

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»

УТВЕРЖДАЮ:

Директор ИТТСУ



П.Ф. Бестемьянов

25 мая 2018 г.



Кафедра «Управление и защита информации»

Автор Стряпкин Леонид Игоревич

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Криптографические методы защиты информации

Специальность:	<u>10.05.01 – Компьютерная безопасность</u>
Специализация:	<u>Информационная безопасность объектов информатизации на базе компьютерных систем</u>
Квалификация выпускника:	<u>Специалист по защите информации</u>
Форма обучения:	<u>очная</u>

<p style="text-align: center;">Одобрено на заседании Учебно-методической комиссии института Протокол № 10 21 мая 2018 г. Председатель учебно-методической комиссии</p>  <p style="text-align: right;">С.В. Володин</p>	<p style="text-align: center;">Одобрено на заседании кафедры</p> <p>Протокол № 16 15 мая 2018 г. Заведующий кафедрой</p>  <p style="text-align: right;">Л.А. Баранов</p>
---	---

Москва 2018 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Основной целью изучения дисциплины «Криптографические методы защиты информации» является формирование у обучающегося компетенций для следующих видов деятельности:

? научно-исследовательская;

? проектная;

? контрольно-аналитическая;

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности):

Научно-исследовательская деятельность:

- сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности;

Проектная деятельность:

- разработка технических заданий на проектирование, эскизных, технических и рабочих проектов систем и подсистем защиты информации с учетом действующих нормативных и методических документов;

- разработка проектов систем и подсистем управления информационной безопасностью объекта в соответствии с техническим заданием.

Контрольно-аналитическая деятельность:

- предварительная оценка, выбор и разработка необходимых методик поиска уязвимостей; применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты;

- подготовка аналитического отчета по результатам проведенного анализа и выработка предложений по устранению выявленных уязвимостей.

Задачи дисциплины:

- изложение основополагающих принципов защиты информации с помощью криптографических методов и изучение их практического применения.

- развитие у обучаемых системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами с помощью методов криптографии;

- изучение принципов синтеза и анализа криптосистем, математических методов оценки их стойкости.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Криптографические методы защиты информации" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

2.1. Наименования предшествующих дисциплин

Для изучения данной дисциплины необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами:

2.1.1. Информатика:

Знания: основные направления развития информационных технологий

Умения: применять информационные технологии для поиска и обработки информации

Навыки: современными информационными технологиями работы в глобальных КС

2.1.2. Математический анализ:

Знания: основные методы и средства познания для приобретения новых знаний и умений;

Умения: применять полученные теоретические знания для решения конкретных практических задач;

Навыки: методами математического описания физических явлений и процессов, определяющих принципы работы различных технических устройств.

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Криптографические протоколы

2.2.2. Теоретико-числовые методы в криптографии

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины студент должен:

№ п/п	Код и название компетенции	Ожидаемые результаты
1	ПК-5 способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	<p>Знать и понимать: как организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития.</p> <p>Уметь: организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития.</p> <p>Владеть: навыками организации и поддержки выполнения комплекса мер по информационной безопасности, управления процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития.</p>
2	ОПК-4 способностью применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами	<p>Знать и понимать: основные криптографические примитивы и их использование в решении основных задач защиты информации.</p> <p>Уметь: использовать криптографические методы для защиты информации</p> <p>Владеть: навыками использования ПЭВМ при анализе простейших шифров</p>

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ И АКАДЕМИЧЕСКИХ ЧАСАХ

4.1. Общая трудоемкость дисциплины составляет:

5 зачетных единиц (180 ак. ч.).

4.2. Распределение объема учебной дисциплины на контактную работу с преподавателем и самостоятельную работу обучающихся

Вид учебной работы	Количество часов	
	Всего по учебному плану	Семестр 6
Контактная работа	80	80,15
Аудиторные занятия (всего):	80	80
В том числе:		
лекции (Л)	48	48
практические (ПЗ) и семинарские (С)	32	32
Самостоятельная работа (всего)	64	64
Экзамен (при наличии)	36	36
ОБЩАЯ трудоемкость дисциплины, часы:	180	180
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	5.0	5.0
Текущий контроль успеваемости (количество и вид текущего контроля)	КР (1), ПК1, ПК2	КР (1), ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЭК	ЭК

4.3. Содержание дисциплины (модуля), структурированное по темам (разделам)

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	6	Раздел 1 Основы криптографии	4		4		4	12	
2	6	Тема 1.1 Введение в криптографию Структурная схема защищённой системы передачи информации. Роль криптографических методов защиты в её структуре. Понятия модуляции, кодирования, шифрования. Основные задачи защиты информации криптографическими методами. Понятие симметричной шифросистемы и её структурная схема Понятие асимметричной шифросистемы и её структурная схема Исторические шифры, их примеры	2		2			4	
3	6	Тема 1.2 Теоретические положения криптографии Понятия алфавита, стандартной кодировки и шифротекста. Лавинный эффект в шифровании. Частотный криптоанализ Классификация атак в криптографии. Основные понятия. Вычислительно сложные задачи математики. Понятие «односторонней» функции и	2		2		4	8	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		«односторонней функции с секретом». Элементы теории чисел. Функция Эйлера и её особенности, теоремы Эйлера и Ферма.							
4	6	Раздел 2 Криптосистемы с открытым ключом	4		14/10		10	28/10	
5	6	Тема 2.1 Криптосистемы на базе задачи дискретного логарифмирования Криптосистема Диффи — Хеллмана Криптосистема (бесключевой протокол) Шамира Криптосистема Эль-Гамала.	2		8/6		10	20/6	
6	6	Тема 2.2 Криптосистемы на базе задачи факторизации Криптосистема RSA.	2		6/4			8/4	
7	6	Раздел 3 Электронно-цифровая подпись (ЭЦП)	6				13	19	
8	6	Тема 3.1 Общие сведения об ЭЦП Назначение и классификация (НЭП, ПЭП, КЭП)	2					2	
9	6	Тема 3.2 Алгоритмы ЭЦП Алгоритм ЭЦП Эль-Гамала Алгоритм ЭЦП RSA	2					2	
10	6	Тема 3.3 Хеш-функции Понятие и основные свойства хеш-функции. Коллизии первого и второго рода.	2				13	15	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
11	6	Раздел 4 Криптосистемы на эллиптических кривых	4				10	14	
12	6	Тема 4.1 Общие сведения об эллиптических кривых Экспоненциальная и субэкспоненциальная сложность алгоритмов Эллиптические кривые. Понятие дискриминанта и сингулярности. Операция композиции точек на кривой. Свойства точек на эллиптической кривой.	2					2	
13	6	Тема 4.2 Алгоритмы на эллиптических кривых Выбор параметров кривой. Построение криптосистем на эллиптических кривых. Шифр Эль-Гамала на эллиптической кривой. Стандарт ЭЦП ГОСТ Р 34.10	2				10	12	
14	6	Раздел 5 Обзор криптографических алгоритмов и средств	20		8		21	49	
15	6	Тема 5.2 Блочные шифры Основные особенности построения блочных шифров с использованием SP-сетей и сетей Фейстеля			2		7	9	
16	6	Тема 5.3 Алгоритм DES и его	2					2	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		вариации Описание алгоритма DES							
17	6	Тема 5.4 Алгоритм AES Описание алгоритма AES			2		7	9	
18	6	Тема 5.5 Поточные шифры. Основные особенности построения поточных шифров	2		2		7	11	
19	6	Тема 5.6 Аппаратное шифрование и скрембли-рование. Виды скремблирования, особенности аппаратного шифрования	2		2			4	
20	6	Тема 5.7 Управление ключами Распределение ключей на базе алго- ритма Диффи- Хеллмана	2					2	
21	6	Тема 5.8 Стеганография: история и со- временность Обзор стеганографических методов защиты информации	2					2	
22	6	Тема 5.9 Аутентификация и идентификация. Криптографические основы аутентификации пользователей компьютерных систем.	2					2	
23	6	Тема 5.10 Применение криптографии в радиосвязи Системы радиосвязи с ППРЧ и с ис- пользованием шумоподобных сигналов,	2					2	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		расширение спектра, стандарт APCO25.							
24	6	Тема 5.11 Помехоустойчивость шифров. Шифры, не размножающие искажений	2					2	
25	6	Тема 5.12 Современные криптосистемы с открытым ключом Асимметричные криптосистемы, их особенности.	2					2	
26	6	Тема 5.13 Современные криптосистемы с секретным ключом Симметричные криптосистемы, их особенности.	2					2	
27	6	Раздел 6 Генераторы псевдослучайных последовательностей	10		6		6	22	
28	6	Тема 6.1 Общие сведения о генераторах псевдослучайных последовательностей. Основные понятия и свойства генераторов ПСП.	2					2	
29	6	Тема 6.2 Программные и аппаратные генераторы ПСП Принципы построения программных и аппаратных генераторов ПСП	2					2	
30	6	Тема 6.3 Регистры РСЛОС Регистры сдвига с линейными обратными связями как генераторы псевдослучайных последовательностей	2		2			4	
31	6	Тема 6.4 Структуры генераторов ПСП на	2		2		6	10	

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежуточной аттестации
			Л	ЛР	ПЗ	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
		базе РСЛОС Каскадирование РСЛОС и мажоритарная структура на их базе.							
32	6	Тема 6.5 Характеристики генераторов ПСП. Вероятностные характеристики РСЛОС, предсказуемость ПСП.	2		2			4	
33	6	Раздел 7 Курсовая работа						0	КР
34	6	Экзамен						36	ЭК
35		Тема 5.1 Введение Классификация криптографических алгоритмов и средств защиты информации							
36		Всего:	48		32/10		64	180/10	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 32 ак. ч.

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
1	6	РАЗДЕЛ 1 Основы криптографии Тема: Введение в криптографию	Практическое занятие №1 Исторические шифры	2
2	6	РАЗДЕЛ 1 Основы криптографии Тема: Теоретические положения криптографии	Практическое занятие №2 Вычислительно сложные задачи математики.	2
3	6	РАЗДЕЛ 2 Криптосистемы с открытым ключом Тема: Криптосистемы на базе задачи дискретного логарифмирования	Практическое занятие №3 Криптосистема (безключевой протокол) Шамира	4 / 4
4	6	РАЗДЕЛ 2 Криптосистемы с открытым ключом Тема: Криптосистемы на базе задачи дискретного логарифмирования	Практическое занятие №4 Криптосистема Эль-Гамала	4 / 2
5	6	РАЗДЕЛ 2 Криптосистемы с открытым ключом Тема: Криптосистемы на базе задачи факторизации	Практическое занятие №5 Криптосистема RSA.	4 / 2
6	6	РАЗДЕЛ 2 Криптосистемы с открытым ключом Тема: Криптосистемы на базе задачи факторизации	ПК-1 Защита работ, доклады студентов	2 / 2
7	6	РАЗДЕЛ 5 Обзор криптографических алгоритмов и средств Тема: Блочные шифры	Практическое занятие №6 Изучение блочных шифров	2
8	6	РАЗДЕЛ 5 Обзор криптографических алгоритмов и средств Тема: Алгоритм AES	Практическое занятие №7 Алгоритм AES	2

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
9	6	РАЗДЕЛ 5 Обзор криптографических алгоритмов и средств Тема: Поточные шифры.	Практическое занятие №8 Поточные шифры	2
10	6	РАЗДЕЛ 5 Обзор криптографических алгоритмов и средств Тема: Аппаратное шифрование и скремблирование.	Практическое занятие №9 Аналоговое скремблирование	2
11	6	РАЗДЕЛ 6 Генераторы псевдослучайных последовательностей Тема: Регистры РСЛОС	Практическое занятие №10 программные и аппаратные генераторы ПСП	2
12	6	РАЗДЕЛ 6 Генераторы псевдослучайных последовательностей Тема: Структуры генераторов ПСП на базе РСЛОС	Практическое занятие №11 Регистры РСЛОС	2
13	6	РАЗДЕЛ 6 Генераторы псевдослучайных последовательностей Тема: Характеристики генераторов ПСП.	Практическое занятие №12 Структуры генераторов ПСП на базе РСЛОС, защита работ.	2
ВСЕГО:				32 / 10

4.5. Примерная тематика курсовых проектов (работ)

Цель курсовой работы – закрепление знаний по курсу и развитие у обучающихся навыков самостоятельной творческой работы.

Курсовая работа должна иметь следующую структуру: титульный лист, содержание, введение, 3-4 тематических главы, заключение, список использованных источников. При необходимости добавления объемного иллюстративного материала (листинг программ, блок-схемы, объемные расчеты и т.п.) допускается одно или несколько приложений в конце курсовой работы. Объем работы должен составлять 15-45 страниц А4 при использовании шрифта Times New Roman 14 и полуторного междустрочного интервала. Защита курсовой работы происходит в установленные преподавателем сроки в виде доклада с презентацией на 5-10 слайдов.

Примерный список рекомендуемых тем:

1. Исторические шифры и их криптоанализ;
2. Современные криптосистемы с открытым ключом;
3. Современные симметричные криптосистемы;
4. Аппаратное шифрование и скремблирование;
5. Применение криптографических методов защиты информации на различных уровнях

модели OSI;

6. Алгоритм симметричного шифрования AES;
7. Алгоритмы вычисления хеш-функций в криптографических системах;
8. Искусственные нейронные сети и нейрокриптография;
9. Стеганография: история и современность;
10. Блочные шифры с использованием SP-сетей и сетей Фейстеля;
11. Поточные шифры;
12. Квантовая криптография;
13. Задача о ранце и её криптографическое использование;
14. Современные стандарты и системы электронно-цифровой подписи;
15. Технические средства защиты авторских прав;
16. Протокол HTTPS и защита информации в сети Интернет;
17. Идентификация, аутентификация и парольная защита;
18. Помехоустойчивость шифров. Шифры, не размножающие искажений;
19. Криптографическая защита каналов радиосвязи. Стандарт ARCO P25;
20. Системы радиосвязи с ППРЧ и с использованием шумоподобных сигналов.

В ходе учебного процесса тематика работ может быть изменена с учётом пожеланий преподавателя и студентов.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины «Криптографические методы защиты информации» осуществляется в форме лекций и практических занятий.

Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью на 30 % являются традиционными классически-лекционными (объяснительно-иллюстративные), и на 70 % с использованием интерактивных (диалоговых) технологий, в том числе мультимедиа лекция.

Практические занятия организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач). Остальная часть практического курса проводится с использованием интерактивных (диалоговые) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения. Часть практических работ, выполняемых с использованием ПЭВМ, подразумевает оформление соответствующего отчёта.

Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. К интерактивным (диалоговым) технологиям относятся отработка отдельных тем по электронным пособиям, подготовка к промежуточным контролям в интерактивном режиме, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов. Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые опросы, решение тестов с использованием компьютеров или на бумажных носителях.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Вид самостоятельной работы студента. Перечень учебно-методического обеспечения для самостоятельной работы	Всего часов
1	2	3	4	5
1	6	РАЗДЕЛ 1 Основы криптографии Тема 2: Теоретические положения криптографии	Самостоятельная работа №1	4
2	6	РАЗДЕЛ 2 Криптосистемы с открытым ключом Тема 1: Криптосистемы на базе задачи дискретного логарифмирования	Самостоятельная работа №2	10
3	6	РАЗДЕЛ 3 Электронно-цифровая подпись (ЭЦП) Тема 3: Хеш-функции	Самостоятельная работа №3	13
4	6	РАЗДЕЛ 4 Криптосистемы на эллиптических кривых Тема 2: Алгоритмы на эллиптических кривых	Самостоятельная работа №4 Подготовка студентов к экзамену	10
5	6	РАЗДЕЛ 5 Обзор криптографических алгоритмов и средств Тема 2: Блочные шифры	Самостоятельная работа №5	7
6	6	РАЗДЕЛ 5 Обзор криптографических алгоритмов и средств Тема 4: Алгоритм AES	Самостоятельная работа №6	7
7	6	РАЗДЕЛ 5 Обзор криптографических алгоритмов и средств Тема 5: Поточные шифры.	Самостоятельная работа №7	7
8	6	РАЗДЕЛ 6 Генераторы псевдослучайных последовательностей Тема 4: Структуры генераторов ПСП на базе РСЛОС	Самостоятельная работа №8 Подготовка к зачету	6
ВСЕГО:				64

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Основная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
1	Средства защиты информации на железнодорожном транспорте (Криптографические методы и средства)	А.А. Корниенко, М.А. Еремеев, С.Е. Ададулов; Ред. А.А. Корниенко; Под Ред. А.А. Корниенко	Маршрут, 2006 НТБ (ЭЭ); НТБ (уч.3); НТБ (фб.); НТБ (чз.2)	Раздел 1, Раздел 4
2	Основы современной криптографии	С.Г. Баричев, В.В. Гончаров, Р.Е. Серов	Горячая линия - Телеком, 2002 НТБ (фб.); НТБ (чз.1); НТБ (чз.2)	Раздел 2
3	Основы криптографии	А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин	Гелиос АРВ, 2002 НТБ (фб.); НТБ (чз.1); НТБ (чз.2)	Раздел 1, Раздел 3

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
4	Криптография	Н. Смарт	Техносфера, 2006 НТБ (фб.)	Раздел 1, Раздел 2, Раздел 4

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

- Википедия <http://ru.wikipedia.org/>
 - Всё для студента twirpx.com
 - ЭБС МИИТ library.miit.ru
- <http://elibrary.ru/> - научно-электронная библиотека.

Поисковые системы: Yandex, Google, Mail.

Internet, сайты и порталы государственных структур (ФСТЭК России, ФСБ России) и компаний, деятельность которых направлена на проблемы информационной безопасности. Компьютерные презентации, актуальных для данной дисциплины, дипломных проектов выпускников кафедры по компьютерной безопасности.

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Для проведения лекционных занятий необходима специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.

Для проведения практических занятий необходимы компьютеры с рабочими ме-стами в компьютерном классе. Компьютеры должны быть обеспечены лицензионными программными продуктами: Microsoft Office 2003, MathCAD 14.0 или другая система моделирования.

10. ОПИСАНИЕ МАТЕРИАЛЬНО ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Для проведения лекционных и практических занятий требуется комплекс программно-технических средств в составе:

- ноутбук;
- источник бесперебойного питания;
- интерактивная доска;
- проектор с разрешением не менее 1280x1024

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Обучающимся необходимо помнить, что качество полученного образования в не-малой степени зависит от активной роли самого обучающегося в учебном процессе. Обучающийся должен быть нацелен на максимальное усвоение подаваемого лектором материала, после лекции и во время специально организуемых индивидуальных встреч он может задать лектору интересующие его вопросы.

Лекционные занятия составляют основу теоретического обучения и должны давать систематизированные основы знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки, концентрировать внимание обучающихся на наиболее сложных и узловых вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.

Главная задача лекционного курса – сформировать у обучающихся системное представление об изучаемом предмете, обеспечить усвоение будущими специалистами основополагающего учебного материала, принципов и закономерностей развития соответствующей научно-практической области, а также методов применения полученных знаний, умений и навыков.

Основные функции лекций: 1. Познавательная-обучающая; 2. Развивающая; 3. Ориентирующе-направляющая; 4. Активизирующая; 5. Воспитательная; 6. Организующая; 7. Информационная.

Выполнение практических заданий служит важным связующим звеном между теоретическим освоением данной дисциплины и применением ее положений на практике. Они способствуют развитию самостоятельности обучающихся, более активному усвоению учебного материала, являются важной предпосылкой формирования профессиональных качеств будущих специалистов.

Проведение практических занятий не сводится только к органическому дополнению лекционных курсов и самостоятельной работы обучающихся. Их вместе с тем следует рассматривать как важное средство проверки усвоения обучающимися тех или иных положений, даваемых на лекции, а также рекомендуемой для изучения литературы; как форма текущего контроля за отношением обучающихся к учебе, за уровнем их знаний, а следовательно, и как один из важных каналов для своевременного подтягивания отстающих обучающихся.

При подготовке специалиста важны не только серьезная теоретическая подготовка, но и умение ориентироваться в разнообразных практических ситуациях, ежедневно возникающих в его деятельности. Этому способствует форма обучения в виде практических занятий. Задачи практических занятий: закрепление и углубление знаний, полученных на лекциях и приобретенных в процессе самостоятельной работы с учебной литературой, формирование у обучающихся умений и навыков работы с исходными данными, научной литературой и специальными документами. Практическому занятию должно предшествовать ознакомление с лекцией на соответствующую тему и литературой, указанной в плане этих занятий.

Самостоятельная работа может быть успешной при определенных условиях, кото-рые

необходимо организовать. Ее правильная организация, включающая технологии отбора целей, содержания, конструирования заданий и организацию контроля, систематичность самостоятельных учебных занятий, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

Каждому студенту следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтра. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если бы-ли, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Компетенции обучающегося, формируемые в результате освоения учебной дисциплины, рассмотрены через соответствующие знания, умения и владения. Для проверки уровня освоения дисциплины предлагаются вопросы к экзамену и тестовые материалы, где каждый вариант содержит задания, разработанные в рамках основных тем учебной дисциплины и включающие терминологические задания.

Основные методические указания для обучающихся по дисциплине указаны в разделе основная и дополнительная литература. Обучающимся рекомендуется после каждой лекции изучать рекомендованную литературу по изучаемой тематике. Перед выполнением каждой практической работы необходимо прорабатывать теоретический материал и практическую часть. Курсовую работу рекомендуется выполнять поэтапно, регулярно демонстрируя процесс выполнения преподавателю. Рекомендуется защищать курсовую работу досрочно.