

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

Первый заместитель директора
НЧИ КФУ Симонова Л. А.



_____ 20__ г.

подписано электронно-цифровой подписью

Программа дисциплины Методы защиты информации Б1.В.ОД.9

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: 2017

Автор(ы): Товштейн М.Я.

Рецензент(ы): Валиев Р.А.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Карабцев В. С.

Протокол заседания кафедры No ____ от " ____ " _____ 20__ г.

Учебно-методическая комиссия Высшей инженерной школы (Отделение информационных технологий и энергетических систем) (Набережночелнинский институт (филиал)):

Протокол заседания УМК No ____ от " ____ " _____ 20__ г.

Набережные Челны
2019

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы
2. Место дисциплины в структуре основной профессиональной образовательной программы высшего образования
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
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 основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)
 - 7.1. Основная литература
 - 7.2. Дополнительная литература
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 к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

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

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

Выпускник, освоивший дисциплину, 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

Выпускник, освоивший дисциплину:

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.

2. Место дисциплины в структуре основной профессиональной образовательной программы высшего образования

Данная учебная дисциплина включена в раздел "Б1.В.ОД.9 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 защиты.	8	2	0	0	4

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
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

Тема 1. Информация как объект защиты.

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 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.

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 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.

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 пользователя

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 аналитического 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 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.

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"

Положение от 24 декабря 2015 г. № 0.1.1.67-06/265/15 "О порядке проведения текущего контроля успеваемости и промежуточной аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет"

Положение № 0.1.1.67-06/241/15 от 14 декабря 2015 г. "О формировании фонда оценочных средств для проведения текущей, промежуточной и итоговой аттестации обучающихся федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет"

Положение № 0.1.1.56-06/54/11 от 26 октября 2011 г. "Об электронных образовательных ресурсах федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"

Регламент № 0.1.1.67-06/66/16 от 30 марта 2016 г. "Разработки, регистрации, подготовки к использованию в учебном процессе и удаления электронных образовательных ресурсов в системе электронного обучения федерального государственного автономного образовательного учреждения высшего образования "Казанский (Приволжский) федеральный университет"

Регламент № 0.1.1.67-06/11/16 от 25 января 2016 г. "О балльно-рейтинговой системе оценки знаний обучающихся в федеральном государственном автономном образовательном учреждении высшего образования "Казанский (Приволжский) федеральный университет""

Регламент № 0.1.1.67-06/91/13 от 21 июня 2013 г. "О порядке разработки и выпуска учебных изданий в федеральном государственном автономном образовательном учреждении высшего профессионального образования "Казанский (Приволжский) федеральный университет""

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			
	<i>Текущий контроль</i>		
1	Лабораторные работы	ОПК-4	3. Угрозы информационной безопасности предприятия 6. Криптографические симметричные методы защиты информации. 7. Криптографические асимметричные методы защиты информации,
2	Презентация	ОПК-4	1. Информация как объект защиты. 2. Правовые средства защиты информации от несанкционированного доступа 4. Административно-организационные средства защиты информации.
3	Устный опрос	ОПК-4	1. Информация как объект защиты.
	Зачет		

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					
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 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.	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. Используются 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. Используются 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. Используются 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. Используются источники и методы не соответствуют поставленным задачам.	2
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.	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. Лабораторные работы

Темы 3, 6, 7

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

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.

Классификация 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 применения.

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 подвергнута 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 примерах.
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.

2. Презентация

Темы 1, 2, 4

Презентация может быть выбрана на одну из указанных тем.

ПО ТЕМЕ №1 должны быть освещены следующие пункты:

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.

ПО ТЕМЕ ♦2 должны быть освещены следующие пункты:

1. Принципы правового регулирования отношений в информационной сфере. Отношения, регулируемые данным законом "Об информации, информационных технологиях и о защите информации" .
2. Определение понятия "защита информации", цель защиты информации.
3. Определение понятия 'владелец' и 'пользователь информации'. Права владельца и пользователя информации.
4. Сопоставление понятий "информация документированная" и "общедоступная информация".
5. Определение "права на доступ к информации". На какую информацию не может быть ограничен доступ?
6. Правовые меры защиты информации.

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.

3. Устный опрос

Тема 1

ПО ТЕМЕ ♦1 должны быть освещены следующие пункты:

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.

Собственно говоря, сначала на занятии выясняется, насколько студента уяснили, что собой представляет информация и какую специфику она имеет в юридическом аспекте. После такого опроса можно приниматься за разработку презентации.

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			
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.	1	30
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
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.	3	10
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 основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

7.1 Основная литература:

-- Шаньгин В. Ф. Компьютерная защита информации в корпоративных системах [Электронный ресурс]: учебное пособие / В. Ф. Шаньгин. - Москва: ФОРУМ, 2013. - 592 с. - ISBN 978-5-8199-0411-4. - Режим доступа: <http://znanium.com/go.php?id=402686>.

-- Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс] : учебное пособие / В. Ф. Шаньгин. - Москва: ФОРУМ, 2014. - 416 с. - (Профессиональное образование). - ISBN 978-5-8199-0331-5. - Режим доступа: <http://znanium.com/go.php?id=423927>

-- Мельников В. П. Информационная безопасность и защита информации [Текст] : 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 (10 экз)

7.2. Дополнительная литература:

- Баранова Е. К. Основы информатики и защиты информации [Электронный ресурс] : учебное пособие / Е. К. Баранова. - Москва: ИЦРИОР, 2013. - 183 с. - ISBN 978-5-369-01169-0. - Режим доступа: <http://znanium.com/go.php?id=415501>.
 -- Башлы П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва: ИЦ РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Режим доступа: <http://znanium.com/go.php?id=405000>.
 - Интеллектуальные системы защиты информации [Электронный ресурс] : учебные пособие / В. И. Васильев. - 2-е изд., испр. и доп. - Москва : Машиностроение, 2013. - 172 с. - ISBN 978-5-94275-667-3. - Режим доступа: <http://www.studentlibrary.ru/book/ISBN9785942756673.html>

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

Доктрина информационной безопасности Российской Федерации, [Электронный ресурс] Режим доступа: http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm -- Федеральный закон 'Об информации, информатизации и о защите информации' от 27.07.2006 N 149-ФЗ (ред. от 25.11.2017) - <http://files.stroyinf.ru/Data2/1/4293850/4293850350.htm>
 Жельников В. Криптография от папируса до компьютера - М., АБФ, 1996 - <http://textarchive.ru/c-1905418-pall.html>
 Основы защиты информации: учебное пособие. Изд. 5-е, перераб. и доп. ? Томск: В-Спектр, 2011.-- 244 с. - http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_ozh.pdf
 Основы и методы защиты информации. Общие понятия информационной безопасности - <https://studfiles.net/preview/2652666/>
 Сингх С. Книга шифров: тайная история шифров и их расшифровки / Саймон Сингх; пер. с англ. А. Галыгина. - М.: АСТ: Астрель, 2007. - 447, 11] с.: ил. ISBN 978-5-17-038477-8 (ООО ?Издательство АСТ?) - <https://www.litmir.me/br/?b=250762&p=1>
 Федеральный закон 'Об информации, информатизации и о защите информации' от 27.07.2006 N 149-ФЗ (ред. от 25.11.2017) - <http://files.stroyinf.ru/Data2/1/4293850/4293850350.htm>
 Ярочкин В.И. Информационная безопасность : Учебник для студентов вузов. -- М.: Академический проект; Гаудеамус, -- 2004 -- 544 с. - <https://studfiles.net/preview/2204909/>

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. 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. 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 отмачиваться, 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 данных.

Вид работ	Методические рекомендации
самостоятельная 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)

Освоение дисциплины "Методы защиты информации" предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows Professional 7 Russian

Пакет офисного программного обеспечения Microsoft Office 2010 Professional Plus Russian

Браузер Mozilla Firefox

Adobe Reader XI

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.

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

Освоение дисциплины "Методы защиты информации" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB, audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудование имеет соответствующее лицензионное программное обеспечение.

Компьютерный класс, представляющий собой рабочее место преподавателя и не менее 15 рабочих мест студентов, включающих компьютерный стол, стул, персональный компьютер, лицензионное программное обеспечение. Каждый компьютер имеет широкополосный доступ в сеть Интернет. Все компьютеры подключены к корпоративной компьютерной сети КФУ и находятся в едином домене.

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".