МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Московский физико-технический институт (государственный университет)»
МФТИ (ГУ)
Кафедра «Системного программирования»

«УТВЕРЖДАЮ»
Проректор по учебной работе
_____О.А.Горшков
____ _____ 2012 г.

РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА

по дисциплине: Современные компьютеры и сети передачи данных
Часть II. Организация сетей открытых систем и обеспечение их безопасности
по направлению: 010900 «Прикладные математика и физика»
профиль подготовки: Системное программирование
факультеты: ФУПМ
кафедра Системного программирования
курс: 5 (магистратура)
семестр: осенний **экзамен 9 семестр**
Трудоёмкость в зач. ед.: вариативная часть – **2 зач. ед**.;
в т.ч.:

лекции: вариативная часть – **34 час**,
практические (семинарские) занятия: нет,
лабораторные занятия: нет.
мастер классы, индивид. и групповые консультации: нет,
самостоятельная работа: вариативная часть – **8 час,**
курсовые работы: нет,
подготовка к экзамену: вариативная часть – **1 зач. ед.**

ВСЕГО АУДИТОРНЫХ ЧАСОВ 34

Программу составил профессор, д.т.н., Шнитман В.З.
Программа обсуждена на заседании кафедры Системного программирования
«____» _____2012 г.

Заведующий кафедрой
академик РАН В. П. Иванников

Программа обсуждена и одобрена на методической комиссии факультета
"___" _____ 2012 г.
Председатель методической комиссии ФУПМ
чл.-корр. РАН Ю.А.Флеров

ОБЪЁМ УЧЕБНОЙ НАГРУЗКИ И ВИДЫ ОТЧЁТНОСТИ.

Вариативная часть, в т.ч. :	__1___ зач. ед.
Лекции	__34___ часа
Практические занятия	__нет___ часов
Лабораторные работы	__нет___ часов
Индивидуальные занятия с преподавателем	__нет___ часов
Самостоятельные занятия	__8__ часов
Итоговая аттестация	**Экзамен 9 семестр - 1 зач. ед.**
ВСЕГО	**2 зач. ед. 72 часа**

1. ЦЕЛИ И ЗАДАЧИ

Цель курса – Целью курса является ознакомление студентов с современным состоянием и тенденциями стандартизации сетевых протоколов, в особенности в части вопросов обеспечения безопасности передачи информации.

Задачами данного курса являются:

- освоение студентами базовых знаний в области обеспечения безопасности передачи информации в компьютерных сетях;
- приобретение знаний о сервисах и механизмах безопасности, используемых в современных компьютерных сетях;
- оказание консультаций и помощи студентам в проведении собственных исследований и разработок в областях, использующих средства обеспечения безопасности, в частности для создания распределенных систем обработки информации;
- приобретение навыков работы в современных сетях компьютеров с использованием различных технологий обеспечения безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП БАКАЛАВРИАТА

Дисциплина **Современные компьютеры и сети передачи данных. Часть II. Организация сетей открытых систем и обеспечение их безопасности** ***включает в себя разделы, которые могут быть отнесены к вариативным части цикла _Б.3_ кода УЦ ООП.***

Дисциплина **Современные компьютеры и сети передачи данных. Часть II. Организация сетей открытых систем и обеспечение их безопасности** ***базируется на циклах Б.2 курса 1,2,3 базовой и вариативных частях.***

КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины **Современные компьютеры и сети передачи данных. Часть II. Организация сетей открытых систем и обеспечение их безопасности** ***направлено на формирование следующих общекультурных и профессиональных интегральных компетенций бакалавра:***

а) общекультурные (ОК):

- способность анализировать научные проблемы и физические процессы, использовать на практике фундаментальные знания, полученные в области естественных и гуманитарных наук (ОК-1);
- способность осваивать новую проблематику, терминологию, методологию, овладевать научными знаниями, владеть навыками самостоятельного обучения (ОК-2);
- способность логически точно, аргументировано и ясно формулировать свою точку зрения, владеть навыками научной и общекультурной дискуссий (ОК-3);
- готовность к творческому взаимодействию с коллегами по работе и научным коллективом, способность и умение выстраивать межличностное взаимодействие, соблюдая уважение к товарищам и проявляя терпимость к иным точкам зрения (ОК-4).

б) профессиональные (ПК):

- способность применять в своей профессиональной деятельности знания, полученные в области физических и математических дисциплин, включая дисциплины: алгоритмы и языки программирования, программирование на языке ассемблера, математическая логика, теория графов, линейная алгебра (ПК-1);
- способность понимать сущность задач, поставленных в ходе профессиональной деятельности, использовать соответствующее открытое программное обеспечение и алгоритмы для их постановки и решения (ПК-3);
- способность использовать знания в области физических и математических дисциплин для дальнейшего освоения дисциплин в соответствии с профилем подготовки (ПК-4);
- способность работать с современным программным обеспечением, приборами и установками в избранной области (ПК-5).

3. КОНКРЕТНЫЕ ЗНАНИЯ, УМЕНИЯ И НАВЫКИ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины «Современные компьютеры и сети передачи данных. Часть II. Организация сетей открытых систем и обеспечение их безопасности » обучающийся должен:

1. Знать:

- стандартные методы организации открытых компьютерных сетей;
- основные угрозы нарушения безопасности в открытых компьютерных сетях;
- методы и средства противодействия угрозам нарушения безопасности в открытых компьютерных сетях, включая Интернет.
- стандартизованные методы криптографии, используемые для защиты информации в современных компьютерных сетях;
- методы аутентификации пользователей и других сущностей в компьютерных сетях;
- цели и методы обеспечения конфиденциальности и целостности данных;
- механизмы авторизации и контроля доступа к сетевым ресурсам;
- размещение сервисов безопасности в многоуровневой сетевой архитектуре и стандартизованные средства их реализации;

2. Уметь:

- грамотно подобрать средства безопасности, необходимые при выполнении научных исследований с использованием компьютерных сетей;
- проводить самостоятельные научные исследования по теме дисциплины;
- применять изученные методы, протоколы и алгоритмы для решения поставленных задач.

3. Владеть:

- навыками освоения большого объема информации;
- навыками самостоятельной работы в Интернете;
- культурой обеспечения безопасности разработки и реализации системного программного обеспечения современных компьютеров и сетей;

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Структура дисциплины

Перечень разделов дисциплины и распределение времени по темам

№ темы и название	Количество часов
1. Стандарты открытых систем	0,5
2. Концепции и терминология открытых систем	1,5
3. Основы безопасности сетей	1
4. Сервисы безопасности и уровневая архитектура.	1
5. Методы криптографии	4
6. Аутентификация	4
7. Контроль доступа	2
8. Конфиденциальность и целостность	2
9. Неотказуемость	2
10. Инфраструктура открытых ключей (PKI)	2
11. Справочные системы	4
12. Безопасность электронной почты и электронного обмена документами	4
13. Управление сетью	2
14. Обеспечение безопасности на транспортном уровне	2
15. Обеспечение безопасности на сетевом уровне	2
ВСЕГО (зач. ед.(часов))	34 час (1 зач. ед.)

ВИД ЗАНЯТИЙ

ЛЕКЦИИ:

№ п.п.	Темы	Трудоёмкость в зач. ед. (количество часов)
1	Стандарты открытых систем Концепции и терминология открытых систем	2
2	Основы безопасности сетей Сервисы безопасности и уровневая архитектура	2
3	Методы криптографии	4
4	Аутентификация	4
5	Контроль доступа	2
6	Конфиденциальность и целостность	2
7	Неотказуемость	2
8	Инфраструктура открытых ключей (PKI)	2
9	Справочные системы	4
10	Безопасность электронной почты и электронного обмена документами	4
11	Управление сетью	2
12	Обеспечение безопасности на транспортном уровне	2
13	Обеспечение безопасности на сетевом уровне	2
ВСЕГО (зач. ед.(часов))		34 часа (1 зач. ед.)

ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

№ п.п.	Темы	Трудоёмкость в зач. ед. (количество часов)
1	Изучение теоретического курса – выполняется самостоятельно каждым студентом по итогам каждой из лекций, результаты контролируются преподавателем на лекционных занятиях, используются конспект (электронный) лекций, учебники, рекомендуемые данной программой, методические пособия.	8 час.
2	Подготовка к экзамену	30 час.
ВСЕГО (зач. ед.(часов))		1 зач. ед. (38 час.)

Содержание дисциплины

№ п/п	Название модулей	Разделы и темы лекционных занятий	Содержание	Объем	
				Аудиторная работа (зачетные единицы/ часы)	Самостоятельная работа (зачетные единицы/ часы)
1		Стандарты открытых систем	Процессы стандартизации OSI и Internet. Стандарты, профили, соглашения по реализации и тестирование на соответствие стандартам.	0,5	
2		Концепции и терминология открытых систем	Архитектуры. Открытые системы. Уровни. Краткий обзор семи уровней модели OSI. Краткий обзор уровней Internet. Терминология. Объекты. Система обозначений. Службы. Модель очередей. Службы с установлением и без установления соединения. Отношения между службами и протоколами. Протокольные заголовки и пользовательские данные. Временные диаграммы. Обзор служб распределенных приложений.	1,5	
3		Основы безопасности сетей	Политика безопасности. Угрозы и меры безопасности. Пять основных сервисов безопасности: аутентификация, контроль доступа, конфиденциальность, целостность данных и невозможность отказа. Обнаружение вторжений и аудит безопасности.	1	
4		Сервисы безопасности и уровневая архитектура	Размещение сервисов безопасности в многоуровневой сетевой архитектуре. Безопасность прикладного уровня. Безопасность уровня оконечных систем. Безопасность уровня подсети. Безопасность уровня канала связи. Взаимодействие с людьми. Управление сервисами безопасности.	1	
5		Методы криптографии	Симметричные криптосистемы. Типы алгоритмов и режимы шифрования. Режим электронной кодовой книги. Режим сцепления блоков шифра. Режим обратной связи по выходу. Режим обратной связи по шифру. Режим счетчика.	4	2

			Общие принципы построения блочных шифров. Стандарт шифрования данных DES. Усовершенствованный стандарт шифрования AES. Алгоритм ГОСТ 28147-89. Криптосистемы с открытым ключом. Алгоритм RSA. Алгоритм Эль Гамаля. Коды аутентификации сообщений. Цифровые подписи. Стандарт цифровой подписи США. Алгоритм цифровой подписи ГОСТ. Хэш-функции. Общие принципы управления криптографическими ключами. Методы распределения секретных ключей. Распределение ключей с помощью симметричных методов. Распределение ключей посредством принудительного обращения к серверу ключей. Распределение ключей с помощью методов реверсивных открытых ключей. Алгоритм создания ключа Диффи-Хеллмана. Методы распределения ключей для асимметричных криптосистем. Распределение открытых ключей. Генерация пары ключей. Аннулирование сертификатов. Пример: Инфраструктура сертификации PEM.		
6		Аутентификация	Общие концепции. Парольные механизмы. Противодействие внешнему разглашению и угадыванию пароля. Противодействие прослушиванию линии связи. Противодействие компрометации верификатора. Противодействие повторному воспроизведению. Другие механизмы, не использующие криптографию. Одноразовые пароли. Окрик-отзыв. Механизмы на основе адреса. Механизмы, использующие характерные особенности человека. Карты аутентификации личности. Использование методов криптографии. Роль оперативных серверов. Роль автономных серверов. Методы доказательства с нулевым разглашением. Аутентификация личности. Некоторые тонкости протоколов аутентификации. Атаки перехвата и по-	4	1

			вторного воспроизведения. Использование неповторяющихся значений. Протоколы взаимной аутентификации. Защита аутентификации. Некоторые конкретные механизмы. Система Kerberos. Аутентификационные обмены X.509. Аутентифицированный обмен Диффи-Хеллмана. Стойкие парольные протоколы. Основная идея. Расширенная версия протокола EKE. Стойкий парольный протокол SRP. Аутентификация источника данных. Требования к протоколам. Аутентификационные обмены. Обмен информацией с оперативным сервером. Обмен информацией о сертификатах. Местоположение в архитектуре. Аутентификация сущностей. Аутентификация источника данных.		
7		Контроль доступа	Политики контроля доступа. Механизмы контроля доступа. Списки контроля доступа. Возможности. Метки безопасности. Информационная модель, связанная с механизмами контроля доступа. Механизмы на основе паролей. Пример механизма контроля доступа из приложения FTAM. Общая модель распределения функций контроля доступа в сетевой среде. Требования к управлению и распространению информации, связанной с контролем доступа, в сетевой среде. Контроль доступа к коммуникациям и контроль маршрутизации. Требования к протоколам и вопросы определения местоположения в уровневой архитектуре.	2	
8		Конфиденциальность и целостность	Общие средства обеспечения конфиденциальности. Два подхода к обеспечению конфиденциальности. Средства управления потоками данных. Степень детализации данных. Конкретные типы механизмов конфиденциальности. Шифрование. Дополнение данных. Дополнение трафика. Другие ме-	2	

			ханизмы. Общие средства обеспечения целостности. Уровень детализации данных. Восстановление. Конкретные типы механизмов целостности. Контрольные слова. Печати или подписи. Шифрование. Целостность последовательности. Дублирование. Восстановление целостности. Комбинирование механизмов конфиденциальности и целостности. Требования к протоколам, предъявляемые механизмами конфиденциальности и целостности. Криптографические преобразования. Управляющая информация протокола. Метки безопасности. Местоположение конфиденциальности и целостности в архитектуре системы. Дополнительные возможности физического оборудования.		
9		Неотказуемость	Фазы и роли в процессе обеспечения неотказуемости. Запрос сервиса. Генерация свидетельства. Передача и сохранение свидетельства. Верификация свидетельства. Разрешение спора. Неотказуемость инициатора. Цифровая подпись инициатора. Цифровая подпись данных доверенной третьей стороной. Цифровая подпись доверенной третьей стороной дайджеста элемента данных. Маркер доверенной третьей стороны. Участие доверенной третьей стороны в процессе передачи данных. Комбинации механизмов. Использование меток времени. Неотказуемость от доставки. Подтверждение, подписанное получателем. Подтверждение получения маркером. Доверенный агент доставки. Двухэтапная доставка. Последовательные отчеты о доставке. Функции доверенных третьих сторон. Требования к протоколам.	2	0
10		Инфраструктура открытых ключей (PKI)	Модели доверия PKI. Модель монополии. Монополия плюс центры регистрации. Уполномоченные центры сертификации. Олигархия. Модель анархии. Ограничения имен. Модель «сверху-вниз» с	2	1

			ограничениями имен. Модель «снизу-вверх» с ограничениями имен. Относительные имена. Ограничения имен в сертификатах. Политики в сертификатах. Аннулирование сертификатов. PKI и справочные системы. Сертификаты PKIX и X.509. Авторизация с помощью PKI.		
11		Справочные системы	Модель телефонного справочника. Принципы организации справочной системы. Справочные службы открытых систем. Справочная система X.500. (Серия стандартов. Архитектура. Информационная модель справочной системы). Модель Справочной Системы (Службы справочной системы. Взаимодействие между агентами справочной службы. Протоколы справочной системы. Модель безопасности справочной системы). Система аутентификации X.509 (аутентификационные обмены, форматы сертификатов, процедуры управления сертификатами). Контроль доступа к справочной системе. Упрощенный протокол доступа к справочной системе (LDAP). Система доменных имен (Доменные имена. Как работает DNS. Обратный поиск. Обмен почтой). Расширения DNSSEC. Базовые принципы работы. Процедуры поиска. Доверенные анкеры и аутентификационные цепочки. Управление ключами.	4	1
12		Безопасность электронной почты и электронного обмена документами	Система обработки сообщений X.400 MHS (Общая архитектура. Администрирование систем обработки сообщений. Имена и адреса в MHS). Угрозы в среде MHS и сервисы безопасности, используемые для противодействия этим угрозам. Протокольные элементы MHS, используемые для обеспечения безопасности. Обеспечение основных сквозных сервисов безопасности MHS. Обеспечение других сервисов безопасности MHS. Методы безопасности, используе-	4	1

			мые в MHS. Специальные меры для защиты обмена транзакциями EDI. Почта Интернет (Общая архитектура. Почтовые адреса. Списки рассылки. Многоцелевое расширение почты Интернет – MIME). Почта Интернет с расширениями конфиденциальности (PEM). Структура сообщения PEM. Установление ключей. Иерархия сертификатов PEM. Списки аннулированных сертификатов. Шифрование. Аутентификация источника и защита целостности. Сообщение для нескольких получателей. Пересылка сообщения и вложения. Незащищенная информация. Форматы сообщений. Расширение почты Интернет – SMIME. Отличия S/MIME и PEM. Иерархия сертификатов S/MIME. Почтовый протокол PGP. Обзор. Распределение ключей. Эффективное кодирование. Аннулирование сертификатов и ключей. Типы подписей. Закрытый ключ. Связка ключей. Форматы объектов.		
13		Управление сетью	Подход Интернет (Общая организация управления в Интернет. База управляющей информации. Структура управляющей информации. Протокол SNMP, SNMP и стек протоколов. Протоколы безопасности для SNMPv2). Управление сетями OSI (Модель управляющей информации OSI и GDMO. CMIP/CMIS, CMIP и семейство протоколов. CMIP и удаленные операции. Функции управления системой. Профили). Обеспечение безопасности управления сетью.	2	
14		Обеспечение безопасности на транспортном уровне	Семейство протоколов SSL/TLS. Краткая история. Базовый протокол SSL/TLS. Возобновление сеанса. Вычисление ключей. Аутентификация клиента. PKI, применяемая SSL. Согласование наборов шифров. Возможные виды атак на SSL/TLS. Форматы сообщений SSL/TLS.	2	1
15		Обеспече-	Недостатки протокола IPv4. Крат-	2	1

		ние безопасности на сетевом уровне	кий обзор протокола IPv6. Экранирование. Туннелирование. Обзор IPsec. Контексты безопасности. База данных контекстов безопасности. База данных политик безопасности. Типовое применение IPsec. Протоколы AH и ESP. Туннельный и транспортный режимы. Протоколы автоматического установления контекстов безопасности и управления ключами в Интернет. Обзор протокола IKE. Особенности работы протокола IKE. Структура сообщений ISAKMP/IKE.		

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

№ п/п	Вид занятия	Форма проведения занятий	Цель
1	Лекция	Изложение теоретического материала	Получение теоретических знаний по дисциплине
2	Лекция	Изложение теоретического материала с помощью презентаций	Повышение степени понимания материала
3	Лекция	Разбор конкретных примеров применения методов криптографии для реализации защиты протоколов передачи данных	Осознание связей между теорией и практикой, а также взаимозависимостей разных дисциплин
4	Самостоятельная работа студента	Подготовка к экзамену	Повышение степени понимания материала

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Перечень контрольных вопросов для экзамена в конце 9 семестра

1. Зачем нужны стандарты, профили, соглашения по реализации и тестирование на соответствие стандартам?
2. Поясните отношения между сетевыми службами и протоколами.
3. Семиуровневая модель взаимосвязи открытых систем OSI.
4. Стек протоколов TCP/IP.
5. Классификация угроз и мер безопасности.
6. Сервисы безопасности.
7. Размещение сервисов безопасности в многоуровневой архитектуре.
8. Симметричные криптосистемы. Приведите примеры стандартных алгоритмов.
9. Асимметричные криптосистемы. Приведите примеры стандартных алгоритмов.
10. Коды MAC.
11. Цифровые подписи.
12. Распределение секретных ключей.
13. Распределение ключей криптосистем с открытым ключом.

14.Общие концепции аутентификации.
15.Парольные системы.
16.Система Kerberos.
17.Аутентификационные обмены X.509.
18.Аутентифицированный обмен Диффи-Хеллмана.
19. Основная идея и реализации стойких парольных протоколов.
20. Политики и механизмы контроля доступа.
21.Общие средства обеспечения конфиденциальности и конкретные типы механизмов конфиденциальности.
22.Общие средства обеспечения целостности.
23.Фазы и роли в процессе обеспечения неотказуемости. Механизмы неотказуемости.
24.Инфраструктуры открытых ключей и модели доверия PKI.
25.Язык ASN.1
26.Справочная система X.500. Модель безопасности справочной системы.
27.Упрощенный протокол доступа к справочной системе (LDAP).
28.Система доменных имен. Расширения DNSSEC.
29.Система обработки сообщений MHS X.400. Угрозы в среде MHS и сервисы безопасности, используемые для противодействия этим угрозам.
30.Почта Интернет. Расширение почты Интернет – SMIME. Отличия S/MIME, PEM и PGP.
31.. Протокол SNMP и организация управления в Интернет. Обеспечение безопасности управления сетью.
32.Транспортный уровень в семействе TCP/IP. Семейство протоколов SSL/TLS.
33.Межсетевой уровень в семействе TCP/IP. Недостатки IPv4 и возможности IPv6.
34. Механизмы экранирования и туннелирования в Интернет.
35.Типовое применение IPsec.
36.Протоколы AH и ESP.
37.Туннельный и транспортный режимы.
38.Основной и агрессивный режимы IKE.
39.Быстрый режим IKE.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Необходимое оборудование для лекций и практических занятий: компьютер и мультимедийное оборудование (проектор, звуковая система)
Необходимое программное обеспечение: любой браузер для доступа в Интернет
Обеспечение самостоятельной работы: Основная и дополнительная литература, доступная в библиотеке ИСП РАН, конспекты лекций и слайды курса, доступные через Интернет, а также текстовые файлы, доступные на сайтах http://www.iso.org, http://www.itu.int, http://www.ietf.org .

8. НАИМЕНОВАНИЕ ВОЗМОЖНЫХ ТЕМ КУРСОВЫХ РАБОТ

– УЧЕБНЫМ ПЛАНОМ НЕ ПРЕДУСМОТРЕНЫ

9. ТЕМАТИКА И ФОРМЫ ИНДИВИДУАЛЬНОЙ РАБОТЫ

– УЧЕБНЫМ ПЛАНОМ НЕ ПРЕДУСМОТРЕНЫ

10. ТЕМАТИКА ИТОГОВЫХ РАБОТ

– УЧЕБНЫМ ПЛАНОМ НЕ ПРЕДУСМОТРЕНЫ

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература.

1. Танненбаум Э. Компьютерные сети. СПб.: Питер, 2003.
2. Халсалл Ф. Передача данных, сети компьютеров и взаимосвязь открытых систем. М.: Радио и связь, 1995.

3. Семенов Ю.А. Протоколы и ресурсы Internet. М.: Радио и связь, 1996.
4. С. Бенет, С. Пэйн. Криптография. Официальное руководство RSA Security. М.: Бином-Пресс, 2002

Дополнительная литература.

1. Б. Шнайер. Прикладная криптография. М.: ТРИУМФ, 2003
2. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. СПб.: БХВ-Петербург, 2009.
3. В.А. Галатенко. Основы информационной безопасности. М.: ИНТУИТ.РУ «Интернет-Университет», 2003.
4. В.А. Галатенко. Стандарты информационной безопасности. М.: ИНТУИТ.РУ «Интернет-Университет», 2004.
5. М.Р. Биктимиров, А.Ю. Щербаков. Избранные главы компьютерной безопасности. Казань: Издательство Казанского математического общества, 2004.
6. К.В. Ребриков, В.З. Шнитман. "Протоколы автоматического установления контекстов безопасности и управления ключами в Интернет", Препринт 19 ИСП РАН, М., 2007.

Пособия и методические указания.

1. Слайды лекций (Интернет)

Пособие по лекциям разрабатывается.

Программу составил

В.З. Шнитман, профессор, д.т.н.

«_____»_____2012 г.