МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Елабужский институт (филиал)
Факультет математики и естественных наук

УТВЕРЖДАЮ
Директор Елабужского института КФУ
Мерзон Е.Е.
"___" _____20___ г.

подписано электронно-цифровой подписью

Программа дисциплины

Информационная безопасность Б1.В.ДВ.05.01

Направление подготовки: 44.04.01 - Педагогическое образование
Профиль подготовки: Цифровое образование
Квалификация выпускника: магистр
Форма обучения: заочное
Язык обучения: русский
Год начала обучения по образовательной программе: 2019
Автор(ы): Галимуллина Э.З.
Рецензент(ы): Ибатуллин Р.Р.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Анисимова Т. И.
Протокол заседания кафедры No ___ от "____" _____ 20__г.
Учебно-методическая комиссия Елабужского института КФУ (Факультет математики и естественных наук):
Протокол заседания УМК No ____ от "____" _____ 20__г.

Содержание

Программу дисциплины разработал(а)(и) старший преподаватель, б/с Галимуллина Э.З. (Кафедра математики и прикладной информатики, Факультет математики и естественных наук), EZGalimullina@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	Способен проектировать организацию совместной и индивидуальной учебной и воспитательной деятельности обучающихся, в том числе с особыми образовательными потребностями
ПК-1	Способен самостоятельно и в команде осваивать цифровые инструменты на аппаратном и программном уровне.
ПК-3	Способен реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов с использованием самых современных методик и технологий

Выпускник, освоивший дисциплину:

Должен знать:

виды угроз ИС и методы обеспечения информационной безопасности;

технические и программные средства обеспечения безопасности информационных систем;

методику выбора оптимального решения по уровню информационной безопасности как компромисса между различными требованиями, связанными с безопасностью, качеством разработки, стоимостью и сроками выполнения работ;

основные понятия и задачи криптографии;

способы разграничения доступа и средства их реализации;

отечественные и зарубежные стандарты в области информационной безопасности;

Должен уметь:

использовать в практической деятельности существующие методы и средства контроля и защиты информации;

применять программные пакеты для шифрования;

владеть средствами борьбы с компьютерными вирусами.

Должен владеть:

инструментальными средствами проектирования баз данных и знаний, управления проектами ИС и защиты информации, а также иметь представление о перспективах развития и организации систем комплексной защиты информации;

методами анализа программных реализаций алгоритмов защиты.

Должен демонстрировать способность и готовность:

реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов;

использовать систематизированные теоретические и практические знания для постановки и решения исследовательских задач в области образования.

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 44.04.01 "Педагогическое образование (Цифровое образование)" 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 - 16 часа(ов), в том числе лекции - 6 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 10 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 52 часа(ов).

Контроль (зачёт / экзамен) - 4 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. Основные понятия и анализ угроз информационной безопасности.	3	2	0	0	10
2.	Тема 2. Политики безопасности. Модели политик безопасности	3	2	0	2	8
3.	Тема 3. Стандарты информационной безопасности	3	2	0	0	8
4.	Тема 4. Криптографическая защита информации.	3	0	0	4	16
5.	Тема 5. Технологии аутентификации.	3	0	0	4	10
	Итого		6	0	10	52

4.2 Содержание дисциплины

Тема 1. Основные понятия и анализ угроз информационной безопасности.

Основные понятия и анализ угроз информационной безопасности. Основные понятия информационной безопасности. Общие понятия информационной безопасности. Анализ угроз информационной безопасности. Классификация угроз информационным системам. Основные методы обеспечения информационной безопасности информационных систем.

Тема 2. Политики безопасности. Модели политик безопасности

Политика безопасности. Общие принципы моделей политик безопасности. Классификация существующих моделей политики информационной безопасности. Свободные и мандатные модели политик безопасности. Модель Белла - Ла-Падулы. Модель Биба. Модель контроля целостности Кларка-Вилсона. Политика избирательного разграничения доступа. Анализ моделей политик безопасности.

Тема 3. Стандарты информационной безопасности

Стандарты информационной безопасности. Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Отечественные стандарты безопасности информационных технологий. Государственные (национальные) стандарты РФ. Руководящие документы. Нормативные документы информационной безопасности.

Тема 4. Криптографическая защита информации.

Криптографическая защита информации. Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Функция хэширования. Электронная цифровая подпись. Методы криптографической защиты информации. Простейшие алгоритмы шифрования (Система шифрования Цезаря, Простая моноалфавитная замена, G-контурная многоалфавитная замена, Простая перестановка, Перестановки Гамильтона). Элементы криптоанализа. Оценка частотности символов в тексте.

Тема 5. Технологии аутентификации.

Технологии аутентификации. Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие пароли и PIN-коды. Биометрическая аутентификация пользователя. Аппаратно-программные системы идентификации и аутентификации. Подсистемы парольной аутентификации пользователей. Генераторы паролей. Оценка степени стойкости парольной защиты. Биометрическая аутентификация пользователя по клавиатурному почерку. Анализ динамики нажатия клавиш.

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 29 декабря 2018 г. № 0.1.1.67-08/328 "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 3			
	Текущий контроль		
1	Устный опрос	ОПК-3 , ПК-3	1. Основные понятия и анализ угроз информационной безопасности. 2. Политики безопасности. Модели политик безопасности 3. Стандарты информационной безопасности 4. Криптографическая защита информации. 5. Технологии аутентификации.
2	Реферат	ОПК-3 , ПК-1 , ПК-3	1. Основные понятия и анализ угроз информационной безопасности. 2. Политики безопасности. Модели политик безопасности 3. Стандарты информационной безопасности 4. Криптографическая защита информации. 5. Технологии аутентификации.
3	Лабораторные работы	ПК-1 , ПК-3	2. Политики безопасности. Модели политик безопасности 4. Криптографическая защита информации. 5. Технологии аутентификации.
	Зачет	ОПК-3, ПК-1, ПК-3	

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					
Устный опрос	В ответе качественно раскрыто содержание темы. Ответ хорошо структурирован. Прекрасно освоен понятийный аппарат. Продемонстрирован высокий уровень понимания материала. Превосходное умение формулировать свои мысли, обсуждать дискуссионные положения.	Основные вопросы темы раскрыты. Структура ответа в целом адекватна теме. Хорошо освоен понятийный аппарат. Продемонстрирован хороший уровень понимания материала. Хорошее умение формулировать свои мысли, обсуждать дискуссионные положения.	Тема частично раскрыта. Ответ слабо структурирован. Понятийный аппарат освоен частично. Понимание отдельных положений из материала по теме. Удовлетворительное умение формулировать свои мысли, обсуждать дискуссионные положения.	Тема не раскрыта. Понятийный аппарат освоен неудовлетворительно. Понимание материала фрагментарное или отсутствует. Неумение формулировать свои мысли, обсуждать дискуссионные положения.	1
Реферат	Тема раскрыта полностью. Продемонстрировано превосходное владение материалом. Использованы надлежащие источники в нужном количестве. Структура работы соответствует поставленным задачам. Степень самостоятельности работы высокая.	Тема в основном раскрыта. Продемонстрировано хорошее владение материалом. Использованы надлежащие источники. Структура работы в основном соответствует поставленным задачам. Степень самостоятельности работы средняя.	Тема раскрыта слабо. Продемонстрировано удовлетворительное владение материалом. Использованные источники и структура работы частично соответствуют поставленным задачам. Степень самостоятельности работы низкая.	Тема не раскрыта. Продемонстрировано неудовлетворительное владение материалом. Использованные источники недостаточны. Структура работы не соответствует поставленным задачам. Работа несамостоятельна.	2
Лабораторные работы	Оборудование и методы использованы правильно. Проявлена превосходная теоретическая подготовка. Необходимые навыки и умения полностью освоены. Результат лабораторной работы полностью соответствует её целям.	Оборудование и методы использованы в основном правильно. Проявлена хорошая теоретическая подготовка. Необходимые навыки и умения в основном освоены. Результат лабораторной работы в основном соответствует её целям.	Оборудование и методы частично использованы правильно. Проявлена удовлетворительная теоретическая подготовка. Необходимые навыки и умения частично освоены. Результат лабораторной работы частично соответствует её целям.	Оборудование и методы использованы неправильно. Проявлена неудовлетворительная теоретическая подготовка. Необходимые навыки и умения не освоены. Результат лабораторной работы не соответствует её целям.	3
	Зачтено		**Не зачтено**		
Зачет	Обучающийся обнаружил знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности, справился с выполнением заданий, предусмотренных программой дисциплины.		Обучающийся обнаружил значительные пробелы в знаниях основного учебно-программного материала, допустил принципиальные ошибки в выполнении предусмотренных программой заданий и не способен продолжить обучение или приступить по окончании университета к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.		

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

Семестр 3

Текущий контроль

1. Устный опрос

Темы 1, 2, 3, 4, 5

1. Охарактеризуйте направление "криптография". Что называют криптографическим ключом?
2. Проклассифицируйте традиционные алгоритмы шифрования. Кратко охарактеризуйте эти классы.
3. Охарактеризуйте методы шифрования Цезаря, простую моноалфавитную замену, G-контурную многоалфавитную замену, простую перестановку, перестановки Гамильтона.
4. Что понимается под криптоанализом?
5. Что понимают под криптоанализом?
6. Охарактеризуйте методику криптоанализа, основанную на исследовании частотности закрытого текста.
7. Сформулируйте правило А. Керхоффа.
8. Что понимается под идентификацией и аутентификацией пользователя?
9. Чем определяется стойкость к взлому подсистемы идентификации и аутентификации пользователя?
10. Перечислите основные требования к выбору пароля и к реализации подсистемы парольной аутентификации пользователя.
11. Как количественно оценить стойкость подсистемы парольной аутентификации к взлому?
12. Как изменится стойкость к взлому подсистемы парольной аутентификации при увеличении характеристик P,V,T? При их уменьшении?

2. Реферат

Темы 1, 2, 3, 4, 5

Примерная тематика рефератов

1. Технические каналы утечки информации.
2. Выявление технических каналов утечки информации.
3. Организация и проведение поисковых мероприятий на объекте с целью обнаружения каналов утечки информации, выявления средств съема информации.
4. Методы и средства защиты информации от утечки по техническим каналам.
5. Информационная безопасность в среде Windows NT.
6. Информационная безопасность на основе Novell NetWare
7. Информационная безопасность на основе Unix.
8. Вопросы безопасности электронной торговли.
9. Защита Internet-торговли: инфраструктура и стандарты.
10. Криптография для электронной коммерции.
11. Нормативно-правовые аспекты электронного бизнеса.
12. Безопасность при работе в Интернет.
13. Стеганография - искусство сокрытия самого факта передачи информации
14. Интеллектуальная собственность в области программных продуктов.
15. Защита баз данных.
16. Защита от несанкционированного доступа.
17. Вирусы и вредоносные программы.
18. Комплексное обеспечение информационной безопасности в коммерческих структурах.
19. Исследование места и роли проблем информационной безопасности в становлении современного информационного общества.
20. Исследование проблем обеспечения баланса интересов личности, общества и государства в информационной сфере.
21. Исследование роли и места информационной безопасности в обеспечении военной, экономической, экологической, иных видов национальной безопасности.
22. Национальные интересы России и информационное противостояние в современном мире.
23. Ценностная ориентация личности, ее информационное обоснование.
24. Информационная безопасность и политическая этика.
25. Информационное пространство и проблема целостности российского государства.
26. Исследование места и роли СМИ в решении задач информационного обеспечения государственной политики Российской Федерации.
27. Правовые механизмы регулирования в сфере производства и эксплуатации криптографических продуктов.
28. Разработка правовых механизмов регулирования электронного документооборота.
29. Проблемы правового обеспечения создания и функционирования системы мониторинга угроз информационных атак на критически важные сегменты информационной инфраструктуры Российской Федерации.
30. Разработка и научное обоснование путей обеспечения информационно-психологической безопасности личности и общества.
31. Исследование проблем обеспечения информационной безопасности национальных платежных систем на базе российских интеллектуальных карт.
32. Исследование проблем создания и развития национальной системы управления цифровыми сертификатами.

33. Разработка методов и средств проведения экспертизы и контроля качества защиты информации и информационных ресурсов, в том числе вопросов оценки базовых общесистемных программных средств на соответствие требованиям информационной безопасности.
34. Разработка методов и средств обеспечения информационной безопасности информационных и телекоммуникационных систем, в том числе автоматизированных систем управления безопасностью, методов и средств распределения ключей и защиты информации и информационных ресурсов от несанкционированного доступа и разрушающего информационного воздействия, антивирусных технологий, решение проблемы гарантированного уничтожения остаточной информации на магнитных носителях, исследование и развитие методов построения защищенных систем, использующих ненадежные (с точки зрения информационной безопасности) элементы, включая проблему их тестирования.
35. Исследование проблем безопасности общероссийской информационной инфраструктуры в условиях ее вхождения в глобальные инфраструктуры.
36. Исследование проблем обеспечения информационной безопасности ИТКС, в том числе разработка нормативно-технической документации по безопасности, автоматизированных систем управления безопасностью, унифицированного ряда средств процесса защиты с учетом используемых в ИТКС технологий обработки информации.
37. Исследование проблем информационной безопасности корпоративных сетей, в том числе сетей науки и образования (в рамках комплексной программы Минпромнауки России "Научное, научно-методическое, материально-техническое и информационное обеспечение системы образования").
38. Проблемы лицензирования деятельности в области информационно-телекоммуникационных систем.
39. Анализ тенденций в развитии глобальной информационной сети и состояния участия в ней России.
40. Разработка фундаментальных проблем теоретической криптографии и смежных с ней областей математики.
41. Разработка криптографических проблем создания перспективных отечественных шифрсистем (в частности, высокоскоростных).
42. Разработка и обоснование новых методов криптографического анализа современных шифрсистем.
43. Разработка перспективных криптографических протоколов взаимодействия абонентов в сложных иерархических глобальных сетях и распределенных информационно-аналитических системах.
44. Исследование существующих и разработка новых систем с открытым ключом, соответствующих этим системам схем аутентификации и электронной цифровой подписи.
45. Совершенствование нормативно-методической базы по вопросам защиты информации с применением криптографических средств.
46. Анализ основных направлений и тенденций развития отечественных и зарубежных средств криптографической защиты информации.
47. Анализ возможности использования достижений физики и техники для получения доступа к информации, обрабатываемой на современных технических средствах, в том числе исследование физических основ утечки информации от технических средств по побочным каналам, разработку проблем аналитической обработки побочных сигналов.
48. Исследование алгоритмических и технологических особенностей новейших зарубежных и отечественных технических средств обработки информации.
49. Исследование проблем и методов информационного доступа к каналам связи.
50. Разработка методологии оценивания защищенности, комплексных методов и средств защиты технических средств обработки информации от физико-технических методов несанкционированного доступа, совершенствование соответствующей нормативной базы.
51. Разработка проблем создания технических средств обработки информации, защищенных от физико-технических методов информационного доступа.
52. Сравнительный анализ тенденций развития физико-технических проблем защиты информации в стране и за рубежом.
53. Исследование архитектурных вариантов построения вычислительных систем высокой производительности, алгоритмического и программного обеспечения с учетом особенностей криптографических задач.
54. Исследование проблем построения автоматизированных систем обработки криптографической информации в неоднородной вычислительной среде.
55. Исследование проблем управления распределенными вычислительными процессами.
56. Разработка и научное обоснование моделей угроз и стратегий защиты объектов от технических разведок.
57. Разработка методов и средств противодействия техническим разведкам с учетом эффективности их функционирования.
58. Разработка методов и средств контроля состояния и достаточности принимаемых мер по противодействию техническим разведкам на объектах защиты.
59. Разработка современной методологии обеспечения противодействия техническим разведкам на объектах защиты.
60. Разработка, теоретическое и экспериментальное исследование современных методов стеганографии, других средств тайнописи и защиты от подделки.
61. Исследование и разработка отечественных защитных экранов с учетом моделей угроз для уже существующих и перспективных цифровых АТС.
62. Проблемы кадрового обеспечения информационной безопасности Российской Федерации.

63. Обоснование облика, структуры и путей реализации единой системы подготовки кадров в области современных информационных технологий и информационной безопасности.
64. Обоснование структуры и функций Учебно-методического комплекса по подготовке, повышению квалификации и переподготовке кадров в области информационной безопасности.

3. Лабораторные работы

Темы 2, 4, 5

Тема. Криптографическая защита информации.

Лабораторная работа 1.

Методы криптографической защиты информации. Простейшие алгоритмы шифрования (Система шифрования Цезаря, Простая моноалфавитная замена, G-контурная многоалфавитная замена, Простая перестановка, Перестановки Гамильтона).

Лабораторная работа 2.

Элементы криптоанализа. Оценка частотности символов в тексте.

Тема. Технологии аутентификации.

Лабораторная работа 3.

Подсистемы парольной аутентификации пользователей. Генераторы паролей. Оценка степени стойкости парольной защиты.

Зачет

Вопросы к зачету:

1. Основные понятия информационной безопасности.
2. Классификация угроз информационным системам. Неумышленные и умышленные угрозы.
3. Классификация угроз информационным системам (отказ в услуге, незаконное использование привилегий, "скрытые каналы", "маскарад", "сборка мусора", "люки").
4. Классификация угроз информационным системам (вредоносные программы: вирус, троянский конь, червяк, жадная программа, бактерия, логическая бомба, лазейки).
5. Основные методы обеспечения безопасности информационных систем. Правовое обеспечение безопасности.
6. Основные методы обеспечения безопасности информационных систем. Организационно-административное обеспечение.
7. Основные методы обеспечения безопасности информационных систем. Инженерно-технические меры обеспечения безопасности.
8. Основные методы обеспечения безопасности информационных систем. Основные функции технических средств подсистем безопасности.
9. Основные методы обеспечения безопасности информационных систем. Механизмы реализации функций технических средств подсистем безопасности.
10. Модели политик безопасности. Свободный и мандатный контроли за доступом.
11. Модели политик безопасности. Мандатные политики безопасности.
12. Модели политик безопасности. Модель Белла-Ла-Падулы.
13. Модели политик безопасности. Модель Биба.
14. Модели политик безопасности. Модель контроля целостности Кларка-Вилсона.
15. Модели политик безопасности. Политики избирательного разграничения доступа.
16. Идентификация и аутентификация субъектов.
17. Парольные системы идентификации и аутентификации пользователей. Основные требования к выбору и использованию паролей.
18. Парольные системы идентификации и аутентификации пользователей. Количественная оценка стойкости парольных систем.
19. Идентификация и аутентификация пользователей с использованием технических устройств.
20. Идентификация и аутентификация с использованием индивидуальных биометрических характеристик пользователя.
21. Криптографические методы защиты информации. Основные понятия криптографии.
22. Криптографические методы защиты информации. Классификация криптографических алгоритмов.
23. Криптоалгоритмы с ключом. Симметричные и асимметричные криптогалгоритмы.
24. Криптографические методы защиты информации. Виды атак на шифры.
25. Традиционные симметричные криптосистемы. Шифрование методом замены. Шифрование методом цезаря.
26. Традиционные симметричные криптосистемы. Шифрование методом замены. Простая моноалфавитная замена.
27. Традиционные симметричные криптосистемы. Шифрование методом замены. Шифрующие таблицы Трисемуса.
28. Традиционные симметричные криптосистемы. Шифрование методом замены. Многооалфавитная замена. Шифр Гронсфельда.
29. Традиционные симметричные криптосистемы. Шифрование методом замены. Многооалфавитная замена. Система шифрования Вижинера.
30. Традиционные симметричные криптосистемы. Шифрование методом замены. Многооалфавитная замена. Шифрование методом Вернама.

31. Традиционные симметричные криптосистемы. Шифрование методом замены. Многооалфавитная замена. G-контурная многоалфавитная замена.
32. Традиционные симметричные криптосистемы. Шифрование методами перестановки. Метод простой перестановки.
33. Традиционные симметричные криптосистемы. Шифрование методами перестановки по маршрутам Гамильтона.
34. Традиционные симметричные криптосистемы. Шифрование методами перестановки. Шифрование методом гаммирования.
35. Симметричные криптосистемы шифрования. Основные принципы блочного симметричного шифрования.
36. Симметричные криптосистемы шифрования. Алгоритм шифрования DES.
37. Симметричные криптосистемы шифрования. Комбинирование блочных алгоритмов.
38. Симметричные криптосистемы шифрования. Стандарт шифрования ГОСТ 28147-89.
39. Симметричные криптосистемы шифрования. Американский стандарт шифрования AES.
40. Симметричные криптосистемы шифрования. Другие симметричные криптоалгоритмы.
41. Симметричные криптосистемы шифрования. Особенности применения алгоритмов симметричного шифрования.
42. Асимметричные криптосистемы шифрования. Особенности асимметричных криптосистем шифрования.
43. Асимметричные криптосистемы шифрования. Алгоритм шифрования RSA.
44. Асимметричные криптосистемы шифрования. Прцедуры шифрования и расшифрования в алгоритме RSA.
45. Асимметричные криптосистемы шифрования. Асимметричные криптосистемы на базе эллиптических кривых.
46. Асимметричные криптосистемы шифрования. Алгоритм асимметричного шифрования ECES.

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			
Устный опрос	Устный опрос проводится на практических занятиях. Обучающиеся выступают с докладами, сообщениями, дополнениями, участвуют в дискуссии, отвечают на вопросы преподавателя. Оценивается уровень домашней подготовки по теме, способность системно и логично излагать материал, анализировать, формулировать собственную позицию, отвечать на дополнительные вопросы.	1	10
Реферат	Обучающиеся самостоятельно пишут работу на заданную тему и сдают преподавателю в письменном виде. В работе производится обзор материала в определённой тематической области либо предлагается собственное решение определённой теоретической или практической проблемы. Оцениваются проработка источников, изложение материала, формулировка выводов, соблюдение требований к структуре и оформлению работы, своевременность выполнения. В случае публичной защиты реферата оцениваются также ораторские способности.	2	10
Лабораторные работы	В аудитории, оснащённой соответствующим оборудованием, обучающиеся проводят учебные эксперименты и тренируются в применении практико-ориентированных технологий. Оцениваются знание материала и умение применять его на практике, умения и навыки по работе с оборудованием в соответствующей предметной области.	3	30

Форма контроля	Процедура оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций	Этап	Количество баллов
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.Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин В. Ф. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2016. - 416 с. - URL: http://znanium.com/bookread2.php?book=549989

2. Жук А. П., Жук Е. П., Лепешкин О. М., Тимошкин А. И. 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.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6 - Режим доступа: http://znanium.com/bookread2.php?book=474838

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

7.2. Дополнительная литература:

1. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие/ГлинскаяЕ.В., ЧичваринН.В. - М.: НИЦ ИНФРА-М, 2016. - 118 с. - URL: http://znanium.com/bookread2.php?book=507334

2. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - URL: http://znanium.com/bookread2.php?book=405000

3. Информационная безопасность предприятия: Учебное пособие / Гришина Н.В., - 2-е изд., доп - М.:Форум, НИЦ ИНФРА-М, 2016. - 240 с. - URL: http://znanium.com/bookread2.php?book=544554

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

Антивирусная защита компьютерных систем НОЧУ ВПО "Национальный открытый университет "ИНТУИТ" - http://www.intuit.ru/studies/courses/2259/155/info

Барсуков В., Физическая защита информационных систем - http://www.jetinfo.ru/1997/1/1/article1.1.1997.html

Беззубцев О., Ковалев А., О лицензировании и сертификации в области защиты информации - http://www.jetinfo.ru/1997/4/1/article1.4.1997.html

Браунли Н., Гатмэн Э., Как реагировать на нарушения информационной безопасности (RFC 2350, BCP 21) - http://www.jetinfo.ru/2000/5/1/article1.5.2000.html

Винклер А., Задание: шпионаж - http://www.jetinfo.ru/1996/19/1/article1.19.1996.html

Основы информационной безопасности В.Галатенко НОЧУ ВПО "Национальный открытый университет "ИНТУИТ" - http://www.intuit.ru/studies/courses/10/10/info

Симонов С., Анализ рисков, управление рисками - http://www.jetinfo.ru/1999/1/1/article1.1.1999.html

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

Вид работ	Методические рекомендации
лекции	В ходе лекционных занятий следует вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание темы, научные выводы и практические рекомендации. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, практических рекомендаций, разрешения проблемных ситуаций. В ходе подготовки к лекционным занятиям повторить изложенный ранее учебный материал, ознакомиться с основной и дополнительной литературой, информацией из рекомендованных Интернет-ресурсов по изученной теме. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из рекомендованной основной и дополнительной литературы, Интернет-ресурсов по проблемным вопросам.
лабораторные работы	Выполнение лабораторных работ направлено на обобщение, систематизацию, углубление теоретических знаний; формирование умений применять полученные знания в практической деятельности; развитие аналитических, проектировочных, конструктивных умений; выработку самостоятельности, ответственности и творческой инициативы. В ходе выполнения лабораторной работы студент должен проявить умение самостоятельно работать с учебной и научной литературой, Интернет-ресурсами, продемонстрировать навыки владения компьютерной техникой и пакетами прикладных программ соответствующего назначения. Контрольной точкой лабораторной работы является ее защита. Защита проводится в устной форме: студент должен уметь объяснить и обосновать каждый выполненный этап работы.
самостоятельная работа	Самостоятельная работа по данной дисциплине включает: повторение теоретического материала; подготовка к лабораторным занятиям; подготовка к тестированию и зачету. Любая форма самостоятельной работы начинается с изучения конспекта лекции, соответствующей учебной и научной литературы, а также информации из рекомендованных Интернет-ресурсов. Во всех рекомендуемых учебниках и учебных пособиях содержатся контрольные вопросы, которые помогают повторить ключевые моменты соответствующей темы, и практические задания, нацеленные на выявление логических взаимосвязей.
устный опрос	При устном опросе устанавливается непосредственный контакт между преподавателем и студентом, в процессе которого преподаватель получает сведения об индивидуальных особенностях усвоения учебного материала. Устный опрос может состоять из вопросов, задач или примеров, которые будут предложены для проверки усвоения знаний. Для подготовки к устному опросу рекомендуется повторить изложенный ранее учебный материал, ознакомиться с основной и дополнительной литературой, информацией из рекомендованных Интернет-ресурсов по соответствующей теме дисциплины.
реферат	Подготовка рефератов направлена на развитие и закрепление навыков самостоятельного, творческого и всестороннего анализа научной, методической и другой литературы по актуальным проблемам дисциплины; на выработку навыков и умений грамотно и убедительно излагать материал, четко формулировать теоретические обобщения, выводы и практические рекомендации. В работе на заданную тему приводится обзор материала в определённой тематической области либо предлагается собственное решение теоретической или практической проблемы. Оцениваются анализ использованной литературы и Интернет-ресурсов, изложение материала, формулировка выводов, соблюдение требований к структуре и оформлению работы, своевременность выполнения.

Вид работ	Методические рекомендации
зачет	Зачет проводится в устной форме по билетам, в которых содержатся вопросы (задания) по всему разделу дисциплины. Оценивается владение теоретическим материалом, его системное освоение, взаимосвязь основных понятий дисциплины, способность применять знания и умения при решении практических заданий, приобретение навыков самостоятельной работы. Для подготовки к зачету рекомендуется повторить весь учебный материал по дисциплине, а также использовать основную и дополнительную литературу, информацию из рекомендованных Интернет-ресурсов.

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

Освоение дисциплины "Информационная 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

Браузер Google Chrome

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 "Информационная 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.

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 44.04.01 "Педагогическое образование" и магистерской программе Цифровое образование .