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. Д.А. Таюрский
_____ «___»_____20__г.

подписано электронно-цифровой подписью

Программа дисциплины

Комплексное обеспечение информационной безопасности Б1.Б.32

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность компьютерных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2019
Автор(ы): Ишмухаметов Ш.Т.
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.

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

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-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
ПК-13	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации

Выпускник, освоивший дисциплину:

Должен знать:

основные положения нормативно-правовых документов по обеспечению ин-формационной безопасности в экономических системах;

основные положения нормативно-правовых документов по обеспечению юридической значимости электронного документооборота;

основные требования нормативно-методических документов ФСБ России по организации и обеспечению функционирования шифровальных (криптографических) средств,

ипользуемых в банковских и экономических системах;

основные положения о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами;

методы и способы криптографической защиты информации;

принципы функционирования инфраструктуры открытых ключей;

Должен уметь:

строить адекватную модель функциональных процессов в сфере электронного документооборота в банковской и экономической сфере, применять понятия и методы

теории информационной безопасности для оценки экономических рисков и построения адекватной системы их предотвращения;

определять необходимость применения шифровальных (криптографических) средств в системе защиты информации организации (предприятия);

оценивать и выбирать шифровальные (криптографические) средства, кото-рые могут быть использованы при создании (дооборудовании) и дальнейшей эксплуатации информационных систем;

Должен владеть:

навыками работы с правовыми базами данных;

навыками разработки необходимых документов в интересах организации работ по защите информации ограниченного доступа с использованием

шифровальных (криптографических) средств;

навыками применения сертифицированных шифровальных (криптографических) средств для защиты экономической информации;

практическими навыками построения модели угроз и нарушителей ИБ в банковской сфере и экономике.

Должен демонстрировать способность и готовность:

Определять и обосновывать необходимость применения средств криптографической защиты информации для защиты банковской и бизнес информации;

аргументированно выбирать средства криптографической защиты информации, удовлетворяющие потребностям организации - обладателя информации;

правильно организовать эксплуатацию средств криптографической информации;

самостоятельно разрабатывать требуемую организационно-распорядительную документацию;

успешно эксплуатировать шифровальные (криптографические) средства;

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

Данная учебная дисциплина включена в раздел "Б1.Б.32 Дисциплины (модули)" основной профессиональной образовательной программы 10.03.01 "Информационная безопасность (Безопасность компьютерных систем)" и относится к базовой (общепрофессиональной) части.
Осваивается на 4 курсе в 7 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 - 72 часа(ов).

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

Форма промежуточного контроля дисциплины: зачет в 7 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 комплексное обеспечение информационной безопасности	7	4	0	4	8
2.	Тема 2. Классификация методов защиты информации для предприятий и организаций	7	4	0	4	10
3.	Тема 3. Организационно-правовые методы в системе компьютерной безопасности	7	4	0	4	10
4.	Тема 4. Физические методы защиты информации при хранении на компьютерах и передаче по сетям.	7	6	0	4	10
5.	Тема 5. Технические методы защиты в экономике и бизнесе	7	6	0	8	10
6.	Тема 6. Математические проблемы построения модели безопасности комплексных систем защиты данных.	7	6	0	6	12

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
7.	Тема 7. Обзор криптографических методов защиты информации в экономике и бизнесе. Защита банковской информации. Технология 3D - Secure.	7	6	0	6	12
	Итого		36	0	36	72

4.2 Содержание дисциплины

Тема 1. Введение в комплексное обеспечение информационной безопасности

Значение экономической и банковской информации в жизни современного общества. Проблемы защиты информации. Типы нарушений. Характеристика современных видов атак на банковские структуры и системы. Схема удаленной аутентификации в сетях электронной коммерции. Модель защиты 3D-secure. Основные участники электронного документооборота.

Тема 2. Классификация методов защиты информации для предприятий и организаций

Обзор методов и средств защиты банковской и экономической информации. Комплексный подход как современная парадигма решения задач в сфере безопасноти экономической информации. Физические, организационно-правовые и технические методы, особенности их применения в сфере безопасности экономической информации.

Тема 3. Организационно-правовые методы в системе компьютерной безопасности

Основные законы и постановления правительства РФ в сфере решения задач защиты информации в экономических системах. Основные положения федеральных закоов "Об электронной подписи" 2011 года, законы "О персональных данных", "О коммерческой информации" . Современные проблемы в сфере хранения и передаче конфиденциальной экономической информации.

Тема 4. Физические методы защиты информации при хранении на компьютерах и передаче по сетям.

Развертывание системы физической защиты информации на предприятии. Допуск сотрудников к к работе с конфиденциальной информацией. Технические средства ограничения и предупреждения несанкционированного допуска к экономической информации. Роль физических методов защиты в системе электронной коммерции.

Тема 5. Технические методы защиты в экономике и бизнесе

Разхворачивание системы комплексной защиты информации на предприятии, оценка информационных активов, анализ рисков и выбор адекватной системы защиты даных и содержащей ее инфраструктуры. Технические средства защиты информациии.

Криптографические методы защиты информации. Проверка данных удалённых пользователей.

Тема 6. Математические проблемы построения модели безопасности комплексных систем защиты данных.

Введение в проблематику математических проблем, связанных с защитой данных. Математические основы построения электронных цифровых подписей, проверка подлинности информации. Методы аутентификации и поддержки конфиденицальности в сфере экономики.

Использование сертифицированных средств аутентификации в банковской сфере.

Тема 7. Обзор криптографических методов защиты информации в экономике и бизнесе. Защита банковской информации. Технология 3D - Secure.

Криптографические методы и средства защиты информации: классические методы шифрования, хеш-функции, методы шифрования с открытым ключом.

Математические трудно разреши сын проблемы, используемые в криптографии. Проблема факторизации натуральных чисел. Алгоритм RSA. Проблема распределения ключей и её решение.

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 7			
	Текущий контроль		
1	Устный опрос	ПК-10	4. Физические методы защиты информации при хранении на компьютерах и передаче по сетям.
2	Контрольная работа	ПК-13	6. Математические проблемы построения модели безопасности комплексных систем защиты данных.
3	Научный доклад	ПК-15	3. Организационно-правовые методы в системе компьютерной безопасности
	Зачет	ОПК-7, ПК-10, ПК-13, ПК-4, ПК-5	

6.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Форма контроля	Критерии оценивания				Этап
	Отлично	**Хорошо**	**Удовл.**	**Неуд.**	
Семестр 7					

Форма контроля	Критерии оценивания				Этап
	Отлично	**Хорошо**	**Удовл.**	**Неуд.**	
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
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.	2
Научный доклад	Тема полностью раскрыта. Продемонстрирован высокий уровень владения материалом по теме работы. Использованы надлежащие источники в нужном количестве. Структура работы и применённые методы соответствуют поставленным задачам.	Тема в основном раскрыта. Продемонстрирован средний уровень владения материалом по теме работы. Использованы надлежащие источники. Структура работы и применённые методы в основном соответствуют поставленным задачам.	Тема частично раскрыта. Продемонстрирован удовлетворительный уровень владения материалом по теме работы. Использованные источники, структура работы и применённые методы частично соответствуют поставленным задачам.	Тема не раскрыта. Продемонстрирован неудовлетворительный уровень владения материалом по теме работы. Использованные источники, структура работы и применённые методы не соответствуют поставленным задачам.	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 7

Текущий контроль

1. Устный опрос

Тема 4

- Обсуждение современных требований к обеспечению комплексной защиты информации, анализ угроз;
- Обсуждение современных методов защиты информации, выбор и сравнение различных подходов к построению комплексной системы защиты;
- Классификация правовых методов в сфере системы защиты экономической информации. Разбор основных законов и постановлений в области защиты информации;
- Подготовить и разобрать порядок применения физических методы защиты информации на примере предприятия в экономической сфере;
- Подготовить и разобрать порядок применения физических методы защиты информации на примере предприятия в экономической сфере;
- Разобрать способы построения и виды электронных цифровых подписей их роль и правовые основы в экономической сфере. Использование криптографии для скрытия конфиденциальной информации.

2. Контрольная работа

Тема 6

Типовой вариант контрольной работы (отличия других вариантов заключаются с использовании других числовых данных).

1. Проверить число n=57 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 расширенный алгоритм Евклида: p=17, q=29, e=239, 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: n=779, e=277, m=625.

3. Научный доклад

Тема 3

Сделать обзорный доклад на заданную тему с области организационной правовых методов защиты информации. Использовать материалы соответствующих стандартов 27000-27016. Рассмотреть модели построения защит информации на предприятиях, выявить их сильные и слабые стороны. Изучить модели рисков и методы их улучшения.

Зачет

Вопросы к зачету:

1. Комплексная информационная безопасность автоматизированных систем:

1.1 Понятие информационной безопасности;

1.2 Информационные технологии и автоматизированные системы (АС);

1.3 Методологическая основа и принципы построения систем безопасности в АС;

1.4 Системы защиты информации в АС

2. Защита АС с помощью криптографических методов:

2.1 Симметричные системы шифрования Фундаментальная основа симметричных систем шифрования; Поточные шифры (RC4, SEAL и др.) Алгоритмы, методы реализации, применение; Блочные шифры (AES, DES, ГОСТ 28147-89.) Алгоритмы, методы реализации, применение; Хеш - функция

2.2 Системы шифрования с открытом ключом Фундаментальная основа систем шифрования с открытым ключом; Особенности системы, алгоритмы, методы и применение; Асимметричные шифры (RSA, DSA, Elgamal (Эль-Гамаля), Diffie-Hellman, ГОСТ Р34.11);

2.3 Инфраструктура открытых ключей (PKI) и ЭЦП Использование Электронной цифровой подписи (ЭЦП) Архитектура Инфраструктуры открытых ключей (ИОК\PKI); Управление отрытыми ключами. Удостоверяющий центр. Сертификаты. Аутентификация с использованием отрытых ключей

2.4 Правовое регулирование вопросов криптографической защиты Российская законодательная база в области криптографической защиты информации; Международные стандарты и соглашения в области криптографии; Специальные требования ФСБ к ФСТЭК к криптосредствам; Сертификация, аттестация и лицензирование СКЗИ

3. Защита обрабатываемых данных в АС в сетевом взаимодействии:

3.1 Технологии защита АС на платформе ОС MS Windows;

3.2 Технологии защита АС на платформе ОС GNU\Linux, Unix.

4. Специализированное ПО и программно-аппаратные комплексы защиты в АС:

4.1 Программно-аппаратные комплексы защиты от НСД;

4.2 Сравнение отечественного рынка продуктов

5. Система Управления Базами Данных (СУБД):

5.1 Управление доступом в СУБД;
5.2 Управление целостностью в СУБД;
5.3 Транзакции и операции в СУБД;
5.4 Ролевая модель, иерархия ролей, пользователи и привилегиями ;
5.5 Восстановление и безопасность хранения данных

6. Безопасность в СУБД Microsoft SQL Server:
6.1 Управление правами и доступом, пользователи и роли;
6.2 Аудит безопасности;
6.3 Физическая безопасность сервера;
6.4 Атаки на SQL. Методы взлома;
6.5 Защита СУБД MS SQL Server

7. Технические мероприятия по обеспечению безопасности автоматизированных систем:
7.1 Требования к системе защиты АС;
7.2 Специальные методические документы ФСБ и ФСТЭК;
7.3 Сертификация, Аттестация по требованиям ФСБ и ФСТЭК;
7.4 Технические мероприятия по обеспечению безопасности АС.

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 7			
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	20
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.	2	15
Научный доклад	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 оцениваются также ораторские способности.	3	15

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 и защита информации [Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 2014. - Режим доступа:
http://www.studentlibrary.ru/book/ISBN9785940747680.html

2. Глинская Е. В. Информационная безопасность конструкций ЭВМ и систем : учеб. пособие / Е.В. Глинская, Н.В. Чичварин. - М. : ИНФРА-М, 2018. Режим доступа: http://znanium.com/bookread2.php?book=925825

3. Мельников Д.А., Информационная безопасность открытых систем [Электронный ресурс] / Мельников Д.А. - М. : ФЛИНТА, 2014. - 448 с. - ISBN 978-5-9765-1613-7 - Режим доступа:
http://www.studentlibrary.ru/book/ISBN9785976516137.html

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. Режим доступа: 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. Девянин П.Н., Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс] : Учебное пособие для вузов / Девянин П.Н. - 2-е изд., испр. и доп. - М. : Горячая линия - Телеком, 2013. - 338 с. - ISBN 978-5-9912-0328-9 - Режим доступа:
http://www.studentlibrary.ru/book/ISBN9785991203289.html

7.2. Дополнительная литература:

1. Практическая криптография: Пособие / Масленников М.Е. - СПб:БХВ-Петербург, 2015. - 465 с. - Режим доступа: http://znanium.com/catalog/product/944503

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. - Режим доступа: http://znanium.com/bookread2.php?book=474838

3. Каратунова, Н. Г. Защита информации. Курс лекций [Электронный ресурс] : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - Режим доступа: http://znanium.com/bookread2.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. - Режим доступа: http://znanium.com/bookread2.php?book=491597

5. Хорев П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - 352 с. - Режим доступа: http://znanium.com/bookread2.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/studies/courses?service=0&option_id=9&service_path=1

Информационный портал по защите информации - http://all-ib.ru/

Портал с ресурсами по алгоритмике и защите информации - http://algolist.manual.ru/

Учебник - http://lib.tuit.uz/books/kitob/Завгородний Комплексная защита информации в компьютерных системах.pdf

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

Вид работ	Методические рекомендации
лекции	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.
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, изучаются специальных разделы программирования комплексных систем информационной безопасности.
самостоя-тельная 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.
устный опрос	Текущий контроль успеваемости студентов осуществляется с помощью устного опроса, который призван показать основные практические навыки решения задач, связанных с математическим обеспечением задач информационной безопасности. При выполнении устного рекомендуется обращаться внимание на основные задачи, решенные в течение семестра, периодически решать аналогичные задачи, программировать основные вычислительные алгоритмы, чтобы лучше понять их тонкости.
контрольная работа	Также для выполнения контроля успеваемости студентов проводится контрольная работа, 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.
научный доклад	Выполнить научный доклад на предложенную преподавателем тему из области комплексной защиты инфляционной безопасности. Для доклада использовать не менее 10 источников литературы и Интернете ресурсов. Создать компьютерную презентацию на тему доклада, составить план доклада и список вопросов для само проверки.
зачет	При подготовке к зачету рекомендуется разбить 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 лекции, полезно ознакомиться с более подробным изложением материала в учебнике. Список литературы разделен на две категории: необходимый для сдачи экзамена 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 "Комплексное обеспечение 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.

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 "Комплексное обеспечение 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 10.03.01 "Информационная безопасность" и профилю подготовки "Безопасность компьютерных систем".