МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ 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

Введение в компьютерную безопасность Б1.В.ДВ.05.01

Направление подготовки: 01.04.02 - Прикладная математика и информатика
Профиль подготовки: Открытая информатика
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2018
Автор(ы): Латыпов Р.Х.
Рецензент(ы): Ишмухаметов Ш.Т.

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
2019

Содержание

Программу дисциплины разработал(а)(и) заведующий кафедрой, д.н. (профессор) Латыпов Р.Х. (кафедра системного анализа и информационных технологий, отделение фундаментальной информатики и информационных технологий), Roustam.Latypov@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
ПК-3	Руководство проектированием программного обеспечения
ПК-2	Управление аналитическими работами и подразделением, управление инфраструктурой разработки и сопровождение требований к системам
ПК-4	Выполнение работ и управление работами по созданию, модификации и сопровождению ИС

Выпускник, освоивший дисциплину:

Должен знать:

Студент должен знать:

- Математические принципы, лежащие в основе асимметричных криптографических алгоритмов.
- Существующие атаки на асимметричные криптосистемы.
- Значения параметров криптосистем, приводящие к возможности проведения криптоаналитической атаки.

Должен уметь:

Студент должен уметь:

- Проводить анализ стойкости криптографического алгоритмов при заданных параметрах.
- Идентифицировать причины снижения криптостойкости.

Должен владеть:

Студент должен владеть:

- Криптографической терминологией.

Должен демонстрировать способность и готовность:

Студент должен демонстрировать способность и готовность:

- Анализировать стойкостькриптосистемы.
- Вырабатывать рекомендации по повышению стойкости криптосистемы.

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

Данная учебная дисциплина включена в раздел "Б1.В.ДВ.05.01 Дисциплины (модули)" основной профессиональной образовательной программы 01.04.02 "Прикладная математика и информатика (Открытая информатика)" и относится к дисциплинам по выбору.
Осваивается на 2 курсе в 3 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 2 зачетных(ые) единиц(ы) на 72 часа(ов).

Контактная работа - 28 часа(ов), в том числе лекции - 0 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 28 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 44 часа(ов).

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

Форма промежуточного контроля дисциплины: зачет в 3 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. Введение в криптографические протоколы.	3	0	0	4	8
2.	Тема 2. Модель интерактивной системы доказателства.	3	0	0	6	8
3.	Тема 3. Протоколы совместных вычислений.	3	0	0	4	8
4.	Тема 4. Протоколы разделения секрета.	3	0	0	4	6
5.	Тема 5. Протоколы анонимности.	3	0	0	4	8
6.	Тема 6. Протоколы консенсуса.	3	0	0	6	6
	Итого		0	0	28	44

4.2 Содержание дисциплины

Тема 1. Введение в криптографические протоколы.

История возникновения криптографических протоколов. Односторонние функции и гипотеза о существовании односторонних функций. Идеи Диффи-Хеллмана. Криптографический протокол формирования ключей Диффи-Хеллмана. Атака "man-in-the-middle". Идея криптографического протокола цифровой подписи Диффи-Хеллмана.

Тема 2. Модель интерактивной системы доказателства.

Определение интерактивной системы доказательства. Пример интерактивной системы доказательства, основанный на теории чисел. Свойства интерактивной системы доказательства. Доказательства с нулевым разглашением. Задача"пещера Али-Бабы". Структура доказательств с нулевым разглашением. Вероятностные доказательства.

Тема 3. Протоколы совместных вычислений.

Формализованная постановка задачи многосторонних вычислений. Требования к безопасности многосторонних вычислений. Пример решения задачи миллионеров. Проблемы реализации. Пример протокола - удаленное подбрасывание монеты. Реалзация криптографического протокола подбрасывания монеты. Практическое применение.

Тема 4. Протоколы разделения секрета.

Постановка проблемы разделения секрета. Примеры: кодовый замок и проекции геометрических фигур. Криптографический протокол разделения секрета. Пороговые системы. Схема Блекли. Схема Шамира. Схема на основе китайской теоремы об остатаках. Совершенные и идеальные схемы разделенгия секрета. Приложения.

Тема 5. Протоколы анонимности.

Формализованная постановка задачи обеспечения анонимности. Задача о трех обеда.щих криптографах. Вариант решения задачи об обедающих криптографах. Идеи Дэвида Чаума обеспечения анонимности в сети. Протокол тайного цифрового голосования. Формальные требования к системам цифрового голосования. Пример простого протокола. Протокол Фудзиока-Окамото-Охта.

Тема 6. Протоколы консенсуса.

Формализованная постановка задачи обеспечения консенсуса в сети. Обычные ошибки и византийские ошибки. Задача византийских генералов. Протокол Delegated Byzantine Fault Tolerance. Протокол Practical Byzantine Fault Tolerance. Протокол Federated Byzantine Agreement. Протоколы криптовалют: Proof-of-Work, Proof-of-Stake, Delegated Proof-of-Stake. Протоколы не для блокчейна.

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 3			
	Текущий контроль		
1	Контрольная работа	ПК-4 , ПК-3 , ПК-2	3. Протоколы совместных вычислений. 4. Протоколы разделения секрета.
2	Контрольная работа	ПК-2 , ПК-3 , ПК-4	5. Протоколы анонимности.
3	Курсовая работа по дисциплине	ПК-2 , ПК-3 , ПК-4	6. Протоколы консенсуса.
	Зачет	ПК-2, ПК-3, 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 3					
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
Курсовая работа по дисциплине	Продемонстрирован высокий уровень владения материалом по теме работы. Использованы надлежащие источники в нужном количестве. Структура работы и применённые методы соответствуют поставленным задачам. Работа характеризуется оригинальностью, теоретической и/или практической ценностью. Оформление соответствует требованиям.	Продемонстрирован средний уровень владения материалом по теме работы. Использованы надлежащие источники. Структура работы и применённые методы в целом соответствуют поставленным задачам. Работа в достаточной степени самостоятельна. Оформление в основном соответствует требованиям.	Продемонстрирован низкий уровень владения материалом по теме работы. Использованные источники, методы и структура работы частично соответствуют её задачам. Уровень самостоятельности низкий. Оформление частично соответствует требованиям.	Продемонстрирован неудовлетворительный уровень владения материалом по теме работы. Использованные источники, методы и структура работы не соответствуют её задачам. Работа несамостоятельна. Оформление не соответствует требованиям.	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 3

Текущий контроль

1. Контрольная работа

Темы 3, 4

1.Требования к безопасности многосторонних вычислений.
2. Задача миллионеров.
3. Удаленное подбрасывание монеты.
4. Протокол знания дискретного логарифма.
5. Кодовый замок и проекции геометрических фигур.
6. Схема Блекли.
7. Схема Шамира.
8. Схема на основе китайской теоремы об остатаках.
9. Совершенные схемы разделенгия секрета.

10. Идеальные схемы разделения секрета.

2. Контрольная работа

Тема 5

1. Интерактивная система доказательства.
2. Нулевое разглашение.
3. Теоретико графовая интерпретация.
4. Задача о трех обедающих криптографах.
5 Анонимности в сети.
6. Протокол тайного цифрового голосования.
7. Формальные требования к системам цифрового голосования.
8. Пример простого протокола.
9. Протокол Фудзиока-Окамото-Охта.
10. Приложения.

3. Курсовая работа по дисциплине

Тема 6

1. Формализованная постановка задачи обеспечения консенсуса в сети.
2. Мажоритарные системы.
3. Византийские ошибки.
4. Задача византийских генералов.
4. Протокол Delegated Byzantine Fault Tolerance.
5. Протокол Practical Byzantine Fault Tolerance.
6. Протокол Federated Byzantine Agreement.
7. Протокол Proof-of-Work.
8. Протокол Proof-of-Stake.
9. Протокол Delegated Proof-of-Stake.
10. Протоколы не для блокчейна.

Зачет

Вопросы к зачету:

1.История возникновения криптографических протоколов. Односторонние функции и гипотеза о существовании односторонних функций.

2. Идеи Диффи-Хеллмана. Криптографический протокол формирования ключей Диффи-Хеллмана.

3. Атака "man-in-the-middle". Идея криптографического протокола цифровой подписи Диффи-Хеллмана.

4. Определение интерактивной системы доказательства. Пример интерактивной системы доказательства, основанный на теории чисел. Свойства интерактивной системы доказательства.

5. Доказательства с нулевым разглашением. Задача"пещера Али-Бабы".

6. Структура доказательств с нулевым разглашением. Вероятностные доказательства.

7. Постановка проблемы разделения секрета. Примеры: кодовый замок и проекции геометрических фигур. Криптографический протокол разделения секрета.

8. Пороговые системы. Схема Блекли.

9. Схема Шамира.

10. Схема на основе китайской теоремы об остатаках. Совершенные и идеальные схемы разделенгия секрета.

11. Формализованная постановка задачи многосторонних вычислений. Требования к безопасности многосторонних вычислений.

12. Реализация криптографического протокола подбрасывания монеты. Практическое применение.

13. Формализованная постановка задачи обеспечения анонимности.

14 Задача о трех обеда.щих криптографах. Вариант решения задачи об обедающих криптографах.

15. Идеи Дэвида Чаума обеспечения анонимности в сети. Протокол тайного цифрового голосования. Формальные требования к системам цифрового голосования.

16. Пример простого протокола.

17. Протокол Фудзиока-Окамото-Охта.

18. Формализованная постановка задачи обеспечения консенсуса в сети. Обычные ошибки и византийские ошибки. Задача византийских генералов.

19. Протокол Delegated Byzantine Fault Tolerance. Протокол Practical Byzantine Fault Tolerance. Протокол Federated Byzantine Agreement.

20. Протоколы криптовалют: Proof-of-Work, Proof-of-Stake, Delegated Proof-of-Stake. Протоколы не для блокчейна.

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 3			
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	15 15
Курсовая работа по дисциплине	Курсовую работу по дисциплине обучающиеся пишут самостоятельно дома. Темы и требования к работе формулирует преподаватель. Выполненная работа сдаётся преподавателю в сброшюрованном виде. В работе предлагается собственное решение определённой теоретической или практической проблемы. Оцениваются проработка источников, применение исследовательских методов, проведение отдельных стадий исследования, формулировка выводов, соблюдение требований к структуре и оформлению работы, своевременность выполнения.	3	20
Зачет	Зачёт нацелен на комплексную проверку освоения дисциплины. Обучающийся получает вопрос (вопросы) либо задание (задания) и время на подготовку. Зачёт проводится в устной, письменной или компьютерной форме. Оценивается владение материалом, его системное освоение, способность применять нужные знания, навыки и умения при анализе проблемных ситуаций и решении практических заданий.		50

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

7.1 Основная литература:

1. Кельберт, М.Я. Вероятность и статистика в примерах и задачах. Т.3: Теория информации и кодирования [Электронный ресурс] /
М.Я. Кельберт, Ю.М. Сухов. - Электрон. дан. - Москва : МЦНМО, 2016. - 567 с.
Режим доступа: https://e.lanbook.com/book/80125

2. Штарьков, Ю.М. Универсальное кодирование. Теория и алгоритмы [Электронный ресурс] : учебное пособие / Ю.М. Штарьков. ? Электрон. дан. - Москва : Физматлит, 2013. - 288 с.
Режим доступа: https://e.lanbook.com/book/59667

3. Основы теории кодирования: Учебное пособие /
Кудряшов Б.Д. - СПб:БХВ-Петербург, 2016. - 400 с. ISBN 978-5-9775-3527-4
Режим доступа: http://znanium.com/catalog/product/944069

4. Криптографическая защита информации : учеб. пособие /
С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.]; под ред. проф. С.О. Крамарова. - М. : РИОР : ИНФРА-М, 2018. - 321 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1716-6
Режим доступа: http://znanium.com/catalog/product/901659

5. Введение в криптографию. Курс лекций / В.А. Романьков. - 2-е изд., испр. и доп. - М. : ФОРУМ : ИНФРА-М, 2018. - 240 с. - (Высшее образование: Бакалавриат).
Режим доступа: http://znanium.com/catalog/product/924700

7.2. Дополнительная литература:

1. Сидельников, В. М. Теория кодирования [Электронный ресурс] / В. М. Сидельников. - М.: ФИЗМАТЛИТ, 2008. - 324 с.

URL: http://znanium.com/bookread2.php?book=544713

2. Масленников М. Е. Практическая криптография: Пособие / Масленников М.Е. СПб:БХВ-Петербург, 2015. - 465 с.
URL: http://znanium.com/bookread2.php?book=944503

3. 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.
URL: http://znanium.com/bookread.php?book=474838

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

5. Искусство защиты и взлома информации: Пособие / Скляров Д.В. - СПб:БХВ-Петербург, 2014. - 289 с.
URL: http://znanium.com/bookread2.php?book=940261

6. Чечёта, С.И. Введение в дискретную теорию информации и кодирования [Электронный ресурс] : учеб. пособие - Электрон. дан. - Москва : МЦНМО, 2011. - 224 с.
URL: https://e.lanbook.com/book/9437

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

Интернет-портал образовательных ресурсов по ИТ - http://www.intuit.ru
Интернет--портал ресурсов по математическим наукам - http://www.math.ru/
Интернет--портал ресурсов по математическим наукам - http://www.mathnet.ru
Интернет--портал ресурсов по математическим наукам - http://www.allmath.com/
Интернет-портал со статьями по алгоритмике и программированию - http://algolist.manual.ru/

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

Вид работ	Методические рекомендации
лабораторные работы	Лабораторные занятия призваны дать такой практический навык, а также навыки программирования криптографических алгоритмов и их внедрения в информационные системы. В ходе выполнения работ происходит отработка знаний студентов по программированию криптографических алгоритмов, изучение специальных разделов программирования алгоритмов сетевого взаимодействия.
самостоятельная работа	Самостоятельная работа предполагает выполнение домашних работ при подготовке к контрольной работе и выполнении компьютерной программы. Самостоятельная работа выполняется в несколько этапов. Сначала предполагается изучение теоретического материала. Также рекомендуется каждый раздел программы сопровождать практической работой, выполняя лабораторные занятия
контрольная работа	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.
курсовая работа по дисциплине	Курсовая работа по дисциплине предназначена закрепления практических навыков работы с алгоритмами криптографии, расширения кругозора и поучения новых теоретических знаний. Курсовая работа состоит из теоретической части, описывающей соответствующий алгоритм, историю его создания, особенности использование, и практическую часть, описывающую программную реализацию исследуемого алгоритма.

Вид работ	Методические рекомендации
зачет	Рекомендуется разбивать материал на смысловые блоки и изучать его, выписывая краткое содержание блока. По каждому блоку надо составить контрольные вопросы и самостоятельно составить краткие ответы по вопросам. Прочитав конспекты теоретического материала, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи зачета минимум и дополнительная литература.

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

Освоение дисциплины "Введение в компьютерную безопасность" 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

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.

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

Освоение дисциплины "Введение в компьютерную безопасность" 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.

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 01.04.02 "Прикладная математика и информатика" и магистерской программе Открытая информатика .