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

УТВЕРЖДАЮ

Проректор по образовательной деятельности КФУ

Проф. Таюрский Д.А.

_____ "___" _____20___ г.

подписано электронно-цифровой подписью

Программа дисциплины

Комплексное обеспечение информационной безопасности экономических систем Б1.В.ОД.5

Направление подготовки: 09.04.03 - Прикладная информатика
Профиль подготовки: Информационная безопасность экономических систем
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Ишмухаметов Ш.Т.

Рецензент(ы):

Латыпов Р.Х.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Латыпов Р. Х.
Протокол заседания кафедры No ___ от "____" _____ 201__г

Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 943716

Казань
2016

ЭЛЕКТРОННЫЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА КФУ

Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

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. Цели освоения дисциплины

Данный курс предполагает изучение методов и средств построения комплексного обеспечения систем информационной безопасности в экономике и бизнесе.

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

Данная учебная дисциплина включена в раздел " Б1.В.ОД.5 Дисциплины (модули)" основной образовательной программы 09.04.03 Прикладная информатика и относится к обязательные дисциплины. Осваивается на 2 курсе, 3 семестр.

Данный куср является является продолжением курсов "Введение в информационную безопасность" и "Безопасность компьютерных сетей", читаемых для бакалавров направления Прикладная информатика. В предыдущих курсах было выполнено предварительное ознакомление с кругом проблем информационной безопасности, вопросами безопасности информационных технологий, средствами и методами защиты информации.

В курсу "Комплексное обеспечение информационной безопасности экономических систем" выполняется обсуждение проблем общего, комплексного подхода к проблемам защиты экономической информации, изучаются спецефические методы, привязанные к защите экономической и бизнес информации, вопросы безопасной обработки баековских карт, безопасной передачи критических данных пользователей через компьютерные сети.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-1 (общекультурные компетенции)	способностью к абстрантному мышлению, анализу и синтезу
ОК-3 (общекультурные компетенции)	готовностью к саморазвитию, самореализации, использованию творческого потенциала
ОПК-3 (профессиональные компетенции)	способностью исследовать современные проблемы и методы прикладной информатики и научно-технического развития ИКТ
ОПК-5 (профессиональные компетенции)	способностью на практике применять новые научные принципы и методы исследований
ПК-1 (профессиональные компетенции)	способностью использовать и развивать методы научных исследований и инструментария в области проектирования и управления ИС в прикладных областях
ПК-2 (профессиональные компетенции)	способностью формализовывать задачи прикладной области, при решении которых возникает необходимость использования количественных и качественных оценок
ПК-3 (профессиональные компетенции)	способностью ставить и решать прикладные задачи в условиях неопределенности и определять методы и средства их эффективного решения

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-4 (профессиональные компетенции)	способностью проводить научные эксперименты, оценивать результаты исследований
ПК-5 (профессиональные компетенции)	способностью исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций

В результате освоения дисциплины студент:

1. 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;

2. 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;

3. 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.

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;

ЭЛЕКТРОННЫЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННО-АНАЛИТИЧЕСКАЯ СИСТЕМА КФУ

самостоятельно разрабатывать требуемую организационно-распорядительную документацию;

успешно эксплуатировать шифровальные (криптографические) средства;

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) 72 часа(ов).

Форма промежуточного контроля дисциплины зачет в 3 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Введение в информационная безопасность экономических систем.	3	1-2	0	4	0	домашнее задание
2.	Тема 2. Классификация методов информационной безопасности применительно к экономической сфере	3	3-4	0	4	0	домашнее задание
3.	Тема 3. Организационно-правовые методы в системе экономической безопасности	3	5-6	0	4	0	домашнее задание
4.	Тема 4. Физические ментоды защиты экономической информации	3	7-8	0	4	0	домашнее задание
5.	Тема 5. Технические методы защиты в экономике и бизнесе	3	9-10	0	4	0	домашнее задание

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
6.	Тема 6. Математические проблемы построения модели безопасности экономических систем.	3	11-12	0	4	0	контрольная работа
7.	Тема 7. Обзор криптографических методов защиты информации в экономике и бизнесе.	3	13-14	0	4	0	домашнее задание
.	Тема . Итоговая форма контроля	3		0	0	0	зачет
	Итого			0	28	0	

4.2 Содержание дисциплины

Тема 1. Введение в информационная безопасность экономических систем.

практическое занятие (4 часа(ов)):

Значение экономической и банковской информации в жизни современного общества. Проблемы защиты информации. Типы нарушений. Характеристика современных видов атак на банковские структуры и системы.

Тема 2. Классификация методов информационной безопасности применительно к экономической сфере

практическое занятие (4 часа(ов)):

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

Тема 3. Организационно-правовые методы в системе экономической безопасности

практическое занятие (4 часа(ов)):

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 ментоды защиты экономической информации

практическое занятие (4 часа(ов)):

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.

Тема 5. Технические методы защиты в экономике и бизнесе

практическое занятие (4 часа(ов)):

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.

Тема 6. Математические проблемы построения модели безопасности экономических систем.

практическое занятие (4 часа(ов)):

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.

Тема 7. Обзор криптографических методов защиты информации в экономике и бизнесе.

практическое занятие (4 часа(ов)):

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

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Введение в информационная безопасность экономических систем.	3	1-2	подготовка домашнего задания	6	домашнее задание
2.	Тема 2. Классификация методов информационной безопасности применительно к экономической сфере	3	3-4	подготовка домашнего задания	8	домашнее задание
3.	Тема 3. Организационно-правовые методы в системе экономической безопасности	3	5-6	подготовка домашнего задания	6	домашнее задание
4.	Тема 4. Физические ментоды защиты экономической информации	3	7-8	подготовка домашнего задания	6	домашнее задание
5.	Тема 5. Технические методы защиты в экономике и бизнесе	3	9-10	подготовка домашнего задания	6	домашнее задание
6.	Тема 6. Математические проблемы построения модели безопасности экономических систем.	3	11-12	подготовка к контрольной работе	6	контрольная работа
7.	Тема 7. Обзор криптографических методов защиты информации в экономике и бизнесе.	3	13-14	подготовка домашнего задания	6	домашнее задание
	Итого				44	

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекций, лабораторных занятий, а также самостоятельной работы студентов.

Изучение курса подразумевает овладение теоретическим материалом и получения практических навыков для глубокого понимания дисциплины

"Комплексное обеспечение информационной безопасности экономических систем". Практические знания студенты получают на основе решения задач

и упражнений, иллюстрирующих доказываемые теоретические положения, выполнения лабораторных занятий. Кроме того, курс помогает студентам развивать

теоретические знания в обюласти построения систем защит и способность самостоятельно оценивать степень защищенности информационных объектов

и выбирать адекватные средства защиты. Самостоятельная работа предполагает выполнение домашних работ, подготовку к лабораторным занятиям.

Кроме того, самостоятельная работа включает подготовку к зачету. При подготовке к сдаче зачета весь объем работы рекомендуется распределять

равномерно по дням, отведенным для подготовки к зачету, контролировать текущие темы курса.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Введение в информационная безопасность экономических систем.

домашнее задание , примерные вопросы:

Углубленное изучение литературы. Обсуждение современных требований к обеспечению комплексной защиты информации, анализ угроз.

Тема 2. Классификация методов информационной безопасности применительно к экономической сфере

домашнее задание , примерные вопросы:

Обсуждение современных методов защиты информации, выбор и сранение различных подходов к построению комлексной системы защиты.

Тема 3. Организационно-правовые методы в системе экономической безопасности

домашнее задание , примерные вопросы:

Классификация правовых методов в сфере системы защиты экономической информации. Разбор основных законов и постановлений в области защиты информации.

Тема 4. Физические ментоды защиты экономической информации

домашнее задание , примерные вопросы:

Подготовить и разобрать порядок применения физических методы защиты ифформации на примере предприятия в экономической сфере.

Тема 5. Технические методы защиты в экономике и бизнесе

домашнее задание , примерные вопросы:

Пример построения технической схемы для комплексной защиты информации для предприятия, разделенного территориально на несколько филиалов.

Тема 6. Математические проблемы построения модели безопасности экономических систем.

контрольная работа , примерные вопросы:

Контрольная работа. Шифрование RSA. 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

Тема 7. Обзор криптографических методов защиты информации в экономике и бизнесе.

домашнее задание , примерные вопросы:

Разобрать способы построения и виды электронных цифровых подписей их роль и правовые основы в экономической сфере. Использование криптографии для скрытия конфидениальной информации.

Тема . Итоговая форма контроля

Примерные 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;

Ассиметричные 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 обрабатываемы 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;

7.1. Основная литература:

1. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: ИНФРА-М, 2012. - 416 с. URL: http://znanium.com/bookread.php?book=335362
2. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с. URL: http://znanium.com/bookread.php?book=402686
3. 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/bookread.php?book=405000

7.2. Дополнительная литература:

1. Партыка Т. Л. Информационная безопасность: Учебное пособие для студентов учреждений среднего проф. обр. / Т.Л. Партыка, И.И. Попов. - 3-е изд., перераб. и доп. - М.: Форум, 2014. - 432 с. - ЭБС "Знаниум": http://znanium.com/bookread.php?book=420047
2. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с. - ЭБС "Знаниум": http://znanium.com/bookread.php?book=491597
3. Хорев П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - 352 с. - ЭБС "Знаниум": http://znanium.com/bookread.php?book=169345

7.3. Интернет-ресурсы:

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

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Комплексное обеспечение информационной безопасности экономических систем" 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.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. 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, УМК, 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 профессионального образования (ФГОС ВПО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен студентам. 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.

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.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 09.04.03 "Прикладная информатика" и магистерской программе Информационная безопасность экономических систем .

Автор(ы):
Ишмухаметов Ш.Т. _____
"__" _____ 201 __ г.

Рецензент(ы):
Латыпов Р.Х. _____
"__" _____ 201 __ г.