МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
проф. Таюрский Д.А.
"___"_____20___ г.

Программа дисциплины

Основы информационной безопасности Б1.В.ОД.8

Направление подготовки: 09.03.03 - Прикладная информатика
Профиль подготовки: не предусмотрено
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2017
Автор(ы): Ишмухаметов Ш.Т. , Ямалеев М.М.
Рецензент(ы): Латыпов Р.Х.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Латыпов Р. Х.
Протокол заседания кафедры No ___ от "____" _____ 20__г.
Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 20__г.

Казань
2018

Содержание

Программу дисциплины разработал(а)(и) профессор, д.н. (доцент) Ишмухаметов Ш.Т. (кафедра системного анализа и информационных технологий, отделение фундаментальной информатики и информационных технологий), Shamil.Ishmukhametov@kpfu.ru ; доцент, к.н. Ямалеев М.М. (Кафедра алгебры и математической логики, отделение математики), Mars.Yamaleev@kpfu.ru

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-3	способностью использовать основные законы естественнонаучных дисциплин и современные информационно-коммуникационные технологии в профессиональной деятельности
ПК-2	способностью разрабатывать, внедрять и адаптировать прикладное программное обеспечение
ОПК-2	способностью анализировать социально-экономические задачи и процессы с применением методов системного анализа и математического моделирования
ПК-1	способностью проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе
ПК-4	способностью документировать процессы создания информационных систем на стадиях жизненного цикла

Выпускник, освоивший дисциплину:

Должен знать:

- сущность и актуальность проблемы информационной безопасности; изучить концептуальные подходы к обеспечению информационной безопасности; угрозы информации, средства и методы обеспечения информационной безопасности

Должен уметь:

- - ориентироваться в проблемах ИБ, методах и средствах защиты информации

Должен владеть:

- теоретическими знаниями о принципах построения безопасных ИС;

- навыками представление о проблемах информационной безопасности, способах, методах и средств их решения

Должен демонстрировать способность и готовность:

-применять полученные знания в своей профессиональной деятельности

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

Данная учебная дисциплина включена в раздел "Б1.В.ОД.8 Дисциплины (модули)" основной профессиональной образовательной программы 09.03.03 "Прикладная информатика (не предусмотрено)" и относится к обязательным дисциплинам.
Осваивается на 2 курсе в 4 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 - 72 часа(ов), в том числе лекции - 36 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 36 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 18 часа(ов).

Контроль (зачёт / экзамен) - 54 часа(ов).

Форма промежуточного контроля дисциплины: экзамен в 4 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	Раздел дисциплины/ модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Сущность, задачи информационной безопасности.	4	6	0	6	3
2.	Тема 2. Методы контроля доступа к информации.	4	6	0	6	3
3.	Тема 3. Организационно-правовые средства защиты.	4	6	0	6	3
4.	Тема 4. Криптографические средства защиты информации. Метод RSA.	4	6	0	6	3
5.	Тема 5. Сертификаты X.509. Аутентификация на основе сертификатов.	4	6	0	6	3
6.	Тема 6. Системы шифрования на основе эллиптических кривых.	4	6	0	6	3
	Итого		36	0	36	18

4.2 Содержание дисциплины

Тема 1. Сущность, задачи информационной безопасности.

Сущность, задачи и проблемы информационной безопасности 1.1. Введение в защиту информации. 1.2. Современная постановка задачи защиты информации. 1.3. Угрозы безопасности информационным системам и их классификация. 1.4. Меры противодействия угрозам безопасности ИС.

Тема 2. Методы контроля доступа к информации.

Методы контроля доступа к информации 2.1. Методы идентификации и аутентификации пользователей, технических средств обработки, программ и баз данных. 2.2. Классификация информационных систем по степени защищенности. 2.3. ?Общие критерии? стран Европейского сообщества, их основные положения. 2.4. Парольная идентификация и аутентификация в сетевых операционных системах.

Тема 3. Организационно-правовые средства защиты.

Организационно-правовые средства защиты 3.1. Законодательный уровень защиты информации. 3.2. Основные положения закона "Об информации, информатизации и защите информации" от 20 февраля 1995 года, определение понятий информации, документированной информации (документа), информационных процессов, информационной системы, информационных ресурсов. 3.3. Закон "О лицензировании отдельных видов деятельности" от 8 августа 2001 г

Тема 4. Криптографические средства защиты информации. Метод RSA.

Криптографические средства защиты информации 4.1. Криптографические средства защиты информации. 4.2. Криптосистемы с секретным ключом. 4.3. Математические основы современной криптологии. 4.4. Хэш-функции. 4.5. Открытое распределение ключей

Тема 5. Сертификаты X.509. Аутентификация на основе сертификатов.

Эллиптические кривые. 5.1. Математические основы построения ЭК. Прямые и обратные операции в конечных полях. 5.2. Система шифрования Эль-Гамаля. 5.3. Реализации системы Эль ? Гамаля на ЭК. 5.4. Алгоритм электронной подписи на ЭК.

Тема 6. Системы шифрования на основе эллиптических кривых.

Математические основы построения эллиптические кривых. Прямые и обратные операции в конечных полях.

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 N301).

Письмо Министерства образования Российской Федерации N14-55-996ин/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 N 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 N 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 N 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 N 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 N 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 4			
	Текущий контроль		
1	Контрольная работа	ПК-2 , ПК-1 , ОПК-3 , ОПК-2 , ПК-4	4. Криптографические средства защиты информации. Метод RSA.
2	Контрольная работа	ОПК-2 , ОПК-3 , ПК-1 , ПК-2 , ПК-4	6. Системы шифрования на основе эллиптических кривых.
	Экзамен	ОПК-2, ОПК-3, ПК-1, ПК-2, ПК-4	

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 4					
Текущий контроль					

Форма контроля	Критерии оценивания				Этап
	Отлично	**Хорошо**	**Удовл.**	**Неуд.**	
Контрольная 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 серьёзные 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 2
Экзамен	Обучающийся обнаружил всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой дисциплины, усвоил взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявил творческие способности в понимании, изложении и использовании учебно-программного материала.	Обучающийся обнаружил полное знание учебно-программного материала, успешно выполнил предусмотренные программой задания, усвоил основную литературу, рекомендованную программой дисциплины, показал систематический характер знаний по дисциплине и способен к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.	Обучающийся обнаружил знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справился с выполнением заданий, предусмотренных программой, знаком с основной литературой, рекомендованной программой дисциплины, допустил погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладает необходимыми знаниями для их устранения под руководством преподавателя.	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 4

Текущий контроль

1. Контрольная работа

Тема 4

Решение задач на шифрование текстов и построение цифровой подписи на основе алгоритма RSA.

1. Проверить число n=53 на простоту, используя одну итерацию теста Миллера-Рабина с базой a=2.

2. Используя заданные значения p, q и e, вычислить остальные параметры RSA и расшифровать число m. Для вычисления d использовать алгоритм Евклида: p=19, q=37, e=349, m=24.

3. Нехороший мальчик Плохиш назначил встречу у башенных часов вражескому агенту Крису для передачи военных секретов, закодировав время встречи с помощью RSA. Но бдительный мальчик Вова перехватил записку. Помоги Вове узнать время встречи (оно находится в интервале от 10 до 24 часов): n=943, e=673, m=405.

В других вариантах указаны другие числовые значения.

2. Контрольная работа

Тема 6

Решение задач на использование эллиптических кривых.

1. Задано конечное поле Fp. Найти наименьшее число g>=2, являющееся генератором поля, вычислить открытый ключ y по заданному x. Зашифровать сообщение m и выполнить обратную расшифровку, используя заданный параметр k. p=29, x=5, m=13, k=11

2. Хакер Вася перехватил зашифрованное сообщение (p,g,y,a,b)=(47,5,7,11,45). Помогите Васе расшифровать сообщение, используя метод Шенкса больших и малых шагов(ответ m<=10).

3. Заданы параметры поля Fp p=37, g=2, открытый ключ y=17 и сообщение m=9. Установить цифровую подпись на сообщение m и выполнить проверку, используя секретный ключ x=7

Экзамен

Вопросы к экзамену:

1. Введение в защиту информации.
2. Роль информации в жизнедеятельности современного общества.
3. Влияние информации на современное общество и повышение в связи с этим интерес к ней.
4. Определение информационной безопасности.
5. Современная постановка задачи защиты информации.
6. Основные составляющие информационной безопасности: конфиденциальность, целостность и доступность информации.
7. Угрозы безопасности информационным системам и их классификация. Угрозы конфиденциальности, целостности и доступности информации.
8. Меры противодействия угрозам безопасности ИС.
9. Классификация средств и методов защиты: административные, технические, организационно-правовые, физические методы защиты, их подразделение на предупреждающие, выявляющие (обнаруживающие), корректирующие средства.
10. Методы идентификации и аутентификации пользователей, технических средств обработки, программ и баз данных.
11. Метод паролей.
12. Биометрическая аутентификация.
13. Способы разграничения доступа, методы и средства их реализации.
14. Краткая характеристика современных средств разграничения доступа. Дискреционный и мандатный методы доступа.
15. Классификация информационных систем по степени защищенности.
16. "Оранжевая книга" США как критерий классификации систем информационной безопасности.
17. "Общие критерии" стран Европейского сообщества, их основные положения.
18. Парольная идентификация и аутентификация в сетевых операционных системах: многоразовые и одноразовые пароли, смарт-карты, аутентификация на основе сертификатов.
19. Законодательный уровень защиты информации.
20. Основные положения Конституции РФ о защите информации, правах граждан на получение и распространение информации, законы и законодательные акты Российской Федерации в области защиты информации.
21. Основные положения закона "Об информации, информатизации и защите информации" от 20 февраля 1995 года, определение понятий информации, документированной информации (документа), информационных процессов, информационной системы, информационных ресурсов.
22. Закон "О лицензировании отдельных видов деятельности" от 8 августа 2001 г. определение понятий лицензии, лицензируемого вида деятельности, лицензирования, лицензирующие органов, лицензиата. Положение статьи 17 Закона о видах деятельности, на осуществление которых требуются лицензии.
23. Основные положения закона РФ "Об электронной цифровой подписи" (от 13 декабря 2001 года) об электронном документе и электронной цифровой подписи, сертификате ЭЦП, владельце ЭЦП, закрытом и открытом ключе ЭЦП.
24. Криптографические средства защиты информации.
25. Основные понятия и задачи криптологии (криптографии).
26. Краткий исторический экскурс развития.
27. Примеры шифров замены и перестановки. Методы их дешифрования.
28. Криптосистемы с секретным ключом (симметричные).
29. Криптографические примитивы: перестановки, подстановки, гаммирование.
30. Блочные и потоковые криптосистемы.
31. Проблема распределения ключей.
32. Математические основы современной криптологии.
33. Криптосистемы с открытым ключом (ассиметричные).
34. Система RSA. 35. Хэш-функции. Их свойства.
36. Использование хэш-функций для защиты паролей, целостности и конфиденциальности информации.
37. Открытое распределение ключей.
38. Использование RSA для защиты конфиденциальности сообщений, целостности данных и определения авторства сообщения.
39. Математические основы построения эллиптических кривых.
40. Прямые и обратные операции в конечных полях.

41. Система шифрования Эль-Гамаля.
42. Реализации системы Эль - Гамаля на ЭК.
43. Алгоритм электронной подписи на ЭК

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 4			
Текущий контроль			
Контрольная работа	Контрольная работа проводится в часы аудиторной работы. Обучающиеся получают задания для проверки усвоения пройденного материала. Работа выполняется в письменном виде и сдаётся преподавателю. Оцениваются владение материалом по теме работы, аналитические способности, владение методами, умения и навыки, необходимые для выполнения заданий.	1 2	25 25
		Всего:	50
Экзамен	Экзамен нацелен на комплексную проверку освоения дисциплины. Экзамен проводится в устной или письменной форме по билетам, в которых содержатся вопросы (задания) по всем темам курса. Обучающемуся даётся время на подготовку. 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:

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин В. Ф. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2017. - 416 с URL: http://znanium.com/bookread2.php?book=775200

2. Глинская Е. В. Информационная безопасность конструкций ЭВМ и систем : учеб. пособие / Е.В. Глинская, Н.В. Чичварин. - М. : ИНФРА-М, 2018. URL: http://znanium.com/bookread2.php?book=945331

3. Партыка Т. Л. Информационная безопасность : учеб. пособие / Т.Л. Партыка, И.И. Попов. ? 5-е изд., перераб. и доп. - М. : ФОРУМ : ИНФРА-М, 2018. - 432 с. URL: http://znanium.com/bookread2.php?book=915902

4. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с. URL:http://znanium.com/bookread2.php?book=495249

5. Нестеров, С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие. - Электрон. дан. - СПб. : Лань, 2016. - 324 с. - Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=75515

6. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А. Васильков. - М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с. URL: http://znanium.com/bookread2.php?book=405313

7.2. Дополнительная литература:

1. Маскаева А. М. Основы теории информации: Учебное пособие / А.М. Маскаева. - М.: Форум: НИЦ ИНФРА-М, 2014. - 96 с. - ЭБС 'Знаниум': http://znanium.com/bookread.php?book=429571

2. Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. - ЭБС 'Знаниум': http://znanium.com/bookread.php?book=474838

3. Каратунова, Н. Г. Защита информации. Курс лекций [Электронный ресурс] : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - ЭБС 'Знаниум': http://znanium.com/bookread.php?book=503511

4. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с. - ЭБС 'Знаниум': http://znanium.com/bookread.php?book=491597

5. Хорев П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. 352 с. - ЭБС 'Знаниум': http://znanium.com/bookread.php?book=169345

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

Википедия - http://ru.wikipedia.org

Интернет-портал образовательных ресурсов по ИТ - http://www.intuit.ru

Курс лекций - http://old.kpfu.ru/f9/bin_files/metod_tzis!113.doc

материалы к занятиям - http://kpfu.ru/docs/F366166681/mzi.pdf

Форум по ИТ - http://www.citforum.ru/

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

Обучение происходит в форме лекционных и лабораторных занятий, а также самостоятельной работы студентов.
Теоретический материал излагается на лекциях. Причем конспект лекций, который остается у студента в результате прослушивания лекции не может заменить учебник. Его цель-формулировка основных утверждений и определений. Прослушав лекцию, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи экзамена минимум и дополнительная литература.
Изучение курса подразумевает не только овладение теоретическим материалом, но и получение практических навыков для более глубокого понимания разделов на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать утверждения.
Самостоятельная работа предполагает выполнение домашних работ. Практические задания, выполненные в аудитории, предназначены для указания общих методов решения задач определенного типа. Закрепить навыки можно лишь в результате самостоятельной работы.

Текущий контроль успеваемости студентов осуществляется с помощью контрольной работы, которая призвана показать основные практические навыки решения задач, связанных с математическим обеспечением задач информационной безопасности. При подготовке к контрольной работе рекомендуется обращаться внимание на основные задачи, решенные в течение семестра, периодически решать аналогичные задачи, программировать основные вычислительные алгоритмы, чтобы лучше понять их тонкости.
Кроме того, самостоятельная работа включает подготовку к экзамену. При подготовке к сдаче экзамена весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки к экзамену, контролировать каждый день выполнения работы.

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

Освоение дисциплины "Основы информационной безопасности" предполагает использование следующего программного обеспечения и информационно-справочных систем:

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.

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

Освоение дисциплины "Основы информационной безопасности" 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 оборудованием 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 09.03.03 "Прикладная информатика" и профилю подготовки не предусмотрено .