированного доступа 4. Административно-организационные средства защиты информации.
3	Лабораторные работы	ОПК-4	6. Криптографические симметричные методы защиты информации. 7. Криптографические асимметричные методы защиты информации,
	Зачет	ОПК-4, ПК-5	

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					
Устный опрос	В ответе качественно раскрыто содержание темы. Ответ хорошо структурирован. Прекрасно освоен понятийный аппарат. Продемонстрирован высокий уровень понимания материала. Превосходное умение формулировать свои мысли, обсуждать дискуссионные положения.	Основные вопросы темы раскрыты. Структура ответа в целом адекватна теме. Хорошо освоен понятийный аппарат. Продемонстрирован хороший уровень понимания материала. Хорошее умение формулировать свои мысли, обсуждать дискуссионные положения.	Тема частично раскрыта. Ответ слабо структурирован. Понятийный аппарат освоен частично. Понимание отдельных положений из материала по теме. Удовлетворительное умение формулировать свои мысли, обсуждать дискуссионные положения.	Тема не раскрыта. Понятийный аппарат освоен неудовлетворительно. Понимание материала фрагментарное или отсутствует. Неумение формулировать свои мысли, обсуждать дискуссионные положения.	1

Форма контроля	Критерии оценивания				Этап
	Отлично	**Хорошо**	**Удовл.**	**Неуд.**	
Презентация	Превосходный уровень владения материалом. Высокий уровень доказательности, наглядности, качества преподнесения информации. Степень полноты раскрытия материала и использованные решения полностью соответствуют задачам презентации. Использованы надлежащие источники и методы.	Хороший уровень владения материалом. Средний уровень доказательности, наглядности, качества преподнесения информации. Степень полноты раскрытия материала и использованные решения в основном соответствуют задачам презентации. Использованные источники и методы в основном соответствуют поставленным задачам.	Удовлетворительный уровень владения материалом. Низкий уровень доказательности, наглядности, качества преподнесения информации. Степень полноты раскрытия материала и использованные решения слабо соответствуют задачам презентации. Использованные источники и методы частично соответствуют поставленным задачам.	Неудовлетворительный уровень владения материалом. Неудовлетворительный уровень доказательности, наглядности, качества преподнесения информации. Степень полноты раскрытия материала и использованные решения не соответствуют задачам презентации. Использованные источники и методы не соответствуют поставленным задачам.	2
Лабораторные работы	Оборудование и методы использованы правильно. Проявлена превосходная теоретическая подготовка. Необходимые навыки и умения полностью освоены. Результат лабораторной работы полностью соответствует её целям.	Оборудование и методы использованы в основном правильно. Проявлена хорошая теоретическая подготовка. Необходимые навыки и умения в основном освоены. Результат лабораторной работы в основном соответствует её целям.	Оборудование и методы частично использованы правильно. Проявлена удовлетворительная теоретическая подготовка. Необходимые навыки и умения частично освоены. Результат лабораторной работы частично соответствует её целям.	Оборудование и методы использованы неправильно. Проявлена неудовлетворительная теоретическая подготовка. Необходимые навыки и умения не освоены. Результат лабораторной работы не соответствует её целям.	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. Устный опрос

Тема 1

ПО ТЕМЕ №1 должны быть освещены следующие пункты:

1. Классификация различных подходов в определении понятия "информация": техноцентрический, антропоцентрический, мировоззренческий.
2. Определение, данное в ФЗ "Об информации, информационных технологиях и о защите информации".
3. Определение понятия "информация" с точки зрения физиков.
4. Определение понятия "информация" с точки зрения кибернетиков.
5. Определение понятия "информация" с точки зрения "технарей".
6. Определение понятия "информация" с точки зрения философов.
7. Пять элементов , которые надо иметь в виду при передаче сигналов.

8. Примеры каналов связи, используемых для передачи сигналрв.
9. Характеристика следующих свойств антропоцентрического понимания информации:
- достоверность;
- полнота;
- ценность;
- своевременность.
- понятность;
- доступность;
- краткость.
11. Характеристика следующих свойств антропоцентрического понимания информации:
-- свойство физической неотчуждаемости информации,
-- свойство обособленности информации,.
-- свойство информационной вещи (информационного объекта).
-- свойство тиражируемости (распространяемости) информации,
-- свойство организационной формы,
-- свойство экземплярности информации.
12. Характеристика трёх групп угроз:
А) антропогенные. угрозы, обусловленные действиями субъекта.
-- непреднамеренные,
-- преднамеренные.
Б) техногенные угрозы,
В) естественные (природные).
13. Характеристика воздействий, которым может быть подвернута информация,
-- блокирование,
-- нарушение целостности,
-- нарушение конфиденциальности,
-- несанкционированное тиражирование,
-- разглашение.
Собствнно говоря, сначала на занятии выясняется, насколько студентя уяснили, что собой представляет информация и какую специфику она имеет в юридическом аспекте. После такого опроса можно приниматься за разработку презентации.

2. Презентация

Темы 2, 4
ПО ТЕМЕ №2 должны быть освещены следующие пункты:
1. Принципы правового регулирования отношений в информационной сфере.
2. Отношения, регулируемые данный законом "Об информации, информационных технологиях и о защите информации" .
3. Определение понятия "защита информации".
4. Цель защиты информации.
5. Определение понятия 'владелец информации'. Права владельца информации.
6. Определение понятия 'пользователь информации' . Права пользователя информации.
7. Сопоставление понятий "информация документированная" и "общедоступная информация".
8. Определение "права на доступ к информации".
9. На какую информацию не может быть ограничен доступ?
10. Условия , которые способствуют неправомерному овладению конфиденциальной информацией
ПО ТЕМЕ №4 должны быть освещены следующие пункты:
1. Организационные меры защиты информации
2. Морально-этические меры защиты информации
3. Условия, способствующие неправомерному овладению конфиденциальной информацией..
4. Действия, приводящие к неправомерному овладению конфиденциальной информацией
5. Воздействия, которым может быть подвернута информация.
6. Сведения, относящиеся к конфиденциальной информации.
7. Организационные меры, предпринимаемые работодателем для защиты конфиденциальной информации.
8. Воздействия, которым может быть подвернута информация.
9. Действия, которые приводят к неправомерному овладению конфиденциальной информацией.
10. Условия , которые способствуют неправомерному овладению конфиденциальной информацией?

3. Лабораторные работы

Темы 6, 7

ПО ТЕМЕ №6 должны быть освещены следующие пункты:
- Понятия идентификации и аутентификации.
- Возможности нарушителя и средства защиты.
- Каналы утечки информации.
- Краткие сведения о средствах съёма и защиты информации.

Защита ЭВМ и электронных носителей информации. Классификация основных методов криптографического закрытия. Примеры шифрования симметричным ключом (методами подстановки, перестановки, гаммирования, математическими вычислениями). Разработка программ реализации методов симметрической криптографии.

ПО ТЕМЕ №7 должны быть освещены следующие пункты:

Применение асимметричного шифрования в обмене сообщениями. Протоколы защиты канала связи. Применение сеансового ключа. Электронная цифровая подпись, сопоставление её с рукописной, методика применении.

Разработка программ реализации методов асимметрической криптографии.

Классификация средств защиты информации. Угрозы информационным ресурсам предприятия Внутренние и внешние факторы, способствующие промышленному шпионажу. Роль морально-этических средств защиты информации.

Организационные меры защиты информации:. Организационные меры охраны конфиденциальных сведений на предприятиях малого бизнеса.

лассификация основных методов криптографического закрытия. Примеры шифрования симметричным ключом (методами подстановки, перестановки, гаммирования, математическими вычислениями).

Применение асимметричного шифрования в обмене сообщениями. Протоколы защиты канала связи. Применение сеансового ключа. Электронная цифровая подпись, сопоставление её с рукописной, методика применении.

ЛАБОРАТОРНЫЕ РАБОТЫ ПРИЗВАНЫ ОТВЕТИТЬ НА СЛЕДУЮЩИЕ ВОПРОСЫ:

1. В чём трудность определения понятия "информация"? Как это понятие определено в ФЗ "Об информации, информационных технологиях и о защите информации" ?
2. Как определяют понятие ?информация? физики, кибернетики, ?технари?, философы? Какие 5 элементов имеют в виду, когда определяют понятие ?информация?? Обмениваются ли информацией животные, неживые объекты с животным миром и между собой? Если да, то поясните на примерах.
3. Какие отношения регулирует данный закон ?Об информации, информационных технологиях и о защите информации? ? На какие отношения данный Закон не распространяется ?
4. Что понимается под защитой информации и что является целью защиты информации?
5. Почему важно понимать, кто такие владелец и пользователь информации?
6. Какая информация называется документированной?
7. Что такое общедоступная информация ? Приведите примеры.
8. Как определяется право на доступ к информации. На какую информацию не может быть ограничен доступ ?
9. Какая информация должна быть защищена? Что означает несанкционированный доступ (НСД) к информации?
10. Какие условия способствуют неправомерному овладению конфиденциальной информацией?.
11. Какие действия приводят к неправомерному овладению конфиденциальной информацией
12. Каким воздействиям может быть подвернута информация? Приведите примеры таких воздействий.
13. Какие три группы угроз информации можно отметить? Каковы источники и следствия реализации этих угроз?
14. Какие меры противодействия угрозам известны? Охарактеризуйте их и приведите примеры.
15. Какими принципами следует руководствоваться при организации защиты информации? Поясните на промерах.
16. Что такое идентификация и аутентификация? Какие три принципа аутентификации вам известны.
17. Какие средства физической защиты объектов вам известны? Каковы требования к инженерным и техническим средствам охраны помещений, предназначенных для работы с конфиденциальной информацией?
18. Какие сведения относятся к конфиденциальной информации, какие сведения не могут быть отнесены к конфиденциальной информации ?
19. Какие виды "тайн" защищаются законом?
20. Какие три степени государственной тайны устанавливает ФЗ "О государственной тайне" от 21 июля 1993 года N 5486-1 ?
21. Как определяется коммерческая тайна в ФЗ ?О коммерческой тайне? №98 от 2004 г. и что относится к информации, составляющую коммерческую тайну?
22. Какие организационные меры должен предпринять работодатель для защиты конфиденциальности информации
23. Какие статьи Уголовного кодекса РФ устанавливают ответственность за правонарушения в информационной сфере? Сравните позицию хакера с позицией АйТи-специалиста с точки зрения ответственности по этим статьям.
24. Чем отличаются симметричные от асимметричных методов криптографической защиты информации? Что понимается под ключом шифрования? Приведите примеры симметричных методов шифрования.
25. Какие недостатки симметричных методов шифрования исправляют асимметричными методами? Расскажите об асимметричном методе шифрования.
26. Как выполняются идентификация и аутентификация сообщения?

27. Как сочетанием метода гаммирования с асимметричным методом шифрования обеспечивается защита канала связи между корреспондентами?
28. Достоинства и недостатки ручной подписи. Как ЭЦП борется с недостатками ручной подписи?
29. Что такое дайджест (слепок, контрольная сумма) сообщения и какую роль он играет в защите информации? Приведите пример хеш-функции, реализующей дайджест сообщения.

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 данный 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 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 ихустранение 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			
Устный опрос	Устный опрос проводится на практических занятиях. Обучающиеся выступают с докладами, сообщениями, дополнениями, участвуют в дискуссии, отвечают на вопросы преподавателя. Оценивается уровень домашней подготовки по теме, способность системно и логично излагать материал, анализировать, формулировать собственную позицию, отвечать на дополнительные вопросы.	1	10
Презентация	Обучающиеся выполняют презентацию с применением необходимых программных средств, решая в презентации поставленные преподавателем задачи. Обучающийся выступает с презентацией на занятии или сдаёт её в электронном виде преподавателю. Оцениваются владение материалом по теме презентации, логичность, информативность, способы представления информации, решение поставленных задач.	2	10
Лабораторные работы	В аудитории, оснащённой соответствующим оборудованием, обучающиеся проводят учебные эксперименты и тренируются в применении практико-ориентированных технологий. Оцениваются знание материала и умение применять его на практике, умения и навыки по работе с оборудованием в соответствующей предметной области.	3	30
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 и предоставленных доступов НЧИ КФУ;

- в печатном виде - в фонде библиотеки Набережночелнинского института (филиала) КФУ. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования 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 библиотеки Набережночелнинского института (филиала) КФУ.

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

Котов, Ю. А. Криптографические методы защиты информации. Шифры : учебное пособие / Ю. А. Котов. - Новосибирск : НГТУ, 2016. - 59 с. - 12. Текст�: электронный�// Лань : электронно-библиотечная система - URL: https://e.lanbook.com/book/118209

Антивирусная защита компьютерных систем : учебное пособие. ? 2-е изд. ? Москва : ИНТУИТ, 2016. - 323 с.�- Текст�: электронный�// Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/100728

Киздермишов, А. А. Актуальные вопросы защиты информации : учебное пособие / А. А. Киздермишов, А. В. Шопин. ? Майкоп : АГУ, 2018. ? 108 с. - Текст�: электронный�// Лань : электронно-библиотечная система. - https://e.lanbook.com/book/146128

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

Вид работ	Методические рекомендации
лекции	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. Сравнивать 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 понятия. Необходимо тщательно вслед за лектором делать записи. Если на лекции вы не пучили ответа на возникшие вопросы, разрешается сразу же или в конце лекции задать их лектору. Если лектор задаёт вопросы, желательно не отмалчиваться, а отвечать на них.. И внимательно слушать ответы товарищей.
лабораторные работы	При подготовке к лабораторной работе необходимо прочитать записанную лекцию, обращая внимание на наиболее важные моменты, прочитать рекомендованный материал из учебно-методической литературы. Лабораторные занятия проводятся с использованием активных методов: работа в малых группах (бригадах), обсуждение проблем администрации баз данных посредством анализа предметной области. Лабораторная работа предполагает изучение научной литературы, использование не только учебников и пособий, но и информации, содержащейся в Интернете. Поскольку некоторые темы лабораторной работы могут быть составной частью курсовой работы, предполагается активная позиция студента в роли администратора базы даннщх.
самостоя-тельная работа	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.
презентация	Создавая презентацию, необходимо: а) усвоить представляемый учебный материал, б) рассчитать этот материал по кадрам презентации, в) выбрать оформительский образ слайдов, формат текста, рисунки, г) составить текст, сопровождаемый показ каждого слайда, д) провести хронометраж из расчёта 15 минут на выступление.
устный опрос	В ходе обучения вы сталкиваетесь с необходимостью, во-1-х, понять и, во-2-х, запомнить большой по объему учебный материал. Важным условием для успешного формирования прочных знаний является их упорядочивание, приведение их в единую систему. Информация, организованная в систему, где учебные элементы связаны друг с другом различного рода связями (функциональными, логическими и др.), лучше запоминается. При структурировании учебного материала происходит понимание содержания самой учебной дисциплины. Поэтому остаётся только найти элементы этих систем и выявить существующие между ними связи и отношения.
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.ОД.8 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: 2018

Основная литература:

1. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. - Москва : ФОРУМ : ИНФРА-М, 2018. - 592 с. - (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - URL: https://znanium.com/catalog/product/937502. - Текст : электронный.

2. Мельников В. П. Информационная безопасность и защита информации: учебное пособие для вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 4-е изд., стер. - Москва : Академия, 2009. - 336 с : ил., табл. - (Высшее профессиональное образование). - Рек. УМО. - В пер. - Библиогр.: с. 327-328. - ISBN 978-5-7695-6150-4. - Текст: непосредственный. (10 экз.)

3. Башлы П. Н. Информационная безопасность и защита информации: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - URL: https://znanium.com/catalog/product/405000. - Текст : электронный.

Дополнительная литература:

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. - Москва : ФОРУМ : ИНФРА-М, 2018. - 416 с. - (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - URL: https://znanium.com/catalog/product/945331. - 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://znanium.com/catalog/product/959916. - Текст : электронный.

3. Васильев В.И. Интеллектуальные системы защиты информации : учебное пособие / В.И. Васильев. - 2-е изд., испр. и доп. - Москва: Машиностроение, 2013. - 172 с. - ISBN 978-5-94275-667-3. - URL : https://www.studentlibrary.ru/book/ISBN9785942756673.html. - Текст : электронный.

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.ОД.8 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: 2018

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.